Metode speciale de supraveghere sau cercetare

Mihai Suian

E-Book

Metode speciale
de supraveghere sau cercetare

Mihai Suian este avocat specializat în drept penal (începând cu anul 2013) și cadru didactic asociat la Facultatea de Drept a Universității Babeș-Bolyai din Cluj-Napoca. A obținut licența în drept la Facultatea de Drept a Universității Babeș-Bolyai în anul 2011, iar în anul 2012 a finalizat masterul de Științe penale și criminalistică în cadrul aceleiași instituții de învățământ. În anul 2020, și-a finalizat studiile doctorale cu teza intitulată „Tehnici speciale de investigare a infracțiunilor, prevăzute de Codul de procedură penală și în legi speciale". A participat la numeroase conferințe de pregătire profesională alături de judecători și procurori din Europa, printre care: ERA – Computer Forensics in Legal Proceedings (30 septembrie - 1 octombrie 2019, Zagreb, Croația); ERA/Justicni Akademie – The Life Cycle of Electronic Evidence. The Challenges posed by „Cloud Computing" (10-11 aprilie 2018, Praga, Cehia); ERA – Applying the European Investigation Order (1-2 martie 2018, Cracovia, Polonia); ERA – Investigating, Prosecuting and Adjudicating Criminal Cases in the Online World. Challenges and Opportunities posed by the Internet (25-26 septembrie 2017, Trier, Germania); ERA – Improving Detention Conditions at an EU Level (1-2 iunie 2017, Trier, Germania); ERA – The Life Cycle of E-Evidence. The Rise of Evidence on Mobile Devices [23-24 mai 2017, Madrid, Spania (participant)]; ERA – Basic Training Course on the Legal and Technical Aspects of Cybercrime for Judges and Prosecutors (13-14 februarie 2014, Trier, Germania).

Selecție lucrări de specialitate: Expertiza genetică în cauzele penale (alături de dr. Dragoș-Vasile Leordean și Daniel Ioan Ureche), în Penalmente Relevant nr. 1/2019; Unele aspecte privind reținerea, predarea și percheziționarea trimiterilor poștale, în Penalmente Relevant nr. 2/2018; Unele probleme privind folosirea probelor digitale în procesul penal, în Revista de Criminologie, Criminalistică și Penologie nr. 3/2017; Unele aspecte privind folosirea investigatorilor sub acoperire și a colaboratorilor, în Penalmente Relevant nr. 2/2016; Considerații privind accesul la un sistem informatic ca metodă de supraveghere tehnică (II), în Caiete de Drept Penal nr. 4/2016; Considerații privind accesul la un sistem informatic ca metodă de supraveghere tehnică (I), în Caiete de Drept Penal nr. 3/2016; Obținerea probelor în procesul penal prin intermediul investigatorilor sub acoperire și a colaboratorilor, în Revista de Criminologie, Criminalistică și Penologie nr. 4/2016.

Mihai Suian

Metode speciale
de supraveghere sau cercetare

solomon
2021

Respectați cartea și legea!

Atragem atenția asupra faptului că, în baza Legii nr. 8/1996 privind dreptul de autor și drepturile conexe, constituie **infracțiune** și se pedepsește cu închisoare de la o lună la un an sau cu amendă reproducerea operelor sau a produselor purtătoare de drepturi conexe fără autorizarea sau consimțământul titularului drepturilor recunoscute de prezenta lege (art. 196). Prin **reproducere** se înțelege realizarea, integrală sau parțială, a uneia ori a mai multor copii ale unei opere, direct sau indirect, temporar ori permanent, prin orice mijloc și sub orice formă (art. 14).

De asemenea, constituie **infracțiune** și se pedepsește cu închisoare de la 6 luni la 3 ani sau cu amendă punerea la dispoziția publicului, inclusiv prin internet ori prin alte rețele de calculatoare, fără drept, a operelor sau a produselor purtătoare de drepturi conexe ori de drepturi *sui-generis* ale fabricanților de baze de date sau a copiilor acestora, indiferent de suport, astfel încât publicul să le poată accesa în orice loc sau în orice moment ales în mod individual (art. 194).

Copyright © 2021, Editura Solomon

Toate drepturile sunt rezervate Editurii Solomon.
Nicio parte din această lucrare nu poate fi copiată fără acordul scris al Editurii Solomon.

Descrierea CIP a Bibliotecii Naționale a României
SUIAN, MIHAI
Metode speciale de supraveghere sau cercetare / Mihai Suian. - București : Editura Solomon, 2021
Conține bibliografie. - Index
ISBN 978-606-8892-82-5

34

Editura Solomon

Tel.: 0725.356.750

E-mail:
office@editurasolomon.ro
redactie@editurasolomon.ro

Websites:
www.editurasolomon.ro
www.e-drept.ro
www.taxnews.ro

Redactor: Alina Natalia Maxim

Dedic această carte tatălui meu,
Profesorul Valer Suian

Cuprins

Prefață ..... **XVII**
Abrevieri ..... **XIX**
Titlul I. Aspecte preliminarii **1**
Capitolul I. Necesitatea studierii tehnicilor speciale de investigare a infracțiunilor 1
Capitolul II. Definiția tehnicilor speciale de investigare și caracteristicile generale ale acestora 3
Secțiunea 1. Noțiunea de „tehnici speciale de investigare a infracțiunilor" 3
Secțiunea a 2-a. Importanța reglementării legale a tehnicilor speciale de investigare 7
Secțiunea a 3-a. Caracterul secret al tehnicilor speciale de investigare 10
Secțiunea a 4-a. Restrângerea drepturilor fundamentale ale persoanei – caracteristică a tehnicilor speciale de investigare 12
Titlul II. Compatibilitatea utilizării tehnicilor speciale **17**
Capitolul I. Dreptul la viață privată 17
Capitolul II. Libertatea de exprimare 25
Capitolul III. Secretul corespondenței 30
Capitolul IV. Dreptul la domiciliu 35
Capitolul V. Dreptul la un proces echitabil 39
Titlul III. Regimul metodelor speciale de supraveghere prevăzute de Codul de procedură penală **45**
Capitolul I. Condiții necesare pentru obținerea autorizării 45
Secțiunea 1. Începerea urmăririi penale – condiție prealabilă autorizării supravegherii tehnice 45
Secțiunea a 2-a. Suspiciunea rezonabilă privind săvârșirea ori pregătirea săvârșirii unei infracțiuni 47
§1. Noțiunea de „suspiciune rezonabilă" 47
§2. Problema desfășurării unei urmăriri penale proactive 51
§3. Infracțiunile pentru a căror urmărire se poate încuviința supravegherea tehnică 51
§4. Efectele schimbării încadrării juridice a faptei 53
Secțiunea a 3-a. Proporționalitatea măsurii luate cu restrângerea drepturilor persoanei 54
Secțiunea a 4-a. Subsidiaritatea (imposibilitatea obținerii probelor prin folosirea altor procedee probatorii) 60
Secțiunea a 5-a. Autorizarea supravegherii tehnice a persoanei vătămate, la cererea acesteia 62
Capitolul II. Aspecte procedurale privind autorizarea metodelor speciale de supraveghere tehnică 64
Secțiunea 1. Propunerea autorizării folosirii metodelor speciale de supraveghere tehnică 64

Secțiunea a 2-a. Autorizarea folosirii metodelor speciale de supraveghere sau cercetare de către judecătorul de drepturi și libertăți 68
Secțiunea a 3-a. Autorizarea folosirii metodelor speciale de supraveghere sau cercetare de către procuror....72
Capitolul III. Punerea în executare a metodelor de supraveghere tehnică 80
Secțiunea 1. Organele care pot pune în executare supravegherea tehnică 80
Secțiunea a 2-a. Consecințele Deciziei Curții Constituționale nr. 51/2016 privind punerea în executare a supravegherii tehnice 84
Secțiunea a 3-a. Încetarea supravegherii tehnice înainte de expirarea mandatului 90
Secțiunea a 4-a. Arhivarea datelor rezultate din măsurile de supraveghere tehnică....92
Secțiunea a 5-a. Conservarea materialelor rezultate din supravegherea tehnică 95
Capitolul IV. Semnarea, verificarea și certificarea electronică a datelor realizate din supravegherea tehnică 98
Secțiunea 1. Scopul semnării electronice a rezultatelor activităților de supraveghere tehnică....98
Secțiunea a 2-a. Noțiuni legislative și tehnice privind „certificatele digitale" și „semnătura electronică" 98
Secțiunea a 3-a. Autenticitatea electronică a rezultatelor activităților de supraveghere tehnică....102
Capitolul V. Consemnarea activităților de supraveghere tehnică....105
Secțiunea 1. Natura datelor și informațiilor rezultate din activitățile de supraveghere tehnică 105
Secțiunea a 2-a. Consemnarea activităților de supraveghere tehnică 107
§1. Organul competent 108
§2. Selectarea rezultatelor activităților de supraveghere tehnică 109
§3. Consemnarea activităților realizate și conținutul procesului-verbal de consemnare a rezultatelor activităților de supraveghere tehnică 112
Secțiunea a 3-a. Redarea și certificarea convorbirilor, comunicărilor sau conversațiilor interceptate și înregistrate....114
§1. Redarea integrală a convorbirilor, comunicărilor sau conversațiilor interceptate și înregistrate....115
§2. Certificarea propriu-zisă a proceselor-verbale de redare a convorbirilor, comunicațiilor și conversațiilor interceptate și înregistrate 117
Secțiunea a 4-a. Realizarea suportului digital care conține rezultatele activităților de supraveghere tehnică 118
Capitolul VI. Informarea persoanei supravegheate 122
Secțiunea 1. Dreptul persoanei supravegheate de a fi informată cu privire la măsură....122
Secțiunea a 2-a. Procedura informării persoanei supravegheate....125
Secțiunea a 3-a. Contestarea legalității supravegherii tehnice în urma Deciziei Curții Constituționale nr. 244/2017 privind neconstituționalitatea dispozițiilor art. 145 C.pr.pen. 129
Capitolul VII. Înregistrările care pot fi făcute fără autorizare 133
Capitolul VIII. Avocatul ca subiect al supravegherii tehnice....141
Secțiunea 1. Protejarea secretului profesional al avocatului din perspectiva Curții Europene a Drepturilor Omului 141

§1. Interceptarea comunicațiilor dintre client și avocatul său 143
§2. Accesul la un sistem informatic asupra avocatului și calitatea de corespondență a datelor informatice în interpretarea Curții Europene a Drepturilor Omului 145
§3. Supravegherea audio sau video a interacțiunilor dintre client și avocat la sediul cabinetului 146
§4. Supravegherea audio sau video a interacțiunilor dintre client și avocat la locul de detenție 147
Secțiunea a 2-a. Limitele autorizării supravegherii tehnice față de avocat în legislația națională 149
Capitolul IX. Valorificarea rezultatelor utilizării mijloacelor speciale de supraveghere tehnică 156
Secțiunea 1. Valoarea probatorie a mijloacelor de probă rezultate din supravegherea tehnică 156
Secțiunea a 2-a. Utilizarea în altă cauză a materialului probatoriu rezultat din supraveghere tehnică 159
Secțiunea a 3-a. Contestarea legalității administrării probelor obținute prin supravegherea tehnică 163
§1. Contestarea legalității supravegherii tehnice în camera preliminară 164
§2. Contestarea legalității supravegherii tehnice în cursul judecății în primă instanță și în apel 165
Secțiunea a 4-a. Sancțiunile procesuale în cazul obținerii probelor în mod nelegal 166
§1. Nulitatea absolută a măsurilor de supraveghere tehnică 169
§2. Nulitatea relativă a măsurilor de supraveghere tehnică 173
§3. Efectele constatării nulității supravegherii tehnice 174
Capitolul X. Concluzii 177
Titlul IV. Interceptarea comunicațiilor ori a oricărui tip de comunicare la distanță 181
Capitolul I. Aspecte generale 181
Secțiunea 1. Utilitatea metodei de supraveghere tehnică 181
Secțiunea a 2-a. Interceptarea comunicațiilor ori a oricărui tip de comunicare la distanță înainte de intrarea în vigoare a Codului de procedură penală 186
Secțiunea a 3-a. Forma actuală a interceptării comunicațiilor ori a oricărui tip de comunicare la distanță 188
Capitolul II. Autorizarea interceptării comunicațiilor ori a oricărui tip de comunicare la distanță 193
Secțiunea 1. Condițiile legale pentru autorizarea interceptării comunicațiilor ori a oricărui tip de comunicare la distanță 193
Secțiunea a 2-a. Autorizarea interceptării comunicațiilor ori a oricărui tip de comunicare la distanță 196
Capitolul III. Punerea în executare a interceptării comunicațiilor ori a oricărui tip de comunicare la distanță 200
Secțiunea 1. Particularități privind punerea în executare a interceptării comunicațiilor ori a oricărui tip de comunicare la distanță 200
Secțiunea a 2-a. Modalități de realizare a interceptării comunicațiilor ori a altor mijloace de comunicare la distanță 202

§1. Interceptarea comunicațiilor în sistem centralizat 202
§2. Interceptarea comunicațiilor prin dispozitive mobile tip Stingray 203
Capitolul IV. Problema protocoalelor de cooperare 205
Secțiunea 1. Conflictul de natură constituțională constatat prin Decizia nr. 26/2019 a Curții Constituționale privind încheierea de către Ministerul Public și Serviciul Român de Informații a unor protocoale de colaborare....205
Secțiunea a 2-a. Protocoalele de cooperare dintre organele de urmărire penală și serviciile de informații....210
§1. Protocolul privind organizarea cooperării între Serviciul Român de Informații și Parchetul Național Anticorupție din 28.01.2003....211
§2. Nota anexă din 02.03.2004 la Protocolul privind organizarea cooperării între Serviciul Român de Informații și Parchetul Național Anticorupție din 29.01.2003....212
§3. Protocolul de cooperare dintre Parchetul de pe lângă Înalta Curte de Casație și Justiție și Serviciul Român de Informații pentru îndeplinirea sarcinilor ce le revin în domeniul securității naționale din 30.06.2005....213
§4. Protocolul de cooperare dintre Parchetul de pe lângă Înalta Curte de Casație și Justiție și Serviciul Român de Informații pentru îndeplinirea sarcinilor ce le revin în domeniul securității naționale din 04.02.2009....215
§5. Protocolul privind organizarea cooperării între Serviciul Român de Informații și Parchetul de pe lângă Înalta Curte de Casație și Justiție pentru îndeplinirea sarcinilor ce le revin, potrivit legii, din 08.12.2016....217
§6. Protocolul de cooperare dintre Parchetul de pe lângă Înalta Curte de Casație și Justiție și Departamentul de Informații și Protecție Internă a Ministerului Afacerilor Interne din 07.08.2015....219
Capitolul V. Stadiul actual al reglementării punerii în executare a interceptării comunicațiilor 221
Capitolul VI. Concluzii....226
Titlul V. Accesul la un sistem informatic 227
Capitolul I. Aspecte generale....227
Capitolul II. Autorizarea accesului la un sistem informatic....236
Secțiunea 1. Condițiile legale pentru autorizarea accesului la un sistem informatic 236
Secțiunea a 2-a. Autorizarea accesului la un sistem informatic de către judecătorul de drepturi și libertăți....239
Secțiunea a 3-a. Autorizarea provizorie a accesului la un sistem informatic de către procuror....242
Capitolul III. Punerea în executare a accesului la un sistem informatic 245
Secțiunea 1. Organele competente să pună în executare accesul la un sistem informatic 245
Secțiunea a 2-a. Competența teritorială de realizare a accesului la un sistem informatic 248
Secțiunea a 3-a. Modalități de realizare a accesului la un sistem informatic....254
§1. Accesul direct la un sistem informatic....254
§2. Accesul la distanță 257

Capitolul IV. Distincțiile dintre accesul la un sistem informatic, procedeele probatorii comune și alte metode speciale de supraveghere sau cercetare 259
Secțiunea 1. Predarea obiectelor, înscrisurilor sau a datelor informatice și accesul la un sistem informatic 259
Secțiunea a 2-a. Interceptarea comunicațiilor ori a oricărui tip de comunicare la distanță și accesul la un sistem informatic 261
Secțiunea a 3-a. Supravegherea video, audio sau prin fotografiere și accesul la un sistem informatic 262
Secțiunea a 4-a. Percheziția informatică și accesul la un sistem informatic 263
Capitolul V. Concluzii 266
Titlul VI. Supravegherea video, audio sau prin fotografiere 267
Capitolul I. Aspecte generale 267
Secțiunea 1. Utilitatea metodei speciale de supraveghere 267
Secțiunea a 2-a. Supravegherea video, audio sau prin fotografiere înainte de intrarea în vigoare a Codului de procedură penală 269
Secțiunea a 3-a. Forma actuală a supravegherii video, audio sau prin fotografiere 270
Secțiunea a 4-a. Noțiunea de „spațiu privat" în contextul metodei speciale de supraveghere 273
Secțiunea a 5-a. Clasificarea supravegherii video, audio sau prin fotografiere 275
Capitolul II. Autorizarea supravegherii video, audio sau prin fotografiere 277
Secțiunea 1. Condiții legale pentru autorizarea supravegherii video, audio sau prin fotografiere 277
Secțiunea a 2-a. Autorizarea supravegherii video, audio sau prin fotografiere în spații publice 279
Secțiunea a 3-a. Autorizarea supravegherii video, audio sau prin fotografiere în spații private 281
Capitolul III. Punerea în executare a supravegherii video, audio sau prin fotografiere 285
Secțiunea 1. Particularități privind punerea în executare a supravegherii video, audio sau prin fotografiere 285
Secțiunea a 2-a. Modalități de realizare a supravegherii video, audio sau prin fotografiere 286
§1. Supravegherea ambientală a unui spațiu privat 286
§2. Înregistrări ambientale realizate de un investigator sub acoperire sau un colaborator 287
§3. Supravegherea prin intermediul accesului la un sistem informatic 288
§4. Înregistrări ambientale realizate de o parte sau de o altă persoană 288
§5. Înregistrări ale spațiilor publice 289
§6. Filajul 291
Capitolul IV. Distincțiile dintre supravegherea video, audio sau prin fotografiere și alte metode speciale 292
Secțiunea 1. Interceptarea comunicațiilor ori a oricărui tip de comunicare la distanță 292
Secțiunea a 2-a. Accesul la un sistem informatic 293
Secțiunea a 3-a. Localizarea sau urmărirea prin mijloace tehnice 293
Capitolul V. Concluzii 295

Titlul VII. Localizarea sau urmărirea prin mijloace tehnice 297
Capitolul I. Aspecte generale.....297
Secțiunea 1. Utilitatea metodei speciale de supraveghere 297
Secțiunea a 2-a. Localizarea sau urmărirea prin mijloace tehnice înainte de intrarea în vigoare a Codului de procedură penală 298
Secțiunea a 3-a. Forma actuală a localizării sau urmăririi prin mijloace tehnice 300
Capitolul II. Particularitățile autorizării localizării și urmăririi prin mijloace tehnice.....302
Capitolul III. Particularitățile punerii în executare a localizării și urmăririi prin mijloace tehnice 304
Secțiunea 1. Organul care va pune în executare măsura 304
Secțiunea a 2-a. Consemnarea activităților rezultate din localizarea sau urmărirea prin mijloace tehnice 305
Secțiunea a 3-a. Localizarea prin intermediul telefonului mobil.....306
Secțiunea a 4-a. Localizarea prin dispozitive atașate asupra persoanei sau obiectului 307
Capitolul IV. Concluzii.....310
Titlul VIII. Obținerea datelor privind tranzacțiile financiare ale unei persoane..... 311
Capitolul I. Aspecte generale.....311
Secțiunea 1. Utilitatea reglementării metodei speciale de cercetare a obținerii datelor privind tranzacțiile financiare ale unei persoane.....311
Secțiunea a 2-a. Obținerea datelor privind tranzacțiile financiare ale unei persoane înainte de intrarea în vigoare a Codului de procedură penală 313
Secțiunea a 3-a. Obținerea datelor privind tranzacțiile financiare ale unei persoane, prevăzută de Codul de procedură penală de la forma adoptată de Parlament până la forma în vigoare 315
Capitolul II. Natura juridică a metodei speciale de cercetare 318
Capitolul III. Persoanele care pot fi chemate să comunice date privind tranzacțiile financiare ale unei persoane 320
Secțiunea 1. Instituțiile de credit.....320
Secțiunea a 2-a. Entitățile financiare 321
Secțiunea a 3-a. Agenția Națională de Administrare Fiscală 324
Secțiunea a 4-a. Persoanele fizice.....326
Capitolul IV. Corelația dintre obținerea de date privind situația financiară a unei persoane și obținerea datelor privind tranzacțiile financiare ale unei persoane.....328
Capitolul V. Condițiile legale pentru autorizarea metodei speciale de cercetare 330
Capitolul VI. Procedura autorizării obținerii datelor privind tranzacțiile financiare ale unei persoane.....334
Secțiunea 1. Autorizarea măsurii de către judecătorul de drepturi și libertăți 334
Secțiunea a 2-a. Autorizarea provizorie a măsurii de către procuror 338
Capitolul VII. Punerea în executare a metodei speciale de cercetare 341
Secțiunea 1. Transmiterea mandatului și obligațiile instituției solicitate 341
Secțiunea a 2-a. Informațiile și înscrisurile care pot fi transmise de entitățile financiare.....342
Secțiunea a 3-a. Informarea persoanei supuse metodei speciale de cercetare.....345
Capitolul VIII. Obținerea datelor privind tranzacțiile financiare ale avocatului 347
Capitolul IX. Concluzii 352

Titlul IX. Obținerea de date privind situația financiară a unei persoane 353
Capitolul I. Aspecte generale 353
Secțiunea 1. Utilitatea reglementării metodei speciale de cercetare a obținerii de date privind situația financiară a unei persoane 353
Secțiunea a 2-a. Introducerea obținerii de date privind situația financiară a unei persoane prin Legea de punere în aplicare a Codului de procedură penală 355
Capitolul II. Procedura autorizării obținerii de date privind situația financiară a unei persoane 357
Capitolul III. Punerea în executare a obținerii de date privind situația financiară a unei persoane 360
Capitolul IV. Concluzii 362
Titlul X. Obținerea datelor de trafic și de localizare prelucrate de către furnizorii de rețele publice de comunicații electronice ori furnizorii de servicii de comunicații electronice destinate publicului 363
Capitolul I. Aspecte generale 363
Secțiunea 1. Obținerea datelor de trafic și de localizare de la intrarea în vigoare a Codului de procedură penală până la Decizia Curții Constituționale nr. 440/2014 privind neconstituționalitatea Legii nr. 82/2012 363
Secțiunea a 2-a. Forma în vigoare a metodei speciale a obținerii datelor de trafic și localizare 367
Secțiunea a 3-a. Utilitatea reglementării metodei speciale de cercetare a obținerii datelor de trafic și de localizare 372
Capitolul II. Noțiunile de „furnizori", „date de trafic" și „date de localizare" 376
Secțiunea 1. Persoanele care pot fi chemate să comunice date de trafic și localizare 376
Secțiunea a 2-a. Datele de trafic 377
Secțiunea a 3-a. Datele de localizare 380
Capitolul III. Importanța deciziilor Curții de Justiție a Uniunii Europene și ale Curții Constituționale în aplicabilitatea metodei speciale de cercetare 382
Secțiunea 1. Hotărârea Curții de Justiție a Uniunii Europene în cauza Digital Rights Ireland și alții pentru invalidarea Directivei 2006/24/CE privind reținerea și stocarea datelor cu caracter personal în contextul comunicațiilor electronice 382
Secțiunea a 2-a. Decizia Curții Constituționale nr. 440/2014 referitoare la excepția de neconstituționalitate a dispozițiilor Legii nr. 82/2012 (Legea retenției datelor) 384
Secțiunea a 3-a. Hotărârea Curții de Justiție a Uniunii Europene în cauzele reunite C-203/15 și C-698/15, Tele2 Sverige AB, Secretary of State for the Home Department și alții, privind imposibilitatea folosirii Directivei 2002/58/CE în vederea reținerii datelor privind comunicațiile electronice 387
Capitolul IV. Condițiile legale pentru autorizarea metodei speciale 390
Capitolul V. Procedura autorizării obținerii datelor de trafic și de localizare 394
Capitolul VI. Punerea în executare a obținerii datelor de trafic și de localizare 397
Secțiunea 1. Transmiterea mandatului și obligația de confidențialitate a furnizorului solicitat 397
Secțiunea a 2-a. Transmiterea datelor de trafic și de localizare 397
Secțiunea a 3-a. Informarea persoanei supuse metodei speciale de cercetare 398
Capitolul VII. Concluzii 399

Titlul XI. Reținerea, predarea și percheziționarea trimiterilor poștale 401
Capitolul I. Aspecte generale și istorice 401
Capitolul II. Noțiunea de „trimitere poștală" și reglementarea activității de poștă în România 407
Capitolul III. Corelația dintre reținerea, predarea și percheziționarea trimiterilor poștale și alte procedee probatorii 411
Capitolul IV. Natura măsurii 414
Capitolul V. Condițiile legale pentru autorizarea reținerii, predării și percheziționării trimiterilor poștale 416
Capitolul VI. Procedura autorizării reținerii, predării și percheziționării trimiterilor poștale 419
Capitolul VII. Punerea în executare a reținerii, predării și percheziționării trimiterilor poștale 423
Capitolul VIII. Reținerea, predarea și percheziționarea trimiterilor poștale ale unui avocat 426
Capitolul IX. Concluzii 429
Titlul XII. Utilizarea investigatorilor sub acoperire și a colaboratorilor 431
Capitolul I. Aspecte generale 431
Capitolul II. Condițiile legale pentru autorizarea utilizării investigatorilor sub acoperire și a colaboratorilor 434
Capitolul III. Procedura de autorizare a utilizării investigatorilor sub acoperire și a colaboratorilor 439
Capitolul IV. Obținerea probelor în procesul penal prin intermediul investigatorilor sub acoperire și a colaboratorilor 445
Secțiunea 1. Încuviințarea folosirii dispozitivelor tehnice pentru a obține fotografii sau înregistrări audio și video 446
Secțiunea a 2-a. Audierea investigatorilor sub acoperire și a colaboratorilor 453
Secțiunea a 3-a. Participarea autorizată la anumite activități 458
Capitolul V. Activitățile specifice investigatorilor sub acoperire și colaboratorilor 462
Secțiunea 1. Investigatorul sub acoperire, colaboratorul și informatorul – noțiuni, distincții și activitate specifică 462
§1. Investigatorul sub acoperire 462
§2. Colaboratorul 465
§3. Informatorul 468
Secțiunea a 2-a. Recrutarea și motivarea colaboratorilor și informatorilor 470
§1. Recrutarea colaboratorilor și informatorilor 470
§2. Motivarea colaboratorilor și informatorilor 474
2.1. Reținerea unei cauze de nepedepsire sau a unei cauze de reducere a pedepsei 475
2.2. Banii ca motivație a colaboratorilor și informatorilor 478
2.3. Frica 479
2.4. Răzbunarea 480
2.5. Remușcările ca factor motivant 480
2.6. Altruismul 480
2.7. Colaboratorii și informatorii motivați de ego-ul personal 481
2.8. Colaboratorii și informatorii motivați de simțul civic 481

Capitolul VI. Măsurile de protecție a investigatorilor sub acoperire, a colaboratorilor și informatorilor 482
Capitolul VII. Concluzii....488
Titlul XIII. Participarea autorizată la anumite activități 489
Capitolul I. Aspecte generale....489
Secțiunea 1. Utilitatea reglementării metodei speciale de cercetare a participării autorizate la anumite activități 489
Secțiunea a 2-a. Participarea autorizată la anumite activități sub imperiul Codului de procedură penală anterior și a legislației speciale....491
Secțiunea a 3-a. Participarea autorizată la anumite activități de la momentul adoptării Codului de procedură penală până la forma în vigoare 493
Capitolul II. Condițiile legale pentru autorizarea metodei speciale de cercetare....495
Capitolul III. Procedura autorizării participării autorizate la anumite activități 499
Capitolul IV. Punerea în executare a participării autorizate la anumite activități....502
Capitolul V. Provocarea infracțiunii....504
Secțiunea 1. Considerații generale....504
Secțiunea a 2-a. Condițiile de existență a provocării infracțiunii din perspectiva jurisprudenței Curții Europene a Drepturilor Omului 507
Capitolul VI. Concluzii 511
Titlul XIV. Livrarea supravegheată 513
Capitolul I. Aspecte generale....513
Secțiunea 1. Utilitatea reglementării metodei speciale a livrării supravegheate....513
Secțiunea a 2-a. Livrarea supravegheată în legi speciale înainte de intrarea în vigoare a Codului de procedură penală 516
Secțiunea a 3-a. Livrarea supravegheată în Codul de procedură penală....519
Capitolul II. Natura juridică a livrării supravegheate 521
Capitolul III. Condițiile legale pentru autorizarea livrării supravegheate 523
Secțiunea 1. Condiții generale pentru autorizarea măsurii....523
Secțiunea a 2-a. Condiții speciale în cazul livrării supravegheate naționale....526
Secțiunea a 3-a. Condiții speciale în cazul livrării supravegheate transfrontaliere....527
Capitolul IV. Procedura de autorizare a livrării supravegheate 529
Capitolul V. Punerea în aplicare a livrării supravegheate....533
Secțiunea 1. Procedura punerii în aplicare a livrării supravegheate 533
Secțiunea a 2-a. Organele care pot fi chemate să pună în aplicare livrarea supravegheată....536
§1. Poliția Română 536
§2. Autoritatea Vamală 537
§3. Colaboratorii autorizați de procuror....538
Capitolul VI. Concluzii....539
Titlul XV. Tehnici speciale de investigare prevăzute de legea specială 541
Capitolul I. Aspecte generale....541
Secțiunea 1. Noțiunea de „securitate națională” 541
Secțiunea a 2-a. Utilitatea reglementării tehnicilor speciale de investigare privind securitatea națională....545

Secțiunea a 3-a. Organele cu competențe în domeniul securității naționale.....548
§1. Serviciul Român de Informații.....549
§2. Serviciul de Informații Externe.....551
§3. Serviciul de Protecție și Pază.....552
§4. Ministerul Apărării Naționale – Direcția Generală de Informații a Apărării.....553
§5. Ministerul Afacerilor Interne – Direcția Generală de Protecție Internă.....554
§6. Ministerul Justiției – Direcția Generală de Protecție și Anticorupție.....555
Secțiunea a 4-a. Activitățile specifice culegerii de informații prevăzute de Legea nr. 51/1991.....556
§1. Activitățile specifice culegerii de informații care nu presupun restrângerea drepturilor și libertăților fundamentale ale omului.....557
§2. Activitățile specifice culegerii de informații care presupun restrângerea drepturilor și libertăților fundamentale ale omului.....559
Capitolul II. Aspecte procedurale privind autorizarea tehnicilor speciale de investigare prevăzute de Legea nr. 51/1991.....565
Secțiunea 1. Condițiile legale pentru autorizarea tehnicilor speciale care constituie activități specifice culegerii de informații.....565
Secțiunea a 2-a. Formularea propunerii de autorizare.....568
Secțiunea a 3-a. Autorizarea tehnicilor speciale de investigare prevăzute de Legea nr. 51/1991.....572
Secțiunea a 4-a. Punerea în executare a mandatului emis în baza Legii nr. 51/1991.....576
Capitolul III. Valorificarea rezultatelor utilizării tehnicilor speciale prevăzute de Legea nr. 51/1991.....579
Secțiunea 1. Valoarea probantă a rezultatelor utilizării tehnicilor speciale prevăzute de Legea nr. 51/1991.....579
Secțiunea a 2-a. Contestarea legalității și temeiniciei utilizării tehnicilor speciale prevăzute de Legea nr. 51/1991.....583
§1. Informarea persoanei supuse unei tehnici speciale de investigare prevăzute de Legea nr. 51/1991.....583
§2. Contestarea întrebuințării tehnicilor speciale de investigare prevăzute de Legea nr. 51/1991.....586
Capitolul IV. Concluzii.....590
Bibliografie selectivă 593
Index tematic 613

Prefață

Procedura penală a făcut obiectul unor neîncetate schimbări în ultimii ani, având ca finalitate armarea justiției penale pentru a răspunde provocărilor generate de formele particulare ale criminalității. În prezent, aceasta cuprinde reguli de procedură specifice privind așa-numita «criminalitate confidențială», care, urmând direcția altor sisteme, integrează metodele probatorii speciale pentru infracțiuni determinate printre procedeele probatorii comune.

În acest context normativ, necesitatea unui studiu privind procedeele probatorii derogatorii este evidentă. Ea vizează latura procedurală a unui drept penal special alcătuit din infracțiuni grave, care, în mod normal, nu pot fi descoperite și ai căror autori nu pot fi identificați prin recurgerea la mijloacele de probă tradiționale. De aceea, este bine-venită reflecția cu privire la procedeele probatorii de excepție și la compatibilitatea acestora cu jurisprudența Curții Europene a Drepturilor Omului, care incită în mod inevitabil la distincția din dreptul intern între dreptul comun și dreptul special.

Punerea în operă a acestui demers este meritul unei cercetări științifice autentice din partea autorului, care a reușit să surprindă turbulențele sistemului, derogările importante de la dreptul comun al procedurii și crearea unei jurisdicții de excepție. Prin abordarea sa proprie, autorul a evidențiat măsura în care derogările garantează un mai bun acces la adevărul judiciar și a subliniat particularitățile actualei proceduri, atât în raport de sistemul nostru de inspirație romano-germanică, cât și în raport de sistemul adversial spre care se tinde.

Prezenta monografie reușește să abordeze exhaustiv, într-o manieră originală, toate problemele ridicate de reglementările actuale dedicate procedurilor speciale de supraveghere sau cercetare. Cititorul are la dispoziție o lucrare inedită și valoroasă, care se remarcă nu doar prin dimensiunea sa, ci și prin modalitatea în care a fost structurată și redactată.

Această lucrare este la nivelul unui tratat despre procedurile penale derogatorii. Ea este suportul și consecința unei cercetări complete a unei materii și a unor reguli destul de complicate, cărora însă autorul le dă sens și coerență. Ideea acestei lucrări a îmbogățit spiritul autorului, care s-a detașat de perspectiva clasică a surselor, tratând problematica metodelor speciale de supraveghere și de cercetare a probelor ca o parte autonomă a procedurii penale.

Prin lucrarea sa, autorul pune în scenă două confruntări: *prima* – între procesul penal comun, procedurile de excepție și drepturile omului; *a doua* – între justiția efectivă în materie penală, protecția procesului echitabil și justiția loială. Prima reprezintă obiectul principal al lucrării, iar a doua apare ca un crez al autorului și se reflectă în mod particular în efortul acestuia de a depăși rivalitatea structurală dintre procedeele probatorii utilizate în lupta pentru monopolul aplicării legitime a principiului aflării adevărului și a concilierii acestuia cu deziderатul justiției penale.

Autorul a reușit să extragă această materie din izolarea sa națională, abordând fără nicio ezitare arhitectura și filosofia altor sisteme juridice într-o viziune proprie, unică. Marele merit al operei sale este de a nu se înscrie în continuitate, de a se remarca printr-o abordare extraordinară a unei problematici fundamentale a procesului penal contemporan.

Stilul original și fluent utilizat la redactarea lucrării, dar și valorificarea unui număr impresionant de surse bibliografice, preponderent străine, conferă prezentei lucrări o valoare științifică incontestabilă. Prezenta monografie aduce o serie de clarificări de ordin conceptual și metodologic, având meritul de a oferi soluții concrete de aplicare a metodelor de supraveghere și cercetare.

Fără îndoială, lucrarea reflectă cele două vocații ale domnului Mihai Suian: aceea de maestru al barei și de veritabil doctrinar. Aceasta ne amintește inevitabil de moștenirea spirituală lăsată de tatăl său, reputatul și regretatul Profesor Valer Suian, care a reprezentat cu siguranță o permanentă sursă de inspirație pentru autor, dar și un motiv de datorie morală și recunoaștere infinită.

Fructul unei cunoașteri depline a instituției procedeelor probatorii speciale printr-o cercetare teoretică și practică de mare anvergură, această monografie livrează o expunere aprofundată a diferitelor tehnici de obținere a probelor puse în funcțiune în cadrul urmăririi penale. Din acest motiv, consider că acesta este, înainte de toate, un instrument de muncă, deoarece vizează punerea la dispoziția cititorilor a cunoștințelor necesare pentru a le permite să înțeleagă materia și să o pună în practică. Este vorba atât de studenții care se înscriu într-un proces de învățare, cât și de practicienii care se confruntă cu aspectele practice ale materiei.

Prof.univ.dr. Gheorghiță Mateuț

Cluj-Napoca,
3 aprilie 2021

Abrevieri

I. Abrevieri uzuale

alin.	alineat(ul)
apud	indică o citare preluată de la alt autor, după
art.	articol(ul)
B. Of.	Buletinul Oficial al Republicii Populare/Socialiste România
c.	contra
C. Ap.	Curtea de Apel
C.civ.	Codul civil
C.pen.	Codul penal
C.pr.civ.	Codul de procedură civilă
C.pr.pen.	Codul de procedură penală
C.pr.pen. anterior/1968	Codul de procedură penală din 1968
C.vamal	Codul vamal al României
CCR	Curtea Constituțională a României
CEDO	Curtea Europeană a Drepturilor Omului
CJUE	Curtea de Justiție a Uniunii Europene
C.N.I.C.	Centrul Național de Interceptare a Comunicațiilor
Conv.EDO	Convenția Europeană a Drepturilor Omului
coord.	coordonator(i)
CSJ	Curtea Supremă de Justiție
D.E.A.	U.S. Drug Enforcement Administration
dec.	decizia
dec. civ.	decizia civilă
dec. pen.	decizia penală
D.G.I.A.	Direcția Generală de Informații a Apărării
D.G.P.A.	Direcția Generală de Protecție și Anticorupție
D.G.P.I.	Direcția Generală de Protecție Internă
D.I.I.C.O.T.	Direcția de Investigare a Infracțiunilor de Criminalitate Organizată și Terorism
D.I.P.I.	Departamentul de Informații și Protecție Internă
D.N.A.	Direcția Națională Anticorupție
ed.	ediția
Ed.	Editura
EWCA	England and Wales Court of Appeal
F.B.I.	Federal Bureau of Investigations
H.G.	Hotărârea Guvernului
ibidem	același autor, în același loc
ICCJ	Înalta Curte de Casație și Justiție

idem	același autor
J. Of.	Jurnalul Oficial al Uniunii Europene
Jud.	Judecătoria
lit.	litera
M. Of.	Monitorul Oficial al României, Partea I
n.n.	nota noastră
O.G.	Ordonanța Guvernului
O.N.P.M.	Oficiul Național pentru Protecția Martorilor
O.N.P.C.S.B.	Oficiul Național de Prevenire și Combatere a Spălării Banilor
ONU	Organizația Națiunilor Unite
O.U.G.	Ordonanța de urgență a Guvernului
op. cit.	opera citată
p.	pagina
par. sau §	paragraf(ul)
pct.	punct(ul)
P.N.A.	Parchetul Național Anticorupție
pp.	paginile
s. civ.	secția civilă
s. pen.	secția penală
s.n.	sublinierea noastră
P.I.C.C.J.	Parchetul de pe lângă Înalta Curte de Casație și Justiție
S.I.E.	Serviciul de Informații Externe
S.I.P.A.	Serviciul Independent de Protecție și Anticorupție
S.P.P.	Serviciul de Protecție și Pază
S.R.I.	Serviciul Român de Informații
S.U.A.	Statele Unite ale Americii
sent.	sentința
ș.a.	și alții/altele
Trib.	Tribunalul
U.S.	United States Supreme Court
UKHL	United Kingdom House of Lords
vol.	Volumul
v. infra	*vide infra* (a se vedea mai jos)
v. supra	*vide supra* (a se vedea mai sus)

II. Lucrări citate frecvent

A. Ashworth, M. Redmayne, The Criminal Process, 2014 = *Ashworth, Andrew; Redmayne, Mike*, The Criminal Process, Fourth Edition, Oxford University Press, Oxford, 2014

A. L-T Choo, Evidence, 2018 = *Choo, Andrew L-T*, Evidence, Fifth Edition, Oxford University Press, Oxford, 2018

L.K. Donohue, The Future of Foreign Intelligence, 2016 = *Donohue, Laura K.*, The Future of Foreign Intelligence. Privacy and Surveillance in a Digital Age, Oxford University Press, Oxford, 2016

S. Grădinaru, Supravegherea tehnică, 2014 = *Grădinaru, Sandra*, Supravegherea tehnică în Noul Cod de procedură penală, Ed. C.H. Beck, București, 2014

C. Harfield, K. Harfield, Covert Investigation, 2018 = *Harfield, Clive; Harfield, Karen*, Covert Investigation, Fifth Edition, Oxford University Press, Oxford, 2018

R.J. Krotoszynski, Jr., Privacy Revisited, 2016 = *Krotoszynski, Jr., Ronald J.*, Privacy Revisited. A Global Perspective on the Right to Be Left Alone, Oxford University Press, Oxford, 2016

Gh. Mateuț, Procedură penală, 2019 = *Mateuț, Gheorghiță*, Procedură penală. Partea generală, Ed. Universul Juridic, București, 2019

Gh. Mateuț, Tratat, vol. I, 2007 = *Mateuț, Gheorghiță*, Tratat de procedură penală. Partea generală, vol. I, Ed. C.H. Beck, București, 2007

Gh. Mateuț, Tratat, vol. II, 2012 = *Mateuț, Gheorghiță*, Tratat de procedură penală. Partea generală, vol. II, Ed. C.H. Beck, București, 2012

S. McKay, Covert Policing, 2015 = *McKay, Simon*, Covert Policing Law and Practice, Second Edition, Oxford University Press, Oxford, 2015

M.V. Tudoran, Teoria și practica interceptărilor, 2012 = *Tudoran, Mihai Viorel*, Teoria și practica interceptărilor și înregistrărilor audio sau video judiciare, Ed. Universul Juridic, București, 2012

M. Udroiu, Procedură penală, vol. I, 2019 = *Udroiu, Mihail*, Procedură penală. Partea generală, ed. a 6-a, vol. I, Ed. C.H. Beck, București, 2019

M. Udroiu, Procedură penală, vol. II, 2019 = *Udroiu, Mihail*, Procedură penală. Partea generală, ed. a 6-a, vol. II, Ed. C.H. Beck, București, 2019

M. Udroiu (coord.), Codul de procedură penală, 2015 = *Udroiu, Mihail (coord.); Andone-Bontaș, Amalia; Bodoroncea, Georgina; Bulancea, Marius Bogdan; Constantinescu, Victor; Grădinaru, Daniel; Jderu, Claudia; Kuglay, Irina; Meceanu, Constantin; Postelnicu, Lucreția; Tocan, Isabelle; Trandafir, Andra-Roxana*, Codul de procedură penală. Comentariu pe articole, ed. 1, Ed. C.H. Beck, București, 2015

M. Udroiu (coord.), Codul de procedură penală, 2017 = *Udroiu, Mihail (coord.); Andone-Bontaș, Amalia; Bodoroncea, Georgina; Bogdan, Sergiu; Bulancea, Marius Bogdan; Chertes, Dan-Sebastian; Chiș, Ioan-Paul; Constantinescu, Victor Horia Dimitrie; Grădinaru, Daniel; Jderu, Claudia; Kuglay, Irina; Meceanu, Constantin-Cristinel; Nedelcu, Iuliana; Postelnicu (Cojocaru), Lucreția Albertina; Răduleț u, Sebastian; Șinc, Alexandra-Mihaela; Slăvoiu, Radu; Tocan, Isabelle; Trandafir, Andra-Roxana; Vasiescu, Mihaela; Zlati, George*, Codul de procedură penală. Comentariu pe articole, ed. a 2-a, Ed. C.H. Beck, București, 2017

M. Udroiu, O. Predescu, Protecția europeană, 2008 = *Udroiu, Mihail; Predescu Ovidiu*, Protecția europeană a drepturilor omului și procesul penal român, Ed. C.H. Beck, București, 2008

M. Udroiu, R. Slăvoiu, O. Predescu, Tehnici speciale, 2009 = *Udroiu, Mihail; Slăvoiu, Radu; Predescu, Ovidiu*, Tehnici speciale de investigare în justiția penală, Ed. C.H. Beck, București, 2009

N. Volonciu, A.S. Uzlău (coord.), Noul Cod, 2014 = *Volonciu, Nicolae; Uzlău, Andreea Simona (coord.); Moroșanu, Raluca; Văduva, Victor; Atasiei, Daniel; Ghigheci, Cristinel; Voicu, Corina; Tudor, Georgiana; Gheorghe, Teodor-Viorel; Chiriță, Cătălin Mihai*, Noul Cod de procedură penală comentat, Ed. Hamangiu, București, 2014

Titlul I
Aspecte preliminarii

Capitolul I
Necesitatea studierii tehnicilor speciale de investigare a infracțiunilor

Prezenta lucrare se axează pe o analiză a fiecărei tehnici speciale de investigare a infracțiunilor cunoscute de legislația națională, în contextul în care complexitatea cauzelor actuale și creșterea posibilităților de a eluda vigilența organelor judiciare a crescut, făcând necesară folosirea de noi metode prin care să se asigure prevenirea săvârșirii unor infracțiuni și tragerea la răspundere penală a persoanelor care comit astfel de fapte. Problema tehnicilor speciale de investigare este una curentă și, față de caracterul lor secret și intruziv, dar și din cauza importanței probelor care pot fi obținute, vor fi întotdeauna considerate o problemă de interes deosebit în Dreptul procesual penal.

Contextul internațional este unul deosebit, deoarece atât factori publici, cât și factori privați promovează ideea de limitare voluntară sau obligatorie a dreptului la viață privată. În ultimii ani, au fost făcute multe dezvăluiri despre programe secrete de culegere de informații de către state precum S.U.A. și s-a propagat folosirea de sisteme de supraveghere publică a persoanelor. Spionajul nu este o noutate, el existând din cele mai vechi timpuri, dar tehnicile speciale de investigare permit aflarea de date complete despre o persoană și sistemele de colectare automatizată a datelor personale permit o cunoaștere deplină și completă a tuturor persoanelor, putând fi exploatată de stat la orice moment. Totodată, firmele private care administrează platforme de socializare nu s-au oprit din expansiune, devenind din ce în ce mai implicate în viața noastră privată, încercând să ne cunoască într-un mod intim pentru a ști preferințele și dorințele noastre, totul în scopul de a vinde ceva. În acest context, dacă rețelele de socializare sau aplicațiile online care colectează date personale cu consimțământul nostru (mai mult sau mai puțin informat) sunt gratuite, dar tot adună un profit semnificativ, trebuie să ne întrebăm: ele ce produc, în realitate? Răspunsul este că ele produc informații bazate pe ceea ce noi le acordăm în mod gratuit, prin care comportamentul nostru poate fi anticipat și controlat.

Din perspectiva legislației naționale, tehnicile speciale de investigare au cunoscut schimbări majore, atât ca urmare a intrării în vigoare a noului Cod de procedură penală, dar și ca urmare a unor schimbări politice și juridice care au modificat concepțiile asupra acestor metode. În ultimii ani, se poate observa cum mentalitatea legată de tehnicile speciale de investigare s-a schimbat în sistemul judiciar de la a se accepta tacit o situație de fapt – lipsa unei posibilități reale de a se contesta legalitatea folosirii unor astfel de tehnici, caracterul secret al modului de punere în executare și presiunea ocultă a serviciilor secrete în acest domeniu – la o deschidere largă către acceptarea caracterului excepțional și derogatoriu al folosirii acestor tehnici. În același timp, s-a schimbat percepția asupra noilor instituții introduse prin Codul de procedură penală, trecând de la aplicarea formală a lor, lipsită de înțelegere a esenței din spatele lor, pe care o considerăm firească într-o situație de tranziție, la o înțelegere deplină a caracterului intruziv al acestora și a necesității limitării ingerințelor aduse vieții private. Codul de procedură penală

se bazează pe principii și reguli mai vechi decât actuala reglementare, multe dintre ele preluate din jurisprudența străină și, în special, cea engleză și americană, care reprezintă izvor de drept în sistemul *common law*. Ca o consecință, este firesc că anumite concepte, precum „suspiciunea rezonabilă", „proporționalitatea" și „subsidiaritatea", esențiale în domeniul tehnicilor speciale de investigare, nu pot fi înțelese numai prin intermediul Codului de procedură penală, ci presupun un studiu aprofundat al doctrinei și jurisprudenței străine, aspect care a constituit unul dintre obiectele prezentei lucrări.

Neajunsurile sistemului judiciar român nu se datorează numai introducerii bruște a unor concepte noi, ci mai ales numeroaselor texte legale care au fost constatate de Curtea Constituțională ca fiind contrare legii supreme. Mai mult, chiar dacă au existat decizii în acest sens, aplicabile și în domeniul tehnicilor speciale de investigare, ele nu au condus la modificări legislative, obligând justițiabilii și organele judiciare să se bazeze pe aplicarea directă a jurisprudenței Curții și pe găsirea unor soluții principiale atunci când legea nu prevede, dar ar trebui să prevadă.

Jurisprudența Curții Europene a Drepturilor Omului a cunoscut o dezvoltare continuă în domeniul protejării drepturilor fundamentale garantate prin Convenție, în special în privința dreptului la viață privată și corecta sa aplicare în procesul penal. Aceasta obligă judecătorul național să privească legea națională cu alți ochi și să realizeze întotdeauna o interpretare care să dea prioritate Convenției Europene a Drepturilor Omului atunci când ea conferă o protecție mai bună a drepturilor persoanei.

În ceea ce privește însești tehnicile speciale de investigare, de la momentul adoptării Codului de procedură penală au survenit numeroase modificări, majoritatea producându-se odată cu intrarea în vigoare a Codului de procedură penală, fiind introduse prin legea de punere în aplicare a codului. Denumirea inițială a Capitolului IV al Titlului IV al Codului de procedură penală era de „Tehnici speciale de supraveghere sau cercetare", fiind modificată, odată cu intrarea în vigoare a Codului, în „Metode speciale de supraveghere sau cercetare". Tehnicile speciale de investigare includ atât tehnicile cuprinse în Codul de procedură penală, cât și tehnicile din legislația specială, în cadrul acestei din urmă categorii intrând numai cele prevăzute de Legea nr. 51/1991 privind securitatea națională a României, republicată[1].

[1] Republicată în M. Of. nr. 190 din 18 martie 2014.

Capitolul II
Definiția tehnicilor speciale de investigare și caracteristicile generale ale acestora

Secțiunea 1. Noțiunea de „tehnici speciale de investigare a infracțiunilor"

Tehnicile speciale de investigare constituie o categorie de procedee probatorii și măsuri de investigație cu caracter derogatoriu de la regulile de drept comun privind administrarea probelor, fiind recunoscute la nivel internațional ca un instrument în combaterea infracționalității de mare gravitate.

Deși o parte dintre tehnicile speciale de investigare erau cunoscute și întrebuințate în procesul penal de mai mult timp, chiar fiind prevăzute în unele recomandări și convenții internaționale, legiuitorul român a preluat noțiunea de „tehnici speciale de investigare" în urma Recomandării (2005) 10 a Comitetului de Miniștri al Consiliului Europei[1], care avea ca scop combaterea prin mijloacele legale a criminalității grave cu respectarea drepturilor și libertăților individuale prevăzute în Convenția Europeană a Drepturilor Omului. Chiar dacă în numeroase rânduri se face referire la infracțiuni grave, nu se propune o definiție a acestora, Comitetul de Miniștri rezumându-se la a menționa, în special, infracțiunile de terorism și infracțiunile de criminalitate organizată, tehnicile speciale de investigare trebuind să fie întrebuințate pentru amenințări de o gravitate similară cu acestea.

Din definiția dată de Comitetul de Miniștri, reținem că: „*în sensul prezentei Recomandări, prin «tehnici speciale de investigare» se înțeleg tehnicile aplicate de autoritățile competente în contextul investigațiilor penale în scopul descoperirii și cercetării infracțiunilor grave și a suspecților, în vederea colectării informațiilor astfel de o manieră în care să nu alerteze persoanele vizate de aceste tehnici*". Din această definiție rezultă două aspecte importante pe care le vom relua de mai multe ori pe parcursul lucrării: necesitatea restrângerii folosirii tehnicilor speciale de investigare numai la infracțiunile grave și caracterul secret al acestora[2]. Acestora li se alătură și acela că prin aplicarea lor se aduce o atingere drepturilor și libertăților fundamentale ale persoanei vizate, aspect recunoscut în preambulul Recomandării.

Întrucât trebuie să operăm în prezenta lucrare cu termeni precum „tehnici speciale de investigare a infracțiunilor", „metode speciale de supraveghere sau cercetare" ori „măsuri speciale", se impune a fi făcute delimitări terminologice.

Noțiunea cea mai generală care poate fi întrebuințată în mod corect pentru desemnarea obiectului prezentei lucrări este cea de „tehnici speciale de investigare a infracțiunilor", în cuprinsul acestora putând fi incluse atât metodele speciale de supraveghere, cât și metodele speciale de cercetare. Între cuvântul „tehnici" și cuvântul „metode", din perspectiva problemei în discuție, nu există nicio diferență, termenul folosit la nivel internațional fiind cel de „tehnică",

[1] Recomandarea (2005) 10 a Comitetului de Miniștri al Consiliului Europei adoptată de Comitetul de Miniștri la data de 20 aprilie 2005 în a 924-a întâlnire a Adjuncților Miniștrilor, pe *www.coe.int*

[2] *N. Brady*, Evidence, special investigative techniques and the right to a fair hearing, în revista ERA Forum, vol. 15, no. 1/2014, p. 37.

nu cel de „metodă". Din perspectiva Criminalisticii, ramură de drept cu strânse legături cu Procedura penală, termenul de „tehnică" este înrudit cu cel de „metodă", atunci când în discuție va fi o urmă sau un mijloc material de probă, în literatura de specialitate arătându-se că tehnica criminalistică cuprinde ansamblul metodelor și mijloacelor tehnico-științifice destinate descoperirii, fixării, ridicării și examinării urmelor sau mijloacelor materiale de probă[1]. Definiția este utilă în demersul nostru, având în vedere caracterul preponderent tehnic al majorității metodelor speciale de supraveghere sau cercetare.

Mai avem încă un argument care va explica mai bine și titlul prezentei lucrări – la momentul la care s-a început elaborarea acesteia, era în vigoare Codul de procedură penală din 1968, iar Codul de procedură penală actual nu era în vigoare, dar, în forma sa adoptată de Parlament, Capitolul IV al Titlului IV se denumea „Tehnici speciale de supraveghere sau cercetare", ulterior intrând în vigoare sub forma „Metode speciale de supraveghere sau cercetare". Pentru a nu crea confuzie în lucrare, o să ne rezumăm la folosirea termenului de „tehnici speciale" numai în prima parte a lucrării.

Termenii de „măsură specială de supraveghere" sau „măsură specială de cercetare" trebuie să fie considerați a fi sinonimi cu cei de „metodă specială de supraveghere", respectiv „metodă specială de cercetare", de altfel legiuitorul folosind alternativ termenul de „metodă" cu cel de „măsură" în mai multe rânduri.

După cum s-a arătat în doctrină, tehnicile speciale de investigare constituie procedee probatorii cu caracter derogatoriu, cu reguli și proceduri particulare de autorizare, dar și de punere în aplicare[2]. Prin Recomandarea (2005) 10 a Comitetului de Miniștri s-a urmărit ca fiecare stat să includă măsuri de combatere a criminalității cu un regim probatoriu special[3].

Potrivit pct. 27 al Memorandumului explicativ al Recomandării (2005) 10 a Comitetului de Miniștri[4], prin „tehnici speciale de investigare" se va înțelege, între altele, următoarele metode: *operațiuni sub acoperire; operațiuni sub acoperire disimulate (de exemplu, o societate comercială sub acoperire); folosirea informatorilor; livrarea supravegheată; observarea (inclusiv observarea transfrontalieră); supravegherea electronică; interceptarea comunicațiilor (telefon, fax, e-mail, poștă); percheziții (inclusiv domiciliară, informatică, asupra vehiculelor etc.); urmăriri transfrontaliere; pseudo-cumpărări sau alte „pseudo-infracțiuni", astfel cum sunt definite în legile naționale*[5] (participarea autorizată la anumite activități – n.n.).

În doctrină, au fost considerate „tehnici speciale de investigare a infracțiunilor": *i)* interceptarea și înregistrarea convorbirilor și comunicațiilor; *ii)* supravegherea video, audio sau prin fotografiere; *iii)* localizarea sau urmărirea prin GPS sau prin alte mijloace tehnice de supraveghere; *iv)* obținerea listei apelurilor telefonice efectuate de la un anumit post telefonic; *v)* reținerea, predarea sau percheziționarea trimiterilor poștale; *vi)* conservarea imediată a datelor informatice ori a datelor referitoare la traficul informațional; *vii)* accesul într-un sistem informatic; *viii)* reținerea datelor generate sau prelucrate de furnizorii de servicii de

[1] *Em. Stancu*, Tratat de Criminalistică, ed. a V-a, revăzută și adăugită, Ed. Universul Juridic, București, 2010, p. 31.

[2] *Gh. Mateuț*, Procedură penală, 2019, p. 673.

[3] *Idem*, Observații critice privind noua reglementare a supravegherii tehnice într-o prezentare comparativă, în Caiete de Drept Penal nr. 3/2015, p. 13.

[4] Memorandumul explicativ al Recomandării (2005) 10 a Comitetului de Miniștri al Consiliului Europei, pe *www.coe.int*

[5] Termenul cunoaște o mare variabilitate, de la cumpărări-test, comportament criminal simulat etc. – *N. Brady*, op. cit., p. 38.

comunicații electronice destinate publicului sau de rețele publice de comunicații; *ix)* utilizarea investigatorilor sub acoperire; *x)* livrarea supravegheată; *xi)* unele forme de percheziție[1].

Anterior intrării în vigoare a Codului de procedură penală, legislația procesuală penală era fragmentată în privința tehnicilor speciale de investigare, o parte fiind prevăzută de Codul de procedură penală anterior – interceptarea și înregistrarea convorbirilor sau comunicărilor efectuate prin telefon ori prin orice mijloc electronic de comunicare, înregistrările în mediu ambiental, localizarea sau urmărirea prin GPS ori alte mijloace de supraveghere, utilizarea investigatorilor sub acoperire, reținerea/predarea corespondenței și a obiectelor – și altele de legislația specială – accesul la un sistem informatic, livrarea supravegheată, punerea sub supraveghere a conturilor bancare și a conturilor asimilate acestora. Totodată, legislația specială prevedea, în paralel cu Codul de procedură penală, multe dintre tehnicile speciale prevăzute în Cod, ceea ce nu putea fi acceptat, constituind o problemă de sistematizare a legislației.

În Codul de procedură penală, adoptat prin Legea nr. 135 din 1 iulie 2010[2], metodele speciale de supraveghere sau cercetare sunt cuprinse în Capitolul IV al Titlului al IV-lea al Codului, respectiv între articolele 138 și 153 C.pr.pen.

Prin Codul de procedură penală în vigoare, legiuitorul a urmărit să unifice procedeele probatorii cu caracter derogatoriu și intruziv sub o singură reglementare cu un caracter unitar[3]. În funcție de aparente diferențe ale gradului de intruziune în viața privată a unei persoane, metodele speciale de supraveghere sau cercetare vor cunoaște condiții legale și proceduri diferite de autorizare, unele fiind de competența judecătorului de drepturi și libertăți, iar altele fiind lăsate la aprecierea procurorului.

Diferența dintre măsurile speciale de supraveghere și măsurile speciale de cercetare nu este expusă în Cod, ci este lăsată la interpretarea doctrinei, ca urmare a simplei mențiuni din cuprinsul art. 138 alin. (13) C.pr.pen., în care se arată că: „*prin «supraveghere tehnică» se înțelege utilizarea uneia dintre metodele prevăzute la alin. (1) lit. a)-d)*".

Astfel, vor fi considerate **metode speciale de supraveghere**: *interceptarea comunicațiilor ori a oricărui tip de comunicare la distanță* [art. 138 alin. (1) lit. a) C.pr.pen.]; *accesul la un sistem informatic* [art. 138 alin. (1) lit. b) C.pr.pen.]; *supravegherea video, audio sau prin fotografiere* [art. 138 alin. (1) lit. c) C.pr.pen.] și *localizarea sau urmărirea prin mijloace tehnice* [art. 138 alin. (1) lit. d) C.pr.pen.].

În același timp, vor intra în categoria **metodelor speciale de cercetare**: *obținerea datelor privind tranzacțiile financiare ale unei persoane* [art. 138 alin. (1) lit. e) C.pr.pen.]; *reținerea, predarea sau percheziționarea trimiterilor poștale* [art. 138 alin. (1) lit. f) C.pr.pen.]; *utilizarea investigatorilor sub acoperire și a colaboratorilor* [art. 138 alin. (1) lit. g) C.pr.pen.]; *participarea autorizată la anumite activități* [art. 138 alin. (1) lit. h) C.pr.pen.] și *livrarea supravegheată* [art. 138 alin. (1) lit. i) C.pr.pen.].

Diferențierea dintre metodele speciale de supraveghere și metodele speciale de cercetare rămâne în sarcina doctrinei, exprimându-se opinia că un criteriu aparent al legiuitorului ar fi că, în cazul măsurilor de supraveghere, organele de urmărire penală primesc informațiile chiar în timp ce desfășoară activitățile, dar în cazul măsurilor speciale de cercetare, organele

[1] *M. Udroiu, R. Slăvoiu, O. Predescu*, Tehnici speciale, 2009, pp. 2-3.

[2] Legea nr. 135/2010 din 1 iulie 2010 privind Codul de procedură penală (M. Of. nr. 486 din 15 iulie 2010).

[3] *R.A. Popa*, Aspecte teoretice și practice referitoare la metodele speciale de supraveghere sau cercetare prevăzute în Codul de procedură penală, în Dreptul nr. 6/2015, p. 176.

de urmărire penală primesc informațiile despre activități după ce acestea au avut loc[1]. Chiar și autorul care reflectă acest criteriu subliniază că legiuitorul nu a reușit să determine un criteriu logic de diferențiere între metodele speciale de supraveghere și metodele speciale de cercetare, întrucât unele dintre cele din urmă vor produce informații cu privire la activități în timp real, astfel că modalitatea lor de desfășurare s-ar putea circumscrie metodelor speciale de supraveghere[2]. Este evident că nu s-a stabilit un criteriu clar de delimitare, mai ales în considerarea faptului că există metode speciale de cercetare în care legiuitorul impune, în mod expres, realizarea unei supravegheri, precum în cazul livrării supravegheate, unde va fi necesară „supravegherea permanentă a transportului ilegal sau suspect".

Gruparea în categoria supravegherii tehnice a celor patru măsuri arătate anterior, conform art. 138 alin. (13) C.pr.pen., s-ar face ca urmare a trăsăturilor comune, constând în monitorizarea în timp real a unor activități în curs de desfășurare, „prin folosirea de procedee și dispozitive tehnice"[3]. Criteriul prezentat este unul nedeterminant, deoarece în cazul mai multor metode speciale de cercetare există un caracter prevalent tehnic, precum în cazul obținerii datelor privind tranzacțiile financiare ale unei persoane, unde tranzacțiile financiare monitorizate se derulează printr-un sistem informatic.

După cum s-a arătat și în doctrină, metodele speciale de cercetare au un caracter eterogen, astfel încât fiecare procedeu are condiții și proceduri proprii de autorizare[4]. Acest lucru este adevărat, consolidând faptul că natura fiecărei măsuri speciale este într-atât de diferită încât ele au sfere de aplicație diferite. Variabilitatea mare a condițiilor de autorizare rezultă ca urmare a diferenței nivelului de ingerință ce poate fi adus vieții private a unei persoane, în opinia legiuitorului, care, în ceea ce ne privește, este prea permisiv în cazul unor măsuri.

S-a considerat că este necesară introducerea unei reglementări clare, prin care să se delimiteze procedeele probatorii comune de metodele speciale de cercetare[5]. Un bun exemplu în această privință este măsura obținerii datelor privind situația financiară a unei persoane, care nu presupune nicio condiție specială de autorizare, nu presupune o executare în timp și este minimum intruzivă, putând fi cunoscută situația patrimonială a unei persoane exprimată prin soldul conturilor sale deschise la entități financiare. O atare măsură nu se impune a fi menținută ca tehnică specială de investigație, trebuind să fie eliminată întru totul, spre deosebire de măsura similară a obținerii datelor privind tranzacțiile financiare ale unei persoane. Aceasta din urmă se impune a fi menținută, întrucât prezintă o mai mare ingerință în viața privată a unei persoane.

Încercându-se găsirea unui criteriu logic prin care să se stabilească anumite limite între metodele speciale de supraveghere și metodele speciale de cercetare, au fost identificate anumite abordări care sunt preferabile stadiului actual al tehnicilor speciale de investigare. Într-o primă opinie, s-a arătat că o clasificare s-ar putea face pe baza următoarelor criterii: *i)* organul care autorizează măsura – judecătorul de drepturi și libertăți sau procurorul; *ii)* nivelul de intruziune în viața privată a unei persoane; *iii)* tipul de activitate, în timp real sau după ce faptele au avut loc; *iv)* complexitatea activității[6]. Parțial în acord cu această opinie, în doctrină

[1] *C.M. Chiriță*, în N. Volonciu, A.S. Uzlău (coord.), Noul Cod, 2014, p. 304.

[2] *Ibidem*.

[3] *M. Bulancea, G. Zlati, R. Slăvoiu*, în M. Udroiu (coord.), Codul de procedură penală, 2017, p. 634.

[4] *Ibidem*.

[5] *Gh. Mateuț*, Observații critice privind noua reglementare a supravegherii tehnice într-o prezentare comparativă, în Caiete de Drept Penal nr. 3/2015, p. 13.

[6] *C.M. Chiriță*, în N. Volonciu, A.S. Uzlău (coord.), Noul Cod, 2014, pp. 304-305.

s-a arătat nevoia unei proceduri unice de autorizare, care trebuie să pună în valoare judecătorul ca unic garant viabil al respectării drepturilor și libertăților persoanei în cadrul unui proces penal[1].

În opinia noastră, deși considerăm că ar fi utilă introducerea unei proceduri unice de autorizare a metodelor speciale de supraveghere sau cercetare, nu credem că se impune a fi făcute clasificări și nici găsirea unui criteriu prin care acestea să fie grupate, întrucât nu ar fi de folos nimănui să găsim, precum legiuitorul, criterii artificiale. Mai degrabă, apreciem că procedura de autorizare trebuie să fie unitară și condițiile legale de autorizare să fie diferite pentru fiecare tehnică specială în parte pentru ca, pe baza acestora, judecătorul de drepturi și libertăți să se pronunțe. În realitate, este chiar un deziderat destul de simplu de atins din punct de vedere legislativ, întrucât va trebui să se determine doar categoriile de infracțiuni a căror cercetare va putea justifica fiecare tehnică specială în parte. Afirmăm acest lucru, deoarece alte condiții legale, precum existența unei urmăriri penale legal începute, respectarea proporționalității măsurii cu scopul urmărit și subsidiaritatea acesteia față de alte procedee probatorii mai puțin intruzive, trebuie să fie condiții universale pentru toate tehnicile speciale de investigare.

Se poate remarca și faptul că, în urma unei analize a practicii judiciare, prevalența folosirii metodelor speciale de supraveghere sau cercetare este un temei de îngrijorare, întrucât folosirea lor în mod disproporționat ignoră natura lor de procedee probatorii speciale. Din punctul de vedere al sistematizării Codului de procedură penală, o soluție ar putea fi includerea tuturor metodelor speciale de supraveghere sau cercetare în cadrul procedurilor speciale care, oricum, au un caracter eterogen. Printr-o asemenea măsură s-ar putea propaga ideea că procesul penal trebuie să se întemeieze pe procedeele probatorii comune și numai în cazuri excepționale pot fi folosite aceste procedee probatorii speciale, derogatorii și care restrâng grav drepturile și libertățile fundamentale ale persoanei.

În secțiunile care urmează, vom trata necesitatea prevederii în legislația națională a unor dispoziții care să reglementeze într-un mod cât mai complet metodele speciale de supraveghere sau cercetare, precum și elementele caracteristice ale acestora, care le fac să se distingă față de procedeele probatorii comune.

Secțiunea a 2-a. Importanța reglementării legale a tehnicilor speciale de investigare

Necesitatea instituirii prin lege a tehnicilor speciale de investigare constituie o consecință a respectării drepturilor și libertăților fundamentale ale omului, în condițiile în care dezvoltarea de noi metode de comitere a infracțiunilor și prevalența globală a unor infracțiuni grave impun măsuri drastice pentru combaterea criminalității, împreună cu menținerea unui just echilibru între interesele societății și cele ale individului. Dacă metodele clasice de obținere a probelor și de tragere la răspundere penală a infractorilor se dovedesc a fi ineficiente, legiuitorul este obligat să găsească și să reglementeze noi metode care să acorde puteri sporite organelor de urmărire penală, în același timp stabilind un just echilibru cu drepturile individului, pentru a nu conduce la colapsul democratic al societății[2]. Or, tocmai acesta este rolul Parlamentului, de

[1] *Gh. Mateuț*, Observații critice privind noua reglementare a supravegherii tehnice într-o prezentare comparativă, în Caiete de Drept Penal nr. 3/2015, p. 13.

[2] *C. Olaru*, Mijloace specifice de investigare a infracțiunilor de criminalitate organizată, Ed. Hamangiu, București, 2014, p. 1.

a limita modul de exercitare a puterii executivului, ca acesta să nu dobândească puteri într-atât de mari încât să fie socotite tiranice. Într-un sistem al separației puterilor în stat este firesc ca oricare dintre acestea să încerce să își lărgească puterea, în fiecare dintre ramuri – legislativă, executivă și judecătorească – existând presiuni interne inerente pentru a-și depăși nivelul de putere, însă acestea vor trebui să fie rezistente[1]. Atributul de a menține echilibrul între puteri revine Curții Constituționale, care constată situațiile în care una dintre puteri și-a depășit prerogativele prevăzute în Constituție[2].

O caracteristică pe care o vom dezvolta într-o secțiune ulterioară privește caracterul restrictiv față de drepturile și libertățile fundamentale ale persoanei și de la aceasta pornește necesitatea prevederii în lege a tehnicilor speciale de investigare a infracțiunilor. În temeiul art. 53 alin. (1) din Constituție, o astfel de restrângere nu se va putea realiza decât în măsura în care ea este prevăzută de lege. În același sens, bogata jurisprudență a Curții Europene a Drepturilor Omului ne amintește că o restrângere a drepturilor persoanei, în special a dreptului la viață privată, se va putea face numai dacă aceasta este prevăzută de lege[3]. Întrucât toate metodele speciale de supraveghere sau cercetare vor presupune o ingerință adusă drepturilor persoanei, condiția primordială ca acestea să poată fi utilizate într-o societate democratică este prevederea lor în lege, într-un mod clar și previzibil, pentru ca orice persoană să poată cunoaște gradul de ingerință la care va putea fi supusă dacă ar comite o infracțiune sau s-ar afla în legătură cu persoane care săvârșesc infracțiuni. Dată fiind utilitatea pe care o pot avea măsurile speciale de supraveghere sau cercetare, nu se poate concepe ca ele să nu fie folosite de organele de urmărire penală în cazurile strict necesare, ceea ce impune legiuitorului obligația pozitivă de a reglementa modul lor de întrebuințare și constituirea unor garanții legale suficiente pentru a menține proporționalitatea dintre măsură și scopul urmărit[4].

Reglementarea metodelor speciale de supraveghere sau cercetare va presupune existența unei dispoziții legale specifice fiecărei metode speciale, nefiind acceptabilă abordarea contrară, a admisibilității oricărui procedeu probatoriu, cu excepția celor care sunt expres interzise de lege[5]. O atare abordare a fost sancționată printr-o decizie mai veche a Curții Europene a Drepturilor Omului, stabilindu-se necesitatea prevederii fiecărei metode speciale de supraveghere prin lege[6]. Această obligație reflectă caracterul derogatoriu al tehnicilor speciale de investigație de la dreptul comun[7]. Sub acest aspect, există o limitare absolută în folosirea oricăror tehnici cu caracter ascuns, fără ca acestea să fie prevăzute de lege[8].

Din acest punct de vedere, legislația română, deși delimitează metodele speciale de supraveghere sau cercetare de celelalte procedee probatorii (procedeele probatorii comune), nu impune nicio limitare a lor, fiind corelate dispozițiile art. 97 alin. (3) C.pr.pen. cu cele ale art. 97 alin. (2) C.pr.pen. Potrivit art. 97 alin. (2) lit. f) C.pr.pen., proba se poate obține prin orice alt mijloc de probă care nu este interzis de lege. Printr-o interpretare sistematică a acestei dispoziții

[1] U.S., cauza *INS c. Chadwa*, Hotărârea din 23 iunie 1983, 462 U.S. 919 (1983), pe *supreme.justia.com*

[2] CCR, Dec. nr. 97 din 7 februarie 2008 (M. Of. nr. 169 din 5 martie 2008).

[3] CEDO, cauza *Malone c. Marea Britanie*, Hotărârea din 2 august 1984, §68; cauza *Kruslin c. Franța*, Hotărârea din 24 aprilie 1990, §36; cauza *Govell c. Marea Britanie*, Hotărârea din 14 ianuarie 1998, §62; cauza *Khan c. Marea Britanie*, Hotărârea din 4 octombrie 2000, §26, pe *hudoc.echr.coe.int*

[4] *C. Olaru*, op. cit., p. 2.

[5] *A. Ashworth, M. Redmayne*, The Criminal Process, 2014, p. 125.

[6] CEDO, cauza *Malone c. Marea Britanie*, Hotărârea din 2 august 1984, §79, pe *hudoc.echr.coe.int*

[7] *N. Brady*, op. cit., p. 48.

[8] *Ibidem*, p. 40.

s-ar înțelege că se va aplica și procedeului probatoriu; astfel, ar rezulta că este admis și orice procedeu probatoriu care este în mod expres interzis de lege. În lipsa unei definiții legale a tehnicilor speciale de investigare sau a metodelor speciale de supraveghere sau cercetare, nu se poate susține că există o interdicție legală de a se folosi și alte asemenea metode. În concret, lipsa unei definiții a metodelor speciale prin raportare la trăsături caracteristice poate conduce la posibilitatea organelor de urmărire penală să folosească procedee probatorii noi, care aduc maximă ingerință drepturilor și libertăților fundamentale ale persoanelor și care excedează, din punct de vedere formal, metodelor speciale de supraveghere sau cercetare, întrucât nu ar fi prevăzute de art. 138 alin. (1) C.pr.pen. La acest moment, nu există nicio garanție că o persoană nu poate fi supusă unor alte tehnici speciale de supraveghere care să nu poată fi încadrate în niciuna dintre categoriile art. 138 C.pr.pen. și prin aceasta să se obțină probe.

Importanța reglementării tehnicilor speciale de investigație nu se va rezuma numai la reglementarea fiecărei măsuri individuale, ci va însemna și definirea legală a acestora, stabilirea unor trăsături și caracteristici comune și instituirea unui regim derogatoriu clar și previzibil care să nu permită organelor de urmărire să eludeze legea prin tehnici speciale care nu sunt enumerate de lege[1].

Spre deosebire de Codul de procedură penală anterior, legislația procesuală penală actuală realizează o bună sistematizare a acestora, ușurând aplicarea acestora de către organele de urmărire penală[2]. Aceasta nu înseamnă doar că va fi suficientă copierea tuturor tehnicilor speciale din legislația specială în cuprinsul Codului de procedură penală, fiind necesară și o sistematizare a acestora și o mai bună abstractizare a conceptului de „tehnici speciale de investigație". Deocamdată există suficient de multe lipsuri legislative din perspectiva corelării dintre măsuri, în special în privința procedurii de autorizare, conducând la diferențe de regim juridic care nu pot fi explicate. De pildă, nu se justifică nefolosirea unei singure proceduri de autorizare a măsurilor de supraveghere sau cercetare care sunt date în competența judecătorului de drepturi și libertăți.

În literatura de specialitate s-a subliniat faptul că legiuitorul nu a fost coerent în modalitatea de reglementare a măsurilor de supraveghere și cercetare, deoarece unele măsuri de cercetare vor furniza organelor de urmărire penală informații în timpul desfășurării lor[3], cel mai bun exemplu fiind utilizarea investigatorilor sub acoperire și a colaboratorilor. Cele constatate sunt adevărate și reflectă gradul de superficialitate a legiuitorului în crearea celor două categorii distincte – supravegherea tehnică definită de legiuitor numai prin componentele sale și orice altă măsură considerată măsură de cercetare. Practic, măsurile speciale de cercetare au caracter rezidual în viziunea legiuitorului, neapreciindu-se ca fiind importantă o mai mare abstractizare a acestora. O atare abordare o considerăm greșită, deoarece pune accentul prea mult pe metodele de supraveghere tehnică, în detrimentul altor măsuri care nu sunt suficient de bine definite sau cunoscute și care suferă reglementări incomplete, apte să conducă la prejudicierea persoanelor față de care sunt autorizate.

În ceea ce ne privește, sistematizarea tehnicilor speciale de investigare nu se poate realiza într-un mod arbitrar, precum în prezent, fiind necesar a se recunoaște că fiecare metodă are particularități care nu pot conduce la introducerea lor în categorii exacte. Cel mai bun exemplu în acest sens este metoda specială de cercetare a obținerii datelor privind tranzacțiile financiare

[1] *C. Olaru*, op. cit., p. 6.
[2] *Gh. Mateuț*, Procedură penală, 2019, p. 673.
[3] *Ibidem*.

ale unei persoane care, anterior, reprezenta o măsură de supraveghere tehnică, pentru ca, la acest moment, ea să fie o metodă specială de cercetare.

Secțiunea a 3-a. Caracterul secret al tehnicilor speciale de investigare

O trăsătură definitorie a tehnicilor speciale de investigare este caracterul lor secret, în sensul în care desfășurarea acestora trebuie să aibă loc fără știrea persoanei supravegheate, fapt relevat prin însăși natura fiecărei tehnici concrete. În mod ideal, prin caracterul secret al tehnicilor de investigare, persoana care realizează operațiunea trebuie să fie ascunsă atât de persoana vizată, cât și de terțe persoane, care nu au legătură cu cauza[1]. Acest caracter nu trebuie să fie înțeles doar în sensul fizic, prin imposibilitatea observării persoanei care pune în executare o asemenea măsură, ci și în sensul imposibilității aflării măsurii ca urmare a deghizării sale prin diverse metode, precum prezentarea de identități asumate, acte nereale sau prezentarea activităților ca fiind normale (de pildă, deghizarea operațiunii într-o intervenție la distribuția unei utilități).

Caracterul secret al tehnicilor speciale de investigare limitează folosirea acestora la faza urmăririi penale, neputând fi concepute activități secrete desfășurate față de acuzat în cursul judecății. În faza de judecată, principiul guvernator va fi cel al publicității, prevăzut de art. 352 C.pr.pen., ce derivă din art. 8 C.pr.pen. și art. 6 par. 1 Conv.EDO, astfel că o judecată secretă, desfășurată în absența apărării, nu poate avea loc. În conformitate cu art. 352 alin. (2) C.pr.pen., publicul asistă la desfășurarea judecății, constituind o garanție împotriva arbitrariului în desfășurarea procedurilor judiciare și dând legitimitate instanței. În mod excepțional, unele dintre tehnicile speciale de investigare pot fi întrebuințate și în faza de executare a pedepsei, în cadrul procedurii speciale a dării în urmărire prevăzute de art. 521 C.pr.pen.

Revenind, posibilitatea folosirii metodelor speciale de supraveghere sau cercetare se va limita numai la faza urmăririi penale, ca urmare a caracterului secret, care nu va trebui să fie confundat cu caracterul nepublic al urmăririi penale, prevăzut de art. 285 alin. (2) C.pr.pen. Acesta reflectă împrejurarea că actele de urmărire penală nu vor putea fi aduse la cunoștința persoanelor terțe, în vederea bunei desfășurări a urmăririi penale și în scopul de a proteja prezumția de nevinovăție a persoanelor care sunt cercetate. Cu toate acestea, urmărirea penală nu va avea un caracter secret, întrucât organele de urmărire penală nu vor disimula desfășurarea de acte de urmărire penală, realizând toate actele de procedură necesare chiar și în prezența terților. De pildă, cercetarea locului faptei în cazul unui accident auto în urma căruia au rezultat victime se va realiza pe un drum public, în fața terților, însă va avea tot un caracter nepublic, deoarece aceștia nu participă la efectuarea respectivului act de urmărire penală și nici nu asistă la desfășurarea lui, neavând dreptul de a cunoaște conținutul actelor de procedură desfășurate. Caracterul secret duce la eliminarea chiar și a bănuielii unei persoane că s-ar putea efectua acte de urmărire penală sau că ar exista o cauză penală.

Consecința caracterului secret este creșterea nevoii de supraveghere a autorizării și punerii în executare a acestor măsuri, alături de asigurarea posibilității persoanei supuse măsurii să fie informată despre faptul că a fost supusă unei măsuri intruzive și să i se acorde posibilitatea de a o contesta. O atare abordare este una necesară pentru a asigura o transparență în folosirea

[1] *P. Jenkins*, Advanced Surveillance: The Complete Manual of Surveillance Training, Intel Publications, Oxenhope, 2003, p. 4.

măsurilor intruzive numai atunci când ele sunt strict necesare și cu informarea persoanei supravegheate, pentru a nu se crea impresia în societate de desfășurare a unor acțiuni care să conducă la un sentiment de neliniște, cauzat de aparența de monitorizare continuă. În plus, caracterul secret al tehnicilor speciale de investigare va impune folosirea lor numai în situații excepționale, nefiind de conceput ca activitatea organelor de urmărire penală să își schimbe specificul într-unul similar autorităților ce activează în domeniul siguranței naționale. De altfel, dacă analizăm esența acestor tehnici, ele sunt aplicații în domeniul judiciar ale unor tehnici folosite de serviciile de informații. Bunăoară, interceptarea comunicațiilor, mai înainte de a fi folosită în domeniul judiciar, era folosită de serviciile secrete, un renumit exemplu fiind interceptarea comunicațiilor secrete ale Germaniei naziste în timpul celui de-Al Doilea Război Mondial, prin decriptarea faimosului algoritm de criptare *Enigma*. Mergând și mai departe în trecut, reținerea corespondenței prin interceptarea curierului este cunoscută de la momentul inventării noțiunii de „poștă". Totodată, asumarea unei alte identități decât cea reală este o străveche metodă de culegere de informații.

Dezvăluirea desfășurării unei cercetări penale față de o persoană conduce la o reacție firească pentru aceasta de a preveni tragerea sa la răspundere penală. Aceasta poate îmbrăca forme licite, precum exercitarea dreptului la apărare, dar și forme în care va fi evidențiată reaua-credință a persoanei, precum ascunderea unor mijloace de probă ori distrugerea lor, ceea ce nu poate fi considerat a fi culpabil în sine și nicidecum o probă în sprijinul acuzațiilor. Caracterul secret al măsurilor speciale de supraveghere sau cercetare transcende această problemă, întrucât divulgarea secretului operațiunii conduce la ineficiența măsurii, astfel că nu vor putea fi obținute probe de către organele de urmărire penală. Este greu de imaginat cum vor putea fi obținute probe și, chiar dacă vor fi obținute, dacă acestea vor fi concludente în situația în care o persoană supravegheată ar cunoaște acest lucru.

Din caracterul secret al tehnicilor speciale de investigație rezultă caracterul derogatoriu al acestora, întrucât presupun folosirea unor metode și practici străine procesului penal, pentru că nu vor permite apărării nicio posibilitate să le influențeze înainte sau în timpul desfășurării lor. Deși există procedee probatorii care conduc și ele la o restrângere a drepturilor fundamentale ale unei persoane – percheziția domiciliară, examinarea fizică, examinarea medico-legală psihiatrică etc. – numai în cazul măsurilor speciale de supraveghere sau cercetare, apărarea nu are și nici nu poate avea cunoștință de desfășurarea lor, în mod evident, neavând nici dreptul de a participa la efectuarea acestora. Din acest punct de vedere, apărarea este pusă într-o situație de inegalitate față de acuzare, ceea ce impune garanții suplimentare față de alte procedee probatorii, care să permită, pe de o parte, autorizarea lor numai în condiții restrictive și, pe de altă parte, crearea unor proceduri specializate în favoarea apărării în vederea asigurării echitabilității procedurii. În literatura de specialitate străină a fost observată tendința procesului penal de a adopta elemente proactive, statul trecând de la pedepsirea săvârșirii unor infracțiuni la identificarea persoanelor periculoase și privarea lor de libertate mai înainte de a prejudicia societatea[1], o atare tendință fiind încurajată de tehnicile speciale de investigare, mai ales atunci când sunt folosite în masă[2]. O prevenire, în special în cazul unor infracțiuni care

[1] *A. Ashworth, L. Zedner*, Preventive Justice, Ed. Oxford University Press, Oxford, 2014, p. 10.

[2] *I. Bălan*, Dreptul la respectarea vieții private și supravegherea video, audio sau prin fotografiere. Partea I, în Pandectele Române nr. 7/2015, pp. 96-97.

vatămă în mod grav societatea, va fi de înțeles și de acceptat, însă atenție deosebită va trebui să fie acordată necesității și întinderii acestora[1].

Prin natura lor, tehnicile speciale de investigare presupun un dezechilibru între drepturile apărării și cele ale acuzării, în niciun caz apărarea neavând posibilitatea să procedeze la folosirea acelorași procedee probatorii pentru a obține probe în vederea susținerii poziției sale procesuale. Astfel, tehnicile speciale de investigare vor fi administrate numai de acuzare, cu excepția înregistrărilor realizate de părți în condițiile art. 139 alin. (4) C.pr.pen., care cunosc un regim separat.

Codul de procedură penală conține inclusiv dispoziții privind menținerea secretului operațiunilor de către persoane care nu au calitatea de organe de urmărire penală; în acest sens, vor avea asemenea obligații persoanele care sunt chemate să dea concurs tehnic la executarea măsurilor de supraveghere tehnică [art. 142 alin. (3) C.pr.pen.], instituțiile de credit și entitățile financiare care comunică situația financiară a unei persoane sau tranzacțiile financiare ale acesteia, orice persoană care a aflat identitatea reală a investigatorului sub acoperire ori a colaboratorului, persoanele sau organele care realizează livrarea supravegheată etc.

Divulgarea caracterului secret al operațiunii care se circumscrie unei tehnici speciale de investigare poate conduce și la desfășurarea unei măsuri contrare, cu respectarea dreptului la viață privată. Într-o societate democratică, restrângerea dreptului la viață privată al unei persoane poate fi realizată numai dacă măsura este necesară și proporțională cu scopul urmărit. Or, dacă, prin neglijența organelor de urmărire penală, secretul operațiunii se pierde, atunci măsura va avea un caracter pur intruziv, nemaifiind nici necesară și nici proporțională pentru urmărirea penală. Divulgarea secretului operațiunii va putea conduce și la punerea în pericol a persoanelor care o pun în executare, fiind lesne de imaginat pericolul la care se poate expune un investigator sub acoperire ori un colaborator în această situație.

Caracterul derogatoriu al tehnicilor speciale de investigare – prin natura sa secretă – va permite folosirea unor astfel de măsuri numai ca urmare a ineficienței unor alte procedee probatorii (procedeele probatorii comune) sau măsuri de investigare care nu presupun documentarea infracțiunilor care fac obiectul urmăririi penale prin investigații secrete.

Secțiunea a 4-a. Restrângerea drepturilor fundamentale ale persoanei – caracteristică a tehnicilor speciale de investigare

Un avantaj care vine împreună cu caracterul secret al tehnicilor speciale de investigare este posibilitatea de a obține probe care pot avea caracter determinant în procesul penal, adeseori fiind obținute probe directe care pot stabili vinovăția unei persoane prin ele însele. Această putere deosebită a tehnicilor speciale vine cu costul unei ingerințe grave a dreptului la viață privată al persoanei, care va trebui să se înscrie între limitele prevăzute de lege pentru a putea conduce la obținerea legală de probe în procesul penal[2].

[1] *L. Zedner*, Seeking Security by Eroding Human Rights: The Side-stepping of Due Process, în B.J. Goold, L. Lazarus (coord.), Security and Human Rights, Hart Publishing, Oxford, 2007, p. 260; *A.G. Ferguson*, Big Data and Predictive Reasonable Suspicion, în University of Pennsylvania Law Review, vol. 163, no. 2/2015, 163 U. Pa. L. Rev. 327 (2015), pp. 338-340.

[2] *A. Zarafiu*, Procedură penală. Partea generală. Partea specială, ed. a 2-a, Ed. C.H. Beck, București, 2015, p. 209.

Cealaltă caracteristică importantă a tehnicilor speciale de investigare, în strânsă legătură cu caracterul lor secret, este că folosirea oricărei tehnici speciale de investigare va conduce la restrângerea drepturilor fundamentale ale unei persoane[1]. Această restrângere poate fi într-o asemenea măsură încât va putea conduce la anularea dreptului la viață privată al unei persoane, sens în care legea trebuie să prescrie garanții suficiente împotriva unui abuz. Lesne poate fi înțeles cum o tehnică specială de investigare, precum interceptarea comunicațiilor unei persoane, poate conduce la aflarea unor aspecte intime din viața unei persoane, împrejurări pentru care nu a consimțit să fie dezvăluite unei alte persoane decât cea cu care comunică. În această situație va fi restrâns secretul corespondenței persoanei și dreptul la viață privată. Un alt exemplu este supravegherea activităților unei persoane fără ca aceasta să bănuiască, putând fi relevate aspecte deosebit de intime despre aceasta, în funcție de locul supravegheat. Prin acest exemplu, semnalăm o posibilă ingerință adusă dreptului la viață privată al persoanei și dreptului la domiciliu, în funcție de locul unde se desfășoară supravegherea. Ținând seama și de caracterul modern al comunicațiilor, dar și de prevalența mai mare a laturii „online" a vieții persoanei, accesul la un sistem informatic permite aflarea conținutului unui sistem informatic al persoanei, cu posibilitatea aflării activităților sale anterioare, dar și monitorizarea în timp real a activităților sale, altele decât cele care se circumscriu noțiunii de „comunicații" (ce filme vizionează, dacă redactează documente, ascultă muzică etc.).

Este nepermis ca organelor de urmărire penală sau autorităților statului să li se permită folosirea excesivă sau în mod automat[2] și abuziv a tehnicilor speciale. Sub pretextul necesității protejării securității naționale, instituirea unui sistem secret de supraveghere tehnică a populației poate ajunge la subminarea sau chiar distrugerea democrației prin măsuri care, declarativ, ar fi instituite pentru a o apăra[3].

Atunci când avem în vedere restrângerea dreptului la viață privată al unei persoane, nu ne referim la o restrângere care să se exteriorizeze public (precum restrângerea dreptului la libertate), ci mai degrabă la restrângerea exercitării dreptului într-un caracter liber și deplin. Întrucât drepturile fundamentale cele mai afectate vor fi cele din sfera vieții private a unei persoane, folosirea tehnicilor speciale va constitui o ingerință sau o intruziune a organelor de urmărire penală în libera și neîngrădita exercitare a acestui drept și a componentelor acestuia – dreptul la viață privată în sens restrâns, libertatea de exprimare, secretul corespondenței, dreptul la domiciliu.

Chiar dacă există procedee probatorii care vor putea constitui restrângeri ale drepturilor fundamentale ale unei persoane, situație incidentă și în cazul măsurilor preventive și al celor de siguranță, ingerința va avea un caracter deschis și mai atenuat față de dreptul la viață privată. Afirmăm acest lucru, deoarece și o persoană care este privată de libertate – fiind în stare de detenție preventivă – va avea dreptul la viață privată, astfel că nu va putea fi supravegheată în zona de detenție decât conform prevederilor legale și, în general, numai pentru a se asigura menținerea sa în stare de privare de libertate. De altfel, intruziunea în viața sa privată nu va fi una intenționată, ci va fi o consecință accesorie a măsurii preventive.

---

[1] *A. Galetta, P. De Hert*, Complementing the Surveillance Law Principles of the ECtHR with its Environmental Law Principles: An Integrated Technology Approach to a Human Rights Framework for Surveillance, în Utrecht Law Review, 10 Utrecht L. Rev. 55 (2014), p. 59; *C. Olaru*, op. cit., p. 2; *M. Daniele, E. Calvanese*, Evidence Gathering, în R.E. Kostoris (coord.), Handbook of European Criminal Procedure, Ed. Springer, Cham, 2018, p. 371; *M.F.H. Hirsch Ballin*, Anticipative Criminal Investigation: Theory and Counterterrorism Practice in the Netherlands and the United States, Ed. Springer, Haga, 2012, p. 550.

[2] CEDO, cauza *Iordachi ș.a. c. Moldova*, Hotărârea din 10 februarie 2009, §51-52, pe *hudoc.echr.coe.int*

[3] CEDO, cauza *Roman Zakharov c. Rusia*, Hotărârea din 4 decembrie 2015, §232, pe *hudoc.echr.coe.int*

Prin tehnicile speciale de investigare, chiar și în cazul unei persoane aflate în stare de detenție, se poate realiza o intruziune în viața sa privată care va trebui justificată distinct și care va avea caracter secret. În această situație, ingerința în viața privată va fi una intenționată, în vederea strângerii de probe într-o cauză penală.

Întrucât restrângerea drepturilor persoanei este inerentă utilizării tehnicilor speciale de investigare, este necesar ca legiuitorul să prevadă anumite garanții procesuale care să prevină un abuz din partea organelor de urmărire penală în folosirea excesivă a acestor tehnici. Aceste garanții trebuie să fie prevăzute de lege pentru a limita posibilitatea de autorizare a tehnicilor numai în condiții restrânse și de către o autoritate independentă.

O primă garanție care trebuie avută în vedere este limitarea aplicabilității tehnicilor speciale de investigare la infracțiunile care depășesc o anumită gravitate, acestea trebuind rezervate numai la infracțiunile considerate cele mai periculoase pentru ordinea publică. Lipsa acestei garanții va conduce la o ingerință nepermisă în viața persoanei, întrucât ar contraveni art. 8 par. 2 Conv.EDO, care impune stabilirea oricăror ingerințe în dreptul la viață privată numai prin lege. După cum vom vedea în prezenta lucrare, prin raportare la specificul infracțional din România și la carențele legislative, metodele speciale de supraveghere sau cercetare pot fi, ipotetic, aplicate majorității infracțiunilor pentru care se dispune trimiterea în judecată, conform statisticilor de activitate ale Ministerului Public.

O a doua garanție în vederea limitării ingerințelor în viața privată a unei persoane o constituie autorizarea măsurii de către o autoritate independentă, care mai apoi va supraveghea și controla punerea în executare a măsurii[1]. Prin „autoritate independentă" vom înțelege un organ diferit de cel care manifestă un interes în aplicarea tehnicii speciale. În legislația națională, rolul acesta îl are judecătorul de drepturi și libertăți, însă cu un rol diminuat în controlul ulterior și supravegherea punerii în aplicare a măsurii. În cazul unora dintre măsurile de cercetare, legiuitorul a stabilit că procurorul va avea competența de autorizare, situație pe care o apreciem ca fiind discutabilă în cazul majorității acestora.

A treia garanție pentru respectarea dreptului la viață privată al persoanei îl constituie un control de proporționalitate din partea autorității independente împuternicite de lege pentru a autoriza tehnicile speciale de supraveghere. Proporționalitatea are în vedere echilibrul care trebuie stabilit între ingerința adusă dreptului unei persoane și scopul pentru care se autorizează măsura care aduce această ingerință. În sens larg, termenul de „proporționalitate" nu se va referi numai la condiția prevăzută de art. 139 alin. (1) lit. b) C.pr.pen., ci va cuprinde întreaga procedură de autorizare și toate condițiile care se vor interpreta și aplica prin prisma principiului proporționalității. Organul judiciar care va autoriza tehnicile speciale de investigare va fi cel care va aprecia asupra proporționalității măsurii, ținând cont de mai multe elemente, precum existența unei suspiciuni rezonabile privind pregătirea săvârșirii unei infracțiuni și cât este de puternică această suspiciune prin raportare la fundamentul său obiectiv (date și informații ori probe), subsidiaritatea măsurii față de alte procedee probatorii mai puțin intruzive, dar și caracterul proporțional în sens restrâns prin raportare la activitatea concretă care se impune a fi autorizată și infracțiunea care se investighează (inclusiv gravitatea sa concretă, nu doar prin raportare la limitele de pedeapsă).

A patra garanție o va reprezenta punerea în aplicare a măsurii numai de către organele stabilite prin lege, o problemă des întâlnită în practica judiciară națională, ca urmare a implicării ilicite a serviciilor de informații.

[1] *R.A. Popa*, op. cit., p. 177.

A cincea garanție o constituie folosirea ca probă numai a rezultatelor care prezintă o relevanță cu respectiva cauză penală, trebuind să fie înlăturate toate celelalte rezultate care reprezintă ingerințe la dreptul la viață privată. Din păcate, legea română nu conține și dispoziții suficiente pentru a permite persoanei supravegheate să cunoască toate activitățile de supraveghere tehnică și rezultatele acestora și să aibă dreptul de a suplimenta cele selectate de procuror cu unele pe care le consideră a fi necesare în vederea exercitării dreptului la apărare.

A șasea garanție o constituie posibilitatea solicitării unui control subsecvent de legalitate (inclusiv de proporționalitate) a măsurilor de către persoana supravegheată sau care a făcut obiectul tehnicilor speciale. Această garanție nu este la acest moment prevăzută de legea română în cazul tuturor persoanelor, ci numai în favoarea inculpatului, celelalte fiind doar informate asupra unei măsuri de supraveghere tehnice luate împotriva lor. Exercitarea unui control *a posteriori* presupune și dreptul de a obține anularea măsurii, dar și distrugerea rezultatelor activităților rezultate din tehnicile speciale de investigare a infracțiunilor. O omisiune a legiuitorului român este lipsa prevederii unei proceduri, chiar și una de natură civilă, prin care să fie trași la răspundere funcționarii care au comis abuzuri în autorizarea și punerea în executare a tehnicilor speciale de investigare. Nici în privința răspunderii statului pentru astfel de abuzuri nu s-au instituit dispoziții speciale, practic neexistând nicio modalitate de a preveni abuzuri prin sancționarea persoanelor care greșesc și prin aceasta permit ingerințe grave în viața privată a unor persoane.

În concluzie, folosirea tehnicilor speciale de investigare va presupune, în mod obligatoriu, o restrângere a dreptului la viață privată al persoanei față de care se ia această măsură, situație care nu poate fi evitată ca urmare a caracterului său secret și a caracterului voit invaziv. Din acest motiv, revine legiuitorului obligația pozitivă de a stabili limitele folosirii acestor tehnici prin instituirea unor garanții efective care să prevină abuzul organelor care întrebuințează astfel de măsuri și de a permite persoanei supravegheate să fie informată asupra ingerinței și să poată obține anularea măsurii și distrugerea datelor obținute, precum și alte remedii ca urmare a unui eventual abuz.

Titlul II
Compatibilitatea utilizării tehnicilor speciale în raport cu respectarea drepturilor fundamentale ale omului

Capitolul I
Dreptul la viață privată

În continuarea celor relatate în cuprinsul titlului introductiv al lucrării, tehnicile speciale de supraveghere sau cercetare se caracterizează prin existența unei intruziuni în viața privată a persoanei, definitorie pentru aceste măsuri. Prezentul titlu va fi dedicat compatibilității dintre măsurile de supraveghere sau cercetare prevăzute de Codul de procedură penală și Convenția Europeană a Drepturilor Omului, analizând în mod general dacă acestea sunt în concordanță cu principiile stabilite de Convenție și de jurisprudența Curții.

Fiindcă majoritatea problemelor de convenționalitate presupun explicații mai elaborate prin raportare la anumite probleme (condițiile legale de autorizare, autorizarea măsurii, punerea în executare, informarea persoanei supravegheate, supravegherea tehnică a avocatului etc.), acestea vor fi cuprinse în secțiunile din lucrare dedicate fiecăreia dintre acestea. În prezentul titlu dorim să construim un cadru pentru această lucrare în care trebuie să privim analiza fiecărei metode speciale în parte și să avem în vedere caracterul intruziv în viața privată. Pentru a face acest lucru și pentru a justifica de ce, pe alocuri, în prezenta lucrare vom avea opinii ferme în privința lipsurilor legislației române însă, e necesar să explicăm cadrul în care trebuie să se desfășoare procesul penal pentru a fi considerat minim invaziv pentru persoana care va fi supusă unor tehnici speciale de investigare.

Necesitatea unei analize prin prisma drepturilor fundamentale ale omului este utilă și prin raportare la mentalitatea societății românești care, ca urmare a evenimentelor din luna decembrie 1989, cunoaște o perioadă de tranziție dinspre socialism către capitalism, dar și dinspre afirmarea cu rol prioritar a puterii și prerogativelor statului la o afirmare a drepturilor individului și a restricțiilor pe care trebuie să le suporte statul cu privire la aceste drepturi.

În contextul unei societăți care pune accentul pe digitalizare și pe libera transmitere a informației, precum și pe socializarea publică excesivă și dezvăluirea liberă a amănuntelor din viața privată a unei persoane[1], credem că se impune ca, printr-o analiză a dreptului la viață privată, să ajungem la a determina ce este sacru de protejat într-o societate democratică și de pus la adăpost de orice incursiune a statului sau chiar și a privaților[2] care, prin oferta unor interacțiuni și a unor plăceri de moment, obțin consimțământul nostru, pseudo-informat, și au acces la viața noastră privată.

[1] *M. Andrejevic*, Exploitation in the Data Mine, în C. Fuchs, K. Boersma, A. Albrechtslund, M. Sandoval, Internet and Surveillance, The Challenges of Web 2.0 and Social Media, Ed. Routledge, New York, 2012, pp. 85-86.

[2] Cel mai bun exemplu este acordul dat pentru primirea de oferte comerciale sau de a se toca informații în fișiere tip *cookie*, plus tracking-ul realizat de site-uri, prin care se colectează date și, mai apoi, se transmit acesteia reclame țintite. A se vedea *P.B. Heymann*, An Essay on Domestic Surveillance, în Journal of National Security Law & Policy, vol. 8:421, 2015, p. 428.

Ținând seama de cele propuse mai sus, în prezenta secțiune vom aborda conceptul general de „viață privată" și vom analiza semnificația acestuia în jurisprudența Curții Europene a Drepturilor Omului, cercetând și câteva exemple de ingerințe aduse acestui drept. În secțiunile următoare vom detalia semnificația celorlalte componente ale vieții private, precum și legătura acestora cu metodele speciale de supraveghere sau cercetare, pentru ca, în finalul acestei părți a lucrării, să abordăm problema interacțiunii dintre aceste metode, dreptul la un proces echitabil și modul în care acest drept se leagă de respectarea dreptului la viață privată în contextul desfășurării procesului penal.

Încercându-se definirea dreptului la viață privată, în doctrină s-a apreciat că „*dreptul la viață privată este considerat un complex de valori și drepturi în virtutea cărora individul poate trăi separat de celelalte persoane, liber de a decide cu privire la propria persoană, într-o zonă lipsită de publicitate și unde trebuie să fie protejat de orice intruziune care i-ar putea aduce atingere integrității fizice, psihice ori demnității*"[1].

În literatura de specialitate[2] s-a arătat că, în viziunea conferită prin Convenția Europeană a Drepturilor Omului, sub umbrela dreptului la viață privată (în sens larg) sunt protejate patru interese ale unei persoane: viața privată (în sens restrâns), viața de familie, dreptul la domiciliu și secretul corespondenței, însă, deși aceste aspecte pot fi delimitate, ele se vor suprapune în mod inevitabil și obligatoriu[3].

Viața privată este importantă ca urmare a relației sale cu formarea identității persoanei și pentru modul în care ne ajută să dezvoltăm și să apărăm o anumită viziune asupra propriei persoane[4]. Atunci când ne afirmăm dreptul la viață privată, restabilim controlul asupra informațiilor despre noi și facem mai grea posibilitatea ca persoanele care vor să le afle să ne reducă identitatea la categorii de trăsături sau caracteristici[5].

Definirea conceptului de „viață privată" este, după cum se vede, o căutare care nu va conduce la un rezultat sigur, ci, mai degrabă, viața privată trebuie să se definească prin raportare la caracteristicile sale relevate în contextul Convenției, întrucât prin aceasta se urmărește apărarea lor prin jurisprudența Curții, care este în perpetuă evoluție. Prin interpretarea jurisprudenței Curții, doctrina a ajuns la concluzia că termenul de „viață privată" este un termen larg, care nu este susceptibil de o definiție exhaustivă[6].

Această concluzie de mai sus este în concordanță cu prevederile art. 8 Conv.EDO, care arată că: „*orice persoană are dreptul la respectarea vieții sale private și de familie, a domiciliului său și a corespondenței sale*". Practic, fără a realiza o definiție, se indică principalele componente ale dreptului la viață privată pe care le vom aborda în prezentul titlu al lucrării. Dreptul la viață privată nu este unul absolut, ci unul relativ, întrucât poate cunoaște restrângeri, atunci când ele sunt necesare într-o societate democratică. Din perspectiva tehnicilor speciale de supraveghere sau cercetare, acestea reprezintă astfel de restrângeri care, pentru a putea fi tolerate, trebuie să fie în concordanță cu limitele restrângerii dreptului, cuprinse tot în textul Convenției[7].

---

[1] *S. Șandru*, Protecția datelor personale și viața privată, Ed. Hamangiu, București, 2016, p. 50.

[2] *S. McKay*, Covert Policing, 2015, p. 28.

[3] CEDO, cauza *Miailhe c. Franța*, Hotărârea din 25 februarie 1993, §28, pe *hudoc.echr.coe.int*. În cauză s-a pus în discuție o încălcare a dreptului la viață privată care privea atât dreptul la viață privată (în sens restrâns), cât și dreptul la domiciliu și secretul corespondenței.

[4] *B.J. Goold*, în B.J. Goold, L. Lazarus (coord.), op. cit., p. 63.

[5] *Ibidem*.

[6] *S. McKay*, Covert Policing, 2015, p. 29.

[7] *N. Brady*, op. cit., p. 38.

Potrivit art. 8 par. 2 Conv.EDO, „*nu este admis amestecul unei autorități publice în exercitarea acestui drept decât în măsura în care acesta este prevăzut de lege și constituie, într-o societate democratică, o măsură necesară pentru securitatea națională, siguranța publică, bunăstarea economică a țării, apărarea ordinii și prevenirea faptelor penale, protecția sănătății, a moralei, a drepturilor și a libertăților altora*". Acest articol definește condițiile în care sunt permise intruziunile în viața privată a unei persoane, cea dintâi fiind prevederea de către lege a măsurii care restrânge dreptul. În contextul reglementării măsurilor de supraveghere sau cercetare, acesta este criteriul în funcție de care se va determina dacă un procedeu probatoriu poate fi administrat sau nu, din acest punct de vedere, legea română prevăzând în cuprinsul Codului de procedură penală aceste procedee probatorii. După cum vom vedea, simpla prevedere nu este suficientă, fiind necesar ca legea să aibă o anumită calitate, respectiv să fie clară și previzibilă. Totodată, alte condiții legale importante pe care le vom aborda sunt proporționalitatea și subsidiaritatea. Sub aspectul acestor două condiții, trebuie să indicăm faptul că au caracterul cel mai relativ, limitarea acestora de către stat putând conduce la restrângeri semnificative asupra drepturilor întregii populații, precum în cazul folosirii excesive a supravegherii.

O extremă a ingerințelor aduse dreptului la viață privată o reprezintă supravegherea în masă a persoanelor, aceasta putând fi exercitată prin orice cale și putând avea un grad variabil de ingerință adusă fiecărui individ, însă tendința curentă este cea de a crește gradul de supraveghere a persoanei, atât în spațiile publice (prin camere de supraveghere, de pildă), cât și în spațiul privat, prin monitorizarea interacțiunilor desfășurate online (supravegherea rețelelor de socializare inclusiv prin acces specializat al autorităților[1]). Prin supravegherea în masă desfășurată în scop preventiv, scopul unui proces penal se transferă de la un individ la o un grup social, abstract, creat artificial[2].

În literatura de specialitate au fost evidențiate pericolele unei supravegheri în masă sau excesive, ea fiind nocivă pentru ființa umană, reținându-se că: „*supravegherea neîngrădită, în special a activităților noastre intelectuale, amenință o revoluție cognitivă, care taie în centrul libertății minții pe care instituțiile noastre politice o presupun*"[3].

Dimensiunea problemei ingerințelor la viața privată a unei persoane a cunoscut o creștere deosebită mai ales după atentatele teroriste de la 11 septembrie 2001, moment crucial de la care politica statelor a fost de a sacrifica dreptul la viață privată pentru a asigura securitatea națională și, în mod paradoxal, conservarea libertății cetățeanului[4]. Imediat după respectivele atentate, guvernul S.U.A., prin DARPA[5], a adoptat o strategie numită *total information awareness*[6], bazată pe conceptul de „prevenție polițienească predictivă", cu scopul de a crea, dezvolta, aplica, integra, demonstra componente și sisteme care să combată amenințări asimetrice prin cunoașterea totală a informațiilor[7]. Cu alte cuvinte, s-au creat bazele unui sistem informatic integrat pentru

[1] *J.C. Wong*, US, UK and Australia urge Facebook to create backdoor access to encrypted messages, în ziarul The Guardian din 4 octombrie 2019, pe *www.theguardian.com*

[2] *J. Finn*, Capturing the Criminal Image: From Mug Shot to Surveillance Society, University of Minnesota Press, Minneapolis, 2009, p. 98.

[3] *N.M. Richards*, The Dangers of Surveillance, în Harvard Law Review, vol. 126, 1934, par. 1959 (2013), pe *harvardlawreview.org*

[4] *P.B. Heymann*, An Essay on Domestic Surveillance, în Journal of National Security Law & Policy, vol. 8:421, 2015, p. 428.

[5] Defense Advanced Research Projects Agency, agenție în subordinea U.S. Department of Defence.

[6] En., Cunoaștere totală a informațiilor.

[7] *E.D. Cohen*, Mass Surveillance and State Control: the total information awareness project, Ed. Palgrave Macmillan, New York, 2010, p. 21.

interceptarea, stocarea, căutarea, monitorizarea, citirea și analizarea informațiilor private computerizate a 300 de milioane de cetățeni americani, cât și a unui număr nedeterminat de cetățeni străini[1].

În contextul unei dezvoltări tehnologice de neoprit, folosirea sistemelor informatice interconectate, transferul rapid de date cu caracter personal între servere locale și cele din străinătate – fără cunoștința sau controlul utilizatorilor – transformă problema dreptului la viață privată într-una internațională, astfel că abordarea tradițională a drepturilor fundamentale, prin raportare la o anumită locație geografică, începe să își piardă din valoare[2]. Cele mai avansate state din lume și cele care aparent susțin un standard ridicat al respectării dreptului la viață privată sunt și cele care își permit, pe ascuns și deseori pentru siguranța națională (ceea ce, în cazul României, însemna și cercetarea unor infracțiuni precum cele de corupție[3]), să restrângă drepturile cetățeanului într-un mod greu de imaginat.

După scandalul internațional cauzat de informațiile dezvăluite de Edward Snowden privind desfășurarea de operațiuni în masă de supraveghere a populației americane, dar și a cetățenilor străini prin mijloace automatizate care reflectau și cele mai intime aspecte din viața persoanelor[4], intruziunile imaginate de autorul George Orwell, în cartea *1984*, par banale și lipsite de imaginație[5]. În era actuală, securizarea dreptului la viață privată necesită o cooperare transnațională, altfel, în contextul epocii internetului, securizarea vieții private numai la nivel local, și nu la nivel global, echivalează cu lipsa protejării dreptului la viață privată[6].

Securitatea, supravegherea tehnică, identitatea personală și dreptul la viață privată sunt probleme strâns legate; pe măsură ce statele își cresc capacitatea de a-i apăra pe cetățeni de amenințări externe și interne, ele pun în pericol, în mod indubitabil, posibilitatea persoanei de a trăi liberă de control, suspiciune, clasificare și discriminare, multe dintre garanțiile privind viața privată fiind insuficiente pentru a contracara această tendință[7].

Ca o soluție la această situație, devin din ce în ce mai importante mecanismele internaționale prin care se poate apăra dreptul la viață privată al persoanei, Convenția Europeană a Drepturilor Omului stabilind pentru toate statele care au ratificat-o un punct de pornire comun, în acord cu valorile democratice occidentale împărtășite și de alte state capitaliste dezvoltate din lume. Protecția și reținerea datelor personale în format electronic intră în sfera de aplicare a vieții private, astfel cum este ea protejată de art. 8 Conv.EDO, ce vizează o gamă largă de relații sociale, inclusiv confidențialitatea comunicațiilor și informațiilor în mediul online[8].

---

[1] *Ibidem*.

[2] *L.K. Donohue*, The Future of Foreign Intelligence, 2016, p. 56; *K. Ball, K. Haggerty, D. Lyon*, Routledge Handbook of Surveillance Studies, Ed. Routledge, Abingdon, Oxfordshire, 2012, p. 201.

[3] Consiliul Suprem de Apărare a Țării, Raportul Consiliului Suprem de Apărare a Țării privind activitatea desfășurată în anul 2005, p. 4, pe *csat.presidency.ro*

[4] *J.C. Yoo*, The Legality of The National Security Agency's Bulk Data Surveillance Programs, în Harvard Journal of Law & Public Policy, vol. 37, no. 3/2014, p. 909.

[5] *R. Jeffreys-Jones*, We Know all About You. The Story of Surveillance in Britain and America, Oxford University Press, Oxford, 2017, p. 204.

[6] *R.J. Krotoszynski, Jr.*, Privacy Revisited, 2016, p. 24.

[7] *B.J. Goold*, în B.J. Goold, L. Lazarus (coord.), op. cit., p. 69; *I. Kerr, V. Steeves, C. Lucock*, Lessons from the Identity Trail. Anonymity, Privacy and Identity in a Networked Society, Oxford University Press, New York, 2009, p. 45.

[8] *D. Panc*, Securitatea cibernetică la nivel național și internațional. Instrumente normative și instituționale, Ed. Hamangiu, București, 2017, p. 169.

Dreptul la viață privată nu este unul care să presupună ca statul să îl garanteze în relația sa cu cetățeanul, ci presupune ca statul să creeze un cadru normativ care să prevină ingerințele în viața privată a unei persoane la nivel general, indiferent dacă acestea provin de la o autoritate sau de la un particular. Din acest punct de vedere, revine legiuitorului o obligație pozitivă în a reglementa această restrângere, precum și limitele și condițiile sale[1]. O atare situație a fost reflectată și în jurisprudența Curții cu privire la relațiile dintre angajat și angajator și limitele în care angajatorul poate să aducă o ingerință în viața privată a angajatului[2].

În ceea ce privește restrângerea dreptului la viață privată, pe baza jurisprudenței Curții, doctrina a stabilit că trebuie să fie îndeplinite mai multe condiții pentru care acestea să fie în conformitate cu Convenția: *i)* restrângerea trebuie să fie prevăzută de lege; *ii)* trebuie să fie respectat principiul proporționalității (o intruziune gravă în viața privată va fi justificată numai în cazul infracțiunilor grave); *iii)* măsura trebuie să fie subsidiară (măsurile intruzive trebuie să fie ultima soluție); *iv)* organele judiciare trebuie să răspundă pentru măsurile luate (este necesară o autorizare prealabilă pentru intruziunea asupra dreptului, măsurile trebuie să fie documentate amănunțit și monitorizate de organul care le-a autorizat) și *v)* finalitate (informațiile obținute prin tehnicile speciale pot fi folosite numai pentru scopul pentru care au fost autorizate)[3].

Pentru a se determina dacă vor putea fi incidente dispozițiile art. 8 Conv.EDO, nu este necesară existența unei ingerințe, ci trebuie ca la momentul de dinainte de realizarea măsurii de investigație pe care și-o propune organul de urmărire penală să se stabilească dacă prin măsură se urmărește sau este măcar posibilă producerea unei intruziuni în viața privată a unei persoane și dacă o asemenea activitate de urmărire penală este între scopurile prevăzute de art. 8 Conv. EDO[4]. Dacă măsurile vor consta în observarea unei persoane pentru a afla mișcările sale și persoanele cu care se asociază, în ascultarea conversațiilor purtate de aceasta, în a fotografia sau înregistra video activitățile sale, în a dispune ca o terță persoană să interacționeze cu ea pentru a obține informații ori să îi monitorizeze mișcările prin mijloace tehnice și dacă rezultatul acestor activități va fi folosit ca probă sau informații pentru motive de securitate națională, vor fi vătămate drepturile prevăzute de art. 8 par. 1 Conv.EDO[5].

În aprecierea analizei asupra unei posibile ingerințe asupra dreptului la viață privată care să nu fie în concordanță cu principiile Convenției și cu jurisprudența Curții Europene a Drepturilor Omului, literatura de specialitate străină a stabilit că acest lucru se poate face printr-o analiză de proporționalitate (*lato sensu*) realizată de instanță în patru trepte: *i)* este scopul pentru care se restrâng drepturile unul legitim într-o societate democratică?; *ii)* este măsura care se solicită a fi autorizată adecvată pentru a se atinge acest scop?; *iii)* măsura care se cere autorizată este cel mai puțin intruzivă sau restrictivă de drepturi pentru atingerea scopului? *iv)* este măsura proporțională (*stricto sensu*) și conduce la un just echilibru între scopul acesteia și respectarea drepturilor și libertăților persoanei?[6]

Nerespectarea vreuneia dintre condițiile expuse mai sus în opiniile citate va conduce la constatarea unei ingerințe excesive și contrare Convenției realizate de stat, impunându-se

[1] *A. Ashworth*, Positive obligations in Criminal Law, Hart Publishing, Portland, 2013, pp. 199-200.

[2] CEDO, cauza *Bărbulescu c. România*, Hotărârea din 5 septembrie 2017, §108-111, pe *hudoc.echr.coe.int*

[3] *A. Ashworth, M. Redmayne*, The Criminal Process, 2014, pp. 35-36.

[4] *C. Harfield, K. Harfield*, Covert Investigation, 2018, p. 22.

[5] *Ibidem*, p. 22.

[6] *B.J. Goold, L. Lazarus, G. Swiney,* Public protection, Proportionality and the Search for Balance, în Ministry of Justice Research Series 10/07, London, 2007, pp. 1-2, pe *papers.ssrn.com*

constatarea încălcării art. 8 Conv.EDO. Curtea va fi limitată numai să constate la sfârșitul unui proces penal că a existat o încălcare a dreptului la viață privată, sens în care se impune ca instanțele naționale să poată sancționa orice act al organelor judiciare care aduce o ingerință nepermisă dreptului la viață privată.

În ceea ce privește sancțiunile aplicabile unui act de procedură desfășurat în dezacord cu respectarea dreptului la viață privată, această problemă nu este tranșată în mod ferm de jurisprudența Curții, mai degrabă este lăsată la aprecierea instanțelor naționale. În contextul tehnicilor speciale de supraveghere sau cercetare, s-a considerat că folosirea în procesul penal împotriva persoanei acuzate a unor probe obținute cu încălcarea Convenției, dacă nu va fi automat considerată o încălcare a echitabilității în sensul art. 6 Conv.EDO, însăși protecția drepturilor de către Convenție ar fi pusă sub semnul întrebării[1]. Același autor susține, prin raportare la mai multe opinii separate exprimate în jurisprudența Curții Europene a Drepturilor Omului[2], că excluderea probelor obținute contrar protejării dreptului la viață privată ar trebui să fie un corolar esențial al dreptului, dacă se consideră că dreptul la viață privată are o valoare reală și nu este apărat doar în mod formal[3].

S-a apreciat că instanțele trebuie să țină seama de compatibilitatea măsurii de supraveghere tehnică cu preceptele art. 8 Conv.EDO privind dreptul la viață și că obligația instanței este să nu procedeze ea însăși în mod nelegal atunci când constată că prin respectivele măsuri s-a produs o vătămare a acestui drept și va trebui să decidă admisibilitatea probei prin prisma legislației naționale[4]. Aplicând această constatare la sistemul național, în special ținând seama de condițiile legale ce trebuie îndeplinite pentru autorizarea supravegherii tehnice, dar și de regimul nulităților, o încălcare a dreptului la viață privată prin desfășurarea în afara condițiilor legale a supravegherii tehnice va trebui să conducă la excluderea probei obținute.

Întrucât prezenta lucrare are în vedere dreptul la viață privată în contextul metodelor speciale de supraveghere sau cercetare, în continuare vom analiza acest drept prin raportare la situațiile în care Curtea s-a pronunțat și a apreciat ca fiind încălcat sau nu art. 8 Conv.EDO.

Deși conceptul de „viață privată" este unul greu de definit, în cuprinsul conceptului, Curtea include integritatea fizică și psihologică a unei persoane[5], unele aspecte privind identitatea fizică și socială[6], identitatea de gen, nume, orientarea sexuală și viața sexuală ale unei persoane fiind în sfera de protecție a art. 8 Conv.EDO[7]. În plus, vor fi incluse în sfera vieții private și dreptul la dezvoltare personală[8] și cel de a dezvolta relații cu alte persoane[9], îmbrățând aspecte multiple ale identității fizice și sociale ale unei persoane[10]. Viața privată nu va putea fi limitată numai la aspectele ce țin strict de persoană, ci și la modul în care decide să se exteriorizeze

[1] *A. L-T Choo*, Evidence, 2018, p. 168.

[2] Opinia separată a judecătorului Loucaides în cauza *Khan c. Marea Britanie*, Hotărârea din 12 mai 2000, și a judecătorului Tulkens în cauza *P.G. și J.H. c. Marea Britanie*, Hotărârea din 25 septembrie 2001.

[3] *A. L-T Choo*, Evidence, 2018, p. 168.

[4] *C. Wells*, Abuse of Process, Third Edition, Oxford University Press, Oxford, 2017, p. 107.

[5] CEDO, cauza *X și Y c. Olanda*, Hotărârea din 26 martie 1985, §22, pe *hudoc.echr.coe.int*

[6] CEDO, cauza *Mikulić c. Croația*, Hotărârea din 7 februarie 2002, §53, pe *hudoc.echr.coe.int*

[7] CEDO, cauza *B. c. Franța*, Hotărârea din 25 martie 1992, §63; cauza *Burghartz c. Elveția*, Hotărârea din 22 februarie 1994, §24; cauza *Dudgeon c. Marea Britanie*, Hotărârea din 22 octombrie 1981, §41; cauza *Laskey, Jaggard și Brown c. Marea Britanie*, Hotărârea din 19 februarie 1997, §36, pe *hudoc.echr.coe.int*

[8] *C. Arnett*, Virtual Shackles: Electronic Surveillance and the Adultification of Juvenile Courts, în The Journal of Criminal Law & Criminology, vol. 108, no. 3/2018, p. 406.

[9] CEDO, cauza *Burghartz c. Elveția*, Hotărârea din 22 februarie 1994, §47; cauza *Friedl c. Austria*, Hotărârea din 31 ianuarie 1995, §45, pe *hudoc.echr.coe.int*

[10] CEDO, cauza *S. și Marper c. Marea Britanie*, Hotărârea din 4 decembrie 2008, §66, pe *hudoc.echr.coe.int*

în societate, putând include și activitățile sale profesionale[1], nefiind posibil de multe ori să se distingă între relațiile ce țin de sfera privată și relațiile profesionale[2].

În cadrul dreptului la viață privată va fi socotit și dreptul la propria imagine, ce privește publicarea de fotografii și imagini ale persoanei. S-a reținut că o atare publicare poate afecta dreptul la viață privată, întrucât pozele pot conține aspecte intime despre persoană[3]. Acest drept include și posibilitatea ca o persoană să refuze publicarea unor fotografii ale copilului nou-născut, atunci când aceasta nu a cunoscut că s-a realizat fotografia[4]. În acest context s-a ridicat și problema unor imagini surprinse de camerele video de supraveghere publice, ulterior divulgate presei[5]. O încălcare gravă a dreptului la viață privată o va constitui filmarea unei persoane în propriul său domiciliu, urmată de distribuirea publică a imaginilor, statele având obligația de a proteja viața privată și sub acest aspect[6]. Chiar și activitățile poliției pot fi catalogate intruzive, atunci când, în contextul unui proces penal, autoritățile divulgă imagini de la dosarul cauzei fără consimțământul persoanei[7].

Dreptul la reputație și demnitate va fi considerat ca o componentă a dreptului la viață privată[8], dar în aceste cazuri ingerința va trebui să aibă o anumită gravitate.

În contextul desfășurării unei urmăriri penale, dreptul la viață privată se va manifesta mai ales în legătură cu secretul corespondenței, întrucât majoritatea măsurilor de supraveghere tehnică din România vor consta în interceptarea comunicărilor unei persoane, însă vor putea fi identificate și alte situații de folosire a tehnicilor speciale care vor afecta direct dreptul la viață privată în sens restrâns.

În legătură cu folosirea metodei speciale de supraveghere a localizării sau urmăririi prin mijloace tehnice, prevăzută de art. 138 alin. (1) lit. d) C.pr.pen., se poate identifica în jurisprudența Curții cauza *Uzun c. Germania*, în care s-a stabilit că localizarea prin GPS va constitui un mijloc de supraveghere care va fi invaziv, dar care, după caz, va reprezenta o restrângere permisă a dreptului la viață privată în acord cu Convenția[9]. Nu aceeași a fost concluzia Curții atunci când mișcările unei persoane au fost supravegheate, întrucât era membru al unei organizații ce activa în domeniul drepturilor omului, prin folosirea unei baze de date constituite secretă prin ordin al executivului[10].

În ceea ce privește interceptarea comunicațiilor, Curtea a reținut că acestea vor constitui atât o restrângere a dreptului la viață privată, cât și o restrângere a secretului corespondenței[11].

---

[1] CEDO, cauza *Fernández Martínez c. Spania*, Hotărârea din 12 iunie 2014, §110, pe *hudoc.echr.coe.int*; cauza *Bărbulescu c. România*, Hotărârea din 5 septembrie 2017, §71.

[2] CEDO, cauza *Antović și Mirković c. Muntenegru*, Hotărârea din 28 noiembrie 2017, §42; cauza *Denisov c. Ucraina*, Hotărârea din 25 septembrie 2018, §100, pe *hudoc.echr.coe.int*

[3] CEDO, cauza *Von Hannover c. Germania (nr. 2)*, Hotărârea din 7 februarie 2012, §103, pe *hudoc.echr.coe.int*

[4] CEDO, cauza *Reklos și Davourlis c. Grecia*, Hotărârea din 15 ianuarie 2009, §40, pe *hudoc.echr.coe.int*

[5] CEDO, cauza *Peck c. Marea Britanie*, Hotărârea din 28 ianuarie 2003, §57-63, pe *hudoc.echr.coe.int*

[6] CEDO, cauza *Khadija Ismayilova c. Azerbaidjan*, Hotărârea din 10 ianuarie 2019, §147, pe *hudoc.echr.coe.int*

[7] CEDO, cauza *Toma c. România*, Hotărârea din 24 februarie 2009, §90-93, pe *hudoc.echr.coe.int*

[8] CEDO, cauza *Axel Springer c. Germania*, Hotărârea din 7 februarie 2012, §83; cauza *Petrina c. România*, Hotărârea din 6 aprilie 2009, §28, pe *hudoc.echr.coe.int*

[9] CEDO, cauza *Uzun c. Germania*, Hotărârea din 2 septembrie 2010, §81, pe *hudoc.echr.coe.int*

[10] CEDO, cauza *Shimovolos c. Rusia*, Hotărârea din 21 iunie 2011, §66, pe *hudoc.echr.coe.int*

[11] CEDO, cauza *Halford c. Marea Britanie*, Hotărârea din 25 iunie 1997, §44; cauza *Malone c. Marea Britanie*, Hotărârea din 2 august 1984, §64; cauza *Weber și Saravia c. Germania*, Hotărârea din 29 iunie 2006, §77, pe *hudoc.echr.coe.int*

În special, în cauza *Malone c. Marea Britanie*, Curtea a reținut o încălcare a Convenției, întrucât măsura de supraveghere tehnică a interceptării comunicațiilor nu era prevăzută la acel moment de legislația britanică[1]. Un alt element deosebit de important în respectarea dreptului la viață privată este ca legea să fie clară și previzibilă, mai ales în cazul măsurilor de supraveghere tehnică[2]. Publicitatea legii este o altă condiție, neputând fi întrebuințate tehnici speciale de investigare decât prin legea accesibilă tuturor persoanelor[3]. Totodată, măsura va trebui să fie proporțională cu scopul legitim urmărit, precum a fost considerată păstrarea într-un registru al poliției de informații privind amenințările cu bombă împotriva unei persoane[4].

În autorizarea măsurilor de supraveghere tehnică vor trebui să fie avute în vedere circumstanțele concrete ale cauzei, natura, scopul, durata măsurilor, temeiurile care le justifică, precum și ca autorizarea să se facă de o autoritate independentă care să supravegheze și să controleze măsura, dar să și procedeze la informarea persoanei supravegheate[5]. Va fi necesar ca legea să prevadă în cazul persoanei un remediu pentru a obține anularea măsurii luate împotriva sa și să obțină distrugerea rezultatelor supravegherii tehnice[6].

O altă componentă a dreptului la viață privată va fi interacțiunea dintre aceasta și avocatul său, însă această problemă urmează a fi analizată în mai multe dintre secțiunile următoare privind componentele dreptului la viață privată.

Dreptul la viață privată nu va fi limitat numai persoanelor care se află în libertate, el trebuind să fie respectat și în cazul persoanelor private de libertate, acestea neputând fi supuse unor măsuri de supraveghere video permanentă atunci când se află în celule[7]. În cauza citată, persoanele aflate în stare de arest preventiv au fost supuse unei supravegheri video permanente, fără a exista un motiv anume pentru care față de acestea să se ia o astfel de măsură, Curtea apreciind că o atare ingerință nu este prevăzută de lege, existând o încălcare a dreptului prevăzut de art. 8 Conv.EDO. Într-o cauză similară, Curtea a reținut că va constitui o încălcare a dreptului la viață privată deținerea unei persoane într-o celulă care nu permite acesteia un minim de intimitate dacă trebuie să folosească toaleta de față cu celelalte persoane deținute[8].

În concluzie, dreptul la viață privată constituie principalul drept care va fi restrâns prin folosirea metodelor speciale de supraveghere sau cercetare în cursul unei urmăriri penale. Imposibilitatea definirii sale în mod exhaustiv conduce la necesitatea unei analize aprofundate a fiecărei componente ale sale prin raportare la tehnicile speciale de investigare. Dreptul la viață privată se impune a fi respectat cu atât mai mult cu cât societatea modernă conferă autorităților puteri din ce în ce mai mari în a restrânge drepturile individului prin mijloace tehnologice moderne. Pentru a putea combate ingerințele excesive ale statului în viața privată a unei persoane, este necesar ca toate măsurile de supraveghere sau cercetare să fie prevăzute de legi clare și previzibile, care să reglementeze complet condițiile în care pot fi folosite, iar autorizarea lor să se realizeze cu respectarea principiului proporționalității și subsidiarității.

[1] CEDO, cauza *Malone c. Marea Britanie*, Hotărârea din 2 august 1984, §82.

[2] CEDO, cauza *Kruslin c. Franța*, Hotărârea din 24 aprilie 1990, §35, pe *hudoc.echr.coe.int*

[3] CEDO, cauza *Shimovolos c. Rusia*, Hotărârea din 21 iunie 2011, §70.

[4] CEDO, cauza *Segerstedt-Wiberg ș.a. c. Suedia*, Hotărârea din 6 iunie 2006, §88-89, pe *hudoc.echr.coe.int*

[5] CEDO, cauza *Roman Zakharov c. Rusia*, Hotărârea din 4 decembrie 2015, §232, pe *hudoc.echr.coe.int*

[6] CEDO, cauza *Pruteanu c. România*, Hotărârea din 3 mai 2015, §55, pe *ier.gov.ro*; cauza *Roman Zakharov c. Rusia,* Hotărârea din 4 decembrie 2015, §231.

[7] CEDO, cauza *Gorlov ș.a. c. Rusia*, Hotărârea din 2 iulie 2019, §97, pe *hudoc.echr.coe.int*

[8] CEDO, cauza *Szafrański c. Polonia*, Hotărârea din 15 decembrie 2015, §39, pe *hudoc.echr.coe.int*

Capitolul II
Libertatea de exprimare

Unul dintre drepturile cele mai importante ale unei persoane într-o societate democratică este cel de a putea să își exprime liber opiniile, fără a se teme de o eventuală acțiune punitivă împotriva sa. Metodele speciale de supraveghere sau cercetare oferă statului posibilitatea legală de a restrânge inclusiv acest drept, prin amploarea deosebită pe care o pot avea dacă se ajunge la autorizarea și folosirea lor în mod discreționar de către organele judiciare[1]. Dintr-un stat de drept în care valorile unei societăți democratice sunt considerate a fi valori supreme care se impun a fi apărate, se poate ajunge în mod vertiginos la un stat polițienesc, în care statul controlează toate aspectele sociale, în special interacțiunile dintre oameni.

Prin mijloacele tehnice care evoluează în mod continuu, posibilitatea ca o persoană să își exprime individualitatea poate fi restrânsă, fiind obligată să se conformeze la regulile statului stabilite arbitrar pentru a proteja „ordinea publică" sau „siguranța națională". Într-un mod pervers, se încearcă acreditarea ideii că supravegherea este benefică pentru societate, statele mizând pentru un mariaj între democrație, alături de valorile sale tradiționale, cu știința și tehnologia[2]. Deja există exemple de state care folosesc mijloace tehnice de supraveghere sub umbrela acestor pretexte pentru a realiza un control în masă al populației, în special al unor grupuri etnice. Situația este întâlnită în cazul uigurilor[3] din China, care sunt monitorizați într-un mod identic măsurii de supraveghere tehnice a supravegherii video, audio sau prin fotografiere. Sunt localizați, identificați și monitorizați prin sisteme informatice, fiecare mișcare sau acțiune a lor fiind înregistrată, situația reprezentând un arhetip de stat polițienesc opresiv modern[4]. Chiar dacă situația din China pare departe de societatea occidentală și de protecția drepturilor omului conferită prin semnarea Convenției Europene a Drepturilor Omului, realitatea ne conduce la concluzia că statul modern tinde să își extindă capacitățile de supraveghere a cetățeanului[5]. Într-o cauză recentă, prezentată în fața unei instanțe din Moscova, s-a respins o cerere de chemare în judecată prin care se susținea că sistemul de supraveghere video al Moscovei (de aproximativ 105.000 de camere) care folosește tehnologii de recunoaștere facială[6] încalcă dreptul la viață privată al cetățenilor[7]. În Israel, în special în orașul Ierusalim, sisteme complexe de monitorizare vizibile sunt folosite împotriva palestinienilor, punând viața lor cotidiană într-o zonă de risc continuu și pericol printr-o stare de permanentă monitorizare[8]. Mergând înspre Occident, comportamentul intruziv nu este

---

[1] CEDO, cauza *Iordachi ș.a. c. Moldova*, Hotărârea din 10 februarie 2009, §51-52, pe *hudoc.echr.coe.int*

[2] *G.T. Marx*, Windows into the Soul, Surveillance and Society in an Age of High Technology, Ed. University of Chicago Press, Chicago, 2016, p. 116.

[3] Uigurii sunt o minoritate turcică din Asia Centrală și Asia de Est, practicanți ai Islamului (sunniți), concentrați mai ales în regiunea Xinjiang din China.

[4] *M. Rajagopalan*, This Is What A 21st-Century Police State Really looks like, pe *www.buzzfeednews.com*

[5] *M. Liao*, The Process of Legalizing Special Investigative Techniques in China, în Frontiers of Law in China, vol. 10, no. 3/2015, p. 521.

[6] *C. Cattaneo, D. De Angelis*, în A. Jamieson, A. Moenssens (coord.), Wiley Encyclopedia of Forensic Science, vol. 5, Ed. Wiley-Blackwell, Chichester, 2009, pp. 2612-2614.

[7] *www.themoscowtimes.com*

[8] *N. Shalhoub-Kevorkian*, Security Theology, Surveillance and the Politics of Fear, Cambridge University Press, Cambridge, 2015, p. 137.

cu nimic mai diferit, în Londra ridicându-se suspiciuni privind controlarea populației prin mijloace de supraveghere cu recunoaștere facială, într-un caz recent, 8.600 de persoane fiind scanate de către poliție (evident, fără autorizare), conducând la arestarea unei persoane și la identificarea ca suspecte a 7 persoane nevinovate[1]. Ultimul exemplu dovedește că măsurile de supraveghere în masă sunt disproporționate și nu constituie decât o modalitate de a restrânge drepturile și libertățile fundamentale ale cetățenilor.

Din cele arătate mai sus rezultă și o încălcare a dreptului la viață privată, ceea ce pune în discuție delimitarea acestui drept față de libertatea de exprimare. Considerăm că ambele vor fi restrânse sau încălcate în exemplele date mai sus, întrucât, prin existența unei ingerințe la viața privată sau existența unui pericol că o persoană va fi supusă unei asemenea ingerințe într-un mod facil, ea va trăi cu senzația perpetuă că este sau poate fi urmărită, neputând să dea frâu liber individualității sale în public. Totodată, transformarea supravegherii tehnice în contextul unei urmăriri penale dintr-o măsură excepțională într-o regulă poate conduce la același rezultat, cetățeanul putându-se considera în pericolul de a fi supravegheat în propria casă, în public, dar și în mediul virtual, considerând că „*nimic nu este al său, în afară de cei câțiva centimetri cubi din interiorul craniului*"[2]. Dar această relație dintre dreptul la viață privată și dreptul la libertatea de exprimare poate fi considerată și una conflictuală, atunci când dreptul la viață privată al unuia este pus față în față cu libertatea de exprimare a altuia, în special în contextul libertății presei[3]. Într-o altă extremă, dreptul la liberă exprimare trebuie să fie protejat chiar și atunci când prin acesta aduce suferință celor din jur, dar nu perturbă ordinea publică[4]. Va fi acceptată și conformă cu libertatea de exprimare și expunerea unor opinii sau publicarea unor materiale care ar avea caracter aparent indecent și prin care s-ar parodia public o anumită persoană[5]. Relația dintre cele două drepturi fundamentale este și va fi întotdeauna una conflictuală la nivel individual, însă, la nivelul societății, ele vor fi complementare, deoarece ambele reprezintă elemente cheie în crearea și menținerea unei societăți democratice, mai ales în contextul tehnologiilor de supraveghere în masă[6].

S-a considerat că, pentru a exista libertatea de exprimare în contextul stabilit prin Constituția S.U.A., „*este esențial ca, atunci când vorbim în forul public, noi să nu fim interogați despre aceasta în alte locuri*"[7]. Același autor arată că elementul politic joacă un rol decizional în a stabili dacă există sau nu un pericol sau o necesitate socială, în sens larg, pentru a determina restrângerea dreptului la liberă exprimare, fiind necesară o intervenție a instanțelor (U.S. Supreme Court sau, într-o interpretare națională, Curtea Constituțională) pentru a se declara în mod neechivoc că nicio idee nu poate fi suprimată pentru că un oficial ales de cetățeni a desemnat-o ca fiind periculoasă[8]. Acest punct de vedere este unul mai vechi, datând de la începutul Războiului Rece, dar rămâne relevant astăzi în contextul în care amenințările teroriste și radicalizarea

[1] *I.A. Hamilton*, British police scanned 8,600 people's faces in London without their consent, resulting in just 1 arrest and 7 false positives, pe *www.businessinsider.nl*

[2] *G. Orwell*, 1984, p. 34, pe *www.planetebook.com*

[3] CEDO, cauza *Axel Springer c. Germania*, Hotărârea din 7 februarie 2012, §107-108; cauza *Von Hannover c. Germania (nr. 2)*, Hotărârea din 7 februarie 2012, §108, pe *hudoc.echr.coe.int*

[4] U.S., cauza *Snyder c. Phelps*, Hotărârea din 2 martie 2011, 562 U.S. 443 (2011), pe *supreme.justia.com*

[5] U.S., cauza *Hustler Magazine, Inc c. Falwell*, Hotărârea din 24 februarie 1988, 485 U.S. 46 (1988), pe *supreme.justia.com*

[6] *R.J. Krotoszynski, Jr.*, Privacy Revisited, 2016, p. 183.

[7] *A. Meiklejohn*, Free Speech and Its Relation to Self-Government, Harper Brothers Publishers, New York, 1948, p. 37.

[8] *Ibidem*, p. 93.

unor populații au condus, treptat-treptat, la o limitare a libertății de exprimare deja încetățenită pentru populație. Surprinzător, după cum vom vedea, conștientizarea caracterului intruziv al mijloacelor tehnice conduce la mișcări împotriva acestor forme de control, care reiau teoria unei libertăți de exprimare cât mai largi. Lipsa anonimatului în tendințele moderne (prin rețele de socializare, în special) conduce oricând la posibilitatea identificării unor comportamente care nu sunt conforme cu „interesele" sau „tendințele sociale", aceasta fiind un impediment la o deplină libertate de exprimare.

Convenția Europeană a Drepturilor Omului protejează libertatea de exprimare, stipulând în cuprinsul art. 10 că „*orice persoană are dreptul la libertate de exprimare. Acest drept include libertatea de opinie și libertatea de a primi sau a comunica informații ori idei fără amestecul autorităților publice și fără a ține seama de frontiere (…)*". Vor fi acoperite multe situații, nu toate având legătură cu supravegherea tehnică și cu subiectul acestei lucrări. De pildă, una dintre principalele teme ce se reflectă în nevoia de apărare a libertății de exprimare este libertatea presei, în jurisprudența Curții fiind unul dintre primele cazuri de încălcare a libertății de exprimare[1].

Dreptul prevăzut de Convenția Europeană a Drepturilor Omului nu va fi unul absolut, el fiind considerat unul limitat însuși prin textul Convenției, deoarece la art. 10 par. 2 se reține că: „*exercitarea acestor libertăți ce comportă îndatoriri și responsabilități poate fi supusă unor formalități, condiții, restrângeri sau sancțiuni prevăzute de lege care, într-o societate democratică, constituie măsuri necesare pentru securitatea națională, integritatea teritorială sau siguranța publică, apărarea ordinii și prevenirea infracțiunilor, protecția sănătății, a moralei, a reputației sau a drepturilor altora, pentru a împiedica divulgarea informațiilor confidențiale sau pentru a garanta autoritatea și imparțialitatea puterii judecătorești*".

Chiar dacă se recunoaște dreptul la liberă exprimare în componenta libertății presei, aceasta nu presupune că orice persoană va avea acces la mass-media pentru a putea să își promoveze ideile, existând un drept al ziarelor și entităților media de a decide dacă publică sau nu un material[2]. În acest sens, presa liberă trebuie să fie protejată de stat împotriva unor acțiuni de hărțuire, chiar desfășurate de stat împotriva sa, precum arestări, percheziții, realizarea de urmăriri penale împotriva ziarului, care pot pune în pericol însăși existența unui ziar[3].

Ca o limitare a dreptului la exprimare, s-a arătat în literatura străină că incumbă autorității legislative să definească ce anume constituie o limitare a dreptului la exprimare, acest drept nefiind unul absolut, astfel că va putea fi sancționată îndemnarea directă sau indirectă a unei persoane să comită acte de terorism, precum și exprimări care în mod neintenționat pot fi interpretate ca o susținere și justificare a unor asemenea acte[4].

În jurisprudența engleză se subliniază caracterul relativ al dreptului la liberă exprimare prevăzut de art. 10 Conv.EDO, considerându-se că el nu este unul absolut, ci unul relativ, ce poate comporta o limitare prin voința legiuitorului care incriminează o conduită intenționată sau nesăbuită (*reckless*) prin care se încurajează comiterea de acte de terorism, inclusiv acte de violență în numele unei organizații de acest fel[5]. Chiar și acțiunile retrograde împotriva

[1] CEDO, cauza *The Sunday Times c. Marea Britanie*, Hotărârea din 26 aprilie 1979, pe *hudoc.echr.coe.int*

[2] CEDO, cauza *Saliyev c. Rusia*, Hotărârea din 21 octombrie 2010, §52, pe *hudoc.echr.coe.int*

[3] CEDO, cauza *Özgür Gündem c. Turcia*, Hotărârea din 16 martie 2000, §43; §72, pe *hudoc.echr.coe.int*

[4] *D. Ormerod, D. Perry, P. Murphy (coord.)*, Blackstone's Criminal Practice 2019, Oxford University Press, Oxford, 2018, p. 668.

[5] EWCA, cauza *Regina c. Ali (Humza)*, Dec. din 20 martie 2018, [2018] EWCA Crim 547, §17, pe *www.bailii.org*

terorismului nu pot fi acceptate, astfel că nici incitarea la ură împotriva unei etnii sau religii din care pot face parte unele persoane teroriste nu poate fi acceptată[1].

În cazul în care se va instiga la ură împotriva unei populații, va putea fi cenzurată exprimarea liberă a unei persoane în conformitate cu art. 10 par. 2 Conv.EDO, întrucât dreptul la liberă exprimare nu permite incitarea la ură împotriva unei etnii sau acuzații defăimătoare la adresa sa, fiind contrare cu principiile convenției de toleranță, pace socială și nediscriminare[2].

O situație în care Curtea a constatat o încălcare a dreptului la liberă exprimare în corelație cu o supraveghere realizată prin mijloace tehnice a fost în cauza *Sanoma Uitgevers B.V. c. Olanda*, în care un jurnalist ce lucra pentru societatea reclamantă a filmat o cursă ilegală de mașini, în înțelegere cu organizatorii că nu va divulga numele acestora[3]. Organele judiciare au reușit să oblige jurnalistul să predea toate înregistrările private realizate de acesta și toate cererile sale ca acestea să nu poate fi folosite ca probă au fost respinse, în această privință Curtea constatând o încălcare a libertății de exprimare prin obligarea jurnalistului să își dezvăluie sursa, reținând că modalitatea în care au procedat organele de urmărire penală nu era prevăzută de lege[4]. Din acest punct de vedere, legislația procesuală penală română nu acordă jurnaliștilor o formă de protecție aparte și nici nu le asigură un drept la confidențialitate, ei putând fi supuși măsurilor de supraveghere tehnică la fel ca orice altă persoană.

Din punctul de vedere al condițiilor restrângerii dreptului la liberă exprimare, potrivit art. 10 par. 2 Conv.EDO, acestea se mulează pe cele prevăzute și în cazul dreptului la viață privată: *i)* restrângerea să fie prevăzută de lege; *ii)* restrângerea să fie cu scopul protejării unuia dintre interesele prevăzute de art. 10 par. 2 Conv.EDO și *iii)* restrângerea să fie necesară într-o societate democratică.

Legat de problema restrângerii de către lege, alături de cele constatate în cauza *Sanoma Uitgevers B.V. c. Olanda*, este relevant ca în cazul dreptului la viață privată restrângerea să se facă într-o modalitate clară și previzibilă[5]. Din perspectiva unor anumite metode speciale – obținerea de date de trafic și de localizare, prevăzută de art. 152 C.pr.pen. –, se poate considera că legea este insuficient de previzibilă asupra duratei pentru care pot fi colectate aceste date și durata pentru care pot fi accesate de către organele de urmărire penală. Ținând seama atât de caracterul datelor – de a reflecta comunicațiile unei persoane, cât și de faptul că ele se colectează cu privire la toate persoanele care sunt clienții unui furnizor de servicii publice de comunicații electronice, se poate considera că legea este insuficient de clară și afectează dreptul la liberă exprimare.

În ceea ce privește a doua condiție, a protejării unuia dintre scopurile prevăzute în art. 10 par. 2 Conv.EDO, restrângerea libertății de exprimare trebuie să aibă în vedere protejarea următoarelor valori: securitatea națională, integritatea teritorială sau siguranța publică, apărarea ordinii și prevenirea infracțiunilor, protecția sănătății, a moralei, a reputației sau a drepturilor altora, pentru a împiedica divulgarea informațiilor confidențiale sau pentru a garanta autoritatea și imparțialitatea puterii judecătorești.

---

[1] CEDO, cauza *Norwood c. Marea Britanie*, Hotărârea din 16 noiembrie 2004, declarată inadmisibilă, pe *hudoc.echr.coe.int*

[2] CEDO, cauza *Pavel Ivanov c. Rusia*, Hotărârea din 20 februarie 2007, declarată inadmisibilă, pe *hudoc.echr.coe.int*

[3] CEDO, cauza *Sanoma Uitgevers B.V. c. Olanda*, Hotărârea din 14 septembrie 2010, §11-14, pe *hudoc.echr.coe.int*

[4] *Ibidem*, §101.

[5] CEDO, cauza *Centro Europa 7 S.R.L. și Di Stefano c. Italia*, Hotărârea din 7 iunie 2012, §156, pe *hudoc.echr.coe.int*

În privința protejării securității naționale, s-a apreciat că cenzurarea publicării unor activități nelegale ale serviciilor secrete britanice de către un membru pensionar al acestor servicii este legală și în acord cu Convenția, dar numai până la diseminarea publică pe alte surse a informației respective[1]. În sens contrar, s-a reținut că un document secret vechi de 6 ani referitor la activitățile Partidului Comunist și mișcări antinucleare publicat de un ziar nu poate fi primit ca fiind protejat de Convenție, chiar dacă statul declară conținutul a fi secret, documentul fiind de natură generală[2]. Este discutabil dacă o divulgare a unor protocoale secrete precum cele încheiate de Ministerul Public cu Serviciul Român de Informații cu privire la punerea în executare a mandatelor de supraveghere tehnică ar fi putut să constituie o limitare legală adusă libertății de exprimare dacă ar fi fost divulgate, întrucât, prin conținutul acestora, ascundeau activități ilicite ale statului. Apreciem că, într-o asemenea situație, ar fi fost aplicabile dezlegările date de Curte în cauza *Guja c. Moldova*[3], unde a existat o divulgare de informații către presă dintr-un dosar de urmărire penală, din care rezultau aspecte de interes public, respectiv intervenții din partea factorului politic în desfășurarea urmăririi penale.

În domeniul protejării ordinii publice, Curtea a constatat că libertatea de exprimare a fost încălcată în situația în care autoritățile au luat măsuri împotriva unor demonstrații publice, prin sancționarea penală a participanților care susțineau organizația PKK, deși nu au existat violențe și nimic din atitudinea protestatarilor nu a incitat la astfel de acte[4].

Cea de-a treia condiție, a necesității într-o societate democratică, va presupune un examen de proporționalitate și de subsidiaritate, în cazul metodelor speciale de supraveghere sau cercetare, necesitatea lor fiind cel mai bine evidențiată în cazul supravegherii tehnice, unde acestea sunt prevăzute drept condiții legale în cuprinsul art. 139 alin. (1) lit. b) și c) C.pr. pen. Sub acest aspect trebuie să existe un control real, realizat de o autoritate independentă, și al măsurilor autorizate inițial de judecătorul de drepturi și libertăți, pentru a se preveni desfășurarea de supravegheri tehnice disproporționate sau, dacă acestea au avut loc, ele să fie declarate nelegale și mijloacele de probă obținute să fie distruse.

În concluzie, apreciem că libertatea de exprimare trebuie să fie respectată prin limitarea folosirii măsurilor de supraveghere la cauzele care presupun o maximă atingere adusă valorilor sociale ocrotite prin lege, existând pericolul ca, prin extinderea supravegherii tehnice sau acceptarea desfășurării unor înregistrări în spații publice și alte astfel de utilizări ale mijloacelor tehnice de supraveghere, aceasta să constituie o restrângere a posibilității persoanei să se exprime în mod liber în societate, atât în mediul public, cât și telefonic sau în mediul virtual.

[1] CEDO, cauza *Observer și Guardian c. Marea Britanie*, Hotărârea din 26 noiembrie 1991, §69, pe *hudoc.echr.coe.int*

[2] CEDO, cauza *Vereniging Weekblad Bluf c. Olanda*, Hotărârea din 9 februarie 1995, §41, pe *hudoc.echr.coe.int*

[3] CEDO, cauza *Guja c. Moldova*, Hotărârea din 12 februarie 2008, §71, pe *hudoc.echr.coe.int*

[4] CEDO, cauza *Yılmaz și Kılıc c. Turcia*, Hotărârea din 17 iulie 2008, §61, pe *hudoc.echr.coe.int*

Capitolul III
Secretul corespondenței

Secretul corespondenței este o componentă a dreptului la viață privată prevăzut de art. 8 Conv.EDO. Prin acest drept se urmărește apărarea persoanei față de orice ingerință asupra comunicărilor sale, indiferent de mijlocul prin care se realizează o atare comunicare. Ținând seama de scopul metodelor speciale de supraveghere sau cercetare, acestea sunt cele mai în măsură să afecteze secretul corespondenței, existând metode speciale dedicate atât aflării comunicațiilor la distanță electronice [interceptarea comunicațiilor ori a oricărui tip de comunicare la distanță, prevăzută de art. 138 alin. (1) lit. a) C.pr.pen.], cât și a celor tradiționale (reținerea, predarea sau percheziționarea trimiterilor poștale, prevăzută de art. 147 C.pr.pen.).

Prin raportare la jurisprudența Curții Europene a Drepturilor Omului, s-au reținut încălcări ale secretului corespondenței atunci când s-a aflat conținutul unor convorbiri telefonice[1], realizate fie de particulari, fie de societăți private, inclusiv avocați[2], dar și de persoane aflate în libertate, precum și de persoane aflate în stare de detenție[3]. Vor intra în aceste categorii și mesajele transmise prin fax sau prin SMS ori folosind unde radio prin canale private[4]. O situație particulară privind convorbirile telefonice este că va constitui o restrângere a dreptului la viață privată și aflarea datelor privind numerele de telefon apelate sau de la care au fost primite apeluri[5], aceste informații putând fi obținute prin metoda specială de cercetare a obținerii datelor de trafic și de localizare prelucrate de către furnizorii de rețele publice de comunicații electronice ori furnizorii de servicii de comunicații electronice destinate publicului, prevăzută de art. 152 C.pr.pen.

Nu doar convorbirile telefonice pot constitui obiectul unor măsuri care să constituie o restrângere a dreptului la corespondență, ci și mijloacele mai moderne, precum corespondența electronică e-mail[6] și alte date transmise prin internet[7]. În cazul corespondenței e-mail, chiar dacă nu se va intercepta mesajul sau accesa mesajul pe serverul de e-mail sau pe calculatorul persoanei vizate, va exista o ingerință în secretul corespondenței și atunci când se stabilește o regulă de retransmitere a e-mailurilor către un terț[8].

În noțiunea de „corespondență" se încadrează și unele date informatice care, prin natura lor, vor putea fi considerate ca fiind corespondență, în special dacă ele aparțin unui avocat[9], și chiar suporți de stocare întregi aparținând aceleiași profesii[10] – hard-diskuri sau chiar suporți

---

[1] CEDO, cauza *Ludi c. Elveția*, Hotărârea din 15 iunie 1992, §38-39; cauza *Klass ș.a. c. Germania*, Hotărârea din 6 septembrie 1978, §21; cauza *Malone c. Marea Britanie*, Hotărârea din 2 august 1984, §64, pe *hudoc.echr.coe.int*

[2] CEDO, cauza *Kopp c. Elveția*, Hotărârea din 25 martie 1998, §50, pe *hudoc.echr.coe.int*

[3] CEDO, cauza *Petrov c. Bulgaria*, Hotărârea din 22 mai 2008, §51, pe *hudoc.echr.coe.int*

[4] CEDO, cauza *X și Y c. Belgia*, Hotărârea din 13 mai 1982, pe *hudoc.echr.coe.int*

[5] CEDO, cauza *P.G. și J.H. c. Marea Britanie*, Hotărârea din 25 septembrie 2001, §42,pe *hudoc.echr.coe.int*

[6] CEDO, cauza *Copland c. Marea Britanie*, Hotărârea din 3 iulie 2007, §41; cauza *Bărbulescu c. România*, Hotărârea din 5 septembrie 2017, §72, pe *hudoc.echr.coe.int*

[7] CEDO, cauza *Copland c. Marea Britanie*, Hotărârea din 3 iulie 2007, §42.

[8] CEDO, cauza *Luordo c. Italia*, Hotărârea din 17 iulie 2003, §72, pe *hudoc.echr.coe.int*

[9] CEDO, cauza *Wieser și Bicos Beteiligungen GmbH c. Austria*, Hotărârea din 16 octombrie 2007, §66-67, pe *hudoc.echr.coe.int*

[10] CEDO, cauza *Petri Sallinen ș.a. c. Finlanda*, Hotărârea din 27 septembrie 2005, §71, pe *hudoc.echr.coe.int*

mai vechi, precum dischete (în extensie, putem să includem și suporții optici), dacă aparțin unui avocat[1]. În aceste situații, vom vorbi, cel mai probabil, de percheziții informatice prin care se obțin respectivele date informatice, subsecvente unor percheziții domiciliare (precum în cauzele citate), însă nu este exclus ca acestea să poată fi obținute printr-un acces la un sistem informatic, potrivit art. 138 alin. (1) lit. b) C.pr.pen. Din jurisprudența sa, Curtea este preocupată mai ales de corespondența dintre client și avocat în privința garantării secretului corespondenței, alăturând secretului profesional această garanție. Chiar dacă o comunicare prin alte mijloace cu greu ar fi considerată corespondență – nici scrisă, nici electronică –, au existat situații care, prin raportare la relația dintre client și avocatul său, au condus la constatarea încălcării secretului corespondenței. Într-o cauză mai recentă, Curtea a constatat că este protejată de secretul profesional și secretul corespondenței o foaie de hârtie, pliată în două, pe care avocatul a notat un mesaj către clientul său, astfel că poliția nu poate intercepta acest mesaj[2].

Tot în domeniul corespondenței au fost incluse și documentele cu caracter bancar ce privesc tranzacțiile financiare ale unei persoane[3] chiar dacă acestea au fost copiate de organele de urmărire penală. Din punctul de vedere al legii procesuale penale, Codul prevede o măsură specială de cercetare, denumită „obținerea de date privind tranzacțiile financiare ale unei persoane", care corespunde cu problema expusă în cauza citată.

Convenția previne orice formă de imixtiune a organelor de urmărire penală sau, în general, a statului cu corespondența unei persoane, indiferent de mijlocul prin care se desfășoară aceasta, existând câteva cauze ale căror hotărâri au inițiat o tendință a Curții în protejarea împotriva unor forme de interferență.

În privința interceptării comunicațiilor, prima hotărâre a Curții cu importanță deosebită a fost *Malone c. Marea Britanie*[4], în care s-a stabilit că Regatul Unit nu avea nicio procedură legală de a intercepta comunicațiile telefonice ale unei persoane, constatându-se încălcarea art. 8 Conv.EDO, întrucât ingerința în viața privată nu era „prevăzută de lege", sistemul britanic cunoscând doar reguli prin care unele procedee probatorii erau interzise, fără a fi reglementate procedee probatorii comune sau speciale. Or, din acest punct de vedere, revine legiuitorului o obligație pozitivă în a reglementa această restrângere, precum și limitele și condițiile sale[5]. Din perspectiva acestei forme de supraveghere, va fi necesar ca ea să fie reglementată într-un mod care să permită persoanei supravegheate să fie informată asupra măsurii luate împotriva sa, nefiind permise interceptări secrete[6]. Sub acest aspect, legislația națională nu este numai deficitară, ci vine în contra dispozițiilor Convenției, întrucât nu prevede termene clare care nu pot fi depășite în informarea persoanei supravegheate și nici faptul că acesteia nu i se vor prezenta toate comunicațiile interceptate, ci numai cele selectate conform art. 143 alin. (1) C.pr.pen.

Interceptarea comunicațiilor unei persoane, desfășurată în contextul urmăririi penale, va trebui să respecte toate condițiile prevăzute de art. 8 par. 2 Conv.EDO, în special ca ingerința să fie prevăzută de lege. Aceasta semnifică stabilirea prin lege a măsurilor de supraveghere

[1] CEDO, cauza *Iliya Stefanov c. Bulgaria*, Hotărârea din 22 mai 2008, §42, pe *hudoc.echr.coe.int*

[2] CEDO, cauza *Laurent c. Franța*, Hotărârea din 24 mai 2018, §36, pe *hudoc.echr.coe.int*

[3] CEDO, cauza *M.N. ș.a. c. San Marino*, Hotărârea din 7 iulie 2015, §54, pe *hudoc.echr.coe.int*

[4] CEDO, cauza *Malone c. Marea Britanie*, Hotărârea din 2 august 1984, §64.

[5] *A. Ashworth*, op. cit., pp. 199-200.

[6] CEDO, cauza *Kennedy c. Marea Britanie*, Hotărârea din 18 mai 2010, §144, ulterior, problema a fost abordată în detaliu în cauza *Roman Zakharov c. Rusia*, Hotărârea din 4 decembrie 2015, pe *hudoc.echr.coe.int*

concrete care pot fi realizate, deseori constatându-se încălcarea art. 8 Conv.EDO atât prin prisma dreptului la viață privată, cât și prin raportare la secretul corespondenței atunci când legea nu prevedea interceptări[1]. Scopul pentru care se pot realiza interceptările comunicațiilor va trebui să fie, pe lângă unul legal, și unul clar definit prin lege, cu alte cuvinte, legea să limiteze măsura numai la obținerea de probe în cazul anumitor tipuri de infracțiuni, cu indicarea concretă a duratei maxime pentru care se poate realiza supravegherea[2]. În ceea ce privește previzibilitatea legii, ca o condiție, reglementarea lor cât mai clară revine legiuitorului, această sarcină neputând fi delegată judecătorului care, și dacă exercită diligențe remarcabile, nu va putea complini în totalitate lipsurile legii[3]. Cu referire la legislația națională, supravegherea tehnică este prevăzută într-un mod suficient de detaliat încât să permită judecătorului de drepturi și libertăți să detalieze, în concret, măsurile încuviințate și modul în care se vor pune în executare, ținând de diligența acestora să facă aceste detalii și să oblige procurorul să își detalieze el însuși în mod amănunțit propunerea de autorizare a măsurilor. Sub acest aspect, dacă s-ar constata că legea română permite desfășurarea de supravegheri tehnice în mod arbitrar, aceasta ar trebui să fie considerată ca venind în contradicție cu Curtea Europeană a Drepturilor Omului[4].

Procedura de autorizare a interceptării comunicațiilor sau altor forme de metode speciale de supraveghere trebuie să permită judecătorului de drepturi și libertăți să realizeze un control de proporționalitate asupra măsurilor care vor fi puse în executare, pentru a constata dacă acestea sunt necesare într-o societate democratică prin raportare la faptele care se doresc a fi dovedite în cursul urmăririi penale. În conformitate și cu prevederile naționale, este necesar ca supravegherea tehnică să fie folosită numai în acele situații în care orice alte procedee probatorii mai puțin intruzive ar fi insuficiente[5]. Odată ce au fost obținute date și informații prin interceptarea comunicațiilor unei persoane, va fi obligatorie stocarea lor în condiții care să prevină accesarea lor în mod abuziv, întrucât simpla lor existență va constitui o ingerință adusă secretului corespondenței și vieții private[6]. În nicio situație nu va fi acceptabilă divulgarea corespondenței telefonice a unei persoane supuse unei măsuri de supraveghere tehnică, în special va fi interzisă divulgarea către presă a înregistrărilor aflate la dosarul cauzei, chiar dacă persoana ar fi un politician și cauza ar avea o importanță publică[7].

Întrucât persoana care este afectată prin aceste măsuri de supraveghere nu poate fi informată decât după ce acestea s-au realizat, trebuie să i se ofere posibilitatea de a contesta legalitatea lor. Mergând mai departe, jurisprudența Curții a recunoscut necesitatea reglementării în dreptul intern a unui recurs efectiv *a posteriori* cu privire la măsurile de supraveghere tehnică, reamintind constatările din cauza *Roman Zakharov c. Rusia* privind condiționarea posibilității de a exercita un recurs efectiv de informare a persoanei supravegheate[8]. Acest recurs efectiv nu trebuie să fie unul în sensul obținerii unor daune, ci trebuie să privească legalitatea măsurii și să deschidă posibilitatea concretă ca persoana supravegheată să obțină anularea măsurilor luate împotriva sa[9].

---

[1] CEDO, cauza *Kruslin c. Franța*, Hotărârea din 24 aprilie 1990, §26, pe *hudoc.echr.coe.int*
[2] CEDO, cauza *Huvig c. Franța*, Hotărârea din 24 aprilie 1990, §32; §34, pe *hudoc.echr.coe.int*
[3] CEDO, cauza *Valenzuela Contreras c. Spania*, Hotărârea din 30 iulie 1998, §56-57, pe *hudoc.echr.coe.int*
[4] CEDO, cauza *Bykov c. Rusia*, Hotărârea din 10 martie 2009, §78, pe *hudoc.echr.coe.int*
[5] CEDO, cauza *Roman Zakharov c. Rusia*, Hotărârea din 4 decembrie 2015, §260.
[6] CEDO, cauza *Craxi c. Italia (nr. 2)*, Hotărârea din 17 iulie 2003, §75; §83, pe *hudoc.echr.coe.int*
[7] CEDO, cauza *Drakšas c. Lituania*, Hotărârea din 31 iulie 2012, §61, pe *hudoc.echr.coe.int*
[8] CEDO, cauza *Irfan Güzel c. Turcia*, Hotărârea din 7 mai 2017, §98, pe *hudoc.echr.coe.int*
[9] CEDO, cauza *Xavier Da Silveira c. Franța*, Hotărârea din 21 aprilie 2010, §48, pe *hudoc.echr.coe.int*

Nu se poate susține că nu s-ar impune un recurs efectiv cu privire la legalitatea măsurii, motivând că persoana care a dispus autorizarea măsurii ar avea calitatea de magistrat, această calitate neputând garanta regularitatea actului care este atacat, astfel că respingerea unei cereri pe temeiul acesta constituie o încălcare a art. 8 Conv.EDO. Această concluzie este deosebit de importantă, deoarece subliniază necesitatea ca un control *a posteriori* să privească toate elementele care au stat la baza autorizării măsurii[1]. În dreptul procesual penal român, aceasta ar însemna un control asupra tuturor condițiilor prevăzute de art. 139 C.pr.pen.: competență, existența unei urmăriri penale începute în cauză, existența unei suspiciuni rezonabile, proporționalitatea măsurii, subsidiaritatea măsurii și autorizarea supravegherii tehnice într-o cauză care privește una dintre infracțiunile prevăzute de art. 139 alin. (2) C.pr.pen.

În cauza *Pruteanu c. România*, Curtea a analizat și caracterul efectiv al recursului prin perspectiva solicitărilor reclamantului ca statul să dispună distrugerea rezultatelor supravegherii tehnice care îl priveau pe acesta[2]. Astfel, s-a mers mai departe decât în cauzele precedente, fără a se rezuma numai la nulitatea măsurilor de supraveghere tehnică. Totodată, prin raportare și la problemele incidente în cauză, Curtea a reținut că reclamantul avusese calitatea de avocat în cauza în care au fost interceptate comunicațiile sale, însă această calitate de fost reprezentant nu îi permitea să exercite un drept procesual propriu și să intervină în cauză pentru a cere constatarea nulității supravegherii tehnice[3]. S-a mai reținut și faptul că la dosarul cauzei au fost depuse și redate convorbiri purtate de acesta, apreciate ca fiind relevante de către organele de urmărire penală[4], el neputând să solicite și să obțină distrugerea acestora, sens în care Curtea a constatat o încălcare a Convenției[5].

Referitor la comunicațiile scrise, o cauză de importanță deosebită în formarea jurisprudenței Curții a fost *Campbell c. Marea Britanie*, în care autoritățile din administrația penitenciară au procedat la deschiderea și verificarea corespondenței reclamantului, inclusiv cea cu avocatul său și cu Curtea Europeană a Drepturilor Omului[6]. Din acest ultim punct de vedere, România a fost deja condamnată[7] de mai multe ori pentru nerespectarea secretului corespondenței persoanelor deținute cu Curtea Europeană a Drepturilor Omului sau pentru limitarea acestui drept, prin neoferirea posibilității contactării Curții, în cazul în care persoana deținută nu are mijloacele financiare necesare pentru francarea corespondenței (timbre), fiind nevoită să-și vândă mâncarea celorlalți deținuți din penitenciar pentru a suporta costurile[8]. În domeniul corespondenței scrise, legiuitorul român a prevăzut o metodă specială de supraveghere, denumită „reținerea, predarea și percheziționarea trimiterilor poștale", prevăzută de art. 147 C.pr.pen., prin care se poate restrânge secretul corespondenței, însă procedura de autorizare este una care împrumută elemente de la cea de autorizare a măsurilor de supraveghere tehnică, inclusiv condițiile de proporționalitate și subsidiaritate. De altfel, ca în cazul supravegherii tehnice, va fi interzisă aplicarea măsurii de cercetare asupra corespondenței dintre avocat și persoana pe care acesta o apără.

[1] CEDO, cauza *Matheron c. Franța*, Hotărârea din 29 iunie 2005, §40, pe *hudoc.echr.coe.int*
[2] CEDO, cauza *Pruteanu c. România*, Hotărârea din 3 mai 2015, pe *ier.gov.ro*
[3] *Ibidem*, §53.
[4] *Ibidem*, §52.
[5] *Ibidem*, §55.
[6] CEDO, cauza *Campbell c. Marea Britanie*, Hotărârea din 25 martie 1992, pe *hudoc.echr.coe.int*
[7] CEDO, cauza *Cotleț c. România*, Hotărârea din 3 iunie 2003, §44, pe *hudoc.echr.coe.int*
[8] CEDO, cauza *Gagiu c. România*, Hotărârea din 24 februarie 2009, §89, pe *hudoc.echr.coe.int*

În contextul unei supravegheri tehnice fără autorizare, realizate de un privat, se impun a fi făcute unele menţiuni, în sensul în care şi astfel de înregistrări trebuie să respecte condiţiile art. 8 Conv.EDO. Astfel, nu vor constitui interceptări legale cele realizate de angajator (chiar şi instituţie publică) dacă acestea se realizează în scopul discriminării unui angajat de a obţine o promovare[1]. Şi în măsura în care angajatului i se pune în vedere să nu folosească un mijloc de comunicaţie (mesagerie instant prin internet), angajatorul trebuie să îi respecte dreptul la viaţă privată şi să nu îi înfrângă dreptul la corespondenţă chiar dacă se realizează prin dispozitive aflate la locul de muncă[2]. Din acest punct de vedere, Curtea consideră că astfel de măsuri pot fi luate de angajatori, dar numai în măsura în care vor fi îndeplinite anumite condiţii ce ţin de consimţământul prealabil al angajatului, întinderea interceptării, dacă i se oferă angajatului garanţii suficiente împotriva abuzurilor[3].

În concluzie, secretul corespondenţei reprezintă unul dintre principalele drepturi afectate prin metodele speciale de supraveghere sau cercetare, incluzând majoritatea cazurilor practice de aplicare a unor astfel de măsuri, în special cea a interceptării comunicaţiilor, care va fi cea mai răspândită, dar, după cum se vede în bogata jurisprudenţă a Curţii Europene a Drepturilor Omului, este şi cea care conduce la cele mai multe intruziuni în viaţa privată şi care trebuie să fie strict reglementată.

[1] CEDO, cauza *Halford c. Marea Britanie*, Hotărârea din 25 iunie 1997, §59, pe *hudoc.echr.coe.int*

[2] CEDO, cauza *Bărbulescu c. România*, Hotărârea din 5 septembrie 2017, §74; a se vedea şi: *V. Etsebeth,* Monitoring and Surveillance in the Workplace: Lessons Learnt? Investigating the International Legal Position, în Journal of Digital Forensics, Security and Law, vol. 2, no. 2/2007, p. 24; *I.T. Ştefănescu, R. Dumitru*, Consideraţii referitoare la protecţia datelor personale ale salariaţilor în cadrul raporturilor de muncă, în Dreptul nr. 9/2015, pp. 189-190; *S. Nouwt, B.R. de Vries, C. Prins,* Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy, Ed. TMC Asser Press, Haga, 2005, p. 50.

[3] CEDO, cauza *Bărbulescu c. România*, Hotărârea din 5 septembrie 2017, §121.

Capitolul IV
Dreptul la domiciliu

Printre drepturile fundamentale prevăzute și protejate prin Convenția Europeană a Drepturilor Omului se află și dreptul la domiciliu, prevăzut în mod expres în cuprinsul art. 8 Conv.EDO, alături de dreptul la viață privată și secretul corespondenței. Din perspectiva analizei compatibilității metodelor speciale de supraveghere sau cercetare cu respectarea acestui drept, se impune constatarea că acestea au o sferă de incidență mai redusă în ceea ce privește afectarea dreptului la domiciliu, fiind vizate mai multe aspecte ce țin de viața privată (în sens restrâns) a unei persoane. În general, dreptul la domiciliu este afectat în cazul procedeelor probatorii care presupun pătrunderea în interiorul acestui domiciliu. Cu toate acestea, există măsuri de supraveghere tehnică, precum supravegherea video, audio sau prin fotografiere, care se pot desfășura în spații private ce au natura unui domiciliu în sensul Convenției, sens în care sunt utile unele mențiuni cu privire la astfel de situații. Nu este exclus ca o ingerință adusă domiciliului unei persoane să existe atunci când se va apela la utilizarea investigatorilor sub acoperire și a colaboratorilor, prevăzută de art. 148 C.pr.pen., ori participarea autorizată la anumite activități, prevăzută de art. 150 C.pr.pen., dacă se realizează inclusiv în spații considerate domicilii. De pildă, apreciem că va exista o intruziune în domiciliul unei persoane și dacă va exista acordul persoanei pentru ca un investigator să intre, în condițiile în care se desfășoară în mod ascuns activități împotriva sa în propriul său domiciliu.

Noțiunea de „domiciliu" este una care nu trebuie să fie înțeleasă prin prisma definițiilor date în dreptul intern, întrucât ar permite o aplicare diferențiată a Convenției. Chiar și din prisma traducerilor oficiale ale Convenției, au fost observate diferențe între termenii echivalenți celui de „domiciliu". De pildă, într-o cauză privind un cabinet de avocat, s-a constatat că termenul de *home* din traducerea în engleză este mai restrâns decât cel de *domicile* din franceză, ultimul având o conotație mai largă și extinzându-se și asupra sediului profesional[1]. Conceptul de „domiciliu" este unul autonom și se va baza pe circumstanțele concrete ale cauzei, astfel cum a stabilit Curtea într-o cauză mai recentă, în care a analizat mișcările de populație nevoluntare dintr-o regiune într-alta ca nefiind conforme cu dreptul la domiciliu, extinzând conceptul dincolo de un anumit imobil, chiar la o regiune, prin prisma locului unde persoanele s-au născut, au locuit, unde au locuit antecesorii lor și dacă mutarea lor a fost una voluntară[2]. Desigur, în contextul tehnicilor speciale de supraveghere sau cercetare, va trebui să ne limităm strict la o locație bine definită, sensul de „domiciliu" trebuind să fie circumscris la sfera privată[3]. O situație care ridică astfel de probleme a fost expusă în jurisprudența engleză într-o cauză referitoare la o angajată care a suferit o vătămare la locul de muncă, necesitând îngrijiri și o perioadă de concediu medical. Angajatorul ei a bănuit că își exagerează simptomele, angajând detectivi care au vizitat-o la domiciliu sub pretextul că realizează un sondaj de piață, descoperind că

[1] CEDO, cauza *Niemietz c. Germania*, Hotărârea din 16 decembrie 1992, §30, pe *hudoc.echr.coe.int*

[2] CEDO, cauza *Chiragov ș.a. c. Armenia*, Hotărârea din 16 iunie 2015, §206, pe *hudoc.echr.coe.int*

[3] Comisia de la Veneția, Opinie asupra supravegherii video realizate de operatori privați în public și în sfera privată și de autorități publice în sfera privată și protejarea drepturilor omului, adoptată în a 71-a Sesiune Plenară a Comisiei de la Veneția, 1-2 iunie 2007.

aceasta era sănătoasă și înregistrând-o în propria locuință[1]. O atare situație apreciem că ar încălca dreptul la domiciliu al persoanei. Aceasta ar constitui o simplă restrângere a dreptului, necesară într-o societate democratică, în situația în care s-ar realiza în temeiul unei autorizări din partea judecătorului de drepturi și libertăți ori a procurorului, emise în baza unui control de proporționalitate al scopului măsurii cu restrângerea dreptului.

Legea română include atât în cazul supravegherii tehnice, cât și în cazul utilizării investigatorilor sub acoperire și a colaboratorilor ori a participării autorizate la anumite activități îndeplinirea condiției proporționalității, cu mențiunea că, la ultimele două măsuri, aceasta va fi apreciată de către procuror. Pentru ca măsura să fie considerată proporțională în cadrul supravegherii tehnice prin supraveghere video, audio sau prin fotografiere în spații private, va fi necesar ca judecătorul de drepturi și libertăți să precizeze în mod detaliat circumstanțele în care se va putea proceda la instalarea și dezinstalarea de mijloace tehnice de supraveghere în spații private, menținându-se limitele autorizării, precum locul unde pot fi montate dispozitivele, de câte ori se poate pătrunde în spații private și cât timp pot sta persoanele la acea locație pentru a desfășura activitățile acestea.

Un domiciliu poate constitui nu numai un imobil aflat în proprietatea sau locațiunea unei anumite persoane, ci și dacă persoana respectivă va locui pentru o perioadă mai lungă de timp în casa unei rude, în contextul unor evacuări silite, urmate de distrugerea respectivului domiciliu de către autoritățile statului[2]. Pentru Curte, este necesară existența unei legături efective și durabile între persoană și domiciliu, nefiind considerat domiciliu un așezământ care nu mai este ocupat de mai multă vreme de către proprietarul său[3].

Nu va avea importanță dacă domiciliul este ocupat de persoana care justifică un titlu în nume personal pentru a fi considerat ca atare – nu va trebui să fie titularul contractului de locațiune[4] sau să fie domiciliul său declarat unde ar fi locuit cu fosta soție[5] ori dacă ridicarea imobilului s-a realizat pe un teren ocupat în mod nelegal[6]. Din acest punct de vedere, va fi foarte important să se determine dacă este necesară menționarea într-un eventual mandat de supraveghere tehnică a numelui proprietarului sau persoanei care figurează ca fiind locatorul spațiului respectiv, în contextul în care persoana supravegheată este o alta care locuiește efectiv în acel loc. Din jurisprudența amintită, apreciem că ingerința adusă dreptului la domiciliu se va răsfrânge asupra persoanei care efectiv locuiește în acel spațiu privat sau desfășoară o anumită activitate în mod exclusiv, sens în care un eventual mandat de supraveghere tehnică în spații private va trebui să indice respectiva locație. O altă consecință a definirii relației de domiciliu și persoană supravegheată va fi și că proprietarul imobilului nu va trebui să fie încunoștințat de supravegherea tehnică desfășurată în acel spațiu, în sensul art. 145 alin. (1) C.pr.pen., dacă acesta nu locuia în respectivul imobil, el putând fi afectat cel mult sub aspectul dreptului său la proprietate, ceea ce excedează restrângerile drepturilor fundamentale avute în vedere direct prin supravegherea tehnică.

Curtea a mai considerat că poate fi de ajuns și dorința ca o persoană să locuiască în respectivul domiciliu indiferent de forma pe care ar îmbrăca-o acesta, dacă există o legătură

[1] EWCA, cauza *Jones c. University of Warwick*, Dec. din 4 februarie 2003, [2003] EWCA Civ 151, pe *www.bailii.org*

[2] CEDO, cauza *Menteș ș.a. c. Turcia*, Hotărârea din 28 noiembrie 1997, §73, pe *hudoc.echr.coe.int*

[3] CEDO, cauza *Andreou Papi c. Turcia*, Hotărârea din 22 septembrie 2009, §54, pe *hudoc.echr.coe.int*

[4] CEDO, cauza *Prokopovich c. Rusia*, Hotărârea din 18 noiembrie 2004, §37-38, pe *hudoc.echr.coe.int*

[5] CEDO, cauza *Yevgeniy Zakharov c. Rusia*, Hotărârea din 14 martie 2017, §32, pe *hudoc.echr.coe.int*

[6] CEDO, cauza *Winterstein ș.a. c. Franța*, Hotărârea din 17 octombrie 2013, §141, pe *hudoc.echr.coe.int*

durabilă între acea persoană și locație[1]. Nu este necesar ca domiciliul să îmbrace o anumită formă, putând fi socotite domicilii și locuințele mobile specifice unor populații itinerante[2] sau chiar colibe construite ilegal de populații sărace pe teritoriul statului, ce nu respectă standardele de urbanism[3]. În același timp, nu trebuie ca domiciliul să fie cel exclusiv al unei persoane, putând fi folosit ocazional și ca reședință sau drept casă de vacanță[4]. Ceea ce s-a reținut de către Curte este că persoana își poate împărți timpul între mai multe locații, fiecare dintre acestea putând avea calitatea de domiciliu[5].

În contextul desfășurării de metode speciale de supraveghere sau cercetare în sfera privată a unei persoane, în conceptul de „domiciliu" vor fi incluse și acele locuri unde persoana își desfășoară activitatea profesională. Vor constitui domicilii de acest fel cabinetele de avocați[6], birourile notarilor publici[7], redacțiile unor ziare[8], sediul principal sau punctele de lucru ale societăților comerciale[9], dar și biroul unui profesor din cadrul unei universități[10].

În cazul cabinetelor de avocați, situația este de un interes deosebit, ținând seama de prevederile speciale din cuprinsul art. 139 alin. (4) C.pr.pen. privind interzicerea realizării supravegherii tehnice asupra relației dintre avocat și persoana pe care o reprezintă într-o cauză, trebuind să fie respectat secretul profesional al avocatului. Curtea a constatat că trebuie să existe criterii legale speciale care să permită restrângerea dreptului la domiciliu al sediului profesional al avocatului[11]. Astfel, orice măsură de supraveghere tehnică desfășurată la sediul profesional al avocatului va trebui să reflecte respectarea dispozițiilor legale citate și va presupune ca judecătorul de drepturi și libertăți să acorde o atenție deosebită asupra îndeplinirii condițiilor legale pentru autorizare atât pentru respectarea dreptului la apărare al clienților avocatului, cât și pentru a menține reputația profesională a acestuia[12]. Apreciem că legea nu prevede nicio garanție procedurală specifică în cazul avocaților pentru a preveni un abuz din partea autorităților, condițiile legale neputând fi considerate a fi semnificativ mai stricte[13]. Practic, va trebui să fie îndeplinite aceleași condiții legale și să *existe date că avocatul săvârșește sau pregătește săvârșirea unei infracțiuni dintre cele prevăzute la art. 139 alin. (2) C.pr.pen.*, un standard prea scăzut, în opinia noastră, fiind necesar să existe probe în acest

[1] În cauză s-a reținut ca fiind contrar dreptului la domiciliu refuzul autorităților britanice de a permite construirea de „caravane" pe terenul aflat în proprietatea unei persoane de etnie romă care a adoptat un stil de viață parțial nomad, dar intenționa să locuiască pe respectivul teren și nu a putut obține autorizație ca urmare a suprasaturării zonei cu caravane nomade de rromi – CEDO, cauza *Buckley c. Marea Britanie*, Hotărârea din 29 septembrie 1996, §54, pe *hudoc.echr.coe.int*

[2] CEDO, cauza *Chapman c. Marea Britanie*, Hotărârea din 18 ianuarie 2001, §73, pe *hudoc.echr.coe.int*

[3] CEDO, cauza *Yordanova ș.a. c. Bulgaria*, Hotărârea din 24 aprilie 2012, §11-12, pe *hudoc.echr.coe.int*

[4] CEDO, cauza *Sagan c. Ucraina*, Hotărârea din 23 octombrie 2018, §51; cauza *Halabi c. Franța*, Hotărârea din 16 mai 2019, §41-43, pe *hudoc.echr.coe.int*

[5] CEDO, cauza *Demades c. Turcia*, Hotărârea din 31 iulie 2003, §32, pe *hudoc.echr.coe.int*

[6] CEDO, cauza *Niemietz c. Germania*, Hotărârea din 16 decembrie 1992, §30*;* cauza *Buck c. Germania*, Hotărârea din 28 aprilie 2005, §31, pe *hudoc.echr.coe.int*

[7] CEDO, cauza *Popovi c. Bulgaria*, Hotărârea din 9 iunie 2016, §103, pe *hudoc.echr.coe.int*

[8] CEDO, cauza *Saint-Paul Luxembourg S.A. c. Luxemburg*, Hotărârea din 18 aprilie 2013, §37, pe *hudoc.echr.coe.int*

[9] CEDO, cauza *Société Colas Est ș.a. c. Franța*, Hotărârea din 16 aprilie 2002, §41; cauza *Kent Pharmaceuticals ș.a. c. Marea Britanie*, Hotărârea din 11 octombrie 2005, declarată inadmisibilă, pe *hudoc.echr.coe.int*

[10] CEDO, cauza *Steeg c. Germania*, Hotărârea din 3 iunie 2008, declarată inadmisibilă, pe *hudoc.echr.coe.int*

[11] CEDO, cauza *Petri Sallinen ș.a. c. Finlanda*, Hotărârea din 27 septembrie 2005, §90.

[12] CEDO, cauza *Buck c. Germania*, Hotărârea din 28 aprilie 2005, §45.

[13] CEDO, cauza *André ș.a. c. Franța*, Hotărârea din 24 iulie 2008, §42, pe *hudoc.echr.coe.int*

sens pentru a pune nivelul de protecție pe o poziție mai înaltă decât cel în cazul oricăror alte persoane, în virtutea rolului deosebit al avocatului. Judecătorul de drepturi și libertăți va analiza și proporționalitatea măsurii luate față de avocat, mandatul de supraveghere tehnică trebuind să fie deosebit de precis pentru a nu aduce atingere și activităților avocatului care nu sunt apreciate ca fiind ilicite[1]. În practică, acest lucru poate fi stabilit prin măsurile de supraveghere tehnică încuviințate în mod concret de judecătorul de drepturi și libertăți, putând fi limitată supravegherea numai la observarea interacțiunilor cu alte părți și la înregistrarea doar a anumitor persoane în cabinetul de avocat, ori folosirea unor mijloace tehnice prin care nu va fi necesară pătrunderea în spațiile private.

Ca un mijloc de protecție în cazul unor ingerințe aduse persoanei, se impune ca aceasta să aibă un drept propriu de a contesta măsura și de a obține distrugerea mijloacelor de probă rezultate[2], ceea ce nu este prevăzut în cazul legislației române, unde persoana supravegheată are numai dreptul de a fi informată asupra supravegherii tehnice.

În concluzie, dreptul la domiciliu al persoanei va putea fi afectat de folosirea metodelor speciale de supraveghere sau cercetare, dar într-o măsură mai restrânsă, neputând fi incidente decât o parte dintre măsurile prevăzute de Codul de procedură penală. Dintre acestea, supravegherea video, audio sau prin fotografiere va avea cea mai mare incidență, întrucât presupune pătrunderea în spații private pentru instalarea și dezinstalarea mijloacelor tehnice, precum și realizarea de filmări în spațiile private.

[1] CEDO, cauza *Roemen și Schmit c. Luxemburg*, Hotărârea din 25 februarie 2003, §70, pe *hudoc.echr.coe.int*
[2] CEDO, cauza *Delta Pekárny A.S. c. Cehia*, Hotărârea din 2 octombrie 2014, §92, pe *hudoc.echr.coe.int*

Capitolul V
Dreptul la un proces echitabil

Dreptul la un proces echitabil, din perspectiva metodelor speciale de supraveghere sau cercetare, se poate rezuma la posibilitatea folosirii probelor obținute în mod nelegal sau neloial ca urmare a acestor tehnici speciale și dacă folosirea lor contravine dreptului la un proces echitabil. După cum s-a arătat în literatura de specialitate, consecințele declarării unei probe ca fiind nelegale poate conduce la colapsul întregii acuzații formulate față de o persoană, chiar și în situația săvârșirii unor infracțiuni foarte grave, precum violul sau omorul[1].

Incidente în discuția de față vor fi dispozițiile cuprinse în art. 6 par. 1 Conv.EDO, în care se arată că: „*Orice persoană are dreptul la judecarea cauzei sale în mod echitabil, în mod public și în termen rezonabil, de către o instanță independentă și imparțială, instituită de lege, care va hotărî fie asupra încălcării drepturilor și obligațiilor sale cu caracter civil, fie asupra temeiniciei oricărei acuzații în materie penală îndreptate împotriva sa. Hotărârea trebuie să fie pronunțată în mod public, dar accesul în sala de ședință poate fi interzis presei și publicului pe întreaga durată a procesului sau a unei părți a acestuia, în interesul moralității, al ordinii publice ori al securității naționale într-o societate democratică, atunci când interesele minorilor sau protecția vieții private a părților la proces o impun, sau în măsura considerată absolut necesară de către instanță când, în împrejurări speciale, publicitatea ar fi de natură să aducă atingere intereselor justiției*". În același timp, vor putea fi aplicabile și dispozițiile cuprinse în art. 6 par. 3 lit. c) Conv.EDO privind posibilitatea pregătirii apărării alături de un avocat, în condițiile în care să se respecte confidențialitatea relației client-avocat.

Ținând seama de caracterul de procedeu probatoriu al metodelor speciale de supraveghere sau cercetare, nu vor fi incidente toate situațiile în care desfășurarea activităților din cadrul unui proces penal vor cădea sub incidența art. 6 Conv.EDO, ci numai cele care au în vedere: *i)* administrarea probelor într-un mod echitabil față de dreptul la apărare; *ii)* posibilitatea de a contesta autenticitatea probelor; *iii)* interzicerea obținerii de probe prin provocarea săvârșirii unei infracțiuni și *iv)* garantarea dreptului la apărare prin confidențialitatea raportului client-avocat.

În ceea ce privește administrarea probelor, nu intră în rolul Curții să determine dacă probele au fost administrate conform legii sau dacă acestea trebuiau să fie excluse, ci analiza se va face asupra procesului penal, dacă în sinea lui a fost desfășurat cu respectarea echitabilității[2]. Sub acest aspect, nu trebuie să confundăm rolul și momentul la care are loc un control din partea Curții cu rolul și momentul la care o instanță națională se pronunță asupra cauzei. Instanța națională va trebui să aibă criterii mai stricte în evaluarea legalității administrării probelor, deoarece o nelegalitate nu va avea, în mod necesar, un caracter determinant asupra procesului penal[3], dar o sumă de astfel de nelegalități, trecute cu vederea de instanța națională, va avea un efect cumulat de a conduce la caracterul inechitabil al procesului penal. Această situație se

[1] *A. Ashworth, M. Redmayne*, The Criminal Process, 2014, p. 342.

[2] *T. Weigend*, în D.K. Brown, J.I. Turner, B. Weisser (coord.), The Oxford Handbook of Criminal Process, Oxford University Press, Oxford, 2019, p. 169.

[3] CEDO, cauza *Ulariu c. România*, Hotărârea din 19 noiembrie 2013, §52 privind încălcarea art. 8 Conv.EDO, §71 privind lipsa încălcării art. 6 par. 1 Conv.EDO, pe *hudoc.echr.coe.int*

poate vedea în cazul supravegherii tehnice în contextul separației funcțiilor judiciare, întrucât nu se poate reevalua nelegalitatea supravegherii tehnice ulterior fazei camerei preliminare decât în cazul incidenței nulității absolute. Totodată, anterior pronunțării Deciziei Curții Constituționale nr. 302/2017, invocarea unei nulități absolute în legătură cu actele efectuate și probele administrate în cursul urmăririi penale era o imposibilitate practică[1], putând fi invocată numai o nulitate relativă[2]. Din acest punct de vedere, trebuie să concluzionăm că regulile de excludere a probelor vor fi prevăzute la nivel național și vor varia în funcție de țară, dar și de modificările legislative[3].

În analiza existenței unei încălcări a art. 6 Conv.EDO, adesea se invocă și încălcarea altor articole, în general, dreptul la viață privată în contextul aplicării unor metode speciale de supraveghere sau cercetare, precum sisteme de înregistrare ascunse, fără a exista dispoziții legale prin care folosirea lor să fie reglementată[4], supravegherea în locuința unei persoane, precum și în secția de poliție[5], supravegherea prin mijloace tehnice a unei persoane deținute, prin montarea aparaturii în zona de vizitare și asupra unui alt deținut[6]. În cauza *Allan c. Marea Britanie*, anterior citată, persoana acuzată s-a prevalat de dreptul la tăcere, fiind instalate mijloace tehnice asupra unei persoane aflate în celula sa, prin care organele de urmărire penală au putut obține probe, întrucât colegul său de celulă era instruit de organele de urmărire penală să îl preseze pe acuzat în legătură cu faptele comise, sens în care s-a constatat caracterul inechitabil al procedurii.

Pentru asigurarea dreptului la un proces echitabil, este necesar ca apărarea să dispună de posibilitatea contestării autenticității probelor obținute împotriva sa și să poată obține excluderea acestora, sub acest aspect, trebuind să se țină seama de calitatea probelor, a circumstanțelor în care au fost obținute și dacă aceste circumstanțe aruncă dubii asupra autenticității sau concludenței probei[7]. Ceea ce trebuie subliniat este că încălcarea art. 8 Conv.EDO nu va conduce la constatarea caracterului inechitabil al procedurii, ci va trebui să se analizeze dacă probele obținute în mod nelegal au fost valorificate de instanță într-un mod care să schimbe rezultatul judecății. Într-una dintre cauzele judecate de Curte, s-a reținut că, deși a existat o încălcare a art. 8 Conv.EDO, înregistrarea nu a fost tratată de instanță ca o mărturisire și a reprezentat o singură probă dintr-un material probatoriu complex și amplu pe care acuzarea l-a adus împotriva apărării, astfel că nu a existat o încălcare a dreptului la un proces echitabil[8]. În ceea ce privește alte forme de corespondență, s-a reținut în mod similar că nu va exista o încălcare a dreptului la un proces echitabil nici în situația în care se procedează la reținerea, predarea și percheziționarea trimiterilor poștale ale unei persoane bănuite de trafic de droguri și se constată de Curte nelegalitatea unor astfel de măsuri prin raportare la art. 8 Conv.EDO,

[1] CCR, Dec. nr. 302 din 4 mai 2017 (M. Of. nr. 566 din 17 iulie 2017).

[2] C. Ap. Bacău, s. pen., încheierea nr. 33 din 13 mai 2016, definitivă prin încheierea nr. 919 din 22 iunie 2016 a ICCJ, s. pen., publicată în C. Moisă, Probele în procesul penal. Practică judiciară adnotată, Ed. Hamangiu, București, 2017, p. 72.

[3] *S. McKay*, Covert Policing, 2015, pp. 61-62.

[4] CEDO, cauza *Khan c. Marea Britanie,* Hotărârea din 12 mai 2000, §27 privind art. 8 și §34 privind art. 6 Conv.EDO, pe *hudoc.echr.coe.int*

[5] CEDO, cauza *P.G. și J.H. c. Marea Britanie*, Hotărârea din 25 septembrie 2001, §38 și §63 pentru art. 8 și §80-81 pentru art. 6 Conv.EDO.

[6] CEDO, cauza *Allan c. Marea Britanie*, Hotărârea din 5 februarie 2002, §36 pentru art. 8 și §52 pentru art. 6 Conv.EDO.

[7] CEDO, cauza *Gäfgen c. Germania*, Hotărârea din 1 iunie 2010, §164, pe *hudoc.echr.coe.int*

[8] CEDO, cauza *Bykov c. Rusia*, Hotărârea din 10 martie 2009, §103, pe *hudoc.echr.coe.int*

dacă, din ansamblul probelor numeroase aflate la dosarul cauzei, instanța a putut stabili situația de fapt în mod corect[1].

Situația unei încălcări a art. 8 Conv.EDO nu va determina Curtea să procedeze la reținerea încălcării dreptului la un proces echitabil, dar, în opinia noastră, prin raportare la condițiile nulității relative, o astfel de vătămare va determina întotdeauna nulitatea procedeului probatoriu, al mijloacelor de probă obținute și a excluderii probelor, astfel că instanța națională va trebui să țină seama de această diferență și să înlăture probele administrate în mod nelegal, în toate cazurile. Această concluzie este întărită și de opiniile separate ale judecătorilor Curții Europene a Drepturilor Omului în unele cauze. De pildă, în cauza *Khan c. Marea Britanie* a existat o opinie separată a domnului judecător Loucaides, în care acesta se exprima în sensul că: *„nu pot accepta că un proces poate fi «echitabil», așa cum prevede articolul 6, dacă vinovăția unei persoane pentru o infracțiune este stabilită prin dovezi obținute cu încălcarea drepturilor omului garantate de Convenție. În opinia mea, termenul de «echitabil», atunci când este examinat în contextul Convenției Europene a Drepturilor Omului, implică respectarea statului de drept și aceasta presupune respectarea drepturilor omului prevăzute în Convenție. Nu cred că se poate vorbi despre un proces «echitabil» dacă acesta se desfășoară cu încălcarea legii. Este adevărat că Convenția nu face parte din sistemul juridic intern al Regatului Unit, dar, în sensul întrebării în cauză, ar trebui tratată ca atare, având în vedere ratificarea acesteia de către țara respectivă și obligația să aplice dispozițiile sale prin organele sale. Cu alte cuvinte, în a evalua dacă un proces a fost «echitabil», nu văd niciun motiv pentru a fi permisiv cu unul care a ratificat Convenția, dar nu a încorporat-o în sistemul său”*[2]. În doctrină s-a apreciat că excluderea probelor obținute contrar protejării dreptului la viață privată ar trebui să fie considerată un corolar esențial al dreptului, pentru a se considera că dreptul la viață privată are o valoare reală[3]. Cu toate acestea, în prezent, în jurisprudența Curții numai în cazul încălcării art. 3 Conv.EDO, alături de folosirea probelor obținute prin această încălcare, se va ajunge la pronunțarea unei soluții de încălcare a art. 6 par. 1 Conv.EDO în mod automat[4]. Totodată, s-a subliniat și că jurisprudența Curții nu este una omogenă în a reține existența unei încălcări a dreptului la un proces echitabil, fiind în discuție chiar și aplicarea sau nu de către Curte a principiului proporționalității în toate cazurile[5].

Nu va exista o încălcare a dreptului la un proces echitabil atunci când acuzatului i se oferă posibilitatea să conteste autenticitatea probelor rezultate din supravegherea tehnică și instanțele naționale resping în mod motivat solicitările sale, procedând la constatarea vinovăției sale pe baza declarațiilor acuzatului, ale coacuzaților, coroborându-le cu declarațiile martorilor și numeroase probe obținute în urma unor percheziții domiciliare[6].

Într-o cauză îndreptată împotriva României, Curtea a reținut că a existat o încălcare a art. 6 par. 1 Conv.EDO, prin raportare la înregistrări realizate în mediu ambiental, al căror original (înregistrări pe bandă magnetică) nu a putut fi prezentat în fața instanțelor, deoarece persoana fizică (un particular) care a realizat înregistrările a refuzat să le pună la dispoziția

[1] CEDO, cauza *Dragoș Ioan Rusu c. România*, Hotărârea din 31 octombrie 2017, §55, pe *hudoc.echr.coe.int*

[2] CEDO, cauza *Khan c. Marea Britanie,* Hotărârea din 12 mai 2000, opinie separată.

[3] *A. L-T Choo*, Evidence, 2018, p. 168.

[4] CEDO, cauza *Gäfgen c. Germania*, Hotărârea din 1 iunie 2010, §166; cauza *Ibrahim ș.a. c. Marea Britanie*, Hotărârea din 13 septembrie 2016, §254; cauza *Cēsnieks c. Letonia*, Hotărârea din 11 februarie 2014, §69, pe *hudoc.echr.coe.int*; *R.H. Radu*, Reflecții privind efectele Deciziei nr. 51/2016 a Curții Constituționale a României, în Revista Universul Juridic nr. 3/2016, p. 86.

[5] *B.J. Goold, L. Lazarus, G. Swiney*, op. cit., p. 30.

[6] CEDO, cauza *Dragojević c. Croația*, Hotărârea din 15 ianuarie 2015, §132-135, pe *hudoc.echr.coe.int*

instanței și nici nu a fost audiată de instanță, iar, în cursul urmăririi penale, fiind chemată în fața procurorului, a plecat, invocând o durere de cap și susținând că se va întoarce, ceea ce nu a mai făcut vreodată[1].

O problemă aparte o va constitui situația în care obținerea probelor de către organele de urmărire penală s-a făcut prin provocare, situație care contravine echitabilității procedurii, dar prezintă interes în contextul măsurilor speciale de cercetare, în special în ceea ce privește participarea autorizată la anumite activități.

Pentru existența infracțiunii provocate, este necesar ca acțiunea de provocare să fie desfășurată de organele de urmărire penală sau, în sens general, de un agent al statului care acționează în numele acestora (de pildă, un colaborator).

Întrucât problema provocării infracțiunii se află în strânsă legătură cu problema folosirii tehnicilor speciale de cercetare a unor infracțiuni, Curtea s-a pronunțat în sensul în care nu va constitui o încălcare a dreptului la un proces echitabil folosirea unor astfel de tehnici, însă acestea trebuie să fie limitate la scopul măsurii[2]. Acest scop trebuie să constea doar în dovedirea existenței infracțiunii, și nu în determinarea unei persoane să comită o infracțiune pentru ca prin aceasta să fie dovedită însăși această infracțiune[3] indiferent de gravitatea faptei care face obiectul urmăririi penale sau de necesitatea de a asigura celeritatea în tragerea la răspundere penală a unei persoane[4]. În mod corect a constatat Curtea că, indiferent de gravitatea faptelor, nu se poate justifica întrebuințarea provocării pentru apărarea interesului public, toate probele obținute trebuind să fie excluse[5].

Nu va putea fi tolerată provocarea realizată de agenți ai statului dacă persoana nu era bănuită în mod obiectiv de vreo activitate infracțională trecută sau avea o predispoziție în acest sens[6]. Curtea a amintit, în constatarea provocării la săvârșirea unei infracțiuni, lipsa antecedentelor penale ale persoanei, faptul că nu s-a desfășurat anterior față de aceasta o urmărire penală, că nu era o persoană aflată în atenția poliției, că nu s-au găsit droguri la domiciliul acesteia, și cantitatea de droguri aflată în posesia sa nu era mai mare decât cantitatea cerută de organele de poliție[7].

Curtea a stabilit că nu va exista o infracțiune provocată atunci când un funcționar a cerut, chiar și sub formă deghizată, o sumă de bani drept mită pentru ca, ulterior, la sesizarea persoanei de la care s-a pretins mita, să se realizeze un flagrant prin care funcționarul să primească suma de bani solicitată[8].

O problemă aparte în analiza efectuată de Curte în cazul infracțiunii provocate constă în diferențierea între cine are inițiativa săvârșirii infracțiunii. Dacă vine din partea celui care comite infracțiunea, nu va fi nicio încălcare; o atare situație este dacă o persoană care nu era bănuită de comiterea de infracțiuni se oferă să vândă unui investigator sub acoperire o cantitate de droguri sau să ofere unui funcționar o sumă de bani[9]. Tot în acest sens, dacă o

[1] CEDO, cauza *Nițulescu c. România*, Hotărârea din 22 septembrie 2015, §53-57, pe *hudoc.echr.coe.int*

[2] CEDO, cauza *Ramanauskas c. Lituania*, Hotărârea din 5 februarie 2008, §51, pe *hudoc.echr.coe.int*

[3] *Ibidem*, §55; CEDO, cauza *Teixeira de Castro c. Portugalia*, Hotărârea din 9 iunie 1998, §38, pe *hudoc.echr.coe.int*

[4] CEDO, cauza *Ramanauskas c. Lituania*, Hotărârea din 5 februarie 2008, §53; CEDO, cauza *Delcourt c. Belgia*, Hotărârea din 17 ianuarie 1970, §25, pe *hudoc.echr.coe.int*

[5] CEDO, cauza *Furcht c. Germania*, Hotărârea din 23 ianuarie 2015, §64, pe *hudoc.echr.coe.int*

[6] CEDO, cauza *Bannikova c. Rusia*, Hotărârea din 4 februarie 2011, §38, pe *hudoc.echr.coe.int*

[7] CEDO, cauza *Teixeira de Castro c. Portugalia*, Hotărârea din 9 iunie 1998, §37-38.

[8] CEDO, cauza *Gorgievski c. Macedonia*, Hotărârea din 10 decembrie 2009, §53, pe *hudoc.echr.coe.int*

[9] CEDO, cauza *Ramanauskas c. Lituania (nr. 2)*, Hotărârea din 20 mai 2018, §68, pe *hudoc.echr.coe.int*

persoană contactează un colaborator al organelor de urmărire penală în vederea organizării unui transport de cocaină, iar ulterior colaboratorii participă la transportul ilicit, nu se va considera că a fost provocată în săvârșirea faptei, deoarece intenția inițială i-a aparținut[1]. În schimb, s-a stabilit că a existat o provocare din partea unui investigator sub acoperire atunci când, în lipsa unor elemente obiective privind predispoziția către săvârșirea unei infracțiuni, investigatorul l-a sunat pe inculpat și i-a cerut să îi vândă o cantitate de droguri, astfel reținându-se provocarea la săvârșirea unei infracțiuni[2].

Provocarea la săvârșirea unei infracțiuni din partea investigatorilor sub acoperire poate căpăta și forme deosebit de perverse, prin apelul la compasiunea inculpatului și prin inducerea ideii că investigatorul suferă de sevraj și că s-ar putea sinucide dacă nu i se procură droguri[3].

O altă situație care poate genera încălcări ale dreptului la un proces echitabil va fi folosirea măsurilor speciale de supraveghere asupra relației dintre avocat și persoana acuzată în procesul penal, putându-se obține înregistrări care contravin secretului profesional. Ele vor constitui ingerințe aduse atât art. 8 Conv.EDO privind viața privată, cât și atingeri aduse art. 6 par. 3 Conv.EDO privind dreptul la apărare.

Legea română, de pildă, nu include suficiente garanții în privința măsurilor de supraveghere tehnică asupra avocatului, fiind prevăzute aceleași condiții de autorizare ca în cazul supravegherii unei alte persoane, imposibilitatea procedurală a contestării măsurii luate împotriva avocatului și de a obține distrugerea datelor rezultate din supraveghere[4]. Este drept că, potrivit art. 139 alin. (4) C.pr.pen., avocatul poate fi încunoștințat de faptul că au fost supravegheate accidental interacțiunile cu clientul său, dar cât timp aceasta rămâne o facultate, nu putem afirma că este respectat pe deplin dreptul la apărare al persoanei acuzate.

Pentru apărarea drepturilor unei persoane aflate în stare de detenție – atât preventivă, cât și ca urmare a executării unei pedepse privative de libertate –, persoanei i se permite să ia contact cu avocatul său prin orice mijloc – oral, telefonic sau în scris. Acest drept se aplică atât în cazul avocatului deja angajat, cât și în cazul avocatului care urmărește să angajeze cauza persoanei deținute[5]. Dreptul de a se consulta cu persoana pe care o apără, în condiții de confidențialitate, nu va reprezenta doar un drept care cade sub incidența art. 8 Conv.EDO, ci și unul care cade sub incidența art. 6 par. 3 Conv.EDO, numai prin comunicarea liberă și confidențială dintre avocat și client putând fi asigurată efectiva exercitare a dreptului la apărare ca o componentă a dreptului la un proces echitabil.

În cauza *Altay c. Turcia (nr. 2)*, Curtea a stabilit că va constitui o ingerință adusă dreptului la viață privată – prin raportare la respectarea secretului profesional – prezența obligatorie a unei persoane din cadrul unei autorități publice la interacțiunile personale dintre avocat și client[6]. O persoană aflată în stare de detenție se poate simți inhibată să discute toate aspectele necesare apărării propriei cauze în situații în care vor fi de față reprezentanți ai autorităților publice, aceasta constituind o încălcare a dreptului la un proces echitabil.

Numai în măsura în care întâlnirile dintre avocat și client rămân confidențiale, se poate considera că este respectat și dreptul la apărare al persoanei acuzate, în sensul art. 6 par. 3

[1] CEDO, cauza *Sequeira c. Portugalia*, Hotărârea din 6 mai 2003, pe *hudoc.echr.coe.int*

[2] CEDO, cauza *Burak Hun c. Turcia*, Hotărârea din 15 martie 2010, §44; în același sens, cauza *Sepil c. Turcia*, Hotărârea din 12 noiembrie 2013, §34, pe *hudoc.echr.coe.int*

[3] CEDO, cauza *Vanyan c. Rusia*, Hotărârea din 15 martie 2006, §11, pe *hudoc.echr.coe.int*

[4] CEDO, cauza *Heino c. Finlanda*, Hotărârea din 15 februarie 2011, §45, pe *hudoc.echr.coe.int*

[5] CEDO, cauza *Schönenberger și Durmaz c. Elveția*, Hotărârea din 20 iunie 1988, §29, *hudoc.echr.coe.int*

[6] CEDO, cauza *Altay c. Turcia (nr. 2)*, Hotărârea din 9 iulie 2019, §49-50, pe *hudoc.echr.coe.int*

Conv.EDO, fiind interzise ingerințele la secretul profesional[1], deoarece, dacă nu s-ar asigura această confidențialitate, asistența juridică și-ar pierde din utilitate[2]. În acest sens, supravegherea convorbirilor nu poate avea loc fără o ingerință adusă dreptului la apărare[3], Convenția prevenind posibilitatea autorităților de a percepe conținutul conversației prin ascultarea acesteia[4], nu neapărat acțiunile concrete care au loc între avocat și persoana aflată în locul de detenție. Aceasta însemnă că nu vor fi permise acțiuni precum verificarea documentelor prezentate de către avocat clientului în timpul întâlnirilor sau ca acesta să fie percheziționat cu privire la tipul documentelor sau înscrisurilor pe care le are asupra sa la momentul la care își consultă clientul aflat în detenție[5], întrucât acestea ar face parte și din obiectul comunicării dintre cele două părți.

Astfel, interacțiunea dintre client și avocatul său nu poate face obiectul unei supravegheri tehnice a conținutului conversațiilor atunci când aceasta are loc într-un spațiu de detenție, fiind protejate în mod absolut conversațiile dintre aceștia. Legislația română a consacrat acest principiu în cuprinsul art. 89 alin. (2) C.pr.pen., unde se arată că: „*persoana reținută sau arestată are dreptul să ia contact cu avocatul, asigurându-i-se confidențialitatea comunicărilor, cu respectarea măsurilor necesare de supraveghere vizuală, de pază și securitate, fără să fie interceptată sau înregistrată convorbirea dintre ei. Probele obținute cu încălcarea prezentului alineat se exclud*".

În concluzie, folosirea metodelor speciale de supraveghere sau cercetare într-o cauză nu va presupune numai respectarea dreptului la viață privată al persoanei, ci va însemna ca toate aceste procedee să fie administrate cu respectarea dreptului la un proces echitabil, mai ales prin garantarea acuzatului a posibilității de a-și realiza în mod eficient apărarea, de a putea contesta autenticitatea și fidelitatea probelor, a modului în care au fost administrate, dar și de a beneficia de confidențialitatea discuțiilor sale cu un avocat.

[1] CEDO, cauza *Beuze c. Belgia*, Hotărârea din 9 noiembrie 2018, §133, pe *hudoc.echr.coe.int*

[2] CEDO, cauza *Lanz c. Austria*, Hotărârea din 30 aprilie 2002, §50; cauza *S. c. Elveția*, Hotărârea din 28 noiembrie 1991, §48; cauza *Brennan c. Marea Britanie*, Hotărârea din 16 octombrie 2001, §58, pe *hudoc.echr.coe.int*

[3] CEDO, cauza *Rybacki c. Polonia*, Hotărârea din 13 ianuarie 2009, §56; cauza *Öcalan c. Turcia*, Hotărârea din 12 mai 2005, §135, pe *hudoc.echr.coe.int*

[4] CEDO, cauza *Sakhnovskiy c. Rusia*, Hotărârea din 2 noiembrie 2010, §97; cauza *Castraveț c. Moldova*, Hotărârea din 13 martie 2007, §49, pe *hudoc.echr.coe.int*

[5] CEDO, cauza *Khodorkovskiy și Lebedev c. Rusia*, Hotărârea din 25 iulie 2013, §641, pe *hudoc.echr.coe.int*

Titlul III
Regimul metodelor speciale de supraveghere prevăzute de Codul de procedură penală

Capitolul I
Condiții necesare pentru obținerea autorizării

Secțiunea 1. Începerea urmăririi penale – condiție prealabilă autorizării supravegherii tehnice

Folosirea oricărei metode de supraveghere tehnică presupune restrângerea drepturilor și libertăților persoanei vizate de acest procedeu probatoriu, motiv pentru care se impune restricționarea folosirii acestuia numai în situații prevăzute expres de lege și garantarea respectării proporționalității între interesul public și interesul persoanei. S-a arătat în literatura de specialitate că se impune menținerea unui echilibru just între protejarea vieții private și necesitatea unei lupte eficace contra anumitor tipuri de criminalitate gravă[1], astfel că folosirea oricăror metode de supraveghere tehnică este condiționată de încuviințarea prealabilă a judecătorului de drepturi și libertăți. Legiuitorul a fost ferm în respectarea vieții private a persoanei, prin includerea respectării acestei valori ca un principiu fundamental al procesului penal, fiind prevăzut de art. 11 alin. (2) C.pr.pen., dar și prin subordonarea folosirii metodelor de supraveghere tehnică unor condiții foarte stricte[2].

Necesitatea încuviințării procedeului probatoriu servește un dublu scop, cel de a conferi organelor de urmărire penală puteri sporite în activitatea de administrare a probelor și cel de a garanta legalitatea administrării probei. Deoarece măsurile de supraveghere tehnică se răsfrâng marcant asupra drepturilor persoanei care face obiectul procedeului probatoriu, fapta ar putea constitui o infracțiune în lipsa existenței unei autorizări din partea unui organ competent. De pildă, interceptarea comunicațiilor va constitui infracțiunea de violarea secretului corespondenței prevăzută de art. 302 alin. (2) C.pen., accesul la un sistem informatic va constitui infracțiunea de *acces ilegal la un sistem informatic*, iar supravegherea video, audio sau prin fotografiere va putea fi încadrată ca infracțiune de hărțuire prevăzută de art. 208 C.pen. Ținând seama de protecția penală conferită vieții private a persoanei, autorizarea judecătorului de drepturi și libertăți va servi drept *cauză justificativă*, în sensul prevederilor art. 21 C.pen. Mandatul judecătorului va constitui o *autorizare oficială*[3] pentru exercitarea dreptului de a proceda la realizarea supravegherii tehnice. Este adevărat că efectuarea urmăririi penale este o obligație pentru procuror, însă, în cazul supravegherii tehnice, întrebuințarea procedeului probatoriu constituie un drept limitat astfel: *procurorul nu poate autoriza supravegherea*

[1] *Gh. Mateuț*, Tratat, vol. II, 2012, p. 209.
[2] *Ibidem*.
[3] *Fl. Streteanu*, Tratat de drept penal. Partea generală, vol. I, Ed. C.H. Beck, București, 2008, p. 543.

tehnică (decât în condiții restrânse și cu caracter provizoriu), *procurorul este ținut de limitările spațio-temporale ale mandatului judecătorului de drepturi și libertăți*, *procurorul nu poate pune în executare măsuri de supraveghere tehnică neautorizate sau într-un alt mod concret decât au fost autorizate* (de exemplu, dacă judecătorul de drepturi și libertăți va autoriza supravegherea prin filaj, procurorul nu va putea proceda la supravegherea video sau audio în spații private), *procurorul va trebui să dispună încetarea supravegherii tehnice când dispar temeiurile care justifică măsura*. În exercitarea autorizării date de judecătorul de drepturi și libertăți, procurorul este îndreptățit să aleagă momentul în care va începe punerea în executare a mandatului [sau va delega punerea în executare, potrivit art. 142 alin. (1) C.pr.pen.], procedeele tactice și probatorii suplimentare care se impun și alegerea organelor sau persoanelor care vor acorda concurs tehnic.

Măsurile de supraveghere tehnică pot fi dispune numai atunci când sunt îndeplinite mai multe condiții cumulative de fond, prevăzute în cuprinsul art. 139 alin. (1) și (2) C.pr.pen. Aceste condiții de fond sunt împărțite de doctrină în trei categorii: *suspiciune rezonabilă*, *proporționalitate* și *subsidiaritate*[1].

Mai înainte de orice condiție prevăzută expres de lege, este necesar să fi fost începută urmărirea penală pentru o faptă prevăzută de legea penală săvârșită sau care se pregătește a fi săvârșită. Această condiție a fost în mod corect identificată drept o condiție de *formă*, întrucât folosirea metodelor speciale de supraveghere nu se poate realiza decât în existența unui cadru procesual care debutează cu începerea urmăririi penale *in rem*[2]. Desigur, metodele speciale de supraveghere tehnică vor putea fi întrebuințate și în faza urmăririi penale *in personam*, dar condiția minimă este începerea urmăririi penale *in rem,* aceasta fiind prima fază procesuală a procesului penal reglementat de legislația actuală. Prin Codul de procedură penală din 2010, s-a renunțat la faza *actelor premergătoare* efectuate în vederea începerii urmăririi penale, etapă în cadrul căreia puteau fi autorizate metode speciale echivalente actuale supravegherii tehnice (în special, interceptarea și înregistrarea comunicațiilor).

În literatura de specialitate a fost criticată alegerea legiuitorului de a reglementa faza procesuală a urmăririi penale *in rem*, deoarece permite administrarea de probe și ușurarea aflării adevărului prin metode speciale de supraveghere, deturnând de la scopul ei legitim declanșarea urmăririi penale[3]. Spre deosebire de faza actelor premergătoare, probele obținute prin metodele speciale de supraveghere vor putea fi folosite pentru aflarea adevărului în cauză, și nu doar pentru a se putea demara începerea urmăririi penale. În opinia noastră, problema reală nu stă în folosirea supravegherii tehnice în faza procesuală *in rem* ca atare, ci prin lipsa existenței unor garanții efective împotriva abuzurilor organelor de urmărire penală în a declanșa în mod artificial o urmărire penală în scopul utilizării acestor procedee probatorii pentru a strânge probe în procesul penal. În schimb, înăsprirea condițiilor de autorizare a supravegherii tehnice, condiționarea acestor măsuri de o gravitate mai ridicată a infracțiunilor cercetate decât în prezent, evaluarea corectă a proporționalității măsurii de către judecătorii de drepturi și libertăți sunt singurele metode prin care se pot preveni abuzuri prin desfășurarea de urmăriri penale artificiale, denumite în dreptul englez *fishing expeditions*. În doctrina străină se arată că rolul judecătorului va fi unul esențial în găsirea unui just echilibru între interesul public în desfășurarea unei cercetări penale care să ajungă la aflarea adevărului și protejarea

[1] *Gh. Mateuț*, Procedură penală, 2019, p. 678.
[2] *Ibidem*, p. 684.
[3] *Ibidem*, p. 685.

interesului cetățenilor de a le fi respectate drepturile personale. Judecătorului trebuie să îi fie prezentate suficiente date, informații sau probe pentru a putea lua o decizie asupra măsurii concrete care se impune a fi realizată și să prevină ca organele de urmărire penală să obțină o autorizare atunci când acuzația de natură penală este una generală[1].

În același timp, un control *a posteriori* al legalității autorizării va fi necesar pentru asigurarea respectării drepturilor și libertăților fundamentale ale persoanei, acesta trebuind să privească toate condițiile legale de autorizare a supravegherii tehnice. Deși Codul de procedură penală nu prevede vreo cale de atac împotriva încheierii de autorizare a supravegherii tehnice, aceasta se va contesta în faza camerei preliminare, analizându-se inclusiv dacă măsurile încuviințate de judecătorul de drepturi și libertăți au avut la bază o suspiciune reală de săvârșire a unei infracțiuni, au fost proporționale și subsidiare oricărui alt procedeu probatoriu sau dacă măsurile de supraveghere tehnică încuviințate au fost suficient de clar detaliate în încheiere. Pentru persoanele care nu vor participa în faza camerei preliminare sau dacă o astfel de fază procesuală nu va exista, Codul nu prevede nicio posibilitate de a contesta legalitatea măsurii, fapt constatat ca fiind neconstituțional și care va forma obiectul unei secțiuni distincte[2].

Din dispozițiile legale prevăzute de art. 305 alin. (1) C.pr.pen., reiese faptul că începerea urmăririi penale este actul procesual care creează întreg cadrul pentru desfășurarea activităților de urmărire penală, inclusiv administrarea probelor, supravegherea tehnică fiind un procedeu probatoriu în viziunea actuală a legiuitorului. Condiția începerii urmăririi penale va trebui să fie întrunită mai înainte de a se analiza orice altă condiție de fond. În cazul în care ordonanța de începere a urmăririi penale nu va fi legală (de pildă, lipsind actul de sesizare), nu va putea fi socotită ca fiind îndeplinită condiția începerii urmăririi penale, astfel că supravegherea tehnică vă fi lovită de o nulitate derivată, în sensul art. 280 alin. (2) C.pr.pen.

Întrucât lipsurile în sistematizarea fazelor procesului penal nu fac parte din obiectul prezentei lucrări, vom analiza în secțiunile următoare doar condițiile de fond ale supravegherii tehnice, urmând să dedicăm un capitol întreg problemei procedurii de autorizare[3].

Secțiunea a 2-a. Suspiciunea rezonabilă privind săvârșirea ori pregătirea săvârșirii unei infracțiuni

§1. Noțiunea de „suspiciune rezonabilă"

După cum am arătat în secțiunea precedentă, pentru autorizarea supravegherii tehnice, există mai multe condiții de fond care trebuie să fie îndeplinite. Deși Codul de procedură penală prevede trei condiții de fond, ele nu ar trebui să fie privite independent una de cealaltă, întrucât sunt interdependente și se vor influența reciproc. În acest sens, existența unei suspiciuni rezonabile privind săvârșirea unui anumit tip de infracțiune va fi un factor determinant în evaluarea proporționalității măsurii prin raportare la gravitatea faptei, a tăriei fundamentului probator pe care se bazează acuzația, dar va constitui un factor determinant și pentru evaluarea subsidiarității prin raportare la natura faptei și a modului concret de săvârșire a ei.

[1] *D. Ormerod, D. Perry, P. Murphy (coord.)*, op. cit., p. 1343.
[2] *V. infra*, Titlul III, Capitolul VI.
[3] *V. infra*, Titlul III, Capitolul II.

Prima condiție de fond prevăzută de art. 139 alin. (1) C.pr.pen. este cea a existenței unei *suspiciuni rezonabile cu privire la pregătirea sau săvârșirea unei infracțiuni* dintre cele prevăzute de art. 139 alin. (2) C.pr.pen.

Mai înainte de a analiza infracțiunile care pot conduce la întrebuințarea supravegherii tehnice, este necesar să definim noțiunea de „suspiciune rezonabilă". Expresia constituie un împrumut legislativ din dreptul anglo-saxon, prin intermediul jurisprudenței Curții Europene a Drepturilor Omului, care face referire în mai multe cauze la acest termen[1]. În doctrina română se arată că noțiunea este definită, în general, *prin existența unor date sau informații care sunt în măsură să convingă un observator obiectiv și imparțial că este posibil ca o persoană să fi săvârșit o infracțiune*[2]. În acest sens, trebuie să avem în vedere că termenul este folosit de Convenție în relație cu luarea unor măsuri preventive față de persoana acuzată, în același mod prevăzând și legiuitorul român această condiție în cuprinsul art. 202 alin. (1) C.pr.pen.

Este drept că jurisprudența Curții Europene a Drepturilor Omului face referire la un test de obiectivitate în ceea ce privește interpretarea sensului termenului folosit în art. 5 par. 1 Conv.EDO[3], însă apreciem că interpretarea termenului se impune atât prin raportare la elemente obiective, cât și subiective, relevate în jurisprudența și doctrina străină[4].

În dreptul S.U.A., noțiunea de *reasonable suspicion* a fost tratată de Curtea Supremă a S.U.A. în cauza *Terry c. Ohio*[5], în care s-a arătat că, în conformitate cu Al Patrulea Amendament la Constituția S.U.A., un polițist poate opri pe stradă o persoană suspectă și poate realiza o percheziție corporală, chiar dacă nu are temei pentru a o reține, în măsura în care polițistul are **suspiciunea rezonabilă** că persoana a comis, comite sau pregătește comiterea unei infracțiuni și are credința întemeiată că persoana este înarmată și prezintă un pericol. În cauza citată, Curtea Supremă a constatat că polițistul a acționat în conformitate cu legea, întrucât acțiunile sale s-au întemeiat pe intima sa convingere că anumite persoane urmăreau să săvârșească o infracțiune, aceasta fiind susținută de temeiuri obiective. S-a reținut că un detectiv din Cleveland care patrula zilnic, de mai mulți ani, o zonă a orașului a observat două persoane străine de cartier că discutau la colțul unei străzi și că au început să se plimbe pe aceeași rută prin fața vitrinei unui magazin de 24 de ori, ulterior acestea discutând și cu o a treia persoană, care a plecat subit. Cele două persoane s-au deplasat în fața altui magazin, reîntâlnindu-se cu cea de-a treia, moment în care polițistul s-a apropiat și le-a cerut să se legitimeze, persoanele rostind ceva neinteligibil, imediat fiind controlate sumar, depistându-se două revolvere asupra acestora. Suspiciunea rezonabilă s-a bazat pe două elemente: convingerea subiectivă a polițistului ca urmare a experienței sale personale, inclusiv prin faptul că era arondat pentru patrularea acelei zone, dar și pe un factor obiectiv – comportamentul nefiresc al persoanelor observat întâmplător de polițist.

În dreptul englez, în mod similar, pentru a justifica acțiunile unui polițist, este necesar să existe o suspiciune rezonabilă și ca suspiciunea să fie una autentică și bazată pe elemente

[1] *R.A. Popa*, op. cit., p. 177.

[2] *Gh. Mateuț,* Procedură penală, 2019, p. 678.

[3] CEDO, cauza *Fox, Campbell și Hartley c. Marea Britanie*, Hotărârea din 30 august 1990, §32; cauza *Erdagöz c. Turcia*, Hotărârea din 22 octombrie 1997, §51; cauza *Ilgar Mammadov c. Azerbaidjan*, Hotărârea din 13 octombrie 2014, §88, pe *hudoc.echr.coe.int*

[4] *L. Leo, S. Chen*, Reasonable Suspicion or Real Likelihood: A Question of Semantics, în Singapore Journal of Legal Studies, 2008, Sing. J. Legal Stud. 446 (2008), p. 449.

[5] U.S., cauza *Terry c. Ohio*, Hotărârea din 10 iunie 1968, 392 U.S. 1 (1968), pe *supreme.justia.com*

obiective, respectiv pe date și informații[1]. Tradiția engleză privind suspiciunea rezonabilă este una veche, ea fiind o instituție de *common law* legată în mod obligatoriu de un element subiectiv[2]. Distincția față de jurisprudența Curții Europene a Drepturilor Omului este că va fi mutat testul caracterului rezonabil în sfera privată a persoanei care realizează actul și se va analiza dacă suspiciunea rezonabilă a existat în mintea acestuia la momentul realizării actului. În jurisprudența engleză se răspunde ferm la problemă, în sensul în care este necesar ca suspiciunea rezonabilă să existe cu adevărat în mintea organului de urmărire penală pentru ca măsura luată să fie legală[3]. Astfel, în aprecierea existenței unei suspiciuni rezonabile, instanța trebuie să analizeze dacă în mintea organului de urmărire penală s-a format o suspiciune autentică privind săvârșirea unei infracțiuni, ca parte a testului subiectiv, existând parțial și un test obiectiv. Acest test obiectiv nu se va raporta, ca în jurisprudența Curții Europene a Drepturilor Omului, la un observator independent, ci trebuie analizat dacă în mintea organului de urmărire penală existau temeiuri rezonabile[4] bazate pe fapte și dacă la momentul la care s-a realizat actul, acestea au fost analizate în mod obiectiv[5]. Trebuie subliniat că o analiză asupra existenței suspiciunii rezonabile nu va putea să se axeze pe împrejurări cunoscute după realizarea actului, legalitatea trebuind să fie analizată prin raportare la temeiurile și poziția subiectivă a organului de urmărire penală de la momentul efectuării acestuia[6].

Nu considerăm că abordările din *common law* sunt incompatibile cu cele relevate prin jurisprudența Curții Europene a Drepturilor Omului, reprezentând laturi diferite asupra aceleiași probleme, iar coroborându-le putem determina esența expresiei de „suspiciune rezonabilă". De pildă, un aspect de consens îl reprezintă faptul că suspiciunea rezonabilă trebuie să privească săvârșirea unei fapte care constituia la acel moment o infracțiune, în sens contrar, nu se va putea pune în discuție existența unei suspiciuni rezonabile[7]. Nu va fi obligatoriu, pentru formarea suspiciunii rezonabile, ca organul de urmărire penală să poată determina încadrarea juridică a faptei[8], fiind suficient să se constate că acesta a considerat că fapta avea natură infracțională[9]. Desigur, în cazul autorizării supravegherii tehnice în sistemul român, va avea o importanță deosebită natura faptei, însă acest aspect este adițional față de explicația noțiunii de „suspiciune rezonabilă".

---

[1] *D. Ormerod, D. Perry, P. Murphy (coord.),* op. cit., p. 1276; *T. Skolnik*, The Suspicious Distinction between Reasonable Suspicion and Reasonable Grounds to Believe, în Ottawa Law Review, 47 Ottawa L. Rev. 223 (2016), p. 232.

[2] *J.Q. Whitman*, The Origins of Reasonable Doubt. Theological Roots of the Criminal Trial, Yale University Press, Orwigsburg, Pennsylvania, 2008, p. 205; *L. Laudan*, Is Reasonable doubt Reasonable?, în Legal Theory, vol. 9, no. 4/2003, p. 329.

[3] *C.S. Lerner*, Reasonable Suspicion and Mere Hunches, în Vanderbilt Law Review, 59 Vand. L. Rev. 405 (2006), p. 459; *A.G. Ferguson*, Predictive Policing and Reasonable Suspicion, în Emory Law Journal, 2 Emory L. J. 259 (2012), p. 303.

[4] *A.E. Taslitz*, Cybersurveillance without restraint? The meaning and social value of the probable cause and reasonable suspicion standards in governmental access to third-party electronic records, în The Journal of Criminal Law & Criminology, vol. 103, no. 3/2013, p. 891.

[5] England and Wales High Court (Queen's Bench Division), cauza *Parker c. Chief Constable of Essex Police*, dec. din 18 august 2017, [2017] EWHC 2140 (QB), §19, pe *www.bailii.org*

[6] Supreme Court of Judicature, Queen's Bench Division (Secția echivalentă contenciosului administrativ – n.n.), cauza *Redmond-Bate c. Director of Public Prosecutions*, Dec. din 23 iulie 1999, [1999] EWHC Admin 733, pe *www.bailii.org*

[7] CEDO, cauza *Kavala c. Turcia*, Hotărârea din 10 decembrie 2019, §128, pe *hudoc.echr.coe.int*

[8] EWCA, cauza *Coudrat. c. Commissioners of Her Majesty's Revenue and Customs*, Dec. din 26 mai 2005, [2005] EWCA Civ 616, pe *www.bailii.org*

[9] *D. Ormerod, D. Perry, P. Murphy (coord.)*, op. cit., p. 1277.

Pentru a se constata că există o suspiciune rezonabilă, organele de urmărire penală trebuie să fi efectuat verificări în această privință, decizia organului de urmărire penală neputându-se baza numai pe aspecte subiective[1].

Pentru a susține existența unei suspiciuni rezonabile, nu va fi necesar ca datele sau informațiile pe care se bazează organul de urmărire penală să aibă aceeași valoare probantă ca în cazul în care se urmărește obținerea condamnării unei persoane sau dispunerea trimiterii sale în judecată [2], standardul fiind unul mult mai scăzut[3]. De asemenea, existența unor temeiuri obiective pentru a susține posibilitatea formării unei suspiciuni rezonabile se va analiza în funcție de circumstanțele particulare ale fiecărei cauze.

În contextul supravegherii tehnice, pentru a exista o suspiciune rezonabilă, apreciem că, în analiza efectuată de judecătorul de drepturi și libertăți, acesta va trebui să se raporteze la el însuși pentru a determina dacă este îndeplinit acest standard de probă. Nu va avea importanță dacă organele de urmărire penală ar avea o suspiciune rezonabilă cu privire la săvârșirea infracțiunii, întrucât este necesară raportarea condițiilor legale la activitatea desfășurată de organul competent să autorizeze măsura, care va trebui să analizeze în mod imparțial asupra măsurii. Cu alte cuvinte, condiția existenței unei suspiciuni rezonabile formate în mintea judecătorului de drepturi și libertăți constituie o garanție împotriva ingerințelor nelegale aduse drepturilor fundamentale ale persoanei. Pentru ca această suspiciune rezonabilă să existe, este necesar ca ea să se poată forma pe baza experienței și percepției subiective asupra faptelor, realizată de judecătorul de drepturi și libertăți pe baza analizării elementelor obiective (date și informații) aflate la dosarul cauzei. Caracterul rezonabil presupune că, în formarea convingerii sale – implicit, și în motivarea încheierii de încuviințare –, judecătorul de drepturi și libertăți trebuie să ajungă prin procesul inferenței ca, din datele și informațiile prezentate, să conchidă că se poate să se fi săvârșit sau urmează să se săvârșească o infracțiune. Suspiciunea rezonabilă nu poate exista în lipsa unor acuzații formulate clar și cu privire la faptele determinate, neputându-se justifica o suspiciune rezonabilă prin acuzații cu caracter vag și care să nu poată fi încadrate juridic, răspundere care revine organelor de urmărire, dar, prin prisma căreia, judecătorul de drepturi și libertăți va trebui să decidă asupra îndeplinirii condiției legale[4].

În concluzie, apreciem că, în dreptul procesual penal român, pentru a se determina existența suspiciunii rezonabile cu privire la existența unei infracțiuni, judecătorul de drepturi și libertăți: va trebui să constate că există începută urmărirea penală cu privire la o infracțiune, că descrierea faptelor este una clară și că încadrarea juridică este una corectă, să aprecieze că există date și informații prezentate și că din acestea se poate concluziona, pe baza experienței judecătorului și a analizei datelor și informațiilor, că există o suspiciune cu privire la săvârșirea unei infracțiuni. Întrucât suspiciunea se va forma în mintea judecătorului de drepturi și libertăți, pe baza analizei datelor și informațiilor prezentate ce susțin o acuzație clară și credibilă în cauză, aceasta va constitui o suspiciune rezonabilă în sensul art. 139 alin. (1) lit. a) C.pr.pen.

---

[1] CEDO, cauza *Stepuleac c. Moldova*, Hotărârea din 6 februarie 2008, §73; cauza *Elci ș.a. c. Turcia*, Hotărârea din 24 martie 2004, §674, pe *hudoc.echr.coe.int*

[2] CEDO, cauza *Merabishvili c. Georgia*, Hotărârea din 28 noiembrie 2017, §184, pe *hudoc.echr.coe.int*

[3] *D. Ormerod, D. Perry, P. Murphy (coord.)*, op. cit., p. 1277.

[4] În acest sens, CEDO a constatat că formularea unor acuzații vagi și cu o încadrare juridică neclară nu poate justifica obținerea datelor privind tranzacțiile financiare ale unei persoane în cauza *Sommer c. Germania*, Hotărârea din 27 iulie 2017, §61. Jurisprudența este relevantă, întrucât condiția existenței unei suspiciuni rezonabile este prevăzută și în cazul acestei metode speciale de cercetare (anterior O.U.G. nr. 18/2015 – măsuri de supraveghere tehnică) prin dispozițiile art. 146[1] C.pr.pen.

§2. Problema desfășurării unei urmăriri penale proactive

Față de conținutul art. 139 alin. (1) lit. a) C.pr.pen., se recunoaște în mod universal că este posibilă folosirea supravegherii tehnice și într-o anchetă *proactivă*, având ca scop prevenirea săvârșirii unor infracțiuni grave. Această situație a fost criticată în literatura de specialitate ca putând fi considerată în opoziție cu principiul constituțional al legalității incriminării, dar fiindcă legislația penală consacră principiul neincriminării actelor pregătitoare, se impune ca, în cazul faptelor care nu cunosc incriminarea lor, să fie necesară existența unei suspiciuni rezonabile cu privire la punerea în executare a săvârșirii unei infracțiuni dintre cele menționate la art. 139 alin. (2) C.pr.pen.[1]. Chiar și în literatura de specialitate străină a fost observată tendința procesului penal de a adopta elemente proactive, statul trecând de la pedepsirea săvârșirii unor infracțiuni la identificarea persoanelor periculoase și privarea lor de libertate mai înainte de a prejudicia societatea[2]. Supravegherea tehnică oferă un mijloc seducător prin care se pot obține astfel de probe și se pot desfășura cercetări penale într-o asemenea manieră. Trebuie să recunoaștem că vor exista situații în care va fi foarte greu să se justifice o anchetă proactivă prin specificul infracțiunii. O atare situație nu credem că va fi posibilă, fiind chiar ilegală, din perspectiva argumentelor expuse de autorul citat, în cazul unei infracțiuni precum cea de viol.

Credem că problema ridicată, deși este una reală, trebuie să fie enunțată și din perspectiva respectării drepturilor fundamentale ale omului, în contextul unei continue dezvoltări a tehnologiei de supraveghere și implementarea acesteia pe scară largă. În vederea prevenirii infracțiunilor, pot fi adoptate măsuri care afectează grav viața privată a unei persoane, reușind în mod eficient să conducă la atingerea acestui scop (de pildă, supravegherea video permanentă a locurilor publice). Însă nu poate fi acceptată renunțarea sau restrângerea generalizată a dreptului la viață privată în vederea prevenirii generale de infracțiuni, putându-se ușor cădea în capcana unei supravegheri tehnice în masă a populației, cu consecința înfrângerii drepturilor și libertăților fundamentale ale persoanei. Problema este însă una mai complicată, întrucât supravegherea trebuie să se bazeze pe o suspiciune rezonabilă autentică mai înainte de autorizarea ei, astfel că nu va fi suficient să se urmărească o prevenție generală a infracțiunilor, ci trebuie să se cunoască dinainte că se pregătește săvârșirea unei infracțiuni determinate și că au fost efectuate acte pregătitoare[3].

§3. Infracțiunile pentru a căror urmărire se poate încuviința supravegherea tehnică

Astfel cum am arătat mai sus, nu este suficientă existența unei suspiciuni rezonabile cu privire la săvârșirea sau pregătirea săvârșirii unei infracțiuni, fiind obligatoriu ca aceasta să aibă o anumită gravitate abstractă, determinată de legiuitor în cuprinsul art. 139 alin. (2) C.pr.pen. Acest criteriu are două funcții: limitează posibilitatea autorizării supravegherii tehnice numai în cazul infracțiunilor considerate de legiuitor ca fiind de o gravitate sporită și prezintă într-un mod previzibil și clar care sunt faptele la care, dacă le-ar comite, ar trebui să aibă în vedere posibilitatea restrângerii dreptului la viață privată. Din perspectiva ultimei funcții, apreciem

[1] *Gh. Mateuț,* Procedură penală, 2019, p.679.

[2] *A. Ashworth, L. Zedner*, op. cit., p. 10; *T. Sorell,* Preventive Policing, Surveillance and European Counter-Terrorism, în Criminal Justice Ethics, vol. 30, no. 1/2011, pp. 2-3.

[3] Trib. Satu Mare, s. pen., sent. nr. 26/JDL din 12 aprilie 2017, pe *portal.just.ro*

că, prin art. 139 alin. (2) C.pr.pen. (alături și de alte dispoziții legale), se realizează respectarea art. 8 par. 2 Conv.EDO privind existența dispozițiilor legale care să acopere oricare posibilă restrângere a dreptului la viață privată.

Desigur, criteriul gravității legale abstracte se va completa cu cel al gravității concrete apreciate de organele judiciare prin prisma condiției proporționalității.

Referitor la infracțiunile care pot atrage utilizarea supravegherii tehnice, legiuitorul a prevăzut o listă exhaustivă de asemenea infracțiuni, nominalizându-le în cuprinsul art. 139 alin. (2) C.pr.pen., în concret, procedeul probatoriu putând fi utilizat în cazul: *infracțiunilor contra securității naționale prevăzute de Codul penal și de legi speciale, precum și în cazul infracțiunilor de trafic de droguri, de efectuare de operațiuni ilegale cu precursori sau cu alte produse susceptibile de a avea efecte psihoactive, infracțiunilor privind nerespectarea regimului armelor, muniților, materialelor nucleare, al materiilor explozive și al precursorilor de explozivi restricționați, de trafic și exploatarea persoanelor vulnerabile, acte de terorism, de spălare a banilor, de falsificare de monede, timbre sau de alte valori, de falsificare de instrumente de plată electronică, în cazul infracțiunilor care se săvârșesc prin sisteme informatice sau mijloace de comunicare electronică, contra patrimoniului, de șantaj, de viol, de lipsire de libertate în mod ilegal, de evaziune fiscală, în cazul infracțiunilor de corupție și al infracțiunilor asimilate infracțiunilor de corupție, infracțiunilor împotriva intereselor financiare ale Uniunii Europene*. Această listă exhaustivă este o reflecție a politicii penale a statului român, fiind evidențiate infracțiunile care prezintă cel mai înalt grad de risc pentru orânduirea socială contemporană. Dovada caracterului incoerent al politicii penale a statului este că în această listă sunt cuprinse și infracțiunile contra patrimoniului, dar și unele care pot fi cercetate numai la plângerea prealabilă a persoanei vătămate și trădând o gravitate mai redusă a faptei.

Remarcăm faptul că legiuitorul a inclus în cuprinsul acestei liste și *infracțiunile care se săvârșesc prin sisteme informatice sau mijloace de comunicare electronică*, astfel că gravitatea infracțiunii care poate atrage folosirea supravegherii tehnice nu este corelată în mod necesar cu limitele de pedeapsă și cu valoarea socială ocrotită, ci și cu *mijlocul de săvârșire*. Însă nu vom interpreta aceste dispoziții în sensul elementului laturii obiective, a *mijlocului* (instrumentului) de săvârșire a infracțiunii, deoarece textul art. 139 alin. (2) se referă la *infracțiuni care se săvârșesc*, și nu la infracțiuni săvârșite. Distincția este importantă, deoarece sensul presupune o condiție *a priori* față de săvârșirea unei infracțiuni, sugerând că mijlocul constituie un element constitutiv al respectivei infracțiuni, sfera de aplicare a supravegherii tehnice limitându-se numai la anumite infracțiuni. Astfel, nu este suficient ca infracțiunea să fie *in concreto* săvârșită prin sisteme informatice sau mijloace de comunicații electronice, ci este necesar ca această împrejurare să fie un element de tipicitate al infracțiunii. În mod corect arată și literatura de specialitate în același sens, cu privire la Codul de procedură penală anterior[1], că prevederea se referea la infracțiuni care aveau ca specific comiterea acestora prin mijloace de comunicare electronică. Sub acest aspect, criteriul legal este eterogen, întrucât mijlocul de săvârșire va influența criteriul de subsidiaritate a supravegherii tehnice. Ceea ce trebuia să fie avut în vedere este caracterul gravității abstracte a faptei. Într-o altă opinie, la care nu aderăm, s-a considerat că, în această situație, criteriul folosit de legiuitor este lipsit de previzibilitate, trebuind să fie interpretat în sensul în care se referă la infracțiunile contra siguranței și integrității sistemelor și datelor informatice prevăzute în Capitolul VI al Titlului VII din Codul penal, neputând fi

[1] *Gh. Mateuț*, Tratat, vol. II, 2012, pp. 225-226.

aplicabilă în cazul oricăror infracțiuni, indiferent de gravitatea acestora, care au fost comise prin sisteme informatice[1].

Legiuitorul a prevăzut și un criteriu subsidiar privitor la pedeapsa prevăzută de lege pentru a include orice infracțiune care ar fi de o anumită gravitate în sfera celor care pot justifica, sub aspectul criteriului de gravitate, dispunerea supravegherii tehnice. Prin teza ultimă a art. 139 alin. (2) C.pr.pen., supravegherea tehnică se poate dispune și *în cazul altor infracțiuni pentru care legea prevede pedeapsa închisorii de 5 ani sau mai mare*.

În mod just s-a arătat în doctrină faptul că dacă actele preparatorii ale unor infracțiuni sunt pedepsite, însă nu vor îndeplini ele însele condițiile prevăzute de art. 139 alin. (2) C.pr.pen., într-o asemenea situație, judecătorul de drepturi și libertăți va trebui să aibă în vedere gravitatea infracțiunii scop pentru a verifica îndeplinirea condiției gravității faptei[2].

Criteriul legiuitorului este unul insuficient de bine expus, întrucât extinde în mod nescuzabil posibilitatea încuviințării supravegherii tehnice la infracțiuni care nu justifică gravitatea ingerinței aduse vieții private a persoanei[3]. Deși legiuitorul instituie un criteriu subsidiar al pedepsei de cel puțin 5 ani pentru întrebuințarea metodelor speciale de supraveghere tehnică, se vor putea aplica astfel de măsuri maxim intruzive și în cazul infracțiunilor contra siguranței circulației pe drumurile publice, unde limita maximă de pedeapsă este, de regulă, de 5 ani[4]. Aceste infracțiuni sunt, la acest moment, cel mai des întâlnite; potrivit bilanțului Ministerului Public pe anul 2018[5], au fost trimise în judecată 22.047 de persoane, pentru comiterea unor asemenea fapte, dintr-un total de 58.737. Dacă vom aduna infracțiunile de furt (pentru care, în anul 2018, au fost trimise în judecată 8.053 de persoane) la infracțiunile contra siguranței circulației pe drumurile publice, vom ajunge la concluzia că majoritatea infracțiunilor săvârșite în România sunt infracțiuni pentru care se poate autoriza supravegherea tehnică. O atare situație este nefirească, *de lege ferenda*, impunându-se limitarea supravegherii tehnice la fapte pedepsite cu închisoare peste o limită superioară celei stabilite în prezent.

§4. Efectele schimbării încadrării juridice a faptei

În doctrină s-au ridicat probleme cu privire la legalitatea supravegherii tehnice atunci când măsura se autorizează pentru o faptă care ar intra sub incidența dispozițiilor art. 139 alin. (2) C.pr.pen., ulterior constatându-se că se impune schimbarea încadrării juridice a faptei într-una care nu ar mai permite autorizarea supravegherii tehnice. În prima opinie s-a susținut că probele obținute din supravegherea tehnică nu ar trebui să fie excluse, întrucât admisibilitatea supravegherii tehnice se va aprecia de judecător prin prisma datelor sau probelor existente la momentul autorizării, iar, prin natura lucrurilor, nu se pot contura cu precizie toate elementele

[1] *M. Udroiu*, Procedură penală, vol. I, 2019, p. 565.

[2] *C.M. Chiriță*, în N. Volonciu, A.S. Uzlău (coord.), Noul Cod, 2014, p. 311.

[3] *V. Pașca*, Principiul egalității armelor în procesul penal român – o realitate sau o ficțiune?, în Revista Universul Juridic nr. 8/2016, p. 8.

[4] Astfel, metoda specială de cercetare se va putea aplica următoarelor infracțiuni contra siguranței pe drumurile publice: punerea în circulație sau conducerea unui vehicul neînmatriculat [prevăzută de art. 334 alin. (2) C.pen.], conducerea unui vehicul fără permis de conducere [prevăzută de art. 335 alin. (1) C.pen.], conducerea unui vehicul sub influența alcoolului sau a altor substanțe (prevăzută de art. 336 C.pen.), refuzul sau sustragerea de la prelevarea de mostre biologice (prevăzută de art. 337 C.pen.), părăsirea locului accidentului ori modificarea sau ștergerea urmelor acestuia (prevăzută de art. 338 C.pen.), nerespectarea atribuțiilor privind verificarea tehnică ori efectuarea reparațiilor [prevăzută de art. 340 alin. (2) C.pen.].

[5] Raportul activității desfășurate de Ministerul Public în anul 2018, disponibil pe *www.mpublic.ro*

de fapt și de drept care țin de rezolvarea completă a cauzei penale[1]. În cea de-a doua opinie se apreciază că se va impune excluderea probelor obținute din două motive: *i)* dispozițiile art. 102 alin. (2) C.pr.pen. nu disting în funcție de cauza nelegalității, sancțiunea excluderii probelor fiind întemeiată pe principiul cauzalității obiective și a celei subiective; *ii)* impunerea unor condiții restrictive pentru supravegherea tehnică urmărește protecția vieții private, iar dacă s-ar admite validarea probelor, ar însemna să se permită implicit o eludare a regulii privitoare la folosirea unor metode intruzive în viața privată numai în cazul infracțiunilor de o anumită gravitate[2].

Considerăm că prima opinie este cea validă, însă nu putem fi de acord cu toate argumentele susținute. În opinia noastră, orice schimbare a încadrării juridice ulterioară efectuării supravegherii tehnice nu va influența legalitatea procedeului probatoriu, el fiind autorizat în mod legal raportat la încadrarea juridică inițială, fiindcă se leagă de noțiunea de „suspiciune rezonabilă", care presupune și o evaluare subiectivă din partea judecătorului de drepturi și libertăți. Datele și informațiile care sunt supuse analizei acestuia nu trebuie să se ridice la standardul probatoriu pentru dovedirea vinovăției, trebuind numai să justifice o suspiciune rezonabilă. Continuându-ne argumentele, nu va fi posibilă o analiză *a posteriori* decât prin raportare la elementele cauzei de la acel moment, impunându-se a se constata că, la momentul autorizării, încadrarea juridică era corect fundamentată[3] și astfel erau îndeplinite condițiile legale de autorizare. În același timp, dacă am accepta argumentele din cea de-a doua opinie, am putea ajunge la situația unei nulități ciclice care să afecteze însăși schimbarea de încadrare în cazul în care, pe baza probelor obținute din supravegherea tehnică, s-ar dispune schimbarea încadrării juridice[4].

O altă situație va fi incidentă dacă are loc o schimbare a încadrării juridice a faptei în timpul efectuării supravegherii tehnice; într-o atare împrejurare, considerăm că procurorul va fi obligat să dispună, conform art. 142 alin. (4) C.pr.pen., încetarea măsurii dacă noua încadrare nu mai permite utilizarea măsurilor de supraveghere tehnică, orice probă obținută după momentul schimbării încadrării juridice a faptei fiind nelegală.

Secțiunea a 3-a. Proporționalitatea măsurii luate cu restrângerea drepturilor persoanei

Proporționalitatea măsurii de supraveghere tehnică este cea mai importantă condiție legală pentru a se decide asupra luării oricărei măsuri de supraveghere tehnică. Credem că nu este numai o condiție specifică supravegherii tehnice, dar este una care trebuie să fie aplicată în cazul tuturor tehnicilor speciale de supraveghere sau cercetare. Nu este de omis propunerea

[1] C. Ap. Galați, s. pen. și pentru cauze cu minori, dec. pen. nr. 96/A/2013, *apud M. Bulancea, R. Slăvoiu*, în M. Udroiu (coord.), Codul de procedură penală, 2017, p. 664.

[2] *Ibidem*.

[3] În cazul în care nu era corectă, și la autorizarea supravegherii tehnice s-a omis acest lucru, atunci am fi de acord că supravegherea tehnică ar fi nelegală.

[4] De pildă, în urma supravegherii tehnice s-ar constata că infracțiunea nu va constitui șantaj, ci amenințare. Admițând că probele ar trebui excluse ca urmare a nelegalității supravegherii tehnice ar însemna că ordonanța de schimbare a încadrării juridice a faptei este și ea nelegală, întrucât se bazează determinant pe probele obținute din supraveghere tehnică, astfel că încadrarea juridică rămâne cea de șantaj și trebuie să se constate nulitatea actului prin care s-a constatat nulitatea actului de autorizare a supravegherii tehnice ș.a.m.d.

potrivit căreia proporționalitatea ar trebui să fie inserată, alături de principiile fundamentale ale dreptului procesual penal, în titlul preliminar al Codului de procedură penală, pentru a reflecta importanța sa deosebită în a găsi un just echilibru între interesul public și protecția intereselor private ale persoanei[1].

Proporționalitatea este o condiție prevăzută de art. 139 alin. (1) lit. b) C.pr.pen., stabilind că, pentru autorizarea supravegherii tehnice, trebuie ca „*măsura să fie proporțională cu restrângerea drepturilor și libertăților fundamentale, date fiind particularitățile cauzei, importanța informațiilor ori a probelor ce urmează a fi obținute sau gravitatea infracțiunii*".

Originea conceptului de „proporționalitate", folosit de legiuitor în această privință, este Convenția Europeană a Drepturilor Omului, unde la art. 8 par. 2 Conv.EDO[2] se instituie condiția ca măsura care aduce o atingere dreptului la viață privată să fie *necesară într-o societate democratică*. În realitate, expresia „necesar într-o societate democratică" vrea să sublinieze caracterul excepțional al măsurii care produce ingerința în viața privată și constituie fundamentul analizei criteriului de proporționalitate.

Într-o decizie mai veche a Curții Europene a Drepturilor Omului s-au stabilit principalele puncte de reper cu privire la ceea ce înseamnă „proporționalitate", stabilindu-se că sintagma „necesar într-o societate democratică" nu trebuie să fie înțeleasă în sensul de „util, rezonabil sau recomandabil", ci exprimă *o nevoie socială apăsătoare*, care justifică restrângerea dreptului la viață privată[3]. Această nevoie va fi determinată de la caz la caz și în funcție de scopul restrângerii drepturilor, dar și de natura activităților care vor conduce la această restrângere (de pildă, supravegherea tehnică). În orice caz, o restrângere a dreptului la viață privată va trebui să fie proporțională cu scopul urmărit, ținând seama de cele două aspecte fundamentale ale unei societăți democratice: toleranța și o deschidere în gândire[4]. În procesul de determinare a proporționalității unei restrângeri a dreptului la viață privată, este necesar a se analiza dacă motivele în baza cărora au fost impuse anumite măsuri erau relevante și suficiente față de scopul legitim urmărit[5].

În domeniul supravegherii tehnice folosite pentru combaterea criminalității, este recunoscută necesitatea existenței unui compromis, cel puțin în sistemul Convenției, între imperativul apărării societății democratice și drepturile individului[6]. Cu toate acestea, va fi necesar ca măsurile de supraveghere să fie restrânse la un minim absolut și ca autorizarea lor să se facă potrivit dispozițiilor legale incidente[7]. În niciun caz nu se va putea ca restrângerea unui drept să ducă la însăși negarea esenței acestuia[8].

---

[1] *Gh. Mateuț,* Procedură penală, 2019, p. 682.

[2] Conform art. 8 par. 2 Conv.EDO: „Nu este admis amestecul unei autorități publice în exercitarea acestui drept decât în măsura în care acest amestec este prevăzut de lege și dacă constituie o măsură care, într-o societate democratică, este necesară pentru securitatea națională, siguranță publică, bunăstarea economică a țării, apărarea ordinii și prevenirea faptelor penale, protejarea sănătății sau a moralei, ori protejarea drepturilor și libertăților altora".

[3] CEDO, cauza *Dudgeon c. Marea Britanie*, Hotărârea din 22 octombrie 1981, §51, pe *hudoc.echr.coe.int*

[4] *Ibidem*, §53.

[5] CEDO, cauza *Z. c. Finlanda*, Hotărârea din 25 februarie 1997, §94, pe *hudoc.echr.coe.int*

[6] CEDO, cauza *Klass ș.a. c. Germania*, Hotărârea din 6 septembrie 1978, §59, pe *hudoc.echr.coe.int*

[7] *Ibidem*.

[8] CEDO, cauza *Rees c. Marea Britanie*, Hotărârea din 17 octombrie 1986, §50, pe *hudoc.echr.coe.int*. În această cauză, deși plângerea reclamantului a fost respinsă ca nefondată, s-a stabilit că nu se poate ca un drept să fie restrâns astfel încât să fie afectată însăși esența sa, fiind practic negat. În cauză, Curtea a stabilit că nu este incidentă o negare a dreptului la viață privată, în condițiile în care dreptul englez nu permitea reclamatului, un transsexual, să se căsătorească cu o persoană care era de același sex biologic ca acesta.

Într-o decizie mai recentă, Curtea recunoaște că statele au dreptul să aprecieze asupra a ceea ce constituie o ingerință necesară într-o societate democratică, însă autoritățile vor trebui să demonstreze existența unei nevoi sociale apăsătoare pentru luarea măsurii[1]. Sub acest aspect, este deosebit de important ca orice autorizare a unei măsuri de supraveghere tehnică să fie temeinic motivată sub aspectul determinării celei mai adecvate metode speciale de supraveghere (dacă se și impune o asemenea măsură) pentru atingerea obiectivului urmărit[2].

Încercând să rezume condițiile impuse de Convenție asupra existenței unei proporționalități în restrângerea drepturilor fundamentale, doctrina străină a arătat că următorii factori au relevanță: *i)* dacă pentru luarea măsurii care restrânge dreptul au fost prezentate motive concludente și suficiente; *ii)* dacă exista o măsură mai puțin intruzivă, dar la fel de eficientă pentru a se realiza același obiectiv (acest criteriu se va analiza împreună cu cel al subsidiarității – n.n.); *iii)* dacă s-a acordat suficientă atenție drepturilor și intereselor persoanelor care ar urma să fie afectate de măsură; *iv)* dacă există garanții care să protejeze împotriva abuzurilor sau erorilor; *v)* dacă restrângerea dreptului nu distruge chiar esența dreptului prevăzut de Convenție[3].

În esență, testul de proporționalitate va trebui să aibă în vedere faptul că în balanță vor trebui puse atât interesele publice – cu gradul lor de importanță, prin raportare la infracțiunea cercetată, cât și gravitatea ingerinței aduse vieții private a persoanei. În jurisprudența Curții Constituționale a Africii de Sud s-a arătat: „*cu cât este mai profund interesul protejat și cu atât mai gravă încălcarea, cu atât controlul este mai strict; la sfârșitul zilei, instanța trebuie să decidă dacă, ținând cont de natura și intensitatea interesului de protejat și de gradul în care și de modul în care este încălcat, este admisă o ingerință*"[4].

După cum am menționat deja, cerința proporționalității se va lega indisolubil de celelalte condiții legale de autorizare, acestea fiind interconectate. S-a arătat astfel că, pentru întrunirea proporționalității, vor trebui să fie prezentate temeiuri concludente și suficiente pentru a justifica o ingerință, aceasta trebuind să se bazeze pe anumite împrejurări pentru a cere autorizarea unei măsuri de supraveghere tehnică. Acest aspect reprezintă legătura proporționalității cu prima condiție a autorizării – *existența unei suspiciuni rezonabile cu privire la săvârșirea unei infracțiuni*. Gradul de certitudine privind săvârșirea respectivei infracțiuni, dar mai ales temeiurile de fapt din care rezultă că supravegherea tehnică va conduce la obținerea de probe în procesul penal vor fi cântărite și puse în balanță cu natura dreptului restricționat, gravitatea ingerinței aduse, importanța elementului de interes public privind măsura și contextul în care are loc[5]. Concludența și suficiența temeiurilor care justifică supravegherea tehnică vor trebui să fie cu atât mai mari atunci când, prin supravegherea tehnică, sunt aduse ingerințe aspectelor intime din viața unei persoane[6] sau se vrea restrângerea secretului profesional al avocatului[7].

Ceea ce trebuie înțeles din cele arătate mai sus este că proporționalitatea nu va fi influențată numai de criteriile stabilite de legiuitorul român la art. 139 alin. (1) lit. b) C.pr.pen., ci și de existența unei suspiciuni rezonabile suficient de bine conturate pentru a justifica ingerința

[1] CEDO, cauza *Piechowicz c. Polonia*, Hotărârea din 17 aprilie 2012, §212, pe *hudoc.echr.coe.int*

[2] *Gh. Mateuț,* Procedură penală, 2019, p. 681.

[3] *D. Ormerod, D. Perry, P. Murphy (coord.)*, op. cit., p. 136.

[4] Curtea Constituțională a Africii de Sud, cauza *Coetzee c. Guvernul Africii de Sud*, Dec. din 22 septembrie 1995, §45, pe *www.saflii.org*

[5] *S. McKay*, Covert Policing, 2015, p. 52.

[6] CEDO, cauza *Dudgeon c. Marea Britanie*, Hotărârea din 22 octombrie 1981, §61.

[7] CEDO, cauza *Silver ș.a. c. Marea Britanie*, Hotărârea din 25 martie 1983, §105, pe *hudoc.echr.coe.int*

adusă, dar și de lipsa unei măsuri mai puțin restrictive care să conducă la același rezultat. Cu alte cuvinte, neîntrunirea oricăreia dintre condițiile legale prevăzute de art. 139 alin. (1) C.pr. pen. va determina și lipsa de proporționalitate a măsurii, aceasta fiind problema esențială în autorizarea supravegherii tehnice.

Încercând să adapteze cerința proporționalității în Codul de procedură penală din 2010, legiuitorul a impus condiția *proporționalității măsurii cu restrângerea drepturilor și libertăților fundamentale* prin raportare la câteva criterii enumerate în mod limitativ. Această condiție este prevăzută de art. 139 alin. (1) lit. b) C.pr.pen. și se impune a fi analizată de judecătorul de drepturi și libertăți prin prisma criteriilor prevăzute de textul de lege: *particularitățile cauzei*, *importanța informațiilor ori a probelor ce urmează a fi obținute sau gravitatea infracțiunii*.

Proporționalitatea trebuie analizată atât raportat la supravegherea tehnică în întregime, cât și cu privire la măsurile concrete de supraveghere tehnică ce sunt solicitate prin propunerea procurorului. S-a apreciat că va fi incorect a se solicita și autoriza fără distincție, față de particularitățile cauzei, toate măsurile de supraveghere tehnică prevăzute la art. 138 alin. (1) lit. a)-d) C.pr.pen.[1]. O atare situație ar prejudicia în mod grav drepturile fundamentale ale persoanei față de care s-ar lua măsura de supraveghere tehnică.

Cel mai important aspect va fi ca analiza judecătorului de drepturi și libertăți să privească măsurile de supraveghere concret propuse, întrucât aceeași măsură generală (astfel cum ele sunt menționate în Cod) poate genera ingerințe asupra vieții private de diferite gravități, în funcție de modalitatea lor concretă. Astfel, judecătorul de drepturi și libertăți va trebui să dispună, de pildă, asupra proporționalității supravegherii video a locului de muncă al unei persoane ori a interiorului domiciliului acestei persoane, cele două situații fiind complet diferite raportat la întinderea restrângerii dreptului la viață privată. În același timp, nici accesul la un sistem informatic nu va fi proporțional în situația în care o persoană este urmărită penal pentru reproducerea de programe informatice fără drept, în condițiile în care un alt procedeu probatoriu, percheziția informatică, ar fi suficient și proporțional pentru stabilirea stării de fapt.

Prin „particularitățile cauzei" vom înțelege acele împrejurări specifice unei anumite cauze penale care vor impune utilizarea supravegherii tehnice pentru soluționarea cauzei, deoarece un altfel de mijloc nu ar fi propice pentru a stabili starea de fapt. De exemplu, în cazul infracțiunii de constituire a unui grup infracțional organizat, prevăzută de art. 367 C.pen., poate fi necesară măsura, raportat la particularitățile cauzei, constând în modul de operare și modul de interacționare a membrilor grupului, care ar evita să se întâlnească în locuri publice sau să aibă vreo interacțiune care să poată fi observată public. Într-o asemenea situație, este posibil ca administrarea probelor să nu poată fi făcută prin audierea persoanelor. O situație de speță[2] poate consta în constituirea unui grup infracțional organizat pe criterii etnice (toți participanții fiind de origine vietnameză), astfel că însuși elementul care îi unește face dificilă interacțiunea lor cu alte persoane și descoperirea motivelor ulterioare, impunându-se folosirea supravegherii video, audio sau prin fotografiere, precum și utilizarea investigatorilor sub acoperire, în mod concomitent, pentru identificarea unor persoane de legătură ale grupării, precum și stabilirea ierarhiei în cadrul grupului.

[1] *M. Bulancea, R. Slăvoiu*, în M. Udroiu (coord.), Codul de procedură penală, 2017, p. 664.

[2] C. Ap. Timișoara, dec. pen. nr. 205/A din 23 octombrie 2013, pronunțată în dosar nr. 5502/108/2013, nepublicată.

Totodată, proporționalitatea va trebui să fie analizată și prin raportare la modalitățile concrete de săvârșire a infracțiunii[1]. O altă infracțiune în care particularitățile cauzei pot impune măsuri de supraveghere tehnică este *luarea de mită*, prevăzută de art. 289 C.pen., unde adeseori se folosesc înregistrările ambientale pentru a surprinde momentul primirii de bani sau alte foloase. În același timp, în cazul aceleiași infracțiuni, se va putea stabili, pe baza interceptării convorbirilor telefonice, că o persoană ar fi remis unui funcționar public un sejur la un hotel de lux din stațiunea Mamaia atunci când funcționarul public încearcă să se cazeze, dar nu cunoaște exact hotelul, rezervarea fiind făcută de mituitor care îi comunică prin telefon hotelul și locația acestuia[2]. Într-o altă situație, așa cum s-a arătat în literatura de specialitate, în cazul infracțiunilor informatice, va fi „mai previzibil" că va fi folosit *accesul la un sistem informatic* decât orice alt mijloc de supraveghere tehnică[3]. Remarcăm faptul că, în ultima perioadă de timp, în cazul infracțiunilor de corupție, se utilizează adeseori percheziția informatică, fiind previzibil ca pe viitor să se apeleze și la accesul la un sistem informatic.

Prin „importanța informațiilor ori a probelor ce urmează a fi obținute" înțelegem contribuția pe care o pot avea informațiile sau probele obține pentru stabilirea împrejurărilor esențiale ale cauzei. Ca atare, considerăm că proporționalitatea trebuie stabilită raportat la utilitatea probei ce urmează a fi obținută și în funcție de împrejurarea concretă care se urmărește a se dovedi. De pildă, nu va fi proporțională măsura supravegherii tehnice a interceptării comunicațiilor soției persoanei bănuite de săvârșirea unei infracțiuni în măsura în care săvârșirea acesteia nu are legătură cu soția. Însă va fi proporțională măsura în cazul în care soția deține calitatea de judecător și obiectul urmăririi penale îl constituie infracțiunea de trafic de influență (funcționarul traficat fiind soția autorului infracțiunii de trafic de influență). Menționăm acest exemplu, deoarece interceptarea convorbirilor unor persoane care au o legătură particulară precum cea arătată mai sus va impune justificări temeinice cu privire la importanța informațiilor și probelor care vor putea fi obținute.

Importanța informațiilor ori a probelor ce urmează a fi obținute prin supraveghere tehnică trebuie să fie cunoscută de la momentul formulării propunerii de autorizare, sub acest aspect, neputându-se justifica o prelungire a supravegherii tehnice odată ce acestea au fost obținute[4]. Desigur, situația poate fi cea contrară, ca din probele obținute din supravegherea tehnică să rezulte faptul că pot fi obținute noi probe importante prin continuarea măsurii cu privire la faptele cercetate. Chiar dacă există temei pentru restrângerea în acest mod a dreptului la viață privată al unei persoane, este important ca organele judiciare să nu depășească ceea ce este strict necesar pentru a obține rezultatul urmărit[5].

Sub aspectul rezultatului potențial al supravegherii tehnice, va trebui să se facă și o distincție între probele directe care pot fi obținute și probele indirecte, primele având o importanță de necontestat în procesul penal și putând justifica o ingerință mai mare în viața privată a unei persoane. Momentul la care se va desfășura supravegherea tehnică va fi unul important, întrucât, după consumarea unei infracțiuni, obținerea de probe prin supraveghere tehnică tinde să scadă, iar acestea vor căpăta un caracter ambiguu. Acest lucru nu înseamnă că dacă există suspiciuni privind repetarea comportamentului sau continuarea lui nu se vor putea

[1] *Gh. Mateuț*, Procedură penală, 2019, p. 681.
[2] ICCJ, s. pen., dec. nr. 347 din 29 octombrie 2014, în dosar nr. 812/46/2009*, nepublicată.
[3] *C.M. Chiriță*, în N. Volonciu, A.S. Uzlău (coord.), Noul Cod, 2014, p. 312.
[4] *C. Harfield, K. Harfield*, Covert Investigation, 2018, p. 29.
[5] *S. McKay*, Covert Policing, 2015, p. 51.

lua măsuri, de exemplu, în cazul infracțiunilor privind traficul și consumul ilicit de substanțe interzise.

Utilitatea maximă a supravegherii tehnice va fi atunci când ea se află în executare concomitent cu săvârșirea infracțiunii sau, după natura faptei, la momentul la care se realizează una dintre acțiunile alternative incriminate (de pildă, situație incidentă în cazul infracțiunii de luare de mită).

„Gravitatea infracțiunii" presupune, în opinia noastră, o analiză a pericolului social concret pe care îl presupune săvârșirea infracțiunii care face obiectul urmăririi penale. Deși gravitatea unei infracțiuni se manifestă în limitele de pedeapsă prevăzute de lege, ca pericol social abstract[1], considerăm că acest criteriu a fost avut în vedere de legiuitor în privința supravegherii tehnice în cazul art. 139 alin. (2) C.pr.pen. Astfel, se va impune analizarea proporționalității sub aspectul gravității concrete care justifică o anumită măsură de supraveghere tehnică și dacă aceasta justifică o anumită ingerință în viața privată a unei persoane[2].

De exemplu, fapta funcționarului public din cadrul unei Direcții Generale Regionale a Finanțelor Publice de a calcula impozitul pe profit al unei societăți la un nivel superior celui real, obținând un avantaj patrimonial în favoarea statului, va constitui infracțiunea de abuz în serviciu prevăzută de art. 297 C.pen., cu aplicarea art. 13[2] din Legea nr. 78/2000[3], însă, raportat la gravitatea faptei, nu se va impune supravegherea video sau audio-video a locuinței sale ori interceptarea comunicațiilor acestei persoane. În schimb, în cazul faptei unui Președinte al Consiliului Județean, care, în exercitarea atribuțiilor de serviciu, propune un proiect de hotărâre al Consiliului Județean prin care s-ar restructura o regie autonomă aflată în subordine, în scopul de a se răzbuna împotriva persoanelor din conducerea acesteia, ar constitui infracțiunea de abuz în serviciu în formă simplă, însă cu toate acestea ar fi proporțională, pentru dovedirea elementului intențional, *interceptarea comunicațiilor acestuia*. În prima situație, gravitatea faptei trebuie raportată la modalitatea de săvârșire a faptei, precum și la importanța atribuțiilor de serviciu ale funcționarului public care stabilește un nivel de impozite în mod nelegal. În cea de-a doua situație, gravitatea faptei se va raporta și la calitatea subiectului activ, a acțiunii sale concrete, a mobilului, precum și la paguba pe care le poate produce săvârșirea acestei infracțiuni.

Chiar dacă legiuitorul a prevăzut posibilitatea autorizării supravegherii tehnice în cazul unora dintre infracțiunile contra siguranței circulației pe drumurile publice [prin raportare la limitele de pedeapsă, art. 139 alin. (2) teza a II-a C.pr.pen.], gravitatea unor asemenea fapte nu o va putea justifica. Chiar dacă recunoaștem că o conducere a unui autovehicul cu număr fals de înmatriculare [art. 334 alin. (2) C.pen.] poate, prin limitele de pedeapsă, să justifice supravegherea tehnică, gravitatea concretă a faptei nu justifică o ingerință în viața privată a persoanei. Cu alte cuvinte, interesul public în cazul acestei infracțiuni nu este unul așa de apăsător încât să justifice supravegherea, simplul act de conducere pe drumurile publice nu pune în pericol ceilalți participanți la trafic.

[1] *M. Basarab*, Drept penal. Partea generală, vol. I, ed. a IV-a, revăzută și adăugită, Ed. Lumina Lex, București, 2002, p. 140.

[2] *L. Zedner*, Seeking Security by Eroding Human Rights: The Side-stepping of Due Process, în B.J. Goold, L. Lazarus (coord.), op. cit., p. 258.

[3] Publicată în M. Of. nr. 219 din 18 mai 2000.

Secțiunea a 4-a. Subsidiaritatea (imposibilitatea obținerii probelor prin folosirea altor procedee probatorii)

A treia condiție de fond impusă de Codul de procedură penală pentru dispunerea supravegherii tehnice este *necesitatea procedeului probatoriu* pentru obținerea probei. Cu alte cuvinte, condiția se referă la *subsidiaritatea*[1] măsurilor de supraveghere tehnică față de orice alt procedeu probatoriu. Această condiție este prevăzută în cuprinsul art. 139 alin. (1) lit. c) C.pr.pen. și limitează folosirea metodelor speciale de supraveghere, cu excepția cazurilor în care *probele nu ar putea fi obținute în alt mod sau obținerea lor ar presupune dificultăți deosebite ce ar prejudicia ancheta ori există un pericol pentru siguranța persoanelor sau a unor bunuri de valoare*. În realitate există două situații prevăzute, în care se poate considera ca fiind necesară autorizarea mijloacelor de supraveghere tehnică: imposibilitatea (absolută sau relativă) obținerii probelor în alt mod și existența unui pericol pentru siguranța persoanei sau a unor bunuri de valoare. În doctrină s-a opinat că legiuitorul a cuprins în art. 139 alin. (1) lit. c) C.pr.pen. trei criterii – subsidiaritatea propriu-zisă, obținerea cu dificultate a probelor în alt mod și existența unui pericol pentru unele valori sociale, numai imposibilitatea absolută a probei reflectând condiția subsidiarității, considerându-se că celelalte două criterii permit dispunerea unor măsuri de supraveghere tehnică în toate cazurile, nu doar în mod excepțional[2]. Nu putem fi cu totul de acord cu această opinie decât în ceea ce privește ultimul criteriu – existența unui pericol pentru siguranța persoanelor sau a unor bunuri de valoare, care nu se justifică în cazul supravegherii tehnice și conduce la o extindere nepermisă a măsurii. Ceea ce mai trebuie apreciat în opinia menționată este că se remarcă în mod corect că aceste criterii sunt *alternative* și că numai primul exprimă condiția subsidiarității[3].

În cazul primului criteriu prevăzut de legiuitor, necesitatea supravegherii tehnice este determinată de imposibilitatea obținerii probei în orice alt mod, adică prin utilizarea unui alt procedeu probatoriu care să nu aducă o ingerință sau să lezeze mai puțin drepturile fundamentale ale persoanei. Prin aceasta, legiuitorul a vrut să sublinieze caracterul excepțional al supravegherii tehnice, impunându-se a fi folosit numai în situațiile în care proba nu ar putea fi obținută prin mijloace mai puțin intruzive, precum procedeele probatorii clasice. Prin această prevedere, legiuitorul subliniază faptul că în cursul urmăririi penale trebuie folosite, ca regulă, alte mijloace mai puțin intruzive dacă ele sunt apte să conducă la aceleași rezultate[4]. De pildă, supravegherea audio-video a unei persoane va putea fi autorizată numai dacă audierea acesteia în calitate de martor nu ar releva aceleași probe și nu există date sau informații că ar avea un interes în ascunderea adevărului. Această abordare a legiuitorului nu este nouă, fiind reglementată și în situația percheziției domiciliare, care va fi subsidiară predării obiectelor, înscrisurilor sau a datelor informatice. Ea este avută în vedere ca un criteriu și în alte state, doctrina americană subliniind fie că au fost folosite alte procedee probatorii și nu au dat rezultate, fie că nu sunt disponibile alte procedee probatorii[5]. Condiția subsidiarității nu va obliga organele de urmărire penală să încerce să obțină probe prin procedee probatorii mai

[1] *Gh. Mateuț*, Observații critice privind noua reglementare a supravegherii tehnice într-o prezentare comparativă, în Caiete de Drept Penal nr. 3/2015, p. 24.

[2] *Idem,* Procedură penală, 2019, p. 683.

[3] *R.A. Popa*, op. cit., pp. 178-179.

[4] *M. Udroiu, O. Predescu*, Protecția europeană, 2008, p. 829.

[5] *D.E. Hall*, Criminal Law and Procedure, Fifth Edition, Ed. Delmar Cengage, New York, 2009, p. 408.

puțin intruzive, fiind suficient ca ele să fi fost avute în vedere de acestea și că organele de urmărire penală furnizează motive pentru care ele să nu poată fi folosite[1]. Sub acest ultim aspect, credem că abordarea jurisprudenței engleze este corectă și subliniază atât nevoia procurorului de a-și motiva în mod temeinic propunerea, cât și ca judecătorul de drepturi și libertăți să motiveze expres de ce un alt procedeu probatoriu mai puțin intruziv nu era apt să fie folosit.

Dacă există o alternativă care va putea aduce o ingerință mai restrânsă drepturilor fundamentale ale persoanei, atunci nefolosirea acesteia conduce la neîndeplinirea condiției subsidiarității și la lipsa de proporționalitate în autorizarea supravegherii tehnice, cu consecința nelegalității actului de autorizare și a mijloacelor de probă obținute. Într-un exemplu prezentat în doctrină, „*acțiunile luate pentru prevenirea unei fapte ilicite pot fi îndreptate față de săvârșirea unui omor sau pentru săvârșirea unei contravenții de parcare: greutatea fiecăreia dintre aceste fapte, comparat cu dreptul fundamental care va fi limitat, nu este aceeași*"[2].

În analiza condiției subsidiarității, va trebui să avem în vedere dacă metodele speciale de supraveghere sau cercetare nu vor avea grade de intruziune diferite și dacă una dintre acestea nu este aptă să conducă la obținerea de probe într-un mod care să fie în acord cu stricta limitare a ingerințelor asupra drepturilor fundamentale ale persoanei. În cauza *Campbell c. Marea Britanie*[3], Curtea Europeană a Drepturilor Omului a stabilit că a constituit o încălcare a dreptului la viață privată deschiderea întregii corespondențe a deținuților pentru a se verifica dacă nu conține obiecte sau substanțe interzise, inclusiv corespondența dintre reclamant cu avocatul său și cu Curtea. Astfel, în respectiva cauză se impunea ca numai o parte din corespondență să fie controlată, apreciind ca nefondate susținerile statului privind necesitatea verificării inclusiv a corespondenței cu Curtea – cea care era trimisă, dar și cea care era primită –, deoarece riscul la care ar fi fost expus sistemul penitenciar ar fi fost unul neglijabil prin raportare la acest tip de corespondență[4].

În ceea ce privește situația în care obținerea probei prin utilizarea unui alt mijloc de probă ar aduce serioase impedimente anchetei, situația trebuie să fie nuanțată. Considerăm că simpla celeritate a desfășurării procesului penal nu poate justifica apelarea la supravegherea tehnică ca o soluție pentru obținerea facilă de probe. Sensul dispozițiilor legale privind autorizarea măsurilor de supraveghere tehnică este cel de utilizare a acestor mijloace doar în situația în care proba s-ar obține în condiții dificile, printr-un efort deosebit al organelor de urmărire penală. Este adevărat că o atare prevedere prezintă pericolul unui abuz din partea organelor de urmărire penală, socotindu-se în mod ușuratic că un alt procedeu probatoriu ar presupune dificultăți deosebite, prin simpla invocare a riscului prejudicierii anchetei[5]. Problema este una reală, însă nu credem că vina este cea a legiuitorului, ci s-ar impune un mai bun control asupra autorizării, de către judecătorul de drepturi și libertăți, a măsurilor de supraveghere tehnică în aceste situații, pentru a se evita orice posibil abuz. Dacă va exista un pericol deosebit ca obținerea unei probe să fie prejudiciată și această situație nu a fost generată intenționat sau din neglijența organelor de urmărire penală, credem că va trebui să fie socotită ca îndeplinită condiția subsidiarității măsurii.

---

[1] EWCA, cauza *R. c. Mason și alții*, Dec. din 13 februarie 2002, [2002] EWCA Crim 385, pe *www.bailii.org*

[2] *D.J. Harris, M. O'Boyle, C. Warbrick*, Law of the European Convention on Human Rights, Ed. Butterworths, 1995, p. 297, *apud S. McKay*, Covert Policing, 2015, p. 53.

[3] CEDO, cauza *Campbell c. Marea Britanie*, Hotărârea din 25 martie 1992, §52-63, pe *hudoc.echr.coe.int*

[4] *Ibidem*, §62.

[5] *Gh. Mateuț,* Procedură penală, 2019, p. 683.

În cazul celui de-al doilea criteriu, se prevede utilizarea mijloacelor de supraveghere tehnică în cazul în care există un *pericol pentru siguranța persoanelor sau pentru unele bunuri de valoare*. Necesitatea ar fi dată de însăși valoarea socială ocrotită de infracțiunea care se urmărește a fi săvârșită. În acest caz vom putea fi numai în situația unei anchete proactive, în care se urmărește prevenirea săvârșirii unei infracțiuni, nu și a strângerii de probe privind o infracțiune deja săvârșită. Acest lucru reiese din înseși valorile sociale determinate generic (siguranța persoanei, incluzând viața, integritatea fizică a persoanei și libertatea persoanei) față de care nu poate exista *un pericol* în măsura în care infracțiunile respective sunt deja consumate. Credem că acest criteriu este introdus în mod tendențios, întrucât pare a nu justifica strângerea de probe prin metode speciale de supraveghere, ci realizarea unor activități specifice de înlăturare a pericolului pentru valorile sociale ocrotite. În situația prevăzută de Cod, însăși lipsa de acțiune din partea organelor de urmărire penală menține starea de pericol existentă pentru a fi strânse probe. În mod corect s-a apreciat că includerea unui astfel de criteriu poate conduce numai la abuzuri față de care apărarea nu se poate apăra[1]. În ceea ce ne privește, credem că legiuitorul a oferit, prin această condiție, posibilitatea procurorului de a eluda condiția subsidiarității, întrucât, în cazul existenței pericolului pentru valorile sociale protejate, se va corela cu prima condiție de fond pentru autorizarea măsurii: existența unei suspiciuni rezonabile cu privire la pregătirea (în acest caz) unei infracțiuni, ceea ce contravine art. 8 par. 2 Conv.EDO. Astfel cum am arătat deja, pentru restrângerea dreptului la viață privată, măsura *trebuie să fie necesară într-o societate democratică*, condiție care nu poate fi îndeplinită atunci când criteriul proporționalității este văduvit de subsidiaritate, chiar dacă se pun în balanță unele valori sociale. Acest lucru ar însemna ca atunci când siguranța unei persoane este pusă în pericol sau este pus în primejdie un bun de valoare (un termen vag, neclar și care vine în contradicție cu principiul legalității), nu va fi obligatoriu ca supravegherea tehnică să constituie singurul procedeu probatoriu de strângere a probelor în procesul penal. Or, a admite această posibilitate va conduce în mod automat la lipsa proporționalității măsurii luate.

În ceea ce ne privește, apreciem că autorizarea supravegherii tehnice în contextul invocării existenței unui pericol pentru siguranța persoanelor sau a unor bunuri de valoare va constitui o ingerință disproporționată în viața privată, *de lege ferenda*, impunându-se abrogarea acestui criteriu alternativ.

Secțiunea a 5-a. Autorizarea supravegherii tehnice a persoanei vătămate, la cererea acesteia

Excepția de la toate condițiile arătate în secțiunile anterioare este prevăzută de art. 140 alin. (9) C.pr.pen. și se referă la interceptarea ori înregistrarea comunicațiilor ori a oricărui alt tip de comunicări efectuate de persoana vătămată, atunci când aceasta formulează o cerere motivată adresată procurorului. Judecătorul de drepturi și libertăți va putea dispune încuviințarea măsurii de supraveghere tehnică prevăzută de art. 138 alin. (1) lit. a) C.pr.pen. fără a mai avea în vedere condițiile prevăzute de lege în cazul supravegherii tehnice prin care măsura se poate autoriza numai în cazul urmăririi penale doar cu privire la săvârșirea anumitor infracțiuni. În opinia noastră, în afară de condițiile prevăzute de art. 139 alin. (2)

[1] *Ibidem*.

C.pr.pen., va trebui să fie îndeplinite condițiile privind existența unei suspiciuni rezonabile, condiția proporționalității și cea a subsidiarității.

În această situație excepțională, observăm faptul că însăși persoana vătămată este cea care consimte la restrângerea dreptului său la o viață privată, astfel că ingerința din partea statului este una acceptată de aceasta în vederea dovedirii săvârșirii unor infracțiuni și a protejării intereselor acesteia. Reamintim faptul că persoana vătămată este îndreptățită să recurgă la înregistrarea convorbirilor sale telefonice ori a celorlalte comunicări efectuate de aceasta cu făptuitorul, însă nu deține mijloacele tehnice necesare pentru a face acest lucru[1]. În același timp, arătăm faptul că eficiența utilizării acestui procedeu probatoriu este mult mai bună decât folosirea unor mijloace proprii de către persoana vătămată, fiind preferabil din acest punct de vedere.

Din textul art. 140 alin. (9) C.pr.pen. reiese că se va realiza o interceptare a comunicațiilor sau comunicărilor *efectuate* de persoana vătămată, formulare deficitară din punctul nostru de vedere, deoarece nu rezultă suficient de clar cine inițiază comunicarea. Un atare amănunt este deosebit de important, întrucât prezintă pericolul folosirii persoanei vătămate pentru provocarea unei infracțiuni, ceea ce este interzis de lege, conform art. 101 alin. (3) C.pr.pen. Organele judiciare vor trebui să acorde o maximă atenție din partea cui vine intenția săvârșirii unei infracțiuni, iar dacă persoana vătămată va fi cea care inițiază săvârșirea infracțiunii, proba obținută va fi neloială. Prin acțiunile sale, persoana vătămată determină săvârșirea infracțiunii, existând o provocare realizată de un particular.

Ne rezervăm anumite critici privind compatibilitatea acestei modalități de autorizare cu art. 8 par. 2 Conv.EDO, întrucât pare că exclude controlul de proporționalitate al judecătorului de drepturi și libertăți prin raportare la gravitatea abstractă a infracțiunii. Chiar și înregistrările private, efectuate de părți, situație similară cu aceasta, trebuie să fie analizate sub aspectul proporționalității lor, cu respectarea dreptului la viață privată al persoanei vizate. În plus, autorizarea unei măsuri de supraveghere tehnică, la cererea persoanei vătămate, trebuie privită cu o oarecare circumspecție dacă aceasta nu este fundamentată pe probe, întrucât persoana vătămată are un interes procesual propriu, existând riscul ca, prin autorizarea supravegherii tehnice, persoana vătămată să acționeze ca un agent al statului în cadrul unei infracțiuni provocate.

[1] De exemplu, unele telefoane mobile dețin capacitatea de a înregistra automat toate apelurile primite sau efectuate. Telefoanele marca Asus au această posibilitate, fiind dotate din fabricație cu software-ul necesar pentru a face aceste înregistrări.

Capitolul II
Aspecte procedurale privind autorizarea metodelor speciale de supraveghere tehnică

Secțiunea 1. Propunerea autorizării folosirii metodelor speciale de supraveghere tehnică

Întrucât urmărirea penală constituie o fază procesuală aflată sub controlul procurorului, Codul de procedură penală a instituit regula că el are rolul decizional suprem asupra administrării probelor. Supravegherea tehnică fiind un procedeu probatoriu, numai procurorul este în măsură să decidă dacă se impune administrarea probelor care ar putea rezulta din acesta. Cu toate acestea, în cazul metodelor speciale de supraveghere, ca urmare a necesității autorizării și controlului măsurii de către o autoritate independentă[1], autorizarea se va face de către judecătorul de drepturi și libertăți, la propunerea procurorului. Ținând seama de analiza condițiilor de fond analizate în secțiunile anterioare, nu putem să afirmăm că doar procurorul va aprecia asupra relevanței și necesității probei care se dorește administrată prin supravegherea tehnică, ci însuși judecătorul de drepturi și libertăți va trebui, în controlul său de proporționalitate (prin raportare la seriozitatea suspiciunii rezonabile, la proporționalitatea propriu-zisă a restrângerii drepturilor fundamentale față de probele care ar putea fi obținute și subsidiaritatea supravegherii tehnice față de alte procedee probatorii), să aprecieze asupra îndeplinirii condițiilor probei. Această situație nu îi dă dreptul judecătorului de drepturi și libertăți să se sesizeze din oficiu cu privire la autorizarea supravegherii tehnice, putând doar să cenzureze o propunere a procurorului, formulată cu nerespectarea condițiilor legale.

Pentru a exista procedura de autorizare a supravegherii tehnice, procurorul trebuia să ia inițiativa de a sesiza judecătorul de drepturi și libertăți în vederea încuviințării procedeului probatoriu. Acest drept este unul exclusiv al procurorului, astfel cum acesta este prevăzut de art. 55 alin. (3) lit. b) C.pr.pen., el neputând fi exercitat de către organele de cercetare penală. Desigur, în măsura în care organul de cercetare penală consideră că se impune supravegherea tehnică a unei persoane, poate formula, prin referat, o propunere în acest sens procurorului care, mai apoi, poate formula propunerea către judecătorul de drepturi și libertăți.

În mod excepțional, procurorul va putea autoriza provizoriu supravegherea tehnică, pentru o durată de maximum 48 de ore, cu controlul ulterior exercitat de judecătorul de drepturi și libertăți. Întrucât aceasta constituie o procedură distinctă, excepțională, o vom trata distinct în prezenta lucrare[2]. Fără a intra în detalii, apreciem că autorizarea provizorie de către procuror a supravegherii tehnice este o procedură viciată sub aspectul constituționalității sale și, în lumina jurisprudenței Curții Europene a Drepturilor Omului mai recente, apreciem că nu își va mai putea găsi locul în procesul penal.

---

[1] CEDO, cauza *Roman Zakharov c. Rusia*, Hotărârea din 4 decembrie 2015, §233; cauza *Irfan Güzel c. Turcia*, Hotărârea din 7 mai 2017, §96; cauza *Klass ș.a. c. Germania*, Hotărârea din 6 septembrie 1978, §56, pe *hudoc.echr.coe.int*

[2] *V. infra*, Titlul III, Capitolul II.3.

În privința dispunerii supravegherii tehnice de către *judecătorul de drepturi și libertăți*, procedura este prevăzută de art. 140 C.pr.pen. și impune, mai întâi, verificarea respectării condițiilor prevăzute de art. 139 C.pr.pen. Această verificare se face pe baza propunerii depuse de către procuror și în urma verificării dosarului cauzei, care va fi înaintat de către procuror împreună cu cererea prin care solicită să se dispună supravegherea tehnică. În cuprinsul propunerii, procurorul trebuie să includă toate elementele prevăzute de art. 140 alin. (2) teza I C.pr.pen., respectiv: „*indicarea măsurilor de supraveghere tehnică care se solicită a fi dispuse, numele sau alte date de identificare a persoanei împotriva căreia se dispune măsura, dacă sunt cunoscute, indicarea probelor ori a datelor din care rezultă suspiciunea rezonabilă cu privire la săvârșirea unei infracțiuni pentru care se poate dispune măsura, indicarea faptei și a încadrării juridice, iar, în cazul măsurii supravegherii video, audio sau prin fotografiere, dacă se solicită și încuviințarea ca organele de urmărire penală să pătrundă în spații private indicate pentru a activa sau a dezactiva mijloacele tehnice ce urmează a fi folosite pentru executarea măsurii supravegherii tehnice, motivarea caracterului proporțional și subsidiar al măsurii*". Toate acestea vor trebui coroborate între ele și completate, după caz, cu prevederile art. 140 alin. (5) C.pr.pen., care indică elementele mandatului și încheierii emise de judecătorul de drepturi și libertăți.

În continuare vom analiza elementele care trebuie să fie cuprinse în propunerea procurorului.

Indicarea măsurilor de supraveghere tehnică solicitate presupune ca procurorul să includă în propunerea sa detalierea tuturor metodelor speciale de supraveghere tehnică pe care acesta le solicită încuviințate. Prin aceasta, legiuitorul a impus ca procurorul să încunoștințeze judecătorul de drepturi și libertăți nu numai asupra categoriei de metode speciale de supraveghere cerute, ci să indice și cum această măsură va fi pusă în executare, trebuind să fie suficient de explicit în descriere, pentru a permite judecătorului de drepturi și libertăți să exercite un control efectiv al proporționalității măsurii.

În cazul interceptării comunicațiilor ori a oricărui tip de comunicare la distanță, s-a introdus numai în art. 140 alin. (5) C.pr.pen. necesitatea precizării în încheiere a elementelor de identificare a fiecărui telefon, nefiind o mențiune care să fie, aparent, cerută a fi inclusă în propunerea procurorului. O asemenea concluzie, deși eronată, subliniază lipsa caracterului clar al normei cu privire la indicarea măsurilor de supraveghere tehnică cerute de procuror. Chiar și în cazul interceptărilor, acestea nu se pot realiza doar asupra unui telefon, ci pot viza orice formă de comunicații. În mod similar, textul legal nu precizează, în cazul supravegherii video, audio sau prin fotografiere, modalitatea concretă de realizare – continuă ori secvențială –, obiectul sau persoana urmărită.

Nu se poate admite ca procurorul să solicite supravegherea tehnică numai prin raportare la definiția măsurilor prevăzute de art. 138 alin. (1) lit. a)-d) C.pr.pen., ci va trebui, în mod obligatoriu, să se raporteze la modul în care se va pune în executare fiecare măsură de supraveghere tehnică, pentru a putea fi evaluat caracterul proporțional al acesteia.

De exemplu, nu va fi suficientă indicarea supravegherii video, audio sau prin fotografiere chiar cu mențiunea că se va realiza în spații private fără a se indica spațiul privat, dacă se va proceda la observare sau și la înregistrare, dacă înregistrarea se va face video, audio-video, audio sau prin fotografiere, dacă măsura va fi continuă pe durata mandatului sau secvențială, unde va fi situat mijlocul tehnic de înregistrare în spațiul privat (sufragerie, dormitor, baie, garaj etc.), cum se va realiza instalarea și dezinstalarea mijlocului tehnic, de câte ori se va putea pătrunde în spațiul privat pentru activarea sau dezactivarea mijloacelor tehnice, câte persoane

vor pătrunde în spațiul privat etc. După cum se poate observa, numai în cazul unei singure măsuri de supraveghere tehnică, există foarte multe elemente de variabilitate care vor afecta, în final, proporționalitatea măsurii, ceea ce reflectă obligația procurorului de a detalia toate aspectele necesare în cererea sa.

Indicarea fiecărei măsuri de supraveghere tehnică în mod concret este obligatorie, întrucât judecătorul de drepturi și libertăți nu poate fi ținut să se substituie procurorului asupra modului concret de punere în executare și să îi propună metode alternative. Desigur, dacă procurorul propune o măsură mai intruzivă (de pildă, supravegherea audio-video a dormitorului unei persoane), judecătorul va putea încuviința una mai puțin intruzivă (supravegherea audio a dormitorului persoanei[1]). În mod corect s-a arătat că actuala modalitate de formulare a dispozițiilor art. 140 alin. (2) și alin. (5) C.pr.pen. ridică probleme de convenționalitate în măsura în care se poate solicita judecătorului să autorizeze toate măsurile de supraveghere tehnică și acesta să le autorizeze pe toate cu aceeași motivare[2].

Indicarea probelor ori a datelor din care rezultă suspiciunea rezonabilă cu privire la săvârșirea unei infracțiuni pentru care se poate dispune măsura constituie o mențiune care trebuie să fie supusă unor critici, întrucât nu corespunde cu condiția existenței suspiciunii rezonabile prevăzută de art. 139 alin. (11) lit. a) C.pr.pen.

Prima critică este în legătură cu expresia „indicarea probelor ori a datelor", care reflectă un procedeu sumar al procurorului de a se referi numai la probele sau datele care ar justifica suspiciunea rezonabilă, ceea ce este în neconcordanță cu respectarea dreptului la viață privată, întrucât suspiciunea rezonabilă presupune existența unui element obiectiv care să îl justifice, nu anumite probe care, după părerea procurorului, ar conduce la suspiciunea rezonabilă. Situația este aparte, întrucât, în cadrul celorlalte cazuri, condițiile legale ale art. 140 alin. (2) C.pr.pen. obligă procurorul să motiveze caracterul proporțional și subsidiar al fiecărei măsuri în parte. Apreciem că se va impune ca procurorul să motiveze existența unei suspiciuni rezonabile cu privire la săvârșirea unei infracțiuni și ca aceasta să se realizeze pe baza unei analize temeinice a probelor sau datelor din care rezultă această suspiciune. Este greșită abordarea legiuitorului de a aprecia că dacă există probe sau date, judecătorul de drepturi și libertăți trebuie să constate că există o suspiciune rezonabilă, întrucât, așa cum am arătat în secțiunile anterioare, gradul de suspiciune rezonabilă va trebui să fie analizat și în raport de gravitatea ingerinței dreptului la viață privată.

A doua critică privește inducerea ideii unei verificări sumare a suspiciunii rezonabile, părând că se sugerează ca judecătorul de drepturi și libertăți să constate că există probe sau date privind o suspiciune rezonabilă, fără ca acesta să constate existența acesteia. Cu alte cuvinte, doar indicarea probelor și datelor din care rezultă suspiciunea rezonabilă mută în sarcina procurorului stabilirea existenței unei suspiciuni rezonabile, ceea ce contravine dispozițiilor art. 139 alin. (1) C.pr.pen. După cum am arătat deja, judecătorul de drepturi și libertăți va verifica el însuși dacă există o suspiciune rezonabilă privind săvârșirea uneia dintre infracțiunile prevăzute de art. 139 alin. (2) C.pr.pen. prin prisma tuturor probelor sau datelor care se află la dosarul cauzei, astfel că indicarea de către procuror numai a anumitor probe sau date este contrară unei analize complete asupra contextului în care se poate încuviința măsura.

[1] Evident, acest exemplu este un exemplu de școală, filmarea și înregistrarea în spații de acest fel trebuind să fie privită cu mare grijă de către judecătorul de drepturi și libertăți, ca urmare a violării dreptului la viață privată într-un mod extrem.

[2] *S. Grădinaru*, Supravegherea tehnică, 2014, p. 45.

Motivarea caracterului proporțional și subsidiar va constitui un alt element deosebit de important care trebuie să fie cuprins în propunerea procurorului. Fără acest element, nu se va putea proceda la judecarea cererii, chiar dacă ar fi îndeplinite condițiile legale, întrucât procurorul trebuie să demonstreze îndeplinirea acestora, cu referire la aceste elemente deosebit de importante. Motivarea va trebuie să privească fiecare dintre metodele speciale de supraveghere în parte, nefiind suficient a se motiva cu privire la necesitatea unei supravegheri tehnice în general, ci fiecare trebuie pusă în balanță cu restrângerea drepturilor fundamentale ale persoanei, prin prisma controlului de proporționalitate și subsidiaritate[1]. Ceea ce va fi deosebit de important este ca procurorul să motiveze de ce procedeele probatorii clasice nu pot fi folosite pentru obținerea probei[2], pentru a fi autorizate măsurile de supraveghere tehnică cerute, fiind de preferat ca acesta să prezinte motive temeinice, precum încercarea de a folosi procedee probatorii clasice și obținerea de probe să fi eșuat[3].

Numele sau alte date de identificare a persoanei împotriva căreia se dispune măsura este un element care ar trebui precizat în orice supraveghere tehnică, lipsa acestuia semnalând o lipsă de diligență din partea organelor de urmărire penală. Chiar dacă Codul de procedură penală permite procurorului să propună măsuri de supraveghere tehnică și dacă nu sunt cunoscute aceste date, nu poate fi admisă inexistența oricărui element de identificare. Prin „date de identificare" nu credem că legiuitorul s-a referit la codul numeric personal, seria cărții de identitate, domiciliul etc., ci la orice element care poate contribui la identificarea persoanei. Va fi suficient ca, pentru emiterea unui mandat de supraveghere tehnică, să fie prezentat un subiect al mandatului ca fiind în legătură cu o altă persoană cunoscută, sens în care o propunere de acest fel ar putea fi primită. Ceea ce va fi inacceptabil ar fi să se dispună supravegherea tehnică fără a se putea identifica nicio persoană. Într-o atare situație, apreciem că va exista o lipsă de diligență din partea organelor de urmărire penală, cererea trebuind să fie respinsă nu doar pentru lipsa elementului, ci pentru că dacă nu se poate identifica nici măcar generic o persoană, este greu de susținut existența condiției legale a suspiciunii rezonabile privind săvârșirea unei infracțiuni.

Indicarea faptei și a încadrării juridice nu presupune dificultăți deosebite, fiind un element care este comun și inclus în majoritatea actelor de urmărire penală. Desigur, analiza judecătorului de drepturi și libertăți va trebui să se facă și prin raportare la fapta și încadrarea juridică, dar aceasta va însemna numai constatarea că respectiva faptă este printre cele enumerate de art. 139 alin. (2) C.pr.pen. Asupra gravității faptelor și asupra existenței unei suspiciuni rezonabile privind comiterea lor, procurorul va trebui să motiveze distinct, astfel cum am arătat deja, sub acest aspect, condiția prevăzută de art. 139 alin. (1) lit. a) C.pr.pen. incluzând indicarea faptei și a încadrării juridice.

Încuviințarea ca organele de urmărire penală să pătrundă în spații private pentru punerea în executare a supravegherii tehnice constituie o mențiune care va fi obligatorie numai în cazul măsurii de supraveghere tehnică a supravegherii video, audio sau prin fotografiere în spații private, situație în care procurorul va trebui să solicite expres judecătorului de drepturi și libertăți să încuviințeze pătrunderea într-un spațiu privat. Menirea acestei mențiuni este de a se obține încuviințarea judecătorului de drepturi și libertăți pentru a se pătrunde în spații private în vederea instalării și dezinstalării mijloacelor tehnice de supraveghere. Deși textul

[1] *Ibidem*, p. 45.

[2] *Gh. Mateuț*, Procedură penală, 2019, p. 683.

[3] CEDO, cauza *Uzun c. Germania*, Hotărârea din 2 decembrie 2012, §78, pe *hudoc.echr.coe.int*

se referă la activarea și dezactivarea unor asemenea mijloace, sensul este cel de instalare și activare, respectiv dezactivare și dezinstalare.

Deși, așa cum vom vedea într-o secțiune ulterioară[1], textul legiuitorului este criticabil sub aspectul ingerinței aduse vieții private prin lipsa de claritate, va trebui ca procurorul să arate judecătorului de drepturi și libertăți în ce condiții se va realiza pătrunderea, prin ce mijloace, de câte ori va avea loc, de câte persoane va fi nevoie pentru instalare și dezinstalare etc., astfel încât autorizarea să fie dată cu maximă precizie și să fie cât mai bine protejate drepturile fundamentale ale persoanei, prin restrângerea acestora numai la strictul necesar pentru scopul legitim autorizat.

Toate elementele arătate mai sus vor trebui cuprinse într-o *propunere* formulată de procurorul care efectuează urmărirea penală sau supraveghează urmărirea penală. Deși Codul se referă la cererea procurorului, apreciem că acest termen este unul impropriu, cererea fiind specifică părților și subiecților procesuali principali, în cazul organelor de urmărire penală, termenul corect fiind cel de „propunere". În plus, observăm că legiuitorul alternează între termenul de „cerere" și cel de „propunere" în tot capitolul dedicat metodelor speciale de supraveghere sau cercetare.

Pentru a se putea analiza propunerea procurorului, va fi obligatoriu, conform art. 140 alin. (2) C.pr.pen., ca procurorul să înainteze dosarul cauzei judecătorului de drepturi și libertăți. O astfel de mențiune este necesară, întrucât judecarea propunerii procurorului nu se va face numai pe baza actului de sesizare a judecătorului de drepturi și libertăți, trebuind să se realizeze o analiză a dosarului pentru ca judecătorul de drepturi și libertăți să se convingă de îndeplinirea condițiilor legale pentru autorizarea măsurii.

Secțiunea a 2-a. Autorizarea folosirii metodelor speciale de supraveghere sau cercetare de către judecătorul de drepturi și libertăți

În privința dispunerii supravegherii tehnice de către *judecătorul de drepturi și libertăți*, procedura este prevăzută de art. 140 C.pr.pen. și impune, mai întâi, verificarea de către judecătorul de drepturi și libertăți a respectării condițiilor prevăzute de art. 139 C.pr.pen.

Această verificare se face pe baza cererii depuse de către procuror și în urma verificării dosarului cauzei, care va fi înaintat împreună cu cererea prin care solicită încuviințarea supravegherii tehnice. În cuprinsul cererii, procurorul trebuie să includă toate elementele prevăzute de art. 140 alin. (2) C.pr.pen.[2].

Competența de încuviințare a supravegherii tehnice va reveni, potrivit art. 140 alin. (1) C.pr.pen., judecătorului de drepturi și libertăți de la instanța căreia i-ar reveni competența să judece cauza în primă instanță sau de la instanța corespunzătoare în grad acesteia în a cărei

[1] *V. infra*, Titlul VI, Capitolul II.3.

[2] Conform acestui articol, cererea trebuie să cuprindă: „indicarea măsurilor de supraveghere tehnică care se solicită a fi dispuse, numele sau alte date de identificare a persoanei împotriva căreia se dispune măsura, dacă sunt cunoscute, indicarea probelor ori a datelor din care rezultă suspiciunea rezonabilă cu privire la săvârșirea unei infracțiuni pentru care se poate dispune măsura, indicarea faptei și a încadrării juridice, iar, în cazul măsurii supravegherii video, audio sau prin fotografiere, dacă se solicită și încuviințarea ca organele de urmărire penală să pătrundă în spații private indicate pentru a activa sau a dezactiva mijloacele tehnice ce urmează a fi folosite pentru executarea măsurii supravegherii tehnice, motivarea caracterului proporțional și subsidiar al măsurii".

circumscripție se află parchetul din care face parte procurorul care a formulat cererea. S-a susținut că prin această prevedere s-a inclus o competență alternativă, pentru că, la momentul formulării propunerii de încuviințare, nu se va putea determina cu exactitate instanța care ar urma să fie sesizată în urma finalizării urmăririi penale[1]. O atare situație poate să apară mai ales în cazul direcțiilor specializate din cadrul Parchetului de pe lângă Înalta Curte de Casație și Justiție, unde nu va fi obligatoriu ca trimiterea în judecată să se realizeze către instanța competentă din circumscripția teritorială a organului de urmărire penală. De exemplu, este posibil ca Serviciul Central al D.N.A. să realizeze urmărirea penală și o instanță din raza unei alte curți de apel decât Curtea de Apel București să fie sesizată cu rechizitoriu.

Judecarea propunerii de încuviințare a supravegherii tehnice are loc în aceeași zi cu formularea ei, în camera de consiliu, fără citarea părților și cu prezența obligatorie a procurorului. Întrucât instituția judecătorului de drepturi și libertăți a fost gândită pentru a permite o judecare cât mai eficientă a cauzelor urgente, se impunea mențiunea ca termenul de judecată să fie stabilit ca fiind unul de maximă urgență. Întrucât toate tehnicile speciale de supraveghere sau cercetare au un caracter secret, este evident că judecarea propunerii procurorului va trebui să se facă în cameră de consiliu, fără participarea publicului. Totodată, lipsa citării părților este esențială pentru orice tehnică specială de supraveghere care ar putea fi autorizată, întrucât orice încunoștințare a persoanei supravegheate despre existența unei supravegheri tehnice față de aceasta va influența în mod determinant și negativ procedeul probatoriu.

Prezența procurorului se impune a fi obligatorie, întrucât el este cel care a sesizat judecătorul de drepturi și libertăți, astfel că este obligat să se prezinte în fața sa și să-și argumenteze propunerea și să confere toate explicațiile care ar fi necesare în vederea obținerii autorizării. Această regulă va fi universal aplicabilă tuturor metodelor speciale de supraveghere sau cercetare prevăzute de Codul de procedură penală în care se impune încuviințarea măsurii de către judecătorul de drepturi și libertăți.

Soluțiile pe care le poate pronunța judecătorul de drepturi și libertăți sunt fie *respingerea propunerii*, fie *admiterea ei* și emiterea, de îndată, a *mandatului de supraveghere tehnică*.

Respingerea cererii se va dispune conform art. 140 alin. (6) C.pr.pen., atunci când judecătorul de drepturi și libertăți va respinge în totalitate cererea procurorului, fie ca inadmisibilă, fie ca nefondată. Considerăm că inadmisibilitatea cererii va fi atrasă în cazul care nu sunt respectate dispozițiile prevăzute de art. 139 alin. (2) C.pr.pen. privind infracțiunile în cazul cărora se poate dispune supravegherea tehnică sau propunerea ar fi formulată direct de către organul de cercetare penală, și nu de procuror. Deși această ultimă ipoteză pare una imposibilă, legiuitorul a greșit în cazul măsurii speciale de cercetare prevăzută de art. 152 C.pr.pen. privind obținerea de date de trafic și de localizare prelucrate de către furnizorii de rețele publice de comunicații electronice ori furnizorii de servicii de comunicații electronice destinate publicului, unde se arată că cererea poate fi formulată în fața judecătorului de drepturi și libertăți de către orice organ de urmărire penală[2]. Evident, numai procurorul are dreptul de a sesiza judecătorul de drepturi și libertăți, mențiunea cuprinsă în art. 152 alin. (2) C.pr.pen. fiind o eroare evidentă a legiuitorului.

[1] *Gh. Mateuț*, Procedură penală, 2019, p. 686.

[2] Conform art. 152 alin. (2) C.pr.pen., „judecătorul de drepturi și libertăți se pronunță în termen de 48 de ore cu privire la solicitarea organelor de urmărire penală de transmitere a datelor, prin încheiere motivată, în camera de consiliu".

Un element aparte este soluția impusă de legiuitor atunci când cererea procurorului este îndreptată unui organ necompetent, contrar dispozițiilor art. 140 alin. (1) C.pr.pen. Astfel, în măsura în care procurorul va formula o cerere de încuviințare a supravegherii tehnice la un alt judecător de drepturi și libertăți decât cel competent, cererea se va trimite pe cale administrativă la organul competent și nu se va proceda la o declinare de competență în sensul art. 50 C.pr.pen., deoarece acest articol cuprinde referiri numai la declinarea competenței *instanței de judecată*. O soluție contrară, cu care nu putem fi de acord, este respingerea cererii ca inadmisibilă, ca urmare a îndreptării sale spre un organ necompetent[1]. O atare soluție este greșită, deoarece nu se poate vorbi despre o lipsă a *competenței funcționale*[2], ci numai despre o lipsă a competenței materiale, personale ori teritoriale, în aceste cazuri, soluția firească fiind trimiterea cererii către organul competent. *De lege ferenda*, considerăm că se impune aplicarea dispozițiilor art. 50 C.pr.pen. și judecătorului de drepturi și libertăți. O situație care va atrage respingerea ca inadmisibilă a cererii procurorului va fi formularea unei cereri de încuviințare identice cu o altă cerere precedentă ce a fost respinsă, în contradicție cu dispozițiile art. 140 alin. (8) C.pr.pen.

În cazul oricăreia dintre soluțiile adoptate de către judecătorul de drepturi și libertăți, aceasta nu va putea fi supusă niciunei căi de atac, însă procurorul va fi îndreptățit să formuleze o nouă cerere de încuviințare în cazul respingerii, dacă vor fi îndeplinite cerințele prevăzute de art. 140 alin. (8) C.pr.pen. Formularea unei a doua cereri de încuviințare a supravegherii tehnice va putea fi făcută numai în măsura în care au apărut ori s-au descoperit fapte sau împrejurări noi, necunoscute la momentul soluționării cererii anterioare. Suntem de părere că această condiție nu trebuie să fie considerată una formală, ea trebuind să fie verificată în mod temeinic de către judecătorul de drepturi și libertăți, raportat la starea de fapt descrisă în cuprinsul primei cereri de încuviințare. Astfel, nu va putea constitui *descoperirea unei fapte noi* simpla schimbare a încadrării juridice, deoarece, în această situație, starea de fapt rămâne aceeași, doar semnificația sa juridică este schimbată. Ținând seama de faptul că, potrivit Regulamentului de ordine interioară al instanțelor judecătorești[3], judecarea unor cereri subsecvente primei cereri soluționate în cauză de judecătorul de drepturi și libertăți se va face de către același judecător, acesta va putea verifica în mod temeinic dacă într-adevăr au fost descoperite fapte sau împrejurări noi[4].

Pentru ca faptele și împrejurările noi să poată justifica formularea unei noi cereri de încuviințare, este necesar ca acestea să nu fi fost cunoscute de judecătorul de drepturi și libertăți la soluționarea primei cereri de încuviințare. Semnificația acestei prevederi este bazată pe faptul că dacă faptele sau împrejurările erau cunoscute de către judecătorul de drepturi și libertăți la momentul în care a respins prima cerere de încuviințare, acesta le-a avut în vedere la soluționarea propunerii.

În cazul *admiterii propunerii de încuviințare a supravegherii tehnice*, judecătorul de drepturi și libertăți este îndreptățit să încuviințeze numai acele mijloace de supraveghere tehnică care

[1] *M.V. Tudoran*, Teoria și practica interceptărilor, 2012, p. 121.

[2] *Gh. Mateuț*, Tratat, vol. I, 2007, p. 449.

[3] Regulamentul de ordine interioară a instanțelor judecătorești, aprobat prin Hotărârea CSM nr. 1375 din 17 decembrie 2015 (republicat în M. Of. nr. 130 din 20 februarie 2017).

[4] Conform art. 102 alin. (5) din Regulamentul de ordine interioară al instanțelor judecătorești: „judecătorul de drepturi și libertăți care soluționează o primă cerere, propunere, plângere sau contestație soluționează, de regulă, și următoarele cereri, propuneri, plângeri ori contestații formulate în cursul urmăririi penale în cadrul aceluiași dosar de urmărire penală, dacă prin hotărâre a colegiului de conducere nu s-a dispus altfel".

sunt proporționale și necesare pentru cauză, urmând să respingă toate celelalte. Totodată, judecătorul se va pronunța și asupra conținutului concret al supravegherii tehnice, fiind în măsură să cenzureze cererea procurorului. Această situație nu trebuie să o considerăm ca fiind o ingerință în competența funcțională a procurorului, ci trebuie văzută din perspectiva rolului de dispoziție și control pe care îl are judecătorul de drepturi și libertăți raportat la proporționalitatea și necesitatea mijloacelor de supraveghere tehnică. Admiterea cererii se face prin încheierea judecătorului de drepturi și libertăți care va proceda la emiterea imediată a mandatului de supraveghere tehnică, întocmind în mod obligatoriu o minută.

Supravegherea tehnică poate fi dispusă pentru o perioadă maximă de 30 de zile, însă, conform art. 144 C.pr.pen., poate fi prelungită, fiecare prelungire neputând depăși 30 de zile. Totodată, conform art. 144 alin. (3) C.pr.pen., durata totală a măsurilor de supraveghere tehnică cu privire la aceeași persoană nu poate depăși 6 luni, cu excepția măsurii de supraveghere video, audio sau prin fotografiere în spații private, care nu poate depăși 120 de zile. Codul de procedură penală actual nu a mai păstrat dispoziția cuprinsă în vechea reglementare privind „reînnoirea mandatului de supraveghere tehnică", reflectând faptul că prelungirea nu se va putea dispune dacă măsura a încetat ca urmare a expirării mandatului de supraveghere tehnică[1].

După admiterea cererii de utilizare a metodelor de supraveghere tehnică, înaintată de procuror, judecătorul de drepturi și libertăți emite, conform art. 140 alin. (5) C.pr.pen., *mandatul de supraveghere tehnică*, acesta trebuind să cuprindă mai multe elemente prevăzute expres de Cod. Menționăm că mandatul de supraveghere tehnică se va emite de îndată, nu și încheierea judecătorului de drepturi și libertăți, care se va motiva ulterior. Deoarece încheierea se va motiva ulterior, Codul de procedură penală prevede, la art. 140 alin. (4) C.pr.pen., întocmirea obligatorie a minutei.

Elementele care sunt cuprinse în mandat sunt cele care trebuie cuprinse și în încheierea de admitere a cererii, motiv pentru care le vom aborda unitar.

Deoarece unele metode speciale de supraveghere tehnică presupun dispoziții speciale, acestea vor fi prevăzute, după caz, de judecătorul de drepturi și libertăți. În cazul interceptării comunicațiilor ori a oricărui tip de comunicare la distanță, vor trebui prevăzute *elementele de identificare a fiecărui telefon sau datele cunoscute pentru identificarea căii de comunicare*[2]. În privința *accesului la un sistem informatic*, ca element specific – *punctul de acces la sistemul informatic*. În cazul supravegherii video, audio sau prin fotografiere în spații private, va fi necesar ca judecătorul de drepturi și libertăți să includă *mențiunea încuviințării pătrunderii în spații private pentru a activa sau dezactiva mijloacele tehnice ce urmează a fi utilizate pentru executarea măsurii supravegherii tehnice*.

Elementele comune care nu pun probleme deosebite sunt cele privind *denumirea instanței*, *data, ora și locul emiterii*, *numele, prenumele* și *calitatea persoanei care a dat încheierea și a emis mandatul*, *semnătura judecătorului și ștampila instanței*. Considerăm că mențiunea privind locul emiterii mandatului de supraveghere tehnică nu era necesar să mai fie prevăzută expres de către legiuitor, deoarece, fiind vorba despre un judecător de drepturi și libertăți, se subînțelege faptul că acesta își va desfășura activitatea numai la sediul instanței, iar judecarea cererii se face în *cameră de consiliu*, cu prezența procurorului, nefiind permisă emiterea mandatului de supraveghere tehnică decât odată cu soluționarea cererii procurorului.

[1] ICCJ, Completul pentru dezlegarea unor chestiuni de drept, Dec. nr. 2/2018 (M. Of. nr. 307 din 5 aprilie 2018).

[2] CEDO, cauza *Calmanovici c. România*, Hotărârea din 1 iulie 2008, §124, pe *hudoc.echr.coe.int*

În schimb, ora emiterii mandatului de supraveghere tehnică, alături de dată, prezintă semnificație deosebită, deoarece de la acel moment curge posibilitatea procurorului de a pune în executare mandatul de supraveghere tehnică.

Un alt element comun care nu ridică probleme este perioada pentru care se dispun măsurile de supraveghere tehnică, aceasta putând fi de maximum 30 de zile. Sub acest aspect, va trebui să se țină cont și de durata măsurii în determinarea caracterului proporțional al acesteia, întrucât, uneori, o activitate poate impune un mandat emis pentru o perioadă restrânsă (de pildă, pentru o zi sau două zile atunci când se pregătește organizarea unui flagrant).

Alături de mențiunile amintite mai sus, în cuprinsul art. 140 alin. (5) lit. e) teza a II-a C.pr.pen., legiuitorul a prevăzut că este obligatorie menționarea *scopului* pentru care s-a încuviințat măsura. În opinia noastră, aceste element este inutil în cuprinsul unui mandat de supraveghere tehnică, deoarece, fiind vorba despre un procedeu probatoriu, scopul măsurilor de supraveghere tehnică este subînțeles. Acest zel al legiuitorului de a prevedea elementul „scop" în cuprinsul mandatului de supraveghere tehnică este de neînțeles atât timp cât nici procurorului nu îi este cerut să prevadă, în cuprinsul cererii formulate conform art. 140 alin. (2) C.pr.pen., scopul pentru care solicită încuviințarea utilizării supravegherii tehnice.

Un alt element care trebuie să se regăsească în cuprinsul mandatului de supraveghere tehnică este *numele persoanei supuse măsurii de supraveghere tehnică*, dacă acesta este cunoscut, fiind aplicabile explicațiile date în secțiunea precedentă.

Cel mai important element cuprins în încheierea judecătorului de drepturi și libertăți care trebuie să fie prevăzut și în mandatul de supraveghere tehnică este *indicarea măsurii de supraveghere concrete încuviințată*. Astfel cum am arătat în secțiunea precedentă, procurorul trebuie să solicite o măsură de supraveghere concretă și nu va fi suficient să precizeze numai categoria de măsură prin raportare la art. 138 alin. (1) lit. a)-d) C.pr.pen. Pentru a fi legală, este necesar ca încheierea judecătorului de drepturi și libertăți să precizeze cât mai precis activitățile care au fost încuviințate.

În toate cazurile, încheierea judecătorului de drepturi și libertăți trebuie să fie temeinic motivată sub aspectul îndeplinirii condițiilor legale prevăzute de art. 139 C.pr.pen. pentru ca, ulterior, să poată fi realizat un control de legalitate în cazul în care autorizarea și supravegherea tehnică vor fi contestate în faza de cameră preliminară sau separat, dacă persoana care contestă nu are o calitate procesuală. Ca în cazul oricărei hotărâri judecătorești, motivarea completă și temeinică trebuie să fie o obligație[1], realizându-se o analiză amplă pe baza căreia să se poată realiza un control judiciar eficient[2], în sens contrar, existând posibilitatea ca autorizarea și, pe cale de consecință, întreaga supraveghere tehnică să poată fi declarată nelegală, în lipsa motivării.

Secțiunea a 3-a. Autorizarea folosirii metodelor speciale de supraveghere sau cercetare de către procuror

În mod excepțional și cu controlul ulterior al judecătorului de drepturi și libertăți, Codul de procedură penală permite procurorului să autorizeze temporar, pentru o perioadă care nu

[1] C. Ap. Cluj, dec. nr. 554 din 5 aprilie 2017; C. Ap. Timișoara, dec. pen. nr. 132/A din 31 ianuarie 2017; C. Ap. Cluj, dec. nr. 54/A din 14 ianuarie 2015.

[2] C. Ap. Oradea, dec. pen. nr. 1/A din 6 ianuarie 2016; C. Ap. Oradea, dec. pen. nr. 447 din 5 iulie 2017; C. Ap. Craiova, dec. pen. nr. 1249/2015.

poate depăși 48 de ore, folosirea oricăror mijloace de supraveghere tehnică. Această posibilitate conferă procurorului puteri excesive și creează riscul unui abuz, procedura autorizării provizorii fiind criticată, fără succes deocamdată, în fața Curții Constituționale, instanța de contencios constituțional apreciind că procedura de autorizare nu lipsește persoana supusă procedurii de garanțiile specifice dreptului la un proces echitabil[1].

Procedura autorizării provizorii a supravegherii tehnice este una excepțională, putând fi utilizată de procuror numai atunci când sunt întrunite condițiile stricte ale art. 141 C.pr.pen., măsura fundamentându-se pe urgența efectuării supravegherii tehnice. Urgența impune procurorului să procedeze direct la autorizarea supravegherii tehnice ca urmare a faptului că nu există timpul necesar pentru parcurgerea procedurii ordinare în fața judecătorului de drepturi și libertăți. Această urgență nu îl va scuti pe procuror să supună măsura unui control de temeinicie și legalitate *a posteriori*, realizat de judecătorul de drepturi și libertăți[2].

Procedura autorizării de către procuror a folosirii metodelor de supraveghere tehnică este o preluare nefericită a instituției similare cuprinse în vechiul Cod de procedură penală. Motivul pentru menținerea acestei instituții este găsirea unei soluții pentru acele situații în care procedura ordinară ar duce la pierderea momentului operativ și, implicit, a oportunității de a obține anumite probe. În doctrină s-a arătat că, deși instituția a rămas neschimbată, ca urmare a modificării fundamentale a procesului penal, dispozițiile art. 141 C.pr.pen. sunt neconstituționale raportat la art. 21 alin. (3) din Constituție, având în vedere că *procurorul nu prezintă garanții suficiente de independență și imparțialitate pentru luarea unor măsuri prin care se aduce atingere gravă drepturilor și libertăților persoanei*[3]. Argumentele autorului sunt corecte și sunt confirmate de jurisprudența Curții Europene a Drepturilor Omului în decizii care au fost pronunțate ulterior emiterii opiniei sale[4]. Se arată, în mod corect, că instituția judecătorului de drepturi și libertăți a fost creată pentru a soluționa probleme urgente[5], inclusiv încuviințarea metodelor speciale de supraveghere, iar dispozițiile art. 141 C.pr.pen. dau prerogative identice procurorului, contrar principiului separării funcțiilor judiciare în procesul penal. Suntem de acord cu ambele susțineri ale autorului citat, întrucât, pentru verificarea caracterului proporțional al măsurii și pentru protejarea drepturilor fundamentale ale unei persoane, este necesar ca autorizarea supravegherii tehnice să fie analizată de o autoritate independentă. Așa cum am arătat, specificul autorizării de către procuror a supravegherii tehnice este urgența, or, noul Cod de procedură penală a creat deja un organ care să soluționeze chestiunile urgente care țin de restrângerea drepturilor și libertăților fundamentale ale persoanei: judecătorul de drepturi și libertăți. De altfel, propunerea de încuviințare a supravegherii tehnice se va judeca în aceeași zi în care are loc sesizarea. Sub imperiul legislației procesuale penale anterioare, s-a remarcat ușurința cu care se proceda la confirmarea interceptărilor și înregistrărilor dispuse provizoriu de către procuror[6]. *De lege ferenda*, considerăm că se impune abrogarea completă a procedurii autorizării de către procuror atât în cazul supravegherii, cât și în cazul metodelor speciale de cercetare care s-ar putea baza pe dispozițiile acesteia.

---

[1] CCR, Dec. nr. 556 din 12 iulie 2016 (M. Of. nr. 624 din 12 august 2016) (decizie de respingere).

[2] CEDO, cauza *Calmanovici c. România*, Hotărârea din 1 iulie 2008, §123, pe *hudoc.echr.coe.int*

[3] *Gh. Mateuț*, Observații critice privind noua reglementare a supravegherii tehnice într-o prezentare comparativă, în Caiete de Drept Penal nr. 3/2015, p. 31.

[4] CEDO, cauza *Roman Zakharov c. Rusia*, Hotărârea din 4 decembrie 2015, §233; cauza *İrfan Güzel c. Turcia*, Hotărârea din 7 februarie 2017, §96.

[5] *Gh. Mateuț*, Observații critice privind noua reglementare a supravegherii tehnice într-o prezentare comparativă, în Caiete de Drept Penal nr. 3/2015, p. 32.

[6] *M.V. Tudoran*, Teoria și practica interceptărilor, 2012, p. 112.

Condițiile care trebuie întrunite pentru autorizarea provizorie sunt tot cele ca în cazul procedurii de emitere a mandatului de supraveghere tehnică, art. 140 alin. (1) lit. b) C.pr.pen. făcând trimitere la art. 139 alin. (1) și (2) C.pr.pen.[1]. Alături de aceste condiții, se mai impune ca autorizarea să fie dispusă numai în măsura în care *există urgență, iar obținerea mandatului de supraveghere tehnică în condițiile art. 140 C.pr.pen. ar conduce la o întârziere substanțială a cercetărilor, la pierderea, alterarea sau distrugerea probelor ori ar putea pune în pericol siguranța persoanei vătămate, a martorului sau a membrilor familiilor acestora*. În privința întârzierii substanțiale a cercetărilor, considerăm că legiuitorul a impus o condiție care nu se justifică raportat la durata relativ scurtă de timp în care se poate obține un mandat de supraveghere tehnică, astfel simplul motiv că cercetarea ar fi întârziată cu o zi sau două nu considerăm că poate constitui motiv suficient pentru autorizarea supravegherii tehnice decât în cazuri excepționale. Dimpotrivă, oferă un criteriu generic care va fi interpretat de procuror în mod abuziv, cu riscul scăzut de a fi cenzurat ulterior de judecătorul de drepturi și libertăți, care va fi influențat de rezultatul obținut în urma supravegherii tehnice.

În cazul pierderii, alterării sau distrugerii probelor, suntem de părere că se impune ca procurorul să ia alte măsuri necesare sau să intervină într-un mod diferit, de pildă, organizarea flagrantului. Întrucât metodele speciale de supraveghere tehnică sunt procedee probatorii, ele nu pot fi deturnate de la scopul lor pentru realizarea altor operațiuni tactice. Cu alte cuvinte, dacă procurorul va dori să obțină proba prin supraveghere tehnică, de ce ar trebui să fie dovedită pierderea, alterarea sau distrugerea unor probe care nu s-au administrat deja în cursul urmăririi penale? În măsura în care probele ar putea fi pierdute, alterate sau distruse, există un procedeu probatoriu clasic care poate fi întrebuințat pentru administrarea acestor probe – percheziția domiciliară –, care a fost gândit inclusiv pentru o atare situație, și față de condiția subsidiarității supravegherii tehnice, nu putem să afirmăm că aceasta nu poate fi considerată o măsură eficientă. În condițiile în care procurorul ar susține că nu s-ar putea realiza o percheziție domiciliară pentru obținerea probelor pe motiv că nu se cunoaște locația acestora, și pentru aceasta s-ar impune supravegherea tehnică, apreciem că nu va fi îndeplinită condiția suspiciunii rezonabile și cea a proporționalității, întrucât procurorul nu poate să garanteze că rezultatul unei supravegheri tehnice va conduce la descoperirea locației probelor care ar putea fi pierdute, alterate sau distruse, însă cu siguranță se va produce o ingerință a vieții private a cel puțin unei persoane.

O situație ipotetică în care ar putea fi îndeplinită o atare condiție este atunci când există date din care rezultă că făptuitorul va încerca să își ascundă urmele prin ștergerea datelor informatice din anumite sisteme informatice. Pentru a preîntâmpina acest lucru, este necesar a se realiza accesul la sistemul informatic și a copia toate datele necesare soluționării cauzei mai înainte de a fi șterse.

Cea de-a treia situație prevăzută de lege este atunci când obținerea întârziată a mandatului de supraveghere tehnică ar pune în pericol siguranța persoanei vătămate, a martorului sau membrilor familiilor acestora. O atare situație ar impune cât mai rapida folosire a supravegherii tehnice pentru a preîntâmpina săvârșirea unei infracțiuni împotriva acestor persoane. De exemplu, în cazul în care persoana vătămată este răpită de făptuitor în sensul art. 205 C.pen., se poate proceda la autorizarea *localizării sau urmăririi prin mijloace tehnice a acesteia* pe baza semnalului telefonului său mobil, în vederea localizării cât mai rapide a persoanei vătămate și a eliberării sale.

[1] *V. supra*, Titlul III, Capitolul I.

Fiind analizată constituționalitatea art. 141 C.pr.pen., Curtea Constituțională a apreciat că textul legal este suficient de clar, oferind criterii pentru a putea fi determinată, în concret, urgența[1]. Nu credem că a fost inspirată decizia de respingere, trebuind să fie avută în vedere instituția judecătorului de drepturi și libertăți care a fost reglementată inclusiv pentru situații de urgență.

Autorizarea de către procuror a folosirii măsurilor de supraveghere tehnică se dispune prin ordonanță, aceasta trebuind să conțină toate elementele prevăzute de art. 140 alin. (5) C.pr.pen., adică să aibă un conținut identic cu mențiunile obligatorii din mandatul de supraveghere tehnică și încheierea care se emit, în procedura obișnuită, de către judecătorul de drepturi și libertăți. Ținând seama atât de caracterul complex al încheierii judecătorului de drepturi și libertăți, de elementele obligatorii pe care trebuie să le includă, cât și de faptul că ordonanța trebuie să fie temeinic motivată, procurorul nu va mai putea justifica urgența, pentru că timpul necesar redactării acesteia va fi unul superior celui în care s-ar putea prezenta judecătorului de drepturi și libertăți o propunere și acesta să o admită, să emită de îndată mandatul de supraveghere tehnică și să redacteze ulterior încheierea. Mai exact, o propunere de încuviințare a supravegherii tehnice nu va avea gradul de complexitate al unei ordonanțe de autorizare provizorie, având în vedere și faptul că judecarea propunerii ar avea loc în fața judecătorului de drepturi, unde procurorul poate face completări orale sau da lămuriri judecătorului de drepturi și libertăți, acestea fiind consemnate în încheiere.

Deși durata autorizării provizorii este limitată la 48 de ore, în doctrină s-a exprimat îngrijorarea justificată referitoare la lipsa unei garanții reale privind încetarea supravegherii tehnice după 48 de ore, existând posibilitatea continuării sale până la pronunțarea judecătorului de drepturi și libertăți[2]. Sub aspectul naturii termenului de 48 de ore, acesta a fost considerat un termen substanțial[3].

La sfârșitul duratei pentru care s-a dispus autorizarea provizorie a supravegherii tehnice, procurorul va trebui să realizeze un *proces-verbal de redare rezumativă a activităților de supraveghere tehnică*, conform art. 141 alin. (1) C.pr.pen. Acest proces-verbal diferă de cel de consemnare a activităților de supraveghere tehnică, întrucât nu va conține toate elementele acestuia, mai ales în cazul în care se dispune interceptarea comunicațiilor sau supravegheri audio, urmând ca procurorul să surprindă și să redea toate conversațiile care pot fi relevante în cauză. În doctrină s-a arătat că acesta va conține numai pasajele esențiale din perspectiva acuzării[4]. Prezentarea rezultatelor supravegherii tehnice dispuse provizoriu ridică o problemă cu privire la modul în care judecătorul de drepturi și libertăți se va pronunța asupra condițiilor legale ale supravegherii tehnice odată ce îi sunt aduse la cunoștință rezultatele, existând o tentație puternică de a confirma măsura în cazul în care se obțin probe importante în soluționarea cauzei. Această situație impune, cu atât mai mult, abrogarea întregii proceduri a autorizării provizorii a supravegherii tehnice.

Conform art. 141 alin. (3) C.pr.pen., procurorul are obligația ca, în termen de cel mult 24 de ore de la expirarea măsurii, să sesizeze judecătorul de drepturi și libertăți competent în vederea *confirmării măsurii*, înaintând un proces-verbal de redare rezumativă a activităților de supraveghere tehnică efectuate. Pentru judecarea cererii de confirmare, alături de procesul-verbal

[1] CCR, Dec. nr. 261 din 24 aprilie 2018 (M. Of. nr. 622 din 18 iulie 2018) (decizie de respingere).

[2] *Gh. Mateuț*, Procedură penală, 2019, p. 689.

[3] *M. Bulancea, R. Slăvoiu*, în M. Udroiu (coord.), Codul de procedură penală, 2017, p. 680.

[4] *C. Olaru*, op. cit., p. 30.

de redare rezumativă a activităților de supraveghere tehnică, procurorul va fi obligat să înainteze întreg dosarul cauzei. Judecarea cererii de confirmare se va realiza în camera de consiliu, cu participarea procurorului, chiar dacă textul legal nu cuprinde această mențiune[1]. Obiectul judecății îl va constitui legalitatea și temeinicia autorizării provizorii a măsurii de către procuror, un astfel de control fiind necesar în conformitate cu jurisprudența Curții Europene a Drepturilor Omului[2].

Termenul de 24 de ore în care procurorul este obligat să sesizeze judecătorul de drepturi și libertăți în vederea confirmării supravegherii tehnice dispuse prin ordonanță nu este un termen de recomandare, ci este un termen de decădere care se va calcula pe ore libere[3].

În doctrină au existat mai multe opinii privind sancțiunea procesuală incidentă în cazul nerespectării de către procuror a termenului de 24 de ore pentru sesizarea judecătorului de drepturi și libertăți în vederea confirmării supravegherii tehnice.

Într-o primă opinie[4] s-a apreciat că termenul va fi un termen procedural de decădere, iar depășirea acestuia va atrage respingerea cererii de confirmare a măsurii de supraveghere tehnică, fără ca judecătorul de drepturi și libertăți să confirme sau să infirme supravegherea tehnică, procedeul probatoriu întrebuințat de către procuror urmând a putea fi anulat în condițiile art. 282 C.pr.pen. privind nulitatea relativă.

Într-o a doua opinie[5] s-a apreciat că nu va putea fi incidentă sancțiunea decăderii, fiind aplicabile dispozițiile art. 268 alin. (3) C.pr.pen., sancțiunea fiind nulitatea relativă, care va putea fi invocată în cursul urmăririi penale sau până la închiderea procedurii de cameră preliminară, autorul considerând că nulitatea relativă va fi condiționată de dovedirea unei vătămări privind însăși ordonanța de autorizare provizorie a supravegherii tehnice fundamentată, de exemplu, pe lipsa caracterului de urgență.

Credem că prima opinie este cea corectă, cu anumite precizări. În mod corect se stabilește că sancțiunea procesuală care trebuie să intervină în cazul nerespectării termenului de 24 de ore pentru sesizarea judecătorului de drepturi și libertăți este cea a decăderii, întrucât autorizarea provizorie a supravegherii tehnice constituie un drept al procurorului, condiționat de lege, inclusiv de obligația de a supune confirmării judecătorului de drepturi și libertăți măsura luată. În ceea ce privește soluția de respingere fără a se infirma sau confirma ordonanța procurorului, aceasta este dată de caracterul deficitar al redactării art. 141 alin. (6) C.pr.pen., în care se arată că infirmarea măsurii se va dispune dacă nu au fost respectate condițiile legale de autorizare provizorie prevăzute de art. 141 alin. (1) C.pr.pen. Era de preferat ca legiuitorul să fi inclus și o referire la art. 141 alin. (3) C.pr.pen., în cazul în care se omite deplin sesizarea judecătorului de drepturi și libertăți cu confirmarea măsurii, întrucât, în stadiul actual al legii, procedeul probatoriu ar rămâne valabil, și probele nu ar fi distruse, așa cum s-ar întâmpla în cazul infirmării măsurii. Acesta constituie unul dintre lipsurile legislației actuale, permițând, prin absurd, desfășurarea unei supravegheri tehnice prin autorizarea procurorului, fără ca aceasta să fie vreodată confirmată de judecătorul de drepturi și libertăți. A doua opinie prezentată o socotim greșită, întrucât ar presupune confirmarea ordonanței procurorului și ar permite invocarea unei nulități relative în privința ordonanței procurorului sau, eventual, asupra

[1] *M.V. Tudoran*, Teoria și practica interceptărilor, 2012, p. 113.
[2] CEDO, cauza *Calmanovici c. România*, Hotărârea din 1 iulie 2008, §123.
[3] *M. Udroiu*, Procedură penală, vol. I, 2019, p. 580.
[4] *Ibidem*.
[5] *M. Bulancea, R. Slăvoiu*, în M. Udroiu (coord.), Codul de procedură penală, 2017, p. 681.

confirmării judecătorului de drepturi și libertăți, în situația în care s-ar dovedi existența unei vătămări. Astfel cum am arătat deja, condițiile pentru autorizarea provizorie sunt construite într-un mod în care să fie permis procurorului să abuzeze de ele, fiind deosebit de greu ca o persoană să dovedească lipsa caracterului urgent al ordonanței în sine, cu atât mai mult dacă aceasta este confirmată și probele se află la dosarul cauzei și ar contribui la incriminarea persoanei. În plus, dovedirea unei vătămări în cazul depășirii termenului de 24 de ore pentru sesizarea judecătorului de drepturi și libertăți în vederea confirmării măsurii este improbabilă, întrucât lezarea dreptului la viață privată s-a realizat deja, prin punerea în executare a supravegherii tehnice.

În opinia noastră, față de lacunele legislației procesuale penale din prezent, judecătorul de drepturi și libertăți va trebui să constate că nu s-a respectat un termen de decădere prevăzut de lege, să nu confirme sau să infirme măsura supravegherii tehnice dispuse de procuror, dar va trebui să invoce din oficiu nulitatea relativă a procedeului probatoriu, în lumina Deciziei Curții Constituționale nr. 554/2017[1], care stabilește posibilitatea invocării din oficiu a nulității relative și de către judecătorul de cameră preliminară. Sub acest aspect, în cazul confirmării supravegherii tehnice dispuse prin ordonanța procurorului, sarcina judecătorului de drepturi și libertăți este similară celei pe care o are judecătorul de cameră preliminară – verificarea legalității unui act de urmărire penală, astfel că se impune invocarea din oficiu a nulității relative. Mai mult, ținându-se cont de funcția judiciară a judecătorului de drepturi și libertăți, anume aceea de dispoziție asupra drepturilor și libertăților fundamentale ale persoanei în faza de urmărire penală, trebuie să ținem cont că supravegherea tehnică va constitui o restrângere tocmai a acestor drepturi, astfel că invocarea din oficiu a nulității relative va constitui o obligație pentru judecătorul de drepturi și libertăți. Fiindcă supravegherea tehnică nu a fost supusă confirmării în termenul stabilit de legiuitor, trebuie să se aprecieze că întreaga procedură de autorizare provizorie este nelegală, întrucât va lipsi elementul esențial al confirmării judecătorului de drepturi și libertăți. Fiind nelegală supravegherea tehnică și existând o evidentă ingerință adusă dreptului la viață privată al unei persoane, va exista și vătămarea procesuală, sancțiunea nulității relative fiind singurul remediu procesual posibil. Din nefericire, nu se putea dispune și distrugerea probelor, fiind necesară o intervenție a legiuitorului în această privință.

De lege ferenda, se impune ca, în cazul nerespectării termenului de sesizare a judecătorului de drepturi și libertăți cu confirmarea autorizării provizorii a supravegherii tehnice, sancțiunea să fie infirmarea ordonanței procurorului și distrugerea imediată a probelor obținute.

Odată cu sesizarea judecătorului de drepturi și libertăți pentru confirmarea supravegherii tehnice, procurorul poate să ceară luarea măsurii supravegherii tehnice în condițiile art. 140 C.pr.pen., putând, de altfel, formula această cerere și separat. În vederea luării măsurii supravegherii tehnice, judecătorul de drepturi și libertăți va proceda ca în cazul art. 140 C.pr.pen., analizând condițiile legale de autorizare la momentul formulării cererii de confirmare. În opinia noastră, va fi posibilă luarea măsurii supravegherii tehnice concomitent cu infirmarea ordonanței procurorului, cele două cereri fiind unite numai sub aspectul formei și al momentului când sunt formulate, nu și în privința condițiilor legale.

Judecătorul de drepturi și libertăți, fiind sesizat de procuror în vederea confirmării supravegherii tehnice, are posibilitatea de a *infirma* sau *confirma* supravegherea tehnică efectuată în baza autorizației emise de procuror. Ne exprimăm serioase îndoieli cu privire la posibilitatea reală a infirmării supravegherii tehnice, în condițiile în care judecătorului i se oferă posibilitatea

[1] CCR, Dec. nr. 554 din 19 septembrie 2017 (M. Of. nr. 1013 din 21 decembrie 2017).

de a evalua datele obținute prin raportare la procesul-verbal de redare rezumativă a activităților de supraveghere tehnică. Cu alte cuvinte, atât timp cât judecătorul are acces direct asupra datelor rezultate în urma supravegherii tehnice, el poate fi tentat să confirme supravegherea tehnică, bazându-se pe o evaluare a valorii lor probante, situație care nu poate fi evitată decât prin desființarea instituției autorizării de către procuror a măsurilor de supraveghere tehnică. Întotdeauna când se va evalua legalitatea unei măsuri de supraveghere tehnică, este necesar ca judecătorul (de drepturi și libertăți sau de cameră preliminară) să se pună în situația de la momentul autorizării și să verifice dacă la acel moment erau îndeplinite condițiile legale, altfel percepția sa poate fi afectată de un rezultat amplu al supravegherii tehnice și poate aprecia că măsura era proporțională numai prin raportare la rezultatul obținut, fără a ține seama dacă, la momentul autorizării, obținerea respectivelor probe și calitatea lor deosebită fusese prevăzută, alături de îndeplinirea celorlalte condiții reglementate de art. 139 alin. (1) C.pr.pen. În același sens, s-ar putea în mod greșit concluziona că era îndeplinită condiția suspiciunii rezonabile prin prisma probelor obținute, însă, la momentul autorizării, procurorul să nu fi avut niciun temei factual (probe sau date) din care să rezulte o suspiciune rezonabilă.

În situația în care judecătorul de drepturi și libertăți va constata că au fost încălcate dispozițiile art. 141 alin. (1) C.pr.pen. privind autorizarea de către procuror a supravegherii tehnice, va infirma măsura și va dispune distrugerea probelor obținute în temeiul acesteia. Împotriva încheierii judecătorului de drepturi și libertăți, nu se poate exercita nicio cale de atac, procurorul fiind obligat să procedeze la distrugerea probelor obținute, consemnând operațiunea într-un proces-verbal. Aceasta va presupune inclusiv distrugerea procesului-verbal de redare rezumativă a activităților de supraveghere tehnică[1]. În doctrină s-a exprimat o îngrijorare justificată privind informațiile obținute în urma unei supravegheri tehnice infirmate de către judecătorul de drepturi și libertăți și care ar putea duce la obținerea de probe prin alte procedee[2]. Cu toate că probele obținute sunt distruse, nu se poate susține că organul de urmărire penală își va șterge din memorie cele constatate și va proceda apoi la administrarea unor probe în mod legal, având în vedere acele informații. În opinia noastră, considerăm că vor constitui **probe derivate**, fiind în același timp nelegale, și acele probe obținute în situațiile în care întrebuințarea procedeului probatoriu era condiționată de cunoașterea informațiilor obținute în urma supravegherii tehnice infirmate de judecătorul de drepturi și libertăți, iar natura acestor informații nu ar fi permis cunoașterea lor prin alte procedee probatorii. De exemplu, dacă, în urma supravegherii tehnice prin localizare sau urmărirea prin mijloace tehnice, se descoperă locul unde sunt depozitate droguri și se va realiza o percheziție domiciliară în baza acestor date, acest din urmă procedeu probatoriu va trebui să fie considerat nelegal, ca fiind derivat dintr-o probă obținută nelegal. O problemă particulară o constituie folosirea probelor și informațiilor rezultate din supravegherea tehnică pentru efectuarea unor acte de urmărire penală mai înainte de a se obține confirmarea judecătorului de drepturi și libertăți, într-o atare situație, și aceste procedee probatorii fiind posibil a fi considerate nelegale ca urmare a infirmării ordonanței de autorizare provizorie a supravegherii tehnice.

În cazul în care judecătorul de drepturi și libertăți va aprecia că autorizarea măsurilor de supraveghere tehnică dispuse de procuror s-a făcut în conformitate cu prevederile art. 141 alin. (1) C.pr.pen., va proceda la *confirmarea măsurii* prin încheiere. Considerăm că numai din

[1] *M.V. Tudoran*, Teoria și practica interceptărilor, 2012, p. 114.

[2] *Gh. Mateuț*, Observații critice privind noua reglementare a supravegherii tehnice într-o prezentare comparativă, în Caiete de Drept Penal nr. 3/2015, pp. 33-34.

acest moment probele obținute de procuror vor putea fi folosite în procesul penal. Cu toate că judecătorul de drepturi și libertăți constată legalitatea autorizării, el *nu se va pronunța asupra legalității probei*, acesta fiind atributul judecătorului de cameră preliminară. Ca atare, legalitatea probei va putea fi contestată de către părți în procedura de cameră preliminară, încheierea de confirmare a măsurii neavând autoritate de lucru judecat asupra legalității probei.

Pentru autorizarea de către procuror a accesului la un sistem informatic pentru o perioadă de 48 de ore, Codul de procedură penală conține o serie de prevederi exprese privind măsura, care nu se regăsesc în cazul accesului la un sistem informatic dispus prin procedura obișnuită. În cuprinsul art. 141 alin. (5) C.pr.pen. se arată că procurorul poate dispune prin ordonanță „*realizarea și conservarea unei copii a acestor date informatice* și *suprimarea accesării sau îndepărtarea acestor date informatice din sistemul informatic*". În același timp, se arată că toate copiile se vor realiza cu mijloace tehnice și proceduri adecvate de natură să asigure integritatea informațiilor conținute de acestea. Nu credem că în cadrul procedurii de autorizare provizorie se impunea ca legiuitorul să facă aceste mențiuni, mai ales în contextul în care, prin comparare cu accesul la un sistem informatic dispus de către judecătorul de drepturi și libertăți, procurorul pare a avea mai multe drepturi atunci când va proceda la autorizarea provizorie a măsurii, chestiune pe care o vom trata distinct la măsura de supraveghere tehnică a accesului la un sistem informatic[1].

[1] *V. infra*, Titlul V, Capitolul II.3.

Capitolul III
Punerea în executare a metodelor de supraveghere tehnică

Punerea în executare a metodelor speciale de supraveghere reprezintă una dintre cele mai importante probleme ale prezentei lucrări, cuprinzând atât cadrul legal prin care se pot obține probele, cât și elementele practice și tehnice prin care se poate realiza aducerea la îndeplinire a mandatului de supraveghere tehnică. În același timp, punerea în executare este și aspectul care a condus la probleme multiple în practică, mai ales în urma sancționării desfășurării de activități specifice punerii în executare de către organe necompetente sau care, deși la momentul punerii în executare erau competente, dispozițiile legale care permiteau delegarea acestora au fost constatate ca fiind neconstituționale.

Întrucât fiecare metodă specială de supraveghere tehnică are anumite particularități privind punerea în executare și dat fiind scopul acestei lucrări de a releva și aspectele practice ale punerii în executare, ne vom limita în prezenta secțiune la analizarea numai a elementelor comune punerii în executare a tuturor metodelor speciale de supraveghere tehnică pentru ca elementele particulare fiecărei măsuri să fie analizate distinct.

Secțiunea 1. Organele care pot pune în executare supravegherea tehnică

Ulterior emiterii mandatului de supraveghere tehnică de către judecătorul de drepturi și libertăți, acesta urmează a fi pus în executare între limitele stabilite de mandat și sub controlul și supravegherea procurorului. Problema centrală relevată de practică în punerea în executare este determinarea organului competent să realizeze activitățile autorizate, sens în care în prezenta secțiune vom discuta stadiul actual al legislației după pronunțarea Deciziei Curții Constituționale nr. 51/2016[1].

În privința competenței de a pune în executare mandatul de supraveghere emis de judecătorul de drepturi și libertăți, aceasta îi aparține *procurorului* ca regulă. Prin aceasta se manifestă o aplicare a faptului că procurorul este singurul titular al acțiunii penale în cursul urmăririi penale[2]. Cu toate acestea, Codul de procedură penală recunoaște că domeniul supravegherii tehnice este unul specializat și poate fi oportună apelarea la alte persoane cu cunoștințe specializate în domeniu care pot acorda concurs tehnic procurorului. În funcție și de întinderea măsurilor de supraveghere tehnică, procurorul va avea posibilitatea de a delega punerea în executare a măsurilor de supraveghere tehnică către organe limitativ menționate de lege. Curtea Constituțională face distincție între concurs tehnic și punere în executare, concursul tehnic nefiind vizat de Decizia Curții Constituționale nr. 51/2016, care se referă doar la expresia „alte organe ale statului" din cuprinsul dispozițiilor art. 142 alin. (1) C.pr.pen. din forma de la momentul pronunțării hotărârii[3].

Deoarece art. 142 C.pr.pen. instituie un regim unitar privind toate metodele de supraveghere tehnică, unele care nu presupun cunoștințe specializate deosebite (de pildă, supravegherea

[1] CCR, Dec. nr. 51 din 16 februarie 2016 (M. Of. nr. 190 din 14 martie 2016).

[2] *Gr.Gr. Theodoru*, Tratat de Drept procesual penal, ed. a 3-a, Ed. Hamangiu, București, 2013, p. 122.

[3] CCR, Dec. nr. 720 din 20 noiembrie 2018 (M. Of. nr. 183 din 7 martie 2019) (decizie de respingere).

video, audio sau prin fotografiere), acestea pot fi realizate de către procuror ori de către *organul de cercetare penală*, în baza unei ordonanțe emise în acest sens. Ordonanța emisă în temeiul art. 142 alin. (1) C.pr.pen. pentru punerea în executare de către organul de cercetare penală a supravegherii tehnice va avea natura unei ordonanțe de delegare în conformitate cu prevederile art. 324 alin. (3) C.pr.pen. În doctrină s-a susținut și opinia contrară, că nu se va putea vorbi de o delegare, ci de o dispunere din partea procurorului și că aceasta nu ar presupune să îmbrace forma unei ordonanțe[1].

În anumite situații, întrebuințarea metodelor de supraveghere tehnică implică cunoștințe tehnice avansate, precum și accesul la aparatură specializată care să faciliteze realizarea activităților specifice. De pildă, în cazul înregistrării convorbirilor purtate de anumite persoane care se impun a fi înregistrate în mediu ambiental, se arată că: „*pentru interceptarea convorbirilor purtate nemijlocit se folosesc diferite tipuri de microfoane cu fir, microemițătoare disimulate ori sisteme direcționale optice. Totalitatea aparaturii necesare desfășurării operațiunii este cunoscută sub denumirea specifică de tehnică operativă*"[2]. Această tehnică operativă poate impune folosirea ei de către persoane special școlite în vederea utilizării cu maximă eficiență a acestora, putând fi *lucrători specializați din cadrul poliției*. Ținând seama că Poliția Română are capacități logistice deosebite, este lesne de înțeles de ce legiuitorul a ales să abiliteze lucrătorii de poliție cu punerea în executare a mandatelor de supraveghere tehnică. Totuși, așa cum corect s-a identificat în literatura de specialitate[3], în cuprinsul Legii nr. 218/2002, republicată[4], nu este definită o structură specializată a poliției pentru punerea în executare a supravegherii tehnice, astfel că termenul de „lucrători specializați" poate fi privit ca unul generic la acest moment. Deși s-a încercat să se lămurească sensul acestui termen, prin identificarea organelor care se circumscriu sintagmei „lucrători specializați din cadrul poliției" în contextul pronunțării Deciziei nr. 51/2016 a Curții Constituționale, Înalta Curte de Casație și Justiție a respins această solicitare, apreciind că nu se poate proceda la interpretarea de către instanța supremă a unei decizii a Curții Constituționale, revenind în sarcina fiecărei instanțe să aplice dezlegările sale în mod direct[5].

Anterior pronunțării Deciziei nr. 51/2016, punerea în executare se putea realiza de lucrători specializați *de la alte organe specializate ale statului*. În concret, era vorba de lucrători din cadrul serviciilor de informații care nu erau competenți să efectueze acte de urmărire în cauzele penale. Ca soluție la problema imixtiunii serviciilor secrete în urmărirea penală, criticată de Curtea Constituțională, legiuitorul a ales să relegalizeze instituția anchetatorului penal din cadrul unui serviciu secret, prin O.U.G. nr. 6/2016, care include ofițerii S.R.I. în categoria organelor de cercetare speciale, în cazul infracțiunilor contra securității naționale și în cazul infracțiunilor de terorism[6]. O atare soluție o considerăm nefericită, deoarece va

[1] *Gh. Ivan, V. Ioniță*, Una din problematicile punerii în executare a mandatelor de supraveghere tehnică, în Revista Pro Lege nr. 1/2017, pp. 129-130.

[2] *M. Udroiu*, Dicționar de drept penal și de procedură penală, Ed. C.H. Beck, București, 2009, p. 212.

[3] *Gh. Mateuț*, Procedură penală, 2019, p. 699.

[4] Publicată în M. Of. nr. 305 din 9 mai 2002 și republicată în M. Of. nr. 170 din 2 martie 2020.

[5] ICCJ, Completul pentru dezlegarea unor chestiuni de drept, Dec. nr. 22 din 25 octombrie 2016 (M. Of. nr. 1057 din 28 decembrie 2016).

[6] Conform art. 13 din Legea nr. 14/1992 privind organizarea și funcționarea Serviciului Român de Informații, „organele Serviciului Român de Informații nu pot efectua acte de cercetare penală, nu pot lua măsura reținerii sau arestării preventive și nici dispune de spații proprii de arest. Prin excepție, organele Serviciului Român de Informații pot fi desemnate organe de cercetare penală speciale conform art. 55 alin. (5) și (6) din Codul de procedură penală pentru punerea în executare a mandatelor de supraveghere tehnică, conform prevederilor art. 57 alin. (2) teza finală din Codul de procedură penală".

permite punerea în executare a supravegherii tehnice de către ofițerii S.R.I., în cazul urmăririi penale a acestor infracțiuni.

Chiar și în situația în care înregistrarea unei conversații este realizată de procuror ori de către organul de cercetare penală, poate fi necesar concursul unor specialiști care, prin folosirea de programe informatice specifice ori aparatură audio avansată, să proceseze înregistrarea audio în vederea eliminării zgomotelor de fundal și a amplificării vocilor persoanelor vizate cu scopul unei mai bune înțelegeri a cuvintelor rostite. Totodată, folosirea unor dispozitive tehnice pentru localizarea sau urmărirea prin mijloace tehnice presupune cunoștințe de specialitate în utilizarea unor dispozitive ce asigură locația prin GPS, care se montează asupra persoanei vizate (de regulă, se atașează de mașina acestei persoane pentru a fi urmărită unde se deplasează cu acel mijloc de transport).

În alte situații, organele de urmărire penală și chiar lucrătorii specializați din cadrul poliției nu au pregătirea tehnică necesară pentru punerea în aplicare a mandatului de supraveghere tehnică. Această problemă este mai puțin întâlnită în cadrul direcțiilor specializate din cadrul P.I.C.C.J. – D.N.A. și, mai ales, D.I.I.C.O.T., care întrebuințează cel mai des metode de supraveghere tehnică[1]. În orice caz, pentru a putea pune în executare supravegherea tehnică, este necesar ca organul să aibă atribuții în domeniul investigării infracțiunilor și lucrătorul de poliție să fi obținut avizul de poliție judiciară, conform Legii nr. 364/2004 privind organizarea și funcționarea poliției judiciare (republicată în M. Of. nr. 305 din 24 aprilie 2014).

În cadrul Direcției Generale Anticorupție din Ministerul Afacerilor Interne există Serviciul tehnic din cadrul Direcției de investigații, căruia îi revin sarcini cu privire la punerea în executare a unui mandat de supraveghere tehnică, acestea fiind prevăzute la art. 46 din Ordinul Ministrului Afacerilor Interne nr. 119 din 25 iulie 2014 pentru aprobarea Regulamentului de organizare și funcționare a Direcției Generale Anticorupție[2]. Serviciul tehnic este responsabil cu punerea în executare a mandatelor de supraveghere tehnică în privința anumitor operațiuni concrete și numai în baza delegării exprese făcute de procuror, putând, totodată, oferi suport tehnic în sprijinul actelor efectuate personal de procuror sau de către organul de cercetare penală delegat. Cu concursul altor autorități ale statului (C.N.I.C. din cadrul S.R.I.), Serviciul

---

[1] *V. Trif, A. Petre*, Activitățile preliminare realizate de către echipa de cercetare în cazul constatării infracțiunilor de corupție, în Curierul Judiciar nr. 4/2017, p. 218.

[2] Art. 46 din Ordinul nr. 119/2014: „Serviciul tehnic este condus de șeful de serviciu, se subordonează conducerii Direcției investigații și are următoarele atribuții principale:

a) efectuează, în baza ordonanței de delegare, activitățile de supraveghere video, audio sau prin fotografiere, precum și urmărirea prin mijloace tehnice, dispuse prin mandatul de supraveghere tehnică;

b) la solicitarea aparatului propriu sau structurilor subordonate ale direcției generale asigură suportul tehnic necesar pe parcursul misiunilor operative;

c) efectuează activități criminalistice în cauzele penale ce intră în competența direcției generale;

d) efectuează activități de mascare, disimulare, adaptare a mijloacelor tehnice speciale, proiectare și execuție circuite electronice conform specificului misiunilor operative;

e) desfășoară activități de prelucrare a înregistrărilor audio-video obținute cu ajutorul mijloacelor tehnice pe parcursul misiunilor operative;

f) asigură utilizarea eficientă, păstrarea, întreținerea și gestionarea tehnicii operative aflate în dotarea serviciului;

g) desfășoară activități de instruire a personalului cu privire la utilizarea mijloacelor tehnice speciale, la solicitarea structurilor aparatului propriu și structurilor subordonate;

h) asigură documentarea permanentă a specialiștilor serviciului în scopul dotării cu mijloace tehnice speciale performante și dezvoltării activității specifice;

i) acordă sprijin de specialitate, prin întocmirea specificațiilor tehnice pentru mijloacele tehnice speciale ce urmează a fi achiziționate pentru dotarea serviciului sau structurilor subordonate".

tehnic din cadrul Direcției Generale Anticorupție va pune în executare în special mandatele de supraveghere privind *interceptarea comunicațiilor și a oricărui tip de comunicare la distanță*[1].

În privința *interceptărilor comunicațiilor telefonice*, competența de a asigura logistica (tehnica) punerii în executare a măsurii de supraveghere tehnică aparține S.R.I., îndatorire prevăzută de legea de organizare a acestei autorități. Această situație de fapt a reprezentat o problemă deosebită în practică anterior Deciziei nr. 51/2016 a Curții Constituționale, deoarece punerea în executare se realiza de către ofițerii S.R.I. În prezent, Serviciul Român de Informații, prin C.N.I.C., asigură doar un concurs tehnic în realizarea supravegherii tehnice prin activități, precum: întreținerea dispozitivelor care permit interceptarea, asigurarea de pregătire în vederea accesării sistemului de către organele de urmărire penală, instalarea și suportul tehnic pentru terminalele din incinta parchetelor folosite pentru accesarea sistemului, fără a avea acces sau control cu privire la datele introduse în sistem de un operator sau cu privire la rezultatele supravegherii tehnice, deși această problemă o vom trata distinct. Trebuie menționat că, față de situația din trecut, Serviciul Român de Informații nu mai intervine în punerea în executare a supravegherii tehnice prin interceptarea, înregistrarea, ascultarea, selectarea și redarea în scris a conversațiilor interceptate, aceste acte fiind esența punerii în executare, ele fiind realizate, în prezent, doar de organele competente amintite de art. 142 alin. (1) C.pr.pen. În mod justificat s-a arătat că activitatea trecută a S.R.I. punea în discuție legalitatea acestei probe[2] prin prisma faptului că procurorul nu participa la supravegherea tehnică efectivă.

Interceptarea comunicațiilor telefonice se poate realiza și prin alte mijloace decât cele administrate de S.R.I.[3], precum dispozitivele Stingray[4], pentru comunicațiile prin telefon mobil, ori metode clasice, în cazul telefoanelor fixe – prin releuri, inducție electromagnetică, crearea unei derivații etc.

Alături de organele arătate mai jos, trebuie să amintim în cadrul problemei competenței și prevederile art. 142 alin. (2) C.pr.pen., prin care se reglementează obligația furnizorilor de rețele publice de comunicații și a furnizorilor de servicii de comunicații electronice sau de orice tip de comunicare ori de servicii financiare de a *colabora cu organele de urmărire penală sau cu autoritățile prevăzute la art. 142 alin. (1) C.pr.pen., în limitele competențelor acestora, pentru punerea în executare a mandatului de supraveghere tehnică*.

Persoanele chemate să dea concurs supravegherii tehnice pot fi furnizorii de rețele publice de comunicații electronice, furnizorii de servicii de comunicații electronice destinate publicului ori un furnizor de servicii de comunicare de orice alt tip. În privința ultimului tip de furnizor, acesta ar presupune furnizori de alte servicii de comunicare decât cele electronice. Totodată, concursul tehnic poate fi oferit în cazul interceptării comunicațiilor și de C.N.I.C. din cadrul S.R.I.

În practica judiciară de după Decizia Curții Constituționale nr. 51/2016, pentru protejarea probelor obținute în mod nelegal de către organele de urmărire penală prin punerea în executare a supravegherii tehnice de către S.R.I., s-a acreditat ideea că acest serviciu a furnizat numai un

[1] *A. Petre, C. Grigoraș*, Înregistrările audio și audio-video, mijloace de probă în procesul penal, Ed. C.H. Beck, București, 2008, pp. 52-53.

[2] *S. Grădinaru*, Supravegherea tehnică, 2014, p. 69.

[3] Orice furnizor de servicii de comunicații electronice este obligat, conform art. 8 alin. (2) lit. k) din O.U.G. nr. 111/2011.

[4] Dispozitivele tip Stingray sunt fabricate de *Harris Corporation*, în S.U.A., și au fost proiectate special pentru a fi folosite de armată, dar sunt mai des folosite și de poliție. Acestea au început să fie folosite și în Europa în anul 2015, fiind depistate în zona Londrei. Aceste dispozitive captează codul IMSI al unui telefon și permit o serie de funcții avansate dintre care cea mai importantă este interceptarea convorbirilor purtate – *news.sky.com*

suport sau sprijin tehnic, procurorii adoptând în mod unitar această susținere. În toate cazurile în care instanțele sau judecătorii de cameră preliminară au cercetat mai amănunțit problema, s-a descoperit o cutumă a transmiterii mandatelor de supraveghere tehnică către serviciile de informații printr-o adresă de înaintare, cu formularea generică „în vederea punerii în executare a măsurii". În aceste situații, deși se susținea că procurorul a pus în executare măsura, nu putea fi indicat niciun act concret realizat de procuror, deoarece interceptarea, înregistrarea, selectarea convorbirilor relevante, redarea lor în format scris se realiza de ofițerii S.R.I. Aceste tipuri de acte vor constitui o punere în executare și se vor diferenția de concursul tehnic care se va desfășura sub controlul și coordonarea organelor de urmărire penală, acestea din urmă fiind singurele abilitate să realizeze acțiunile prin care se obțin probele în procesul penal.

Codul de procedură penală impune tuturor persoanelor care dau concurs tehnic, inclusiv persoanelor prevăzute de art. 142 alin. (2) C.pr.pen., să păstreze secretul operațiunii efectuate, sub sancțiunea legii penale. Prevederea aceasta este una necesară atât pentru a se asigura secretul operațiunilor autorizate, cât și pentru a proteja persoana față de care s-a dispus încuviințarea metodelor de supraveghere tehnică. În măsura în care persoanele în cauză divulgă informații privind realizarea supravegherii tehnice, vor fi întrunite elementele constitutive ale celei de-a doua forme tip a infracțiunii de divulgarea informațiilor secrete de serviciu sau nepublice, prevăzută de art. 304 alin. (2) C.pen.[1], în cazul în care subiectul activ nu va avea calitatea de funcționar, însă dacă are această calitate, i se va putea reține infracțiunea de divulgarea secretului profesional, prevăzută de art. 227 C.pen.[2]. În jurisprudența Curții Europene a Drepturilor Omului s-a arătat că divulgarea de către agenți ai statului (funcționari publici) a unor date cu caracter personal reprezintă o violare a dreptului la viață privată a persoanei, în cazul divulgării în mass-media a convorbirilor private ale unei persoane care face obiectul unei cauze penale[3].

Secțiunea a 2-a. Consecințele Deciziei Curții Constituționale nr. 51/2016 privind punerea în executare a supravegherii tehnice

La momentul intrării în vigoare a Codului de procedură penală, reglementarea punerii în executare a mandatelor de supraveghere tehnică era diferită față de cea prezentă, textul permițând punerea în executare de către un număr nedeterminabil de organe, ceea ce a condus la pronunțarea Deciziei Curții Constituționale nr. 51/2016[4].

Potrivit art. 142 alin. (1) C.pr.pen., în forma de la data intrării în vigoare a legii: „*procurorul pune în executare supravegherea tehnică ori poate dispune ca aceasta să fie efectuată de organul de cercetare penală sau de lucrători specializați din cadrul poliției ori de* ***alte organe specializate ale statului***" (s.n.). Ultima sintagmă a dispozițiilor legale a fost criticată, apreciindu-se ca fiind contrară dispozițiilor art. 1 alin. (3) și (5) din Constituția României. Contextul formulării excepției

[1] Conform art. 304 alin. (2) C.pen., constituie infracțiune: „divulgarea, fără drept, a unor informații secrete de serviciu sau care nu sunt destinate publicității, de către cel care ia cunoștință de acestea, se pedepsește cu închisoare de la o lună la un an sau amendă".

[2] Conform art. 227 alin. (1) C.pen., constituie infracțiune: „divulgarea, fără drept, a unor date sau informații privind viața privată a unei persoane, de natură să aducă un prejudiciu unei persoane, de către acela care a luat cunoștință despre acestea în virtutea profesiei ori funcției și care are obligația păstrării confidențialității cu privire la aceste date, se pedepsește cu închisoare de la 3 luni la 3 ani sau amendă".

[3] CEDO, cauza *Căşuneanu c. România*, Hotărârea din 16 aprilie 2013, §97, pe *hudoc.echr.coe.int*

[4] CCR, Dec. nr. 51 din 16 februarie 2016 (M. Of. nr. 190 din 14 martie 2016).

de neconstituționalitate a fost realizarea de acte de supraveghere tehnică (interceptarea comunicațiilor) în cauzele penale, de către Serviciul Român de Informații, fără ca acest organ să fie un organ de urmărire penală[1]. Acest context este deosebit de important, deoarece gravitatea încălcării drepturilor și libertăților persoanelor care puteau fi vizate este dată de lipsa oricărui control asupra S.R.I. din partea procurorului sau a instanțelor de judecată în realizarea supravegherii tehnice[2]. În plus, nu exista nicio garanție că datele și informațiile rezultate din supravegherea tehnică nu vor putea fi folosite și în scop operativ de către serviciul secret, sens în care puteau fi eludate dispozițiile legale privind arhivarea și distrugerea datelor rezultate care nu au legătură cu cauza.

În evaluarea constituționalității normei atacate, Curtea a reținut că activitățile de punere în executare a mandatelor de supraveghere realizate de *alte organe specializate ale statului* reprezintă procedeele probatorii care stau la baza obținerii procesului-verbal de consemnare a rezultatelor activităților de supraveghere tehnică, care va constitui mijloc de probă, motiv pentru care acestea se pot realiza numai de organele de urmărire penală prevăzute de art. 55 alin. (1) C.pr.pen.[3].

Curtea a motivat că expresia „alte organe specializate ale statului" este lipsită de claritate, precizie și previzibilitate, nepermițând subiecților să înțeleagă care sunt aceste organe, reținându-se că nu se poate stabili nici domeniul de activitate al unor asemenea organe, întrucât în România activează multiple astfel de organe „*în afara Serviciului Român de Informații, la care fac referire autorii excepției, care, potrivit art. 1 și art. 2 din Legea nr. 14/1992 privind organizarea și funcționarea Serviciului Român de Informații, publicată în Monitorul Oficial al României, Partea I, nr. 33 din 3 martie 1992, și art. 6 și art. 8 din Legea nr. 51/1991 privind securitatea națională a României, republicată în Monitorul Oficial al României, Partea I, nr. 190 din 18 martie 2014, are atribuții exclusiv în domeniul siguranței naționale, neavând atribuții de cercetare penală, conform art. 13 din Legea nr. 14/1992, există și alte servicii cu atribuții în domeniul securității naționale, precum și o multitudine de organe specializate ale statului cu atribuții în varii domenii, cum sunt, cu titlu exemplificativ, Garda Națională de Mediu, Gărzile Forestiere, Autoritatea Națională pentru Protecția Consumatorilor, Inspectoratul de Stat în Construcții, Consiliul Concurenței sau Autoritatea de Supraveghere Financiară, niciuna dintre acestea neavând atribuții de cercetare penală*"[4]. O altă constatare importantă a Curții a fost în sensul în care nu se putea stabili o competență a punerii în executare a măsurilor de

[1] *Ibidem*, §14. Astfel cum susținea apărătorul petenților în fața Curții Constituționale: „dispozițiile Codului de procedură penală nu precizează exact care sunt organele ce intră în categoria «altor organe specializate ale statului», dar care, totuși, pot efectua supravegherea tehnică, conform art. 142 alin. (1) din Codul de procedură penală, alături de procuror, de organele de cercetare penală și de lucrătorii specializați din cadrul poliției. Se susține că sintagma criticată dă posibilitatea Serviciului Român de Informații să efectueze acte de procedură în cadrul procesului penal, prin interceptarea și înregistrarea de convorbiri în cauzele penale".

[2] Conform art. 1 alin. (2)-(4) din Legea nr. 14 din 24 februarie 1992 privind organizarea și funcționarea Serviciului Român de Informații:

„(2) Activitatea Serviciului Român de Informații este controlată de parlament. Anual sau când Parlamentul hotărăște, directorul Serviciului Român de Informații prezintă acestuia rapoarte referitoare la îndeplinirea atribuțiilor ce revin Serviciului Român de Informații, potrivit legii.

(3) În vederea exercitării controlului concret și permanent, se constituie o comisie comună a celor două Camere.

(4) Organizarea, funcționarea și modalitățile de exercitare a controlului se stabilesc prin hotărâre adoptată de Parlament".

[3] CCR, Dec. nr. 51 din 16 februarie 2016, §34 (M. Of. nr. 190 din 14 martie 2016).

[4] *Ibidem*, §37.

supraveghere tehnică decât în măsura în care o asemenea competență este prevăzută de lege, și nu de un act normativ cu valoare juridică inferioară acesteia[1]. Date fiind ingerințele aduse vieții private a unei persoane prin metodele de supraveghere tehnică, legea va trebui să aibă un caracter previzibil atât pentru persoanele vizate, cât și pentru organele de urmărire penală și pentru instanțe[2]. Din acest punct de vedere, Curtea consideră că este justificată menționarea organelor de urmărire penală și a lucrătorilor specializați din Poliția Română în cuprinsul art. 142 alin. (1) C.pr.pen., în accepțiunea că aceștia din urmă pot deține avizul de ofițeri de poliție judiciară în condițiile art. 55 alin. (5) C.pr.pen.[3]. Este interesantă soluția dată de Curte în privința lucrătorilor specializați de poliție, în sensul stabilirii ca fiind necesară numai aptitudinea de a fi învestite cu avizul prevăzut de lege pentru a fi organe de cercetare penală speciale, întrucât rezultă că punerea în executare a măsurilor de supraveghere tehnică va putea fi realizată și de către un lucrător specializat al poliției care nu deține un aviz de acest fel. Credem că ceea ce a dorit Curtea să sublinieze este că numai un organ clar definit de lege și cu atribuții judiciare în cursul urmăririi penale poate proceda la punerea în executare a supravegherii tehnice.

În cazul *altor organe specializate ale statului*, Curtea a constatat că expresia nu este prevăzută în Codul de procedură penală și în alte legi speciale, nefiind definită și neprezentând claritate și previzibilitate, fiind încălcat art. 1 alin. (3) din Constituție referitor la statul de drept, în componenta privind garantarea drepturilor, și a art. 1 alin. (5) din Constituție, care consacră principiul legalității.

Gravitatea încălcării drepturilor cetățenilor, prin permiterea unei instituții cu atribuții de securitate națională – serviciu secret – de a avea rolul de organ de urmărire penală, a fost subliniată de Curte prin necesitatea ca instanțele să procedeze la aplicarea efectelor deciziei în toate cauzele pendinte, reținând că „*nu se va aplica în privința cauzelor definitiv soluționate până la data publicării sale, aplicându-se, însă, în mod corespunzător, în cauzele aflate pe rolul instanțelor de judecată*"[4].

Această primă decizie a permis organelor judiciare verificarea legalității interceptărilor în toate cauzele penale, la acel moment, prin prisma sancțiunii nulității relative, care intervenea în cazul încălcării competenței materiale sau funcționale a organelor de urmărire penală. În condițiile în care, la acel moment, S.R.I. deținea monopolul în privința interceptării comunicațiilor prin intermediul furnizorilor de servicii publice de comunicații electronice, toate celelalte servicii secrete apelând la tehnica S.R.I. pentru a realiza astfel de interceptări, instanțele au fost puse în situația verificării legalității acestor procedee probatorii în măsura în care cauza se afla în faza camerei preliminare. Limitarea privind faza procesuală era dată de nulitatea relativă incidentă în cauză care, pentru actele de urmărire penală efectuate într-o cauză, permitea invocarea ei până la închiderea procedurii de cameră preliminară, după acest moment neputând fi invocată o atare nelegalitate.

Efectele Deciziei Curții Constituționale nr. 51/2016 nu au fost resimțite din plin decât după ce Curtea Constituțională a stabilit că normele privind competența organelor de urmărire penală sunt de ordine publică și nu se poate accepta ca încălcarea acestora să fie sancționată numai în condițiile nulității relative, relevându-se un regres major față de Codul de procedură penală anterior.

---

[1] *Ibidem*, §47.

[2] *D. Grădinaru*, Punerea în executare a mandatelor de supraveghere tehnică după Decizia nr. 51/2016 a Curții Constituționale a României, în Curierul Judiciar nr. 6/2017, p. 342.

[3] CCR, Dec. nr. 51 din 16 februarie 2016, §49 (M. Of. nr. 190 din 14 martie 2016).

[4] *Ibidem*, §52.

În urma Deciziei Curții Constituționale nr. 302/2017[1] privind neconstituționalitatea dispozițiilor art. 281 alin. (1) lit. b) C.pr.pen., care sancționau cu nulitatea absolută numai încălcarea dispozițiilor privind competența materială și personală a instanțelor judecătorești, s-a stabilit că este neconstituțională soluția legislativă care limitează această sancțiune. Se arăta la par. 58 din Decizie că: „*eliminarea din categoria nulităților absolute a nerespectării dispozițiilor referitoare la competența materială și după calitatea persoanei a organului de urmărire penală permite aplicarea în procesul penal a unui criteriu subiectiv de apreciere din partea organului de urmărire penală. Astfel, prin nereglementarea unei sancțiuni adecvate în cazul nerespectării de către organul de urmărire penală a competenței sale materiale și după calitatea persoanei, legiuitorul a creat premisa aplicării aleatorii a normelor de competență pe care le-a adoptat*". Ca urmare a caracterului intolerabil al aleatoriului în cauzele penale, mai ales sub aspectul necompetenței după materie și persoană, exista posibilitatea ca orice persoană, fie organ de urmărire penală sau nu, să efectueze acte de urmărire penală prin înfrângerea principiului legalității. Acest aspect era evident în cazul supravegherii tehnice prin interceptarea comunicațiilor, în care nu exista o sancțiune procesuală eficientă pentru înlăturarea încălcărilor cauzate de punerea în executare a acestei măsuri de către S.R.I.

Continuând raționamentul său, Curtea Constituțională arăta că: „*dovedirea unei vătămări a drepturilor unei persoane exclusiv prin nerespectarea de către organul de urmărire penală a dispozițiilor referitoare la competența după materie și după persoană se transformă într-o probă greu de realizat de către cel interesat, ce echivalează, în fapt, cu o veritabilă probatio diabolica, și implicit determină încălcarea dreptului fundamental la un proces echitabil. Tocmai de aceea legiuitorul codurilor de procedură penală anterioare a prevăzut sub sancțiunea nulității absolute nerespectarea normelor de competență materială și după calitatea persoanei a organului de urmărire penală, vătămarea procesuală fiind, în această situație, prezumată iuris et de iure*"[2]. Necesitatea unei asemenea constatări era dată și de jurisprudența instanțelor în domeniul supravegherii tehnice, considerându-se că punerea în executare a măsurii de către S.R.I. – organ necompetent – nu ar produce vătămări, și orice posibilă vătămare ar putea fi acoperită prin certificarea proceselor-verbale de către procuror[3].

Chiar dacă s-a constatat că va fi incidentă sancțiunea nulității absolute în cazul punerii în executare a supravegherii tehnice de către un organ necompetent, Codul de procedură penală nu oferă posibilitatea excluderii unor probe decât în faza camerei preliminare, ceea ce contravenea cu obligația instanțelor de a aplica jurisprudența Curții Constituționale. Soluția jurisprudențială a fost constatarea nulității absolute a punerii în executare a supravegherii tehnice și înlăturarea probelor obținute în mod nelegal.

În jurisprudența recentă a Curții Constituționale, respectiv prin Decizia nr. 26/2019[4], Curtea Constituțională s-a pronunțat asupra soluționării conflictului de natură constituțională dintre Ministerul Public – Parchetul de pe lângă Înalta Curte de Casație și Justiție, Parlamentul României, Înalta Curte de Casație și Justiție și celelalte instanțe judecătorești. Prin decizia antemenționată s-a constatat nelegalitatea încheierii Protocolului nr. 00750 din 04.2009 dintre Parchetul de pe lângă Înalta Curte de Casație și Justiție și Serviciul Român de Informații, în sensul că prin acest protocol s-a procedat la implementarea ocultă a unei proceduri de lucru

[1] CCR, Dec. nr. 302 din 4 mai 2017 (M. Of. nr. 566 din 17 iulie 2017).

[2] *Ibidem*, §62.

[3] C. Ap. Alba Iulia, s. pen., încheierea nr. 77 din 7 iunie 2016.

[4] CCR, Dec. nr. 26 din 16 ianuarie 2019 asupra cererii de soluționare a conflictului juridic de natură constituțională dintre Ministerul Public – Parchetul de pe lângă Înalta Curte de Casație și Justiție, Parlamentul României, Înalta Curte de Casație și Justiție și celelalte instanțe judecătorești (M. Of. nr. 193 din 12 martie 2019).

între parchete și S.R.I. privind punerea în executare a mandatelor de supraveghere tehnică, deși această atribuție o avea procurorul. Consecințele procesuale ale administrării probelor de către un organ necompetent, în speță S.R.I., sunt tratate de Curtea Constituțională: „*Curtea subliniază că administrarea probelor de către alte organe decât cele judiciare încalcă competența materială a organelor de urmărire penală, ceea ce atrage aplicarea sancțiunii prevăzute de art. 281 alin. (1) lit. b) din Codul de procedură penală,* ***respectiv nulitatea absolută a actelor prin care s-a administrat aceasta****. De asemenea, aceeași sancțiune se impune și în privința actelor prin care s-a administrat o probă de către organele de urmărire penală, fără a se ține cont de calitatea persoanei*”[1] (s.n.).

Jurisprudența Curții Constituționale susține fără echivoc că nulitatea absolută a oricărui act procesual sau procedural poate fi invocată în orice fază a procesului penal, și nu doar în procedura camerei preliminare. De aceea, prin Decizia nr. 26/2019, Curtea a stipulat o obligație generală pentru toate organele judiciare de a analiza legalitatea actelor efectuate prin aplicarea protocoalelor dintre P.I.C.C.J. și S.R.I.: „*având în vedere art. 197 alin. (2) din Codul de procedură penală din 1968 și art. 281 din Codul de procedură penală, acest din urmă text coroborat cu Decizia Curții Constituționale nr. 302 din 4 mai 2017, prin care s-a constatat că soluția legislativă cuprinsă în dispozițiile art. 281 alin. (1) lit. b) din Codul de procedură penală, care nu reglementează în categoria nulităților absolute încălcarea dispozițiilor referitoare la competența materială și după calitatea persoanei a organului de urmărire penală, este neconstituțională, revine Înaltei Curți de Casație și Justiție și celorlalte instanțe judecătorești, precum și Ministerului Public – Parchetul de pe lângă Înalta Curte de Casație și Justiție și* ***unităților subordonate să verifice în cauzele pendinte****, în ce măsură s-a produs o încălcare a dispozițiilor referitoare la competența materială și după calitatea persoanei a organului de urmărire penală, și să dispună măsurile legale corespunzătoare*”[2] (s.n.).

În practică, această ultimă decizie a determinat instanțele să cerceteze implicarea S.R.I. sub mai multe aspecte, respectiv: constituirea de echipe operative comune; transmiterea de informații obținute din derularea activităților operative care prezentau relevanță și care ar putea fi valorificate în cadrul procesului penal; acordarea de sprijin prin efectuarea de activități de investigații și supraveghere operativă; punerea la dispoziție de informații și documente care puteau sprijini documentarea faptelor; încheierea unui plan comun de acțiune; furnizarea de informații cu privire la persoanele menționate, pe parcursul anchetei penale; oferirea de sprijin tehnic pentru punerea în executare a unor acte de autorizare a supravegherii tehnice – resurse umane sau materiale, transcriere trafic brut rezultat din exploatarea actelor de autorizare, transmitere convorbiri transcrise, întocmire de procese-verbale de transcriere[3]. Ca atare, rolul instanței va fi unul activ în lumina jurisprudenței Curții Constituționale și va trebui să privească nu numai măsurile de supraveghere tehnică, dar orice colaborare a serviciilor secrete cu organele de urmărire penală. O atare verificare va presupune investigarea întregii corespondențe dintre parchet și serviciul secret, nefiind suficient, după cum vom vedea mai jos, ca instanța să se încreadă în susținerile procurorului.

Ținând seama de jurisprudența Curții antemenționată, instanțele au recunoscut în mod universal obligația cercetării împrejurărilor în care s-a realizat punerea în executare a supravegherii tehnice în cauzele penale, trebuind să identifice orice interferență sau rol pe care l-ar fi avut S.R.I. ori alte organe specializate ale statului.

[1] *Ibidem*, §208.

[2] *Ibidem*, §211.

[3] C. Ap. București, s. a II-a pen., dec. nr. 1123/A din 18 septembrie 2019, pronunțată în dosar nr. 18875/3/2012, nepublicată.

În jurisprudența instanțelor s-a putut observa o poziție constantă a Ministerului Public în a minimaliza rolul S.R.I. și a altor servicii secrete în punerea în executare a mandatelor de supraveghere tehnică în disonanță cu realitățile cauzei. Astfel, într-o cauză aflată în faza camerei preliminare, procurorul a susținut în fața judecătorului de cameră preliminară că D.G.P.I. a realizat numai un suport tehnic în punerea în executare a mandatelor de supraveghere tehnică și nu a pus în executare mandatul judecătorului de drepturi și libertăți în sensul dispozițiilor art. 142 alin. (1) C.pr.pen. Judecătorul de cameră preliminară, la cererea apărării, a solicitat corespondența purtată de unitatea de parchet cu serviciul secret, procurorul general subliniind, în adresa de înaintare, că serviciul secret a furnizat numai suport tehnic. În schimb, din corespondența purtată cu D.G.P.I. rezulta că procurorul a transmis către această instituție mandatele de supraveghere tehnică printr-o adresă în care menționa transmiterea lor „în vederea punerii în executare". Corelativ, fiind solicitat de către judecătorul de cameră preliminară, serviciul secret a recunoscut punerea în executare a supravegherii tehnice, redarea convorbirilor interceptate și transmiterea notelor de redare către organul de urmărire penală. Soluția adoptată a fost cea a nulității absolute a punerii în executare a supravegherii tehnice, a mijloacelor de probă obținute și excluderea probei obținute[1].

Această cauză, precum și multe altele[2] au presupus un control nemijlocit al instanței asupra modului de punere în executare a mandatelor de supraveghere tehnică, printr-un control al corespondenței purtate de organele de urmărire penală cu serviciile secrete care puneau în executare mandatele de supraveghere tehnică. Corespondența indicată are caracter secret și impune declasificarea sa prealabilă mai înainte de a fi transmisă instanței, conținând, de regulă, adrese de transmitere a unor înregistrări realizate de serviciul secret, note de redare, e-mailuri din care rezultă că un organ necompetent a generat, a avut acces și a procesat datele și informațiile rezultate din activitățile de supraveghere tehnică. În cazul în care nu se va putea obține declasificarea corespondenței, ca urmare a refuzului serviciului secret, apreciem că instanța va fi obligată să constate nulitatea absolută a procedeului probatoriu, întrucât nu se va putea realiza un control asupra competenței materiale și personale de efectuare a unui act de urmărire penală. O atare situație impune constatarea nulității pentru salvgardarea drepturilor apărării care este pusă în imposibilitate de a contesta în mod efectiv necompetența fără a avea acces la corespondența dintre parchet și serviciu.

În mod constant, Ministerul Public a susținut lipsa oricărei nelegalități și nicio implicare a S.R.I. în activitatea de punere în executare a supravegherii tehnice, instanțele respingând în mod constant susținerile procurorilor, reținând incidența unor nulități absolute a supravegherii tehnice atât în faza camerei preliminare[3] în faza judecății în primă instanță (în cursul cercetării judecătorești)[4], cât și prin decizii pronunțate în apel[5].

---

[1] Trib. Cluj, s. pen., încheierea nr. 87/CP din 2 octombrie 2019, pronunțată în dosar nr. 1706/117/2018/a1, nepublicată. În privința criticilor privind nelegalitatea supravegherii tehnice, procurorul nu a formulat contestație, soluția rămânând definitivă.

[2] C. Ap. Oradea, s. pen. și pentru cauze cu minori, dec. nr. 703 din 20 decembrie 2019, pronunțată în dosar nr. 4630/83/2006**, nepublicată.

[3] Trib. Cluj, s. pen., încheierea nr. 87/CP din 2 octombrie 2019, pronunțată în dosar nr. 1706/117/2018/a1, nepublicată.

[4] Jud. Baia Mare, s. pen., încheierea din 23 septembrie 2019, pronunțată în dosar nr. 3879/337/2015, nepublicată.

[5] C. Ap. Oradea, s. pen. și pentru cauze cu minori, dec. nr. 703 din 20 decembrie 2019, pronunțată în dosar nr. 4630/83/2006**, nepublicată; C. Ap. București, s. a II-a pen., dec. nr. 1123/A din 18 septembrie 2019, pronunțată în dosar nr. 18875/3/2012, nepublicată.

În concluzie, poziția jurisprudențială a instanțelor a cunoscut o modificare semnificativă în urma deciziilor Curții Constituționale, în prezent fiind anulate în majoritatea cauzelor măsurile de supraveghere tehnică realizate prin punerea în executare de către un serviciu secret. Datorită caracterului complex al unor cauze, este de așteptat ca pentru o perioadă de câțiva ani să mai fie resimțite efectele măsurilor de supraveghere tehnică desfășurate în mod nelegal de către organe necompetente, instanțele fiind abilitate să înlăture probele obținute în orice fază procesuală și să cerceteze temeinic orice implicare a S.R.I. sau a altor servicii secrete în activitatea de urmărire penală.

Secțiunea a 3-a. Încetarea supravegherii tehnice înainte de expirarea mandatului

Pentru garantarea respectării drepturilor persoanei vizate de mandatul de supraveghere tehnică, Codul de procedură penală a introdus instituția încetării supravegherii tehnice mai înainte de expirarea mandatului emis de judecătorul de drepturi și libertăți, prin care procurorul este obligat să dispună încetarea măsurii dacă nu mai există temeiurile care au justificat autorizarea sa[1]. Aceasta constituie o excepție de la regula simetriei, prin aceea că un alt organ decât cel emitent se pronunță asupra încetării supravegherii tehnice. Considerăm că această situație este datorată faptului că, după momentul emiterii mandatului de supraveghere tehnică, legiuitorul nu i-a inclus judecătorului de drepturi și libertăți atributul de supraveghere și control asupra punerii în executare. Rolul îi este atribuit procurorului care, conform art. 142 alin. (4) C.pr.pen., este, în această situație, garantul dreptului la viață privată al persoanei față de care s-a dispus supravegherea tehnică. Din punctul de vedere al Convenției, în jurisprudența mai recentă s-a ridicat problema necesității unui control și a unei supravegheri din partea unei autorități independente[2], condiție pe care procurorul nu o poate îndeplini, astfel că atribuirea acestui rol este o alegere discutabilă. S-ar impune ca întreaga procedură de supraveghere tehnică să poată fi supusă unui control ulterior al judecătorului de drepturi și libertăți pentru a se verifica dacă măsura și-a păstrat caracterul proporțional pe toată durata punerii în executare. Numai în asemenea condiții va putea fi controlată justa respectare a obligației de încetare a măsurii de supraveghere tehnică de către procuror. În practică, în special în domeniul interceptării comunicațiilor unei persoane, au existat situații în care mandatele de supraveghere tehnică au continuat față de unii avocați (fără calitate procesuală) chiar și după arestarea inculpatelor din respectiva cauză[3], fără ca la dosarul cauzei să existe o ordonanță de încetare a supravegherii tehnice sau vreun proces-verbal de consemnare a activităților de supraveghere tehnică privindu-i pe respectivii avocați.

De îndată ce nu mai există temeiuri care să justifice folosirea metodelor de supraveghere tehnică încuviințate, procurorul este obligat să dispună încetarea măsurii, informând de îndată judecătorul care a emis mandatul. Prin încetarea existenței temeiurilor, legiuitorul indică

[1] *M. Udroiu*, Procedură penală, vol. I, 2019, p. 590.

[2] CEDO, cauza *Roman Zakharov c. Rusia*, Hotărârea din 4 decembrie 2015, §233; cauza *Irfan Güzel c. Turcia*, Hotărârea din 7 mai 2017, §96; cauza *Klass ș.a. c. Germania*, Hotărârea din 6 septembrie 1978, §56, pe *hudoc.echr.coe.int*

[3] D.N.A., secția de combatere a corupției, dosar nr. 634/P/2014 (cauză personală).

faptul că nu mai există motivele de fond care au justificat inițial măsura[1]. La nivel conceptual, lipsa temeiurilor care au justificat încuviințarea supravegherii tehnice se va raporta la condițiile legale ale autorizării care vor înceta să mai subziste.

În concret, există o multitudine de cazuri în care temeiurile pot înceta, deseori din datele care sunt strânse până la acel moment se dovedește că o anumită persoană nu are cunoștință despre săvârșirea ori pregătirea săvârșirii infracțiunii care face obiectul cauzei. De exemplu, se încuviințează interceptarea convorbirilor unei persoane, indicându-se în cuprinsul mandatului de supraveghere tehnică mai multe numere de telefon asociate aceluiași abonament, dintre care unul aparținând fiului minor al persoanei față de care s-a emis autorizația. În această situație, ar trebui să se dispună încetarea parțială a mandatului, cu privire la un anumit număr de telefon, deoarece această persoană nu a fost supusă măsurii de supraveghere tehnică. Într-o atare situație, va lipsi condiția legală a suspiciunii rezonabile față de această persoană. Nu va constitui un temei de încetare atunci când persoana cercetată pentru săvârșirea unei infracțiuni de serviciu ar intra în concediu medical în timpul punerii în executare a măsurii[2].

O altă situație în care procurorul va fi obligat să dispună încetarea măsurii de supraveghere tehnică este atunci când se depășește un anumit moment operativ, la care temeiurile care au justificat măsura încetează să mai existe. De exemplu, în cazul începerii urmăririi penale cu privire la o infracțiune de favorizarea făptuitorului săvârșită de avocatul inculpatului, se impune încetarea măsurii de îndată ce se descoperă că o altă persoană, din proprie inițiativă, trecuse la săvârșirea acestei infracțiuni. Din nou, într-o asemenea situație, va lipsi suspiciunea rezonabilă cu privire la activitatea avocatului, impunându-se încetarea supravegherii tehnice.

Odată ce procurorul dispune încetarea măsurii, va fi obligat să încunoștințeze judecătorul de drepturi și libertăți care a emis mandatul de supraveghere tehnică cu privire la încetarea măsurii. S-a arătat în literatura de specialitate că, în măsura în care nu se dispune încetarea mandatului de supraveghere tehnică în condițiile mai sus arătate, iar în urma continuării supravegherii tehnice sunt găsite noi informații, proba obținută va fi legal obținută[3]. Considerăm că opinia este incorectă, deoarece emiterea ordonanței procurorului prin care acesta dispune încetarea supravegherii tehnice constituie o obligație a acestuia. În condițiile în care nu există o supraveghere efectivă din partea judecătorului de drepturi și libertăți, probele obținute vor putea fi excluse numai de către judecătorul de cameră preliminară, fiind incidentă o nulitate relativă într-o asemenea situație. Lesne ne putem imagina o situație în care, deși se impunea încetarea supravegherii tehnice, aceasta continuă, și ulterior acestui moment se descoperă săvârșirea unei infracțiuni de către persoana supusă măsurii, probele obținute fiind folosite împotriva sa pentru tragerea la răspundere penală a faptei noi. Într-o atare situație, descoperirea infracțiunii nu ar fi putut avea loc în lipsa supravegherii tehnice care, la acel moment, trebuie să fi fost încetată de către procuror.

[1] *Gr.Gr. Theodoru*, op. cit., p. 340.

[2] Trib. Suceava, s. pen., încheierea din 4 mai 2015, definitivă prin încheierea nr. 42 din 26 iunie 2015 a C. Ap. Suceava.

[3] *C.M. Chiriță*, în N. Volonciu, A.S. Uzlău (coord.), Noul Cod, 2014, p. 323.

Secțiunea a 4-a. Arhivarea datelor rezultate din măsurile de supraveghere tehnică

În urma folosirii metodelor de supraveghere tehnică, organele de urmărire penală adeseori obțin date și informații care nu par a avea legătură cu cauza, acestea putând fi folosite în alte cauze sau pentru identificarea ori localizarea persoanelor, în caz contrar, acestea trebuind să fie arhivate și stocate în condiții de confidențialitate. Datele rezultate din operațiunile de supraveghere tehnică pot să nu fie utile cauzei penale în care sunt administrate din perspectiva procurorului, caz în care ele vor putea fi folosite în alte cauze, conform art. 142 alin. (5) C.pr.pen., ori vor fi arhivate, conform art. 142 alin. (6) C.pr.pen.

Conform art. 142 alin. (6) teza I C.pr.pen., „*Datele rezultate din măsurile de supraveghere care nu privesc fapta ce formează obiectul cercetării sau care nu contribuie la identificarea ori localizarea persoanelor, dacă nu sunt folosite în alte cauze penale potrivit alin. (5), se arhivează la sediul parchetului, în locuri speciale, cu asigurarea confidențialității*".

Potrivit acestui din urmă articol, dacă datele rezultate nu sunt considerate utile cauzei, ele se vor arhiva la sediul parchetului, în locuri speciale, cu asigurarea confidențialității. Măsura va fi luată pentru a nu permite ca la dosarul cauzei să fie păstrate date – accesibile participanților la procesul penal – care nu pot contribui la aflarea adevărului, dar vor constitui o ingerință continuă adusă vieții private a unei persoane. Prin arhivarea datelor în condiții de confidențialitate, se reduce riscul unor abuzuri prin care să fie cunoscute aspecte privind viața privată a unei persoane și astfel se asigură o minimalizare a ingerinței aduse acestei valori sociale. În corect s-a subliniat că această măsură reprezintă o garanție a respectării dreptului persoanei la viață privată, prin asigurarea confidențialității conținutului comunicărilor care nu privesc fapta cercetată în cauză[1].

Din punctul de vedere al utilității unor date, aceasta va rămâne la aprecierea organului care pune în executare supravegherea tehnică și a procurorului, care vor elimina acele date care fie nu au legătură cu cauza, fie reflectă elemente din viața privată a unei persoane (inclusiv discuțiile personale), fie sunt complet neconcludente și nu conțin activitatea unei persoane (de exemplu, înregistrarea ambientală a unui radio lăsat pornit, înregistrarea ambientală din curtea persoanei vizate ce surprinde câinele acesteia etc.).

Prima situație este atunci când datele rezultate *nu privesc fapta ce formează obiectul cercetării*, reflectând activitățile licite sau ilicite ale persoanei care este supravegheată. În cazul în care activitatea este una ilicită, dar nepenală, datele se vor arhiva și nu vor putea fi folosite într-o altă cauză. Totodată, chiar dacă fapta va constitui o contravenție și ar exista probe privind săvârșirea acesteia, organele de urmărire penală nu vor fi îndreptățite să sesizeze autoritatea competentă în vederea constatării contravenției și aplicării unei sancțiuni. De pildă, prin localizarea unei persoane prin mijloace tehnice, se determină că aceasta conduce cu o viteză peste limita legală, fiind obținute probe în acest sens. Nu se va putea aplica o sancțiune contravențională, întrucât s-ar încălca scopul pentru care a fost dispusă supravegherea tehnică și s-ar încălca și principiul proporționalității supravegherii tehnice cu ingerința în viața privată a unei persoane.

O situație particulară este atunci când se descoperă o faptă prevăzută de legea penală, sens în care se va impune sesizarea din oficiu a organelor de urmărire penală și utilizarea datelor

[1] *Gh. Mateuț*, Tratat, vol. II, 2012, p. 210.

rezultate din supravegherea tehnică într-o altă cauză penală, cu privire la această posibilitate urmând a oferi explicații suplimentare într-o secțiune ulterioară[1].

A doua situație în care se vor arhiva datele rezultate din supravegherea tehnică este atunci când ele nu contribuie *la identificarea persoanelor ori localizarea persoanelor*, o situație pe care o găsim a fi neclară sub ambele variante expuse. În cazul datelor care nu contribuie la identificarea persoanelor, se omite faptul că toate datele obținute din supravegherea tehnică vor contribui, într-o anumită măsură, la identificarea persoanelor. În plus, nu se indică despre ce persoane este vorba, despre persoana vizată, prietenii acesteia, persoana suspectului, inculpatului, martori etc. Credem că o interpretare restrictivă se impune în această privință, fiind necesar a fi păstrate numai acele date privind persoanele supuse măsurii de supraveghere tehnică, care pot fi cunoscute sau necunoscute la momentul emiterii mandatului. A interpreta altfel înseamnă a admite ca fiecare primă interacțiune cu o persoană care nu este supusă mandatului de supraveghere tehnică să fie reținută ca probă la dosarul cauzei, indiferent dacă privește sau nu fapta. În ceea ce privește datele privind localizarea peroanelor, reiese că toate datele care ar putea rezulta din măsura de supraveghere tehnică prevăzută de art. 138 alin. (1) lit. d) C.pr.pen. ar trebui să fie păstrate indiferent dacă au sau nu au legătură cu faptele urmărite, situație pe care o considerăm a fi gravă prin raportare la necesitatea unei stricte limitări a ingerinței privind viața privată.

Condițiile de păstrare a datelor arhivate vor fi de confidențialitate, prin aceasta înțelegându-se restricționarea accesului la date, ele fiind păstrate în locuri anume desemnate de către conducerea fiecărei unități de parchet. Conform Regulamentului de ordine interioară a parchetelor[2], condițiile de păstrare și înregistrare a datelor rezultate din supravegherea tehnică vor fi aceleași ca în cazul tuturor măsurilor speciale de cercetare, a datelor privind măsurile de protecție privind persoanele vătămate, părților civile, a datelor privind identitatea investigatorilor sub acoperire, informatorilor și colaboratorilor și a altor documente care impun un caracter confidențial. Din dispozițiile art. 142 alin. (6) C.pr.pen., reiese că rezultatul supravegherii tehnice se va arhiva sigilat, astfel că orice acces neautorizat la acestea va putea să fie depistat de către personalul parchetului. Practic, aceste date confidențiale nu vor putea fi consultate decât într-un mod care să asigure trasabilitatea fiecărui acces, cu alte cuvinte, fiecare accesare a lor va presupune desigilarea și apoi resigilarea suportului pe care se află, ceea ce sporește gradul de protecție asupra vieții private a persoanei.

Cu toate acestea, uneori se poate constata că aceste date pot servi aflării adevărului, însă nu au fost depuse la dosarul cauzei, fiind arhivate la sediul parchetului. Această împrejurare poate apărea din cauză că aprecierea asupra legăturii cu fapta o va face organul de urmărire penală în mod unilateral, fără ca persoana cercetată să aibă posibilitatea să își exprime o poziție față de măsură. Pentru a evita orice posibilitate ca datele arhivate să nu poată fi folosite pentru aflarea adevărului, legiuitorul a instituit o procedură de dezarhivare a lor.

Potrivit art. 142 alin. (6) teza a II-a C.pr.pen., *„din oficiu sau la solicitarea părților, judecătorul ori completul învestit poate solicita datele sigilate dacă există noi probe din care rezultă că totuși o parte dintre acestea privesc fapta ce formează obiectul cercetării*". În mod corect s-a ridicat în literatura de specialitate ca fiind criticabilă decizia legiuitorului de a impune existența de noi probe pentru a putea solicita depunerea la dosarul cauzei a datelor rezultate din activitățile de

[1] *V. infra*, Titlul III, Capitolul IX.3.

[2] Regulamentul de ordine interioară al parchetelor, adoptat prin Hotărârea CSM – Secția pentru procurori nr. 947/2019 (M. Of. nr. 1004 bis din 13 decembrie 2019).

supraveghere tehnică ce au fost arhivate, reținându-se că persoana care ar formula cererea se poate afla în imposibilitatea prezentării de probe noi[1]. Mai mult, în situația unei interceptări a unei convorbiri telefonice, este îndoielnic dacă o persoană poate prezenta probe noi cu privire la existența respectivei convorbiri, ținându-se seama că nici nu îi este permis accesul la înregistrările arhivate la sediul parchetului. Considerăm că reglementarea posibilității de acces la propriile convorbiri este o obligație a legiuitorului rezultată din jurisprudența Curții Europene a Drepturilor Omului, unde se subliniază că persoana care a fost supusă unei metode de supraveghere tehnică trebuie să aibă posibilitatea ascultării înregistrărilor și de a le contesta veridicitatea[2].

În cazul în care rezultatele activităților de supraveghere tehnică se dovedesc a fi utile, ele vor fi solicitate de către *judecător* ori *completul învestit să soluționeze cauza*. Deși reglementarea a rămas neschimbată de la intrarea în vigoare a Codului de procedură penală, apreciem că, în contextul modificărilor aduse Codului ca urmare a deciziilor Curții Constituționale[3], atât judecătorul de cameră preliminară, cât și instanța vor putea dispune ca datele să fie transmise la dosarul cauzei dacă rezultă că o parte dintre acestea privesc fapta ce formează obiectul cauzei. Apreciem că formularea „privesc fapta ce formează obiectul cercetării" nu este una corectă, întrucât datele rezultate din supravegherea tehnică vor fi administrate ca probă, fiind necesar să îndeplinească toate condițiile probei, inclusiv obiectul probei prevăzut de art. 98 C.pr.pen.

O omisiune flagrantă a legiuitorului constă în modul în care se vor prezenta instanței aceste rezultate, în condițiile în care nu sunt consemnate într-un proces-verbal de consemnare a activităților de supraveghere tehnică potrivit art. 143 alin. (1) C.pr.pen., acesta constituind mijloc de probă în procesul penal. În plus, dacă activitățile de supraveghere tehnică vor consta în interceptarea comunicațiilor sau supravegherea video sau audio a persoanei, vor lipsi și procesele-verbale de redare integrală a convorbirilor, comunicărilor sau conversațiilor prevăzute de art. 143 alin. (4) C.pr.pen., care constituie, la rândul lor, mijloace de probă. Problema ridicată este una reală, judecătorul de cameră preliminară sau instanța neavând competența de a proceda la transcrierea – redarea integrală a conversațiilor și certificarea – unor asemenea procese-verbale, deoarece legea i-a atribuit procurorului atributul exclusiv de a certifica astfel de procese-verbale[4].

În vederea respectării dreptului la viață privată al persoanei, chiar în situația în care datele au fost arhivate, legiuitorul a instituit un termen pentru care acestea vor fi stocate, urmând ca ulterior să fie distruse. Conform art. 142 alin. (6) teza finală C.pr.pen., „*după un an de la soluționarea definitivă a cauzei, acestea sunt distruse de către procuror, care întocmește un proces-verbal în acest sens*". Prin „soluționarea definitivă a cauzei" se va înțelege fie soluționarea în cursul urmăririi penale, printr-o soluție de clasare sau de renunțare la urmărirea penală, fie în urma judecății, prin pronunțarea uneia dintre soluțiile prevăzute de art. 396 C.pr.pen. La un

[1] *S. Grădinaru*, Supravegherea tehnică, 2014, p. 71.

[2] CEDO, cauza *Dumitru Popescu c. România (nr. 2)*, Hotărârea din 26 aprilie 2007, §78, pe *hudoc.echr.coe.int*

[3] În special a Deciziei Curții Constituționale nr. 802 din 5 decembrie 2017 referitoare la excepția de neconstituționalitate a dispozițiilor art. 342 și art. 345 alin. (1) din Codul de procedură penală (M. Of. nr. 116 din 6 februarie 2018), în care s-a apreciat că „soluția legislativă cuprinsă în art. 345 alin. (1) din Codul de procedură penală, care nu permite judecătorului de cameră preliminară, în soluționarea cererilor și excepțiilor formulate ori excepțiilor ridicate din oficiu, să administreze alte mijloace de probă în afara «oricăror înscrisuri noi prezentate» este neconstituțională". Astfel, se va permite ca, pentru soluționarea cererilor și excepțiilor, să se poată administra inclusiv datele rezultate din activitățile de supraveghere tehnică arhivate la sediul parchetului.

[4] *S. Grădinaru*, Supravegherea tehnică, 2014, p. 113.

an după oricare dintre aceste momente, datele rezultate din măsurile de supraveghere tehnică vor fi distruse de procuror prin metode apte de a nu permite recuperarea datelor. Fiindcă aceste date se regăsesc, de regulă, pe suporți optici, distrugerea lor se va face cu dispozitive mecanice într-un mod similar distrugerii înscrisurilor. În situația în care suportul pe care se află este unul magnetic – tip hard-disk –, distrugerea va trebui făcută prin metode specifice – suprascriere multiplă, supunere la câmpuri magnetice extreme – pentru ca datele să poată fi recuperate. În cadrul procesului-verbal se impune ca procurorul să menționeze și modalitatea concretă în care s-a realizat distrugerea datelor.

Ulterior întocmirii procesului-verbal, procurorul nu mai are nicio obligație cu privire la datele rezultate din supravegherea tehnică, situație pe care o apreciem ca nefiind în conformitate cu garanțiile necesare pentru protejarea dreptului persoanei față de un abuz al autorităților și nici cu privire la rolul judecătorului de drepturi și libertăți în supravegherea activităților încuviințate. Mai precis, credem că, *de lege ferenda*, se impune ca procesul-verbal întocmit de procuror să fie transmis judecătorului de drepturi și libertăți, pentru a se asigura respectarea termenului legal pentru distrugerea datelor rezultate din supravegherea tehnică.

Secțiunea a 5-a. Conservarea materialelor rezultate din supravegherea tehnică

În mod distinct de arhivarea datelor rezultate din măsurile de supraveghere tehnică care nu privesc fapta ce formează obiectul cercetării sau nu contribuie la identificarea sau localizarea persoanelor, Codul de procedură penală a inclus și o procedură distinctă privind conservarea materialelor rezultate din supravegherea tehnică. Prin această procedură, legiuitorul a instituit reguli în privința suportului material rezultat din supravegherea tehnică și care conține probe care nu au fost înlăturate de la dosarul cauzei spre arhivare, în conformitate cu art. 142 alin. (6) C.pr.pen., astfel, prin dispozițiile art. 146 C.pr.pen., s-a urmărit reglementarea situației rezultatelor supravegherii tehnice care privesc faptele cercetate în cauză și pe baza cărora se poate stabili adevărul judiciar în respectiva cauză. În concret, s-a avut în vedere împrejurarea că, în momentul punerii în executare a supravegherii tehnice, dacă se obțin date și informații care nu privesc fapta sau nu contribuie la identificarea ori localizarea persoanelor, ele vor fi supuse arhivării încă de la data consemnării rezultatelor activităților de supraveghere tehnică, fiind distincte de datele și informațiile care vor fi folosite în cauză, prevăzute de art. 143 alin. (1) C.pr.pen., și care vor fi depuse anexat la dosarul cauzei, conform art. 143 alin. (2) C.pr.pen.

Prin conservarea materialelor rezultate din supravegherea tehnică se urmărește ca suportul material sau copia acestuia care conțin probe administrate prin supravegherea tehnică să fie arhivate în locuri speciale, sigilate și cu asigurarea confidențialității acestora.

Codul de procedură penală prevede două situații în care se va proceda la conservarea materialelor rezultate din supravegherea tehnică: *i)* în cazul emiterii unei soluții de clasare și *ii)* în cazul în care s-a pronunțat o soluție definitivă de către o instanță.

În prima situație, în care cauza penală s-a finalizat cu terminarea urmăririi penale prin ordonanță de clasare, legiuitorul a prevăzut necesitatea conservării materialelor rezultate din supravegherea tehnică în cuprinsul art. 146 alin. (1) C.pr.pen. Conform acestui articol, conservarea se va dispune atunci când s-a emis o soluție de clasare care nu a fost atacată prin plângere în termenul de 20 de zile prevăzut de art. 340 C.pr.pen. sau în cazul în care, deși a

fost formulată plângere, aceasta a fost respinsă. Conservarea nu se va putea dispune de către procuror, într-o asemenea situație trebuind să fie **înștiințat** judecătorul de drepturi și libertăți care va dispune conservarea suportului material sau a copiei certificate a acestuia prin arhivare la sediul instanței în locuri speciale, în plic sigilat și cu asigurarea confidențialității. În mod corect s-a reținut că ar exista o rațiune pentru o simplă înștiințare a judecătorului de drepturi și libertăți asupra clasării, sens în care trebuie avută în vedere împrejurarea că supravegherea tehnică conduce la o restrângere a dreptului la viață privată al persoanei[1].

În mod justificat, această procedură a fost criticată în literatura de specialitate, deoarece vine în contradicție cu posibilitatea instituită de legiuitor a folosirii rezultatelor activităților de supraveghere tehnică într-o altă cauză[2]. Practic, arhivarea materialelor rezultate din supravegherea tehnică se va face la sediul instanței, fără a se permite ca organele de urmărire penală să poată folosi probele într-o altă cauză, întrucât nu se vor mai afla la sediul parchetului. Același autor critică în mod justificat și faptul că înștiințarea din partea procurorului nu ar avea rolul unei sesizări, ci, practic, judecătorul de drepturi și libertăți ar trebui să se sesizeze din oficiu, ceea ce nu este conform competenței acestuia, el putând fi sesizat numai de procuror sau de o persoană îndreptățită, în condițiile legii.

Remarcăm și faptul că nu se reglementează nicio procedură privind transmiterea suporților materiali ai rezultatelor activităților de supraveghere tehnică, aceștia fiind păstrați la sediul parchetului la finalizarea urmăririi penale când ar trebui să fie transmiși judecătorului de drepturi și libertăți pentru ca acesta să dispună conservarea lor. Legea nu prevede nici măcar actul prin care se dispune conservarea și nici vreo dispoziție legală prin care să fie identificat judecătorul de drepturi și libertăți competent să dispună conservarea materialelor rezultate din supravegherea tehnică. S-a susținut că acesta ar trebui să fie judecătorul de drepturi și libertăți din cadrul instanței care a autorizat supravegherea tehnică, întrucât el este cel care trebuie să cunoască date cu privire la finalizarea procedurii judiciare[3]. Același autor observă în mod corect că, deși procedura este prevăzută în Codul de procedură penală, legiuitorul nu a inclus nicio sancțiune aplicabilă în cazul omisiunii procurorului să încunoștințeze judecătorul de drepturi și libertăți sau vreun termen în care procurorul trebuie să realizeze înștiințarea.

Credem că legiuitorul nu a avut niciun motiv întemeiat pentru a decide conservarea materialelor rezultate din supravegherea tehnică la sediul instanței în contradicție cu faptul că acestea reprezintă mijloace de probă într-un dosar de urmărire penală finalizat și ar trebui să fie păstrate alături de respectivul dosar[4].

Literatura de specialitate a relevat faptul că reglementarea actuală omite situația în care în cursul urmăririi penale se dispune disjungerea cauzei[5]; într-o asemenea situație, apreciem că momentul conservării va depinde de soluționarea ultimei cauze disjunse, ceea ce nu prezintă vreo previzibilitate temporală. Era preferabil ca legiuitorul să prevadă expres procedura în cazul în care se va disjunge cauza. În practică se pot întâlni situații în care se va dispune trimiterea în judecată față de anumite fapte și persoane, iar față de altele se va dispune disjungerea, rezultatele supravegherii tehnice fiind folosite în ambele cauze, presupunând și copierea suporților materiali. Suporții vor fi deopotrivă conservați la sediul instanței după soluționarea definitivă a

[1] *M. Bulancea, R. Slăvoiu*, în M. Udroiu (coord.), Codul de procedură penală, 2017, p. 712.

[2] *Gh. Mateuț*, Procedură penală, 2019, p. 704.

[3] *V. Trif*, Metode de supraveghere tehnică în cadrul procesului penal, Ed. C.H. Beck, București, 2019, p. 194.

[4] În acest sens, *M. Bulancea, R. Slăvoiu*, în M. Udroiu (coord.), Codul de procedură penală, 2017, p. 712.

[5] *Gh. Mateuț*, Procedură penală, 2019, p. 704.

cauzei și atașați dosarului de urmărire penală disjuns până la emiterea vreuneia dintre soluțiile prevăzute de art. 314 alin. (1) C.pr.pen., cele două situații fiind flagrant contradictorii.

Legiuitorul a omis să prevadă o procedură în ipoteza în care se va dispune renunțarea la urmărirea penală, situație care, în opinia doctrinei, va trebui să fie asimilată unei soluții de clasare, aplicându-se în mod corespunzător dispozițiile art. 146 alin. (1) și (2) C.pr.pen.[1].

În cea de-a doua situație avută în vedere de legiuitor în cuprinsul art. 146 C.pr.pen., dacă în cauză instanța a pronunțat o hotărâre de condamnare, de renunțare la aplicarea pedepsei sau de amânare a aplicării pedepsei, de achitare ori încetare a procesului penal, rămasă definitivă, suportul material al rezultatelor supravegherii tehnice sau copia acestuia se conservă prin arhivare odată cu dosarul cauzei la sediul instanței, în locuri speciale, cu asigurarea confidențialității. Într-o astfel de situație, nu se va impune ca instanța să dispună conservarea, aceasta făcându-se în temeiul legii. În doctrină a fost ridicată problema unei necorelări între dispozițiile art. 146 alin. (3) C.pr.pen. și ale art. 142 alin. (6) C.pr.pen., considerându-se că, în același timp, suportul ar trebui arhivat de către instanță, dar și distrus de către procuror[2]. Nu putem fi de acord cu această opinie, întrucât art. 142 alin. (6) C.pr.pen. se referă numai la datele și informațiile rezultate din supravegherea tehnică față de care există obligația arhivării, acestea fiind singurele care pot fi supuse distrugerii. În schimb, datele care sunt supuse conservării sunt datele care rezultă din supravegherea tehnică și care *privesc fapta care face obiectul cercetării sau contribuie la identificarea ori localizarea persoanelor* care vor fi stocate pe suporți optici (sau magnetici) distincți față de cei care vor conține date și informații care nu au legătură cu cauza, în condițiile art. 142 alin. (6) C.pr.pen.

[1] *M. Bulancea, R. Slăvoiu*, în M. Udroiu (coord.), Codul de procedură penală, 2017, p. 713.
[2] *Ibidem*, p. 712.

Capitolul IV
Semnarea, verificarea și certificarea electronică a datelor realizate din supravegherea tehnică

Secțiunea 1. Scopul semnării electronice a rezultatelor activităților de supraveghere tehnică

Un element nou introdus prin Codul de procedură penală îl constituie posibilitatea semnării electronice a datelor rezultate din supravegherea tehnică, în conformitate cu dispozițiile art. 142[1] C.pr.pen. În doctrină s-a arătat că prin introducerea acestei prevederi legale s-a urmărit asigurarea autenticității mijloacelor de probă obținute din supravegherea tehnică prin noi mijloace tehnice[1], alături de certificarea pentru autenticitate de către procuror, care era cunoscută și reglementării anterioare.

Conform art. 142[1] C.pr.pen., semnarea, verificarea și certificarea datelor rezultate din activitățile de supraveghere tehnică constituie o procedură *facultativă* care poate fi realizată de către persoana care efectuează supravegherea tehnică, persoana care transmite rezultatele supravegherii tehnice sau persoana care primește rezultatele supravegherii tehnice. Motivul pentru care ea este facultativă este dat de costurile pe care le implică implementarea de certificate digitale pentru toate organele judiciare, pentru toate organele de cercetare și lucrătorii de poliție care ar putea contribui la desfășurarea urmăririi penale. Aidoma unei semnături obișnuite, fiecare certificat este asociat cu o anumită persoană din sistemul judiciar, acesta nefiind transmisibil.

În esență, introducerea posibilității semnării electronice permite asigurarea trasabilității și autenticității subsecvente obținerii datelor informatice rezultate din supravegherea tehnică. Necesitatea este dată de realitățile tehnologice curente care determină ca majoritatea rezultatelor de supraveghere tehnică să aibă un caracter digital, fiind date informatice. Cel mai comun exemplu poate fi fotografierea unei persoane în cadrul supravegherii tehnice, metodă care, în trecut, presupunea existența unui film care se developa prin procedee chimice și era transpus pe un suport de hârtie fotografică. În prezent, toate fotografiile care se realizează sunt în format digital, astfel că vor constitui date informatice, putând fi transpuse și în format material. În același mod, din cunoștințele noastre, de aproape 20 de ani nu se mai folosesc benzi magnetice sau suporți magnetici pentru înregistrarea sau stocarea interceptării comunicațiilor, acestea fiind realizate prin captare digitală, rezultând date informatice.

Secțiunea a 2-a. Noțiuni legislative și tehnice privind „certificatele digitale" și „semnătura electronică"

Specifică datelor informatice este posibilitatea ca acestea să fie semnate electronic de către o persoană care deține un certificat calificat eliberat de un furnizor de servicii de certificare acreditat, prin aceasta punându-și amprenta asupra respectivelor date.

[1] *Gh. Mateuț*, Procedură penală, 2019, p. 692.

În domeniul semnăturilor electronice, legea care le stabilește regimul este Legea nr. 455/2001 privind semnătura electronică, republicată[1] (în continuare, „Legea nr. 455/2001"), în care sunt definiți mai mulți termeni care vor fi utili în înțelegerea importanței aplicării semnăturii electronice asupra datelor informatice rezultate din supravegherea tehnică.

Prin „semnătură electronică" vom înțelege, în sensul art. 4 pct. 3 din Legea nr. 455/2001, „*date în formă electronică, care sunt atașate sau logic asociate cu alte date în formă electronică și care servesc ca metodă de identificare*". Consecința imediată este că semnătura electronică se va atașa tot timpul unor alte date informatice, întocmai cum semnătura olografă se va lega în mod indisolubil de documentul pe care a fost aplicată.

„Semnătura electronică extinsă" reprezintă, conform art. 4 pct. 4 din Legea nr. 455/2001, acea semnătură electronică care îndeplinește cumulativ următoarele condiții: *i)* este legată în mod unic de semnatar; *ii)* asigură identificarea semnatarului; *iii)* este creată prin mijloace controlate exclusiv de semnatar; *iv)* este legată de datele în formă electronică, la care se raportează în așa fel încât orice modificare ulterioară a acestora este identificabilă.

Câteva elemente trebuie să fie extrase din prezenta definiție pentru a fi înțeleasă importanța semnăturii electronice extinse. Prin „legarea în mod unic de semnatar"[2] trebuie înțeles că semnătura electronică poate fi aplicată numai de o persoană care deține un dispozitiv[3] (numit *token* – similar cu un stick USB) și care știe parola de deblocare a certificatului de pe acel dispozitiv. Prin „asigurarea identității semnatarului" înțelegem că în sistemul informatic va apărea numele real al deținătorului certificatului cu care s-au semnat datele informatice și că semnătura va include întotdeauna identitatea certă a semnatarului. Prin „crearea semnăturii prin mijloace controlate numai de semnatar" se înțelege că dispozitivul pe care este stocat certificatul prin care se realizează semnarea este remis numai semnatarului și că pentru semnare este necesară introducerea unei parole cunoscute numai de semnatar. Prin „legarea de datele electronice" se arată că semnătura nu poate fi disociată de datele informatice semnate, astfel că orice modificare ulterioară este identificabilă (semnarea utilizează coduri hash de verificare[4]).

„Dispozitivul securizat de creare a semnăturii electronice" reprezintă, conform art. 4 pct. 8 din Legea nr. 455/2001, acel dispozitiv de creare a semnăturii electronice care îndeplinește cumulativ următoarele condiții: *i)* datele de creare a semnăturii, utilizate pentru generarea acesteia, să poată apărea numai o singură dată și confidențialitatea acestora să poată fi asigurată; *ii)* datele de creare a semnăturii, utilizate pentru generarea acesteia, să nu poată fi deduse; *iii)* semnătura să fie protejată împotriva falsificării prin mijloacele tehnice disponibile la momentul generării acesteia; *iv)* datele de creare a semnăturii să poată fi protejate în mod efectiv de către semnatar împotriva utilizării acestora de către persoane neautorizate; *v)* să nu modifice datele în formă electronică, care trebuie să fie semnate, și nici să nu împiedice ca acestea să fie prezentate semnatarului înainte de finalizarea procesului de semnare.

---

[1] Legea nr. 455 din 18 iulie 2001 privind semnătura electronică (republicată în M. Of. nr. 316 din 30 aprilie 2014).

[2] Conform art. 4 pct. 5 din Legea nr. 455/2001, „semnatar reprezintă o persoană care deține un dispozitiv de creare a semnăturii electronice și care acționează fie în nume propriu, fie ca reprezentant al unui terț".

[3] Conform art. 4 pct. 7 din Legea nr. 455/2001, „dispozitiv de creare a semnăturii electronice reprezintă software și/sau hardware configurate, utilizat pentru a implementa datele de creare a semnăturii electronice". În cazul semnăturii electronice extinse, va fi necesar un dispozitiv securizat, definit de art. 4 pct. 8 din Legea nr. 455/2001.

[4] *M.V. Tudoran*, Teoria și practica interceptărilor, 2012, p. 203.

Unicitatea datelor generate pentru semnare este asigurată prin adăugarea datei la care s-a aplicat semnătura, neputând fi generată o semnătură în aceleași condiții cu același dispozitiv. În privința posibilității de a deduce datele de creare a semnăturii și utilizate pentru generarea acesteia, ea este consecința funcției matematice folosite pentru generarea semnăturii, ca urmare a folosirii unei chei private cu care se poate semna (genera un cod criptat) și utilizării unei chei publice prin care se poate doar citi și verifica semnătura (decripta). Algoritmul folosit de dispozitiv (prin certificatul de pe acesta) este SHA256, pentru criptare fiind folosită o cheie RSA 2048bit, și presupune un algoritm asimetric de criptare[1]. Protejarea împotriva falsificării este dată de faptul că dispozitivul pe care se află nu poate fi copiat și nu se poate interveni asupra acestuia decât de către un furnizor acreditat. Datele de creare a semnăturii (certificatul propriu-zis) sunt protejate pe dispozitiv prin parolă; în cazul în care se vor introduce multiple parole greșite, dispozitivul va deveni inutilizabil. Ultima condiție privește nemodificarea datelor informatice semnate, care se realizează prin păstrarea lor integrală în timpul semnării și doar atașarea datelor informatice care conțin semnătura digitală.

„Certificatul" reprezintă, potrivit art. 4 pct. 11 din Legea nr. 455/2001, o colecție de date în formă electronică ce atestă legătura dintre datele de verificare a semnăturii electronice și o persoană, confirmând identitatea acelei persoane. Doar un dispozitiv token nu este suficient pentru semnarea unor date informatice, este necesar ca pe acesta să se afle un certificat care conține datele de identificare ale persoanei și cheia privată de criptare prin care se poate utiliza acest certificat. Într-un mod simplist, la semnare se atașează informațiile din acel certificat (în copie) prin folosirea cheii private. Tehnic, un certificat poate exista și fără dispozitiv, caz în care va putea fi folosit pentru alte scopuri decât semnare, în cazul semnăturii electronice fiind necesar un tip particular de certificat, respectiv un certificat calificat. În cazul interceptărilor prin C.N.I.C., rezultatele activităților de supraveghere sunt semnate automat cu certificate interne folosite de S.R.I. (autoritatea emitentă este doar S.R.I., astfel că se validează numai prin serverele acestei instituții), care nu îndeplinesc criteriul unui certificat în sensul legii.

„Certificatul calificat" reprezintă, potrivit art. 4 pct. 12 din Legea nr. 455/2001, un certificat care satisface condițiile prevăzute la art. 18 din Legea nr. 455/2001 și care este eliberat de un furnizor de servicii de certificare ce îndeplinește condițiile prevăzute la art. 20 din Legea nr. 455/2001 (DigiSign S.A., CertSign S.R.L. etc.). Conform art. 18 din Legea nr. 455/2001, certificatul calificat va cuprinde următoarele mențiuni: *a)* indicarea faptului că certificatul a fost eliberat cu titlu de certificat calificat; *b)* datele de identificare a furnizorului de servicii de certificare, precum și cetățenia acestuia, în cazul persoanelor fizice, respectiv naționalitatea acestuia, în cazul persoanelor juridice; *c)* numele semnatarului sau pseudonimul acestuia, identificat ca atare, precum și alte atribute specifice ale semnatarului, dacă sunt relevante, în funcție de scopul pentru care este eliberat certificatul calificat; *d)* codul personal de identificare a semnatarului; *e)* datele de verificare a semnăturii, care corespund datelor de creare a semnăturii aflate sub controlul exclusiv al semnatarului; *f)* indicarea începutului și sfârșitului perioadei de valabilitate a certificatului calificat; *g)* codul de identificare a certificatului calificat; *h)* semnătura electronică extinsă a furnizorului de servicii de certificare care eliberează certificatul calificat; *i)* dacă este cazul, limitele utilizării certificatului calificat sau limitele valorice ale

[1] În termeni simpli, un algoritm asimetric presupune că niciodată nu se va putea recupera cheia cu care se criptează și numai respectiva cheie va putea genera codul criptat care reprezintă semnătura electronică extinsă. Cheia de decriptare publică va fi utilizată numai pentru decriptarea semnăturii electronice extinse, generându-se datele informatice ale semnăturii: atributele și identitatea persoanei care a semnat.

operațiunilor pentru care acesta poate fi utilizat; *j)* orice alte informații stabilite de autoritatea de reglementare și supraveghere specializată în domeniu. Emiterea unui asemenea certificat presupune ca semnatarul să se prezinte personal în fața furnizorului de serviciu de certificare, să i se verifice identitatea mai înainte și să i se remită personal dispozitivul de semnare care conține certificatul calificat.

Pentru semnarea electronică a unor date informatice, dispozitivul securizat de creare a semnăturii electronice extinse trebuie să fie instalat pe un sistem informatic alături de un program specific fiecărui furnizor care permite să se opereze cu certificatul. Odată instalat, există două opțiuni de semnare – semnarea în cadrul unor programe informatice de editare –, Microsoft Word ori Adobe Acrobat sau semnarea oricărui fișier prin intermediul software-ului aferent dispozitivului. Prin prima metodă se vor putea semna inclusiv e-mailuri transmise, sub acest aspect, Codul de procedură penală nefăcând nicio mențiune despre semnarea și certificarea modului de transmitere a datelor informatice deja semnate.

Textul legal nu face nicio distincție între cele două variante, dar cea care va trebui folosită este cea de-a doua. Practic, utilizatorul selectează un fișier (indiferent de tipul acestuia, .pdf, .docx, .mp4, .avi, .mp3 etc.) și va selecta din software-ul dedicat „semnează fișierul", urmând ca acesta să fie întrebat dacă semnează în paralel documentul sau îl contrasemnează pe unul semnat deja. Acest aspect este important, întrucât un fișier poate fi semnat de toate persoanele care intră în posesia acestuia, putându-se realiza trasabilitatea cronologică a fișierului (fiecare semnătură va purta și data semnării) și verificarea identității acestora, inclusiv în sensul dispozițiilor art. 142[1] C.pr.pen., care, în opinia noastră, au fost gândite pentru a fi folosite chiar în acest mod, prin semnarea consecutivă de către persoana care a realizat supravegherea tehnică, persoana care a trimis rezultatele de supraveghere tehnică și persoana care le-a primit. După ce se selectează tipul de semnare, se va alege certificatul de pe dispozitivul de creare a semnăturii (acesta putând conține mai multe semnături ale aceleiași persoane, pentru scopuri diferite) și programul informatic va cere parola de deblocare a certificatului. Odată introdusă aceasta, se va realiza semnarea fișierelor, rezultatul fiind un fișier nou cu extensia „.p7s", relevând că este un fișier semnat. Ulterior, pentru vizualizarea lui, va trebui instalat, pe sistemul informatic pe care se verifică, un software similar de verificare (descărcabil gratuit de pe internet), ce va permite citirea semnăturii electronice, verificarea automată (va exista un buton al programului care va declanșa verificarea automată și integritatea fișierului semnat), dar și, ulterior, deschiderea fișierului semnat sau extragerea acestuia din fișierul semnat (regenerându-se fișierul inițial nesemnat).

Odată semnat, fișierul rezultat va putea fi copiat, transmis prin internet, supus citirii, verificării, fără a se putea altera conținutul acestuia sau semnătura. În cazul în care se va proceda la alterarea lui, acest lucru se va putea detecta în mod facil de către un program de verificare a semnăturii.

O mențiune care se impune a fi făcută este că semnătura electronică extinsă va fi specifică fiecărui fișier, astfel că dacă rezultatele activităților de supraveghere tehnică vor fi cuprinse în mai multe fișiere digitale, fiecare dintre acestea va trebui semnat individual. Procesul va fi unul simplu, întrucât procesul de automatizare va presupune doar selectarea tuturor fișierelor și semnarea lor concomitentă, generându-se un număr egal de fișiere noi cu extensia „.p7s".

Secțiunea a 3-a. Autenticitatea electronică a rezultatelor activităților de supraveghere tehnică

În doctrină s-a exprimat opinia potrivit căreia prin introducerea dispozițiilor art. 142[1] C.pr.pen. au fost deschise noi oportunități privind autenticitatea informației (integritatea datelor informatice), autentificarea autorului acesteia (persoana care semnează electronic) și nerepudierea semnăturii (persoana care semnează electronic nu va putea afirma că semnătura nu îi aparține)[1]. Nu putem fi de acord cu toate aceste afirmații, deoarece autenticitatea informației nu presupune semnarea datelor informatice, ci doar generarea unor coduri de control numite „coduri hash"[2] (pe baza MD5, SHA) despre care autorul opiniei arată că ar fi incidente inclusiv în procesul de semnare. Pretinsa importanță a codurilor hash și semnătura digitală reprezintă doar o consecință a aceleiași aplicații a unui algoritm matematic și a caracterului comun al tehnologiei, dar sistemul nu a fost gândit special pentru crearea certificatelor calificate în sensul legii[3].

Într-o altă opinie s-a afirmat că lipsa semnăturii demonstrează că s-au operat modificări asupra conținutului fișierului, ceea ce face ca proba să nu mai fie valabilă[4]. Nici cu această opinie nu putem fi de acord în totalitate, întrucât presupune ca persoana care a realizat supravegherea tehnică să semneze datele rezultate cu o semnătură electronică. Dacă acest lucru nu s-a realizat, datele inițiale rămân autentice și pot fi semnate ulterior și retransmise la dosarul cauzei. Este posibil ca datele informatice să nu poate fi semnate de către persoana care realizează supravegherea tehnică, ci numai de către persoana care realizează transmiterea lor, situație care nu prezintă o reală problemă, întrucât datele sursă pot fi comparate cu datele informatice semnate folosind un cod hash. În plus, nu se arată lipsa cărei semnături poate conduce la absența autenticității datelor informatice, în condițiile în care fișierul poate fi semnat de mai multe persoane în mod consecutiv.

Pentru ca integritatea datelor informatice să fie asigurată, se impune ca fiecare fișier care rezultă din supravegherea tehnică să aibă calculat un cod hash specific. Codul acesta reprezintă o funcție matematică ireversibilă pe baza unui algoritm (de exemplu, MD5) și valoarea sa este indisolubil legată de fișier. Pentru a se asigura autenticitatea fișierului, datele sale informatice sunt introduse într-o funcție matematică care, prin intermediul algoritmului, dă un cod rezultat neinteligibil, dar care poate fi stocat. Întrucât codul depinde de datele informatice ale fișierului, orice alterare va conduce la alterarea substanțială a codului hash, putând lesne fi identificată o intervenție asupra datelor informatice. Astfel, strict pentru păstrarea integrității datelor se impune verificarea doar a codurilor hash generate pe baza fișierului sursă cu fișierul copie pentru a se constata identitatea acestora. Generarea de coduri hash de verificare este o obligație tactică inerentă operării cu date informatice, întrucât exclude orice posibilitate de modificare ulterioară a fișierului.

Semnătura electronică extinsă are un alt rol decât codul hash al fișierului, respectiv adaugă un element de identificare a persoanei care a realizat o anumită acțiune asupra fișierului, păstrând în același timp integritatea sa. Pentru a se înțelege mai bine, de regulă, semnarea

---

[1] *M. Bulancea, R. Slăvoiu*, în M. Udroiu (coord.), Codul de procedură penală, 2017, p. 697.

[2] *M.V. Tudoran*, Teoria și practica interceptărilor, 2012, p. 203.

[3] *M.H.M. Schellekens*, Electronic Signatures. Authentication Technology from a Legal Perspective, Ed. TMC Asser Press, Haga, 2004, p. 28.

[4] *Gh. Mateuț*, Procedură penală, 2019, p. 693.

presupune înglobarea fișierului vechi într-un fișier nou care va conține atât fișierul inițial, cât și componenta de semnătură. Dacă fișierul inițial poate fi extras din cel semnat, semnătura electronică nu poate fi substituită sau modificată și nici preluată și inserată pe alt document.

Conform art. 142[1] alin. (1) C.pr.pen., „*orice persoană autorizată care realizează activități de supraveghere tehnică, în baza prezentei legi, are posibilitatea de a asigura semnarea electronică a datelor rezultate din activitățile de supraveghere tehnică, utilizând o semnătură electronică extinsă bazată pe un certificat calificat eliberat de un furnizor de servicii de certificare acreditat*". Textul legal are în vedere că persoana care realizează activitățile de supraveghere va fi prima persoană care va putea aplica semnătura electronică extinsă, deoarece este prima care ia contactul cu datele informatice create în urma supravegherii tehnice. În ceea ce ne privește, aceasta este cea mai importantă semnătură care poate fi aplicată, fiind necesar ca ea să fie aplicată cât mai repede după crearea fișierelor digitale care conțin rezultatele activităților de supraveghere tehnică. Aceste date informatice semnate vor putea fi atașate procesului-verbal de consemnare a activităților de supraveghere tehnică într-un mediu digital care nu permite suprascrierea (suport optic).

În cea de-a doua etapă, potrivit art. 142[1] alin. (2) C.pr.pen., „*orice persoană autorizată care transmite date rezultate din activitățile de supraveghere tehnică, în baza prezentei legi, are posibilitatea să semneze datele transmise, utilizând și o semnătură electronică extinsă bazată pe un certificat calificat eliberat de un furnizor de servicii de certificare acreditat și care permite identificarea neambiguă a persoanei autorizate, aceasta asumându-și astfel responsabilitatea în ceea ce privește integritatea datelor transmise*". Observăm că există o omisiune a legii sub acest aspect, întrucât nu se menționează că persoana care transmite datele poate să și verifice semnăturile digitale preexistente. Apreciem că inițial s-au avut în vedere două situații: *i)* atunci când are loc o transmitere realizată de un organ de urmărire penală, caz în care putea exista și o semnătură a persoanei care realiza activitățile de supraveghere tehnică; *ii)* când persoana care a realizat supravegherea tehnică era dintre acelea care erau încadrate în vechea formă a dispozițiilor art. 142 alin. (1) C.pr.pen., respectiv cele desemnate prin expresia „*alte organe specializate ale statului*", adică serviciile de informații, sens în care operatorul care realiza supravegherea tehnică trebuia să fie o persoană a cărei identitate nu putea fi dezvăluită.

Ultima etapă, cea a primirii și verificării datelor, este prevăzută de art. 142[1] alin. (3) C.pr.pen., în care se arată că „*orice persoană autorizată care primește date rezultate din activitățile de supraveghere tehnică, în baza prezentei legi, are posibilitatea să verifice integritatea datelor primite și să certifice această integritate prin semnarea datelor, utilizând o semnătură electronică extinsă bazată pe un certificat calificat eliberat de un furnizor de servicii de certificare acreditat și care permite identificarea neambiguă a persoanei autorizate*". În categoria persoanelor care primesc datele informatice rezultate din supravegherea tehnică putem include organele de urmărire penală, în special procurorul sau chiar instanța de judecată, dacă va solicita o copie în vederea verificării autenticității cu copia datelor informatice aflate la dosarul cauzei. Credem că semnarea la primire a datelor informatice este utilă pentru a se stabili un lanț de trasabilitate, astfel că se va putea cunoaște pe la ce persoane au trecut datele informatice, însă acest deziderat poate fi implementat numai prin introducerea obligativității semnării datelor rezultate din activitățile de supraveghere tehnică.

Conform art. 142[1] alin. (4) C.pr.pen., fiecare persoană care certifică datele sub semnătură electronică răspunde potrivit legii pentru securitatea și integritatea acestor date. Deși acest text legal pare a prevedea o răspundere solidară, în realitate, are meritul de a ajuta în cazul

unui dubiu de neautenticitate ca verificările să se realizeze față de o anumită persoană sau la un anumit nivel. De exemplu, avem un fișier audio rezultat din supraveghere tehnică care a fost semnat electronic de către persoana care a realizat supravegherea tehnică, apoi de către persoana care realizează transmiterea către procuror a fișierului, acesta din urmă semnând și el fișierul la primire. Dacă se va contesta autenticitatea datelor informatice, este evident că problema trebuia să fie la prima verigă, respectiv la persoana care a realizat supravegherea tehnică, întrucât nu este posibilă semnarea unui fișier anterior semnat de către o altă persoană decât dacă se validează mai întâi integritatea datelor (proces realizat automat, de altfel). Evident, pot exista situații în care toate semnăturile sunt invalidate de unele modificări, sens în care s-a produs o alterare după ce fișierul a fost semnat de către procuror, adică la ultima verigă a lanțului trasabilității.

În concluzie, introducerea posibilității semnării electronice a datelor informatice rezultate din supravegherea tehnică este un progres deosebit în digitalizarea procesului penal și înlăturarea oricăror posibile suspiciuni de alterare a unor fișiere video, audio sau de altă natură rezultate din supravegherea tehnică. Limitările actualului Cod de procedură penală sunt date de necesitatea unor investiții în tehnologie – cumpărarea și menținerea validității unor certificate digitale pentru toate organele judiciare –, dar și în pregătirea personalului de a utiliza semnătura electronică extinsă, de a-i înțelege modul de funcționare și de a contribui la o mai bună administrare a actului de justiție.

Capitolul V
Consemnarea activităților de supraveghere tehnică

Secțiunea 1. Natura datelor și informațiilor rezultate din activitățile de supraveghere tehnică

În introducerea explicațiilor privind consemnarea activităților de supraveghere tehnică se impun a fi făcute câteva mențiuni în privința actualei naturi a datelor și informațiilor rezultate din supravegherea tehnică, pentru a elucida viitoare probleme care vor fi supuse analizei.

Prin „natura datelor și informațiilor" nu ne vom referi la natura juridică a lor în această secțiune, ci la natura lor materială, respectiv modul în care acestea există sau se materializează. Indiscutabil, din punct de vedere juridic, rezultatul supravegherii tehnice va fi o probă în sens ideatic; în sens material, va fi un mijloc de probă care conține proba, dar evoluția tehnologiei ne impune să tratăm modul în care se prezintă datele și informațiile după punerea în executare.

În trecut, limitele tehnologice ale echipamentelor folosite conduceau ca rezultatele tehnicilor speciale de investigare să fie, de cele mai multe ori, sub forma unor probe analogice captate prin mijloace tehnice și având forma unor înregistrări audio, video, audiovideo[1]. Prin „probe analogice" vrem să subliniem aspectul tehnologic, respectiv folosirea de circuite analogice în procesul de înregistrare și redare a faptelor și împrejurărilor surprinse prin supravegherea tehnică. Astfel, în discuție sunt doar cele două măsuri de supraveghere tehnică prevăzute de art. 138 alin. (1) lit. a) și c) C.pr.pen., întrucât accesul la un sistem informatic și localizarea sau urmărirea prin mijloace tehnice au un caracter digital.

În contextul unor probe analogice, înregistrarea se făcea pe un suport material fie prin modificarea proprietăților fizice ale suportului (înregistrările tip fonograf pe discuri de vinil, expunerea la lumină în cazul filmului fotografic) sau prin stocarea magnetică a informației pe suport prin polarizarea unei benzi magnetice pentru a reprezenta sunet sau imagine. Aceste înregistrări sunt complet diferite de înregistrările digitale care presupun convertirea unui semnal analog (de pildă, frecvențele audio sunt convertite digital prin eșantionare, transformându-se în diferențe de voltaj), a unei imagini sau a unui sunet într-o reprezentare electronică digitală care nu va fi influențată de proprietățile suportului pe care se află. De altfel, reprezentarea digitală a unei probe nu va necesita un echipament specific pentru a fi stocată ori redată, fiind necesar doar un sistem informatic[2].

O probă analogică va fi supusă limitărilor suportului său material și a echipamentului folosit pentru citirea sau copierea acestuia. Întrucât există o influență între modul în care este citit suportul analogic și rezultat, copierea acestuia nu va fi niciodată una perfectă. Cu alte cuvinte, între original și copia sa nu va exista niciodată identitate, ci vor exista întotdeauna diferențe care se vor amplifica atunci când echipamentele sunt de calitate redusă sau se realizează o copie la o altă copie. Relevanța acestor limitări este deosebită din perspectiva valorificării probelor

[1] *J.J. Barbara (coord.)*, Handbook of Digital and Multimedia Forensic Evidence, Humana Press, Totowa, New Jersey, 2008, p. 6.

[2] *M. Suian*, Unele probleme privind folosirea probelor digitale în procesul penal, în Revista de Criminologie, Criminalistică și Penologie nr. 3/2017, p. 153.

în cursul procesului penal și, mai ales, din perspectiva verificării autenticității și veridicității lor, întrucât orice copiere va conduce la o degradare în semnalul analogic care poate rezulta în urma citirii suportului material, putând introduce (sau masca) elemente care nu existau pe suportul original. Ca atare, în trecut era deosebit de relevantă noțiunea de „suport original".

În prezent, mijloacele tehnice analogice au fost abandonate în favoarea unor mijloace tehnice digitale care nu mai sunt influențate de procedeul de redare sau de copiere, întrucât informația nu mai este stocată pe un mediu fizic care va interpreta anumite proprietăți ca diferențe de voltaj ce vor fi interpretate electronic, ci informația este stocată într-un format numeric care poate fi interpretat de un sistem informatic și redat, la nevoie, chiar și scriptic. Această interpretare numerică presupune că înregistrarea realizată se va putea dedubla, copia își va păstra caracterul identic, chiar dacă suportul copiei va fi diferit, din punct de vedere material, de cel al originalului. În mod plastic, situația este asemenea transcrierii fidele a unei cărți: se va schimba cerneala, se va schimba suportul, dar informația va rămâne aceeași.

Credem că, și din punct de vedere criminalistic, vom putea opera cu conceptul de „identitate", întrucât conceptul presupune descoperirea tuturor asemănărilor și diferențelor dintre două obiecte, urme sau fenomene, unde asemănarea poate fi indiciul unei identități ascunse care se va putea stabili în funcție de limitele tehnicii, fiind vorba de o identitate relativă[1]. Or, dacă datele informatice inițiale și cele copiate prezintă numai asemănări și nu prezintă nicio deosebire, concluzia va fi că ele vor fi identice și dacă se află pe doi suporți de stocare diferiți.

Codul de procedură penală recunoaște că rezultatele activităților de supraveghere tehnică vor avea caracter strict digital prin mențiunea din cuprinsul art. 143 alin. (2^1) C.pr.pen., în care legiuitorul se referă la „*suportul de stocare a datelor informatice care conține rezultatul activităților de supraveghere tehnică*".

Trecând discuția la un alt palier, mijloacele tehnice moderne de realizare a supravegherii tehnice nu mai presupun obligativitatea existenței unor suporți materiali, fiind suficient ca probele digitale să fie păstrate în condiții care asigură autenticitatea acestora, inclusiv prin semnarea lor cu semnătură electronică extinsă. O situație aparte este cea a interceptării comunicațiilor, unde suportul original poate lipsi, fiindcă interceptarea se realizează prin programe informatice aflate pe sistemele informatice ale C.N.I.C. Acestea sunt legate la toți furnizorii de servicii de comunicații electronice, de unde preiau în format digital convorbirea și o stochează în fișiere care se transferă digital către persoana care pune în executare mandatul de supraveghere tehnică. Într-o altă situație, înregistrarea audiovideo se poate realiza prin captarea sunetului și a imaginii pe un suport de memorie atașat camerei video – memorie tip flash, în format card SD comun tuturor aparatelor foto sau video –, ceea ce ar face din acesta suportul original. Din considerente economice, rezultatul activităților de supraveghere tehnică se stochează pe suporți optici – CD/DVD/Blu-Ray –, fiindcă aceștia asigură un preț de zeci de ori mai scăzut decât un suport inițial și împiedică modificarea datelor informatice conținute pe acestea.

Consecința digitalizării rezultatelor activităților de supraveghere tehnică este că acestea vor constitui date informatice, apte să fie copiate de un număr nelimitat de ori și, dacă se respectă regulile tehnice pentru menținerea integrității lor, vor avea aceleași caracteristici ca originalul. Mai mult, astfel cum vom detalia în secțiunea privind semnarea, verificarea și certificarea electronică a datelor rezultate din supravegherea tehnică, se va putea stabili

[1] *L. Ionescu, D. Sandu*, Identificarea criminalistică, ed. a 2-a, Ed. C.H. Beck, București, 2011, p. 44.

identitatea dintre două fișiere – original și copie într-un mod repetabil și care garantează autenticitatea informațiilor[1].

În literatura de specialitate s-a susținut că actuala reglementare a suportului material constituie un regres față de legislația anterioară, întrucât nu se mai vorbește despre suportul original, considerându-se că, în pofida terminologiei actuale, suportul trebuie să fie original, iar copia trebuie să fie certificată pentru autenticitate de persoana autorizată prin intermediul unei semnături electronice extinse, potrivit art. 143 alin. (2[1]) C.pr.pen.[2]. Nu putem fi de acord cu opinia exprimată dintr-o perspectivă tehnică, și nu una juridică, sens în care o apreciem a fi corectă. Din punct de vedere tehnic, la momentul actual, importanța unui suport original a scăzut prin aceea că rezultatul activităților de supraveghere va constitui o probă în format digital, ceea ce permite copierea fără a se pierde caracterul său autentic și fără a i se afecta integritatea. Aceasta nu înseamnă că suportul original nu va avea importanță, însă acesta trebuie să fie redefinit de către legiuitor ca fiind *un suport digital inițial* și ca, la momentul extragerii datelor informatice pe orice alt mijloc de stocare, să fie impus un control de autenticitate și integritate prin semnătură electronică extinsă, în sensul dispozițiilor art. 142[1] C.pr.pen. Sub acest aspect, Codul de procedură penală este deficitar, deoarece nu reglementează un sistem de trasabilitate a rezultatului supravegherii tehnice de la persoana care pune în executare măsura până la persoana care o introduce pe un mijloc de stocare și nu prevede garanții suficiente privind asigurarea integrității și autenticității datelor informatice ce constituie rezultatul activităților de supraveghere tehnică.

Secțiunea a 2-a. Consemnarea activităților de supraveghere tehnică

În urma punerii în executare a mandatului de supraveghere tehnică, vor fi obținute, după cum am arătat, rezultate ale activităților de supraveghere tehnică sub formatul unor date informatice care, pentru a putea fi folosite în procesul penal, vor trebui să fie consemnate într-un proces-verbal, în conformitate cu dispozițiile art. 143 alin. (1) C.pr.pen.[3].

Spre deosebire de Codul de procedură penală anterior, legea procesuală instituie două mijloace de probă în cazul supravegherii tehnice, pe care le apreciem, alături de alți autori[4], ca fiind distincte: *i)* procesul-verbal de consemnare a activităților de supraveghere tehnică și *ii)* procesul-verbal de redare și certificare a convorbirilor, comunicărilor sau conversațiilor interceptate și înregistrate. Alți autori nu fac o asemenea diferență, considerând că dispozițiile art. 143 C.pr.pen. se referă la un singur proces-verbal unitar de consemnare a activităților de supraveghere tehnică, care va conține și redarea convorbirilor interceptate și înregistrate[5].

---

[1] *V. infra*, Titlul III, Capitolul V.I.

[2] *Gh. Mateuț*, Procedură penală, 2019, p. 697.

[3] Conform art. 143 alin. (1) C.pr.pen., „procurorul sau organul de cercetare penală întocmește un proces-verbal pentru fiecare activitate de supraveghere tehnică, în care sunt consemnate rezultatele activităților efectuate care privesc fapta ce formează obiectul cercetării sau contribuie la identificarea ori localizarea persoanelor, datele de identificare ale suportului care conține rezultatul activităților de supraveghere tehnică, numele persoanelor la care se referă, dacă sunt cunoscute, sau alte date de identificare, precum și, după caz, data și ora la care a început activitatea de supraveghere și data și ora la care s-a încheiat".

[4] *Gh. Mateuț*, Procedură penală, 2019, p. 696; *M. Udroiu*, Procedură penală, vol. I, 2019, pp. 591-592; *M. Bulancea, R. Slăvoiu*, în M. Udroiu (coord.), Codul de procedură penală, 2017, pp. 701-703.

[5] *V. Trif*, op. cit., p. 132.

Credem că se poate face o confuzie între consemnarea și certificarea înregistrărilor ca urmare a terminologiei instituite prin legislația procesuală penală mai veche, unde la art. 91[3] C.pr.pen. anterior se instituia o procedură de certificare a rezultatelor interceptărilor și înregistrărilor realizate în cauză. Noul Cod de procedură penală instituie o viziune diferită, care extinde obiectul supravegherii tehnice prin metode speciale care nu impun redarea unor convorbiri sau conversații purtate de persoane, ci constată activități sau împrejurări de fapt care vor trebui cuprinse într-un proces-verbal (de pildă, locația persoanei).

Potrivit art. 138 alin. (13) C.pr.pen., supravegherea tehnică constituie utilizarea oricăreia dintre cele 4 metode speciale prevăzute de art. 138 alin. (1) lit. a)-d) C.pr.pen., astfel că reglementarea art. 143 alin. (1) C.pr.pen. este incidentă în toate aceste situații. În procesul-verbal prevăzut de art. 143 alin. (1) C.pr.pen. vor fi consemnate inclusiv activitățile de acces la un sistem informatic și localizarea sau urmărirea prin mijloace tehnice, metode speciale pentru care nu există nicio obligație de redare și certificare a unor convorbiri, comunicații sau conversații. În aceste condiții, procesul-verbal prevăzut de art. 143 alin. (1) C.pr.pen. va constitui mijloc de probă.

Credem că prin art. 143 alin. (1) C.pr.pen. se instituie obligația ca fiecare activitate de supraveghere tehnică realizată în cauză și care va fi considerată ca fiind relevantă cauzei, potrivit legii, să fie cuprinsă într-un proces-verbal separat întocmit de procuror sau de organul de cercetare penală, constituind mijlocul de probă rezultat din realizarea respectivei activități[1].

Distinct de aceasta, în cazul folosirii metodelor speciale de supraveghere prevăzute de art. 138 alin. (1) lit. a) și c) C.pr.pen., prin dispozițiile art. 143 alin. (4) C.pr.pen. se instituie obligativitatea întocmirii unui proces-verbal de redare integrală a convorbirilor, comunicărilor sau conversațiilor interceptate, act care va trebui să fie certificat pentru autenticitate de către procuror[2]. În această situație, vom putea vorbi de un al doilea proces-verbal care va fi mai elaborat, va conține efectiv probele obținute în cauză prin redarea integrală a convorbirilor, comunicațiilor și conversațiilor purtate. În opinia noastră, procesul-verbal prevăzut de art. 143 alin. (4) C.pr.pen. va putea face corp comun cu procesul-verbal prevăzut de art. 143 alin. (1) C.pr.pen., ținând seama de caracteristicile asemănătoare dintre cele două reglementări.

§1. Organul competent

Procesul-verbal de consemnare a activităților de supraveghere tehnică se întocmește de către procuror sau de către organul de cercetare penală, acestea fiind singurele organe competente să realizeze acest act. Există o distincție făcută de legiuitor în privința dispozițiilor art. 143 alin. (1) C.pr.pen., întrucât nu poate fi remarcată o corespondență între acesta și art. 142 alin. (1) C.pr.pen., situație pe care o apreciem ca fiind intenționată în sensul de a distinge între competența de punere în executare a supravegherii tehnice și consemnarea activităților de supraveghere tehnică. Dacă, în cazul punerii în executare a supravegherii tehnice, competența va fi a procurorului, acesta putând să dispună ca punerea în executare să fie realizată de organul

[1] *C. Olaru*, op. cit., p. 40.

[2] Conform art. 143 alin. (4) C.pr.pen., „convorbirile, comunicările sau conversațiile interceptate și înregistrate, care privesc fapta ce formează obiectul cercetării ori contribuie la identificarea ori localizarea persoanelor, sunt redate de către procuror sau organul de cercetare penală într-un proces-verbal în care se menționează mandatul emis pentru efectuarea acestora, numerele posturilor telefonice, datele de identificare ale sistemelor informatice ori ale punctelor de acces, numele persoanelor ce au efectuat comunicările, dacă sunt cunoscute, data și ora fiecărei convorbiri sau comunicări. Procesul-verbal este certificat pentru autenticitate de către procuror".

de cercetare penală sau de lucrători specializați de poliție, în privința consemnării activităților de supraveghere tehnică, va fi competent procurorul și organul de cercetare penală. Din această împrejurare vor rezulta mai multe consecințe.

În primul rând, chiar dacă există o ordonanță privind punerea în executare a supravegherii tehnice de către organul de cercetare penală sau de un lucrător specializat al poliției, aceasta nu înseamnă că vor fi delegați automat să procedeze și la consemnarea activităților de supraveghere tehnică[1], trebuind să existe o nouă ordonanță emisă de procuror în această privință.

În al doilea rând, legiuitorul nu a inclus posibilitatea ca lucrătorii specializați ai poliției să poată realiza consemnarea activităților de supraveghere tehnică realizate în cauză, alegere înțeleaptă, întrucât procesul-verbal va avea natura de mijloc de probă și se impune a fi întocmit de către un organ de urmărire penală. Literatura de specialitate a constatat în mod corect că și dacă punerea în executare se va realiza de către ofițerii S.R.I., în calitate de organe de cercetare penală speciale în cazul infracțiunilor contra securității naționale și terorism, procurorul va constata toate activitățile realizate de către aceste organe, fiind obligatorie întocmirea procesului-verbal, în condițiile legii[2].

În al treilea rând, spre deosebire de punerea în executare a măsurilor de supraveghere tehnică, care va fi de competența personală a procurorului, consemnarea activităților de supraveghere tehnică va urmări regulile de competență generale ale organelor de urmărire penală. În situația în care cauza care face obiectul urmăririi penale este de competența procurorului, acesta va trebui să întocmească personal procesul-verbal prevăzut de art. 143 alin. (1) C.pr.pen., putând delega această sarcină organului de cercetare penală[3]. În situația, mai puțin probabilă, ținând seama de dispozițiile art. 139 C.pr.pen., că organul de cercetare penală va fi competent să efectueze urmărirea penală, atunci acesta va putea proceda la consemnarea activităților de supraveghere tehnică fără o delegare din partea procurorului. Considerăm că reglementarea actuală constituie un regres față de cea anterioară, unde era obligatorie delegarea organului de cercetare penală în conformitate cu art. 91^3 alin. (1) C.pr.pen. anterior, deoarece, față de gravitatea restrângerii drepturilor fundamentale ale persoanei supuse unei măsuri de supraveghere tehnică, era necesar ca procurorul să rămână competent în a consemna activitățile de supraveghere tehnică, mai ales în contextul în care acestea trebuie să fie evaluate din punctul de vedere al relevanței. În plus, nu se explică de ce legiuitorul a ales ca punerea în executare să se realizeze de procuror și consemnarea de către un alt organ, impunându-se ca, în cazul consemnării, să se mențină aceeași regulă a competenței procurorului prevăzută în cuprinsul art. 142 alin. (1) C.pr.pen.

§2. Selectarea rezultatelor activităților de supraveghere tehnică

Procesul-verbal de consemnare a activităților de supraveghere tehnică va conține numai acele activități care privesc fapta ce formează obiectul cercetării sau contribuie la identificarea ori localizarea persoanelor, ceea ce semnifică existența unui proces de selectare a activităților efectuate și trierea lor. Din acest punct de vedere, Codul de procedură penală prevede în mod confuz acest criteriu atât în cazul consemnării activităților de supraveghere tehnică, cât și în cazul redării și certificării convorbirilor, comunicațiilor sau convorbirilor interceptate și

[1] *Gh. Ivan, V. Ioniță*, Una din problematicile punerii în executare a mandatelor de supraveghere tehnică, în Revista Pro Lege nr. 1/2017, p. 131.

[2] *M. Bulancea, R. Slăvoiu*, în M. Udroiu (coord.), Codul de procedură penală, 2017, p. 701.

[3] *M. Udroiu*, Procedură penală, vol. I, 2019, p. 591.

înregistrate, situație în care, aparent, ar exista două procese de selecție, desfășurate în două etape. Imprecizia legiuitorului este cu atât mai defavorabilă în condițiile în care o parte a doctrinei analizează procedura de selecție a rezultatelor activităților de supraveghere tehnică numai prin raportare la înregistrările efectuate în cauză și prin raportare la redarea certificată a acestora conform art. 143 alin. (4) C.pr.pen.[1].

Selectarea activităților de supraveghere tehnică relevante pentru cauză, în special a înregistrărilor care au fost obținute, este esențială pentru protejarea drepturilor fundamentale ale persoanelor care au făcut obiectul măsurii. În special în cazul înregistrărilor, se impune excluderea acelora care au un caracter personal și nu contribuie la aflarea adevărului în cauză, afectând dreptul la viață privată și de familie[2]. Necesitatea unei selecții a activităților de supraveghere tehnică a fost analizată de Curtea Europeană a Drepturilor Omului prin raportare la problema interceptărilor, stabilindu-se că transcrierea și depunerea la dosarul cauzei a tuturor înregistrărilor de la un post telefonic poate încălca drepturi, precum dreptul la viață privată a altor persoane, fiind excesiv și din punct de vedere practic[3].

În opinia noastră, legiuitorul a stabilit un regim deficitar pentru procesul-verbal de consemnare a activităților de supraveghere tehnică, întrucât nu permite cunoașterea adevăratei întinderi a supravegherii tehnice desfășurate în cauză și nici dacă aceasta s-a realizat între limitele mandatului emise de judecătorul de drepturi și libertăți. Apreciem că, pentru a se garanta limitarea ingerințelor în viața privată a unei persoane și pentru a se constitui garanții reale împotriva arbitrariului, se impune ca fiecare activitate de supraveghere tehnică să fie consemnată pentru ca, mai apoi, cele relevante cauzei să fie folosite în procesul penal și cele care nu sunt relevante să fie arhivate. În actuala legislație, mai întâi are loc o selecție a activităților care privesc fapta ce formează obiectul cercetării sau contribuie la identificarea ori localizarea persoanelor ce urmează a fi consemnate în procesul-verbal prevăzut de art. 143 alin. (1) C.pr.pen., celelalte fiind arhivate conform art. 142 alin. (6) C.pr.pen., fără a fi întocmit niciun proces-verbal care să privească aceste activități. Aceste ultime activități de supraveghere tehnică nu sunt accesibile persoanei vizate, neputându-le consulta sau avea cunoștință de ele în conformitate cu art. 145 alin. (2) C.pr.pen., care limitează consultarea la procesele-verbale de consemnare a activităților de supraveghere tehnică efectuate și la înregistrările rezultate din activitatea de supraveghere tehnică. Afirmăm acest lucru, deoarece în unele situații doar o înregistrare audio sau audiovideo nu poate fi suficientă pentru a se determina în concret activitatea, de pildă, nu se va putea stabili locația unde s-a realizat, în afara unui proces-verbal în care să se consemneze unde a fost realizată înregistrarea.

În doctrină s-a arătat în mod corect că legiuitorul a prevăzut în mod greșit și cu încălcarea drepturilor fundamentale ale persoanei supuse unei măsuri de supraveghere tehnică că participarea părților la evaluarea conținutului convorbirilor interceptate și înregistrate nu este necesară, întrucât orice convorbire pe care procurorul o apreciază utilă pentru aflarea adevărului ar putea fi combătută de orice parte în faza de judecată[4]. Este adevărat că niciuna dintre persoanele supravegheate nu are niciun drept cu privire la selecția convorbirilor sau comunicărilor care ar trebui folosite în cauză. Admitem că este nevoie ca procurorul să decidă asupra procesului de selectare a activităților relevante, dar acest lucru trebuie să se realizeze și

[1] *S. Grădinaru*, Supravegherea tehnică, 2014, p. 131.
[2] *Ibidem*, p. 132.
[3] CEDO, cauza *Dumitru Popescu c. România (nr. 2)*, Hotărârea din 26 aprilie 2007, §78.
[4] *Gh. Mateuț*, Procedură penală, 2019, p. 695.

cu respectarea dreptului persoanei de a face propuneri în acest sens, inclusiv în cursul urmăririi penale, fiind necesar a-i oferi posibilitatea de a cere excluderea sau completarea înregistrărilor cu unele care nu au fost selectate de procuror.

În susținerea opiniei noastre că toate activitățile de supraveghere tehnică trebuie să fie consemnate în procese-verbale, stă și necesitatea ca persoana supusă măsurii să fie încunoștințată de întreaga activitate desfășurată împotriva sa, nu numai de aspectele care au fost selectate de procuror în condițiile art. 143 alin. (1) C.pr.pen. În literatura de specialitate s-a arătat că se impune ca procurorul să comunice persoanei supuse măsurilor de supraveghere tehnică, în conformitate cu art. 145 alin. (2) C.pr.pen., toate înregistrările rezultate din activitățile de supraveghere tehnică și să îi permită să asculte sau să vizualizeze aceste înregistrări indiferent dacă privesc fapta care face obiectul cercetării și au fost consemnate în cadrul unui proces-verbal[1]. Suntem de acord cu această opinie, mai ales în condițiile în care dispozițiile art. 145 alin. (2) C.pr.pen. nu fac vreo distincție între convorbirile comunicările, conversațiile ori imaginile care sunt consemnate în procesele-verbale prevăzute de art. 143 alin. (1) C.pr.pen. și cele care au fost selectate spre arhivare, trebuind să se asigure un acces complet al persoanei supravegheate la aceste înregistrări. Ca atare, dacă se recunoaște accesul în temeiul art. 145 alin. (2) C.pr.pen.[2], se impune și ca procurorul să realizeze procese-verbale de consemnare a activităților de supraveghere tehnică și pentru acestea.

Ținând seama că procesele-verbale întocmite potrivit art. 143 alin. (1) C.pr.pen. pot privi și activități de supraveghere care pot intra în cadrul accesului la un sistem informatic și a localizării sau urmăririi prin mijloace tehnice, se va impune și în aceste situații selectarea activităților care au legătură cu cauza.

În cazul accesului la un sistem informatic, situația va fi una facilă, deoarece, dacă în urma acestuia se descoperă probe care privesc fapta urmărită, întregul rezultat al accesului la un sistem informatic va trebui selectat, respectiv nu vor fi trunchiate numai datele informatice utile cauzei, ci vor trebuie selectate toate datele informatice găsite pe un sistem informatic sau un suport de stocare. Dacă mandatul judecătorului de drepturi și libertăți vizează mai multe sisteme informatice sau mai mulți suporți de stocare, accesarea fiecăruia dintre aceștia va fi socotită o activitate de supraveghere tehnică, în funcție de relevanța rezultatului obținut urmând a se întocmi procesul-verbal conform art. 143 alin. (1) C.pr.pen. Subliniem caracterul maxim intruziv al accesului la un sistem informatic, deoarece vor fi relevate și anumite aspecte privind viața privată a unei persoane de un grad maxim de intimitate. Nu putem concepe neredarea integrală a unei activități sau selectarea doar a unor date informatice, ci vor fi aplicabile aceleași motive ca în cazul interceptărilor și înregistrărilor care presupun o redare integrală. Menționăm că, în cazul accesului la un sistem informatic, este necesară menținerea integrității datelor obținute, astfel că nu pot fi selectate numai unele dintre acestea și altele să fie arhivate, întrucât ar contraveni acestei cerințe.

În privința măsurii localizării sau urmăririi prin mijloace tehnice, apreciem că legiuitorul nu a reglementat niciun filtru prin care să fie protejată persoana de o depășire a caracterului proporțional al folosirii datelor și informațiilor obținute prin această măsură, întrucât toate

[1] *Ibidem*, p. 696.

[2] Conform art. 145 alin. (2) C.pr.pen., „după momentul informării, persoana supravegheată are dreptul de a lua cunoștință, la cerere, de conținutul proceselor-verbale în care sunt consemnate activitățile de supraveghere tehnică efectuate. De asemenea, procurorul trebuie să asigure, la cerere, ascultarea convorbirilor, comunicărilor sau conversațiilor ori vizionarea imaginilor rezultate din activitatea de supraveghere tehnică".

activitățile care vor fi considerate ca făcând parte din această măsură de supraveghere tehnică vor trebui consemnate obligatoriu în procese-verbale. Astfel, potrivit art. 143 alin. (1) C.pr.pen., este instituită o obligație expresă de a se selecta rezultatele activităților efectuate care contribuie la localizarea persoanelor, ceea ce înseamnă că toate rezultatele metodei speciale de supraveghere vor trebui consemnate.

În concluzie, apreciem că selectarea activităților de supraveghere tehnică pentru consemnarea lor în procese-verbale, potrivit art. 143 alin. (1) C.pr.pen., este o etapă obligatorie pentru determinarea relevanței probei care s-a obținut în urma supravegherii tehnice, dar și pentru înlăturarea acelor activități care au produs rezultate nerelevante cauzei.

§3. Consemnarea activităților realizate și conținutul procesului-verbal de consemnare a rezultatelor activităților de supraveghere tehnică

Potrivit art. 143 alin. (1) C.pr.pen., legiuitorul a instituit obligația procurorului de a întocmi câte un proces-verbal pentru fiecare activitate de supraveghere tehnică realizată în cauză și care a produs un rezultat ce este relevant în cauză. Semnificația expresiei de „activitate de supraveghere tehnică" este deosebit de importantă, deoarece, prin prisma sa, se va determina numărul de procese-verbale care trebuie întocmit. Legiuitorul nu definește distinct activitățile de supraveghere tehnică, astfel că există incertitudine referitoare la sensul acestora. Apreciem că prin „activitățile de supraveghere tehnică" nu vom înțelege măsurile de supraveghere tehnică autorizate într-o cauză, ci *modalitățile concrete în care s-a pus în executare supravegherea tehnică*. În mod corect s-a arătat că procesul-verbal trebuie să fie unul elaborat, o oglindă a actului de autorizare[1], întrucât din acesta trebuie să rezulte probele care au fost obținute în cursul punerii în executare a mandatului de supraveghere tehnică. În același sens s-a arătat că procesul-verbal trebuie să reprezinte „*o reproducere fidelă a tuturor* ***activităților efectuate prin diversele metode de supraveghere*** *ce au format obiectul autorizării potrivit legii*"[2] (s.n.). După cum s-a arătat și în jurisprudența Curții Constituționale, procesul-verbal de consemnare a rezultatelor supravegherii tehnice are calitatea de mijloc de probă în procesul penal[3].

În funcție de specificul activității desfășurate, vor putea exista unul sau mai multe procese-verbale, ținând seama și de caracterul continuu sau secvențial al modalităților concrete de supraveghere tehnică.

În situația supravegherii video, audio sau prin fotografiere, vor fi redactate procese-verbale separate în cazul în care se va proceda la utilizarea filajului, fiecare activitate de filaj trebuind să fie consemnată într-un proces-verbal distinct. În cazul în care s-au realizat înregistrări audiovideo ambientale în mod secvențial, pentru fiecare înregistrare se va realiza câte un proces-verbal (de pildă, pentru fiecare întâlnire a persoanei față de care s-a dispus participarea autorizată la anumite activități cu persoana care face obiectul urmăririi penale). În mod corect s-a reținut că în cuprinsul procesului-verbal trebuie să fie incluse imagini care, pentru a putea căpăta valoare probantă, vor trebui să fie descrise de către procuror[4]. Nu se poate concepe ca o activitate de înregistrare video sau prin fotografiere să nu fie cuprinsă în procesul-verbal prin secvențele importante, fiind obligatorie includerea în procesul-verbal a unei planșe fotografice. Momentele importante vor trebui descrise prin raportare la fotografii, indicându-se acțiunile

[1] *C.M. Chiriță*, în N. Volonciu, A.S. Uzlău (coord.), Noul Cod, 2014, p. 325.
[2] *Gh. Mateuț*, Procedură penală, 2019, p. 697.
[3] CCR, Dec. nr. 51 din 16 februarie 2016 (M. Of. nr. 190 din 14 martie 2016), §32.
[4] *S. Grădinaru*, Supravegherea tehnică, 2014, p. 140.

surprinse și identificarea (atunci când e posibilă) a persoanelor care participă, precum și indicarea locului în care acestea s-au întâlnit ori unde a avut loc acțiunea surprinsă. Dacă vor fi surprinse și conversații între persoanele supravegheate, va trebui să se întocmească separat un proces-verbal de redare certificată a acestora, în conformitate cu art. 143 alin. (4) C.pr.pen.

Dacă supravegherea video, audio sau prin fotografiere se va realiza prin pătrunderea în spații private pentru activarea sau dezactivarea mijloacelor tehnice folosite, activitățile respective vor trebui consemnate în procese-verbale distincte. Fiind o activitate care se va autoriza expres de către judecătorul de drepturi și libertăți, aceasta va trebui consemnată în scris. Este deosebit de important, pentru protejarea dreptului la viață privată, să fie consemnate în detaliu: modalitatea de pătrundere, locul prin care s-a pătruns, persoanele care au realizat activitatea, modul și locul în care au fost instalate mijloacele tehnice, caracteristicile acestora, dar și momentul la care a început și a încetat activitatea.

Atunci când activitățile privesc interceptarea comunicațiilor unei persoane, se va întocmi un singur proces-verbal în care vor fi consemnate toate conversațiile, comunicațiile sau convorbirile care sunt apreciate ca având legătură cu cauza, prin menționarea elementelor de identificare a acestora – postul telefonic utilizat, data și timpul la care a avut loc convorbirea, postul telefonic al interlocutorului, adresa de e-mail de la care s-a transmis și destinatarul comunicării. Apreciem că va fi suficient un singur proces-verbal și dacă măsura de supraveghere tehnică se va întrebuința pentru mai multe persoane, față de caracterul automatizat al realizării interceptării[1]. Diferit față de procesul-verbal prevăzut de art. 143 alin. (4) C.pr.pen., vor fi consemnate numai acele date și informații care atestă existența comunicării, identitatea persoanelor care au realizat-o, mijlocul prin care s-a realizat și elementul de timp aferent fiecăreia dintre acestea. Ulterior, conținutul efectiv al fiecăreia va fi redat integral, în conformitate cu dispozițiile art. 143 alin. (4) C.pr.pen.

În cazul accesului la un sistem informatic, activitățile consemnate vor fi unele de natură tehnică, dar vor trebui să includă modalitatea în care s-a realizat activitatea (acces direct sau la distanță), identificarea sistemului informatic, descrierea din punct de vedere tehnic a modului în care s-a pătruns în sistemul informatic, datele informatice identificate și cum s-a realizat modul de extragere a lor și dacă au fost realizate și alte activități în legătură cu alte măsuri de supraveghere tehnică (instalarea de programe în vederea interceptării comunicațiilor, de acționare la distanță a camerei dispozitivului și a microfonului în vederea înregistrării etc.). În măsura în care accesul la un sistem informatic s-a autorizat prin ordonanța procurorului, vor trebui menționate și datele informatice care au fost suprimate, conform art. 141 alin. (5) C.pr.pen.

În privința localizării sau urmăririi prin mijloace tehnice, în cuprinsul procesului-verbal se vor consemna toate mișcările realizate de către obiectul sau persoana la care au fost atașate asemenea mijloace tehnice. În funcție de caracterul secvențial sau continuu, se vor realiza unul sau mai multe procese-verbale. De pildă, în cazul localizării unei mașini printr-un dispozitiv GPS atașat de aceasta, activitatea va fi continuă, putându-se monitoriza locațiile avute de respectivul obiect la perioadele de timp setate în mijlocul tehnic de supraveghere. Față de informațiile care rezultă din localizare, apreciem că se impune ca organele de urmărire penală să interpreteze datele prin realizarea unor hărți care să surprindă traseul pe care l-a avut persoana sau obiectul urmărit. Desigur, vor trebuie menționate coordonatele GPS, dar rezultatul supravegherii va trebui exprimat într-un mod ușor de înțeles, sens în care locațiile numerice trebuie corelate cu cele din teren prin indicarea adresei, localității, străzii, drumului

[1] *M. Bulancea, R. Slăvoiu*, în M. Udroiu (coord.), Codul de procedură penală, 2017, p. 702.

național (cu indicarea sensului de deplasare) etc. Opririle persoanei sau obiectului vor trebui consemnate distinct.

În ceea ce privește conținutul procesului-verbal de consemnare a activităților de supraveghere tehnică, potrivit art. 143 alin. (1) C.pr.pen., acesta va trebui să includă și *datele de identificare ale suportului care conține rezultatul activităților de supraveghere tehnică*, *numele persoanelor la care se referă, dacă sunt cunoscute*, sau alte *date de identificare*, precum și, după caz, *data și ora la care a început activitatea de supraveghere și data și ora la care s-a încheiat*.

O mențiune pe care o considerăm obligatorie, dar care nu este amintită în cuprinsul art. 143 alin. (1) C.pr.pen., este *indicarea actului de autorizare în baza căruia s-au realizat activitățile de supraveghere tehnică*, respectiv mandatul de supraveghere tehnică emis de judecătorul de drepturi și libertăți sau ordonanța de autorizare provizorie emisă de procuror.

Datele de identificare ale suportului care conține rezultatul activităților de supraveghere tehnică trebuie să fie menționate, întrucât, potrivit art. 143 alin. (2) C.pr.pen., va fi obligatorie atașarea acestui suport la procesul-verbal. Se vor menționa tipul de suport folosit – CD, DVD, Blu-Ray sau suport de stocare tip hard-disk sau stick USB ori similare cu menționarea, după caz, a seriei constructive a mediului de stocare. În situația în care suportul de stocare nu va avea o serie constructivă sau aceasta nu va fi vizibilă (situație care poate fi întâlnită la suporții optici), suportul va fi inscripționat de către organul de urmărire penală cu un identificator și va fi inserat într-un plic sigilat pe care se va nota conținutul acestuia.

Numele persoanelor la care se referă activitățile de supraveghere tehnică vor fi precizate în cuprinsul procesului-verbal dacă acestea sunt cunoscute, în caz contrar, vor fi precizate date de identificare a acestora în măsura posibilităților. Ceea ce trebuie subliniat este că una dintre persoanele care sunt supravegheate va fi identificată sau identificabilă în mod obligatoriu, altfel nu ar fi putut fi autorizată măsura de supraveghere tehnică.

Data și ora la care a început activitatea de supraveghere, precum și data și ora la care s-a încheiat vor trebui menționate în funcție de caracterul măsurii de supraveghere folosite. Dacă va avea un caracter continuu, precum interceptarea comunicațiilor prin telefon, atunci aceasta se va realiza numai în limitele mandatului, neavând o relevanță deosebită, întrucât, față de specificul ei, fiecare convorbire efectuată și interceptată va trebui consemnată prin raportare la dată și loc în procesul-verbal prevăzut de art. 143 alin. (4) C.pr.pen. În toate celelalte cazuri va fi obligatorie indicarea acestor mențiuni.

Secțiunea a 3-a. Redarea și certificarea convorbirilor, comunicărilor sau conversațiilor interceptate și înregistrate

În mod distinct de consemnarea rezultatelor activităților de supraveghere tehnică, legiuitorul a impus o sarcină suplimentară în cazul în care în urma supravegherii tehnice au rezultat convorbiri, comunicări și conversații interceptate și înregistrate, fiind obligatorie redarea și certificarea acestora într-un proces-verbal. Obligația de redare în scris a acestora va exista numai în măsura în care, potrivit art. 143 alin. (4) C.pr.pen., privesc fapta care formează obiectul cercetării ori contribuie la identificarea ori localizarea persoanelor.

Deși, în cele mai multe cazuri, supravegherea tehnică se va rezuma numai la interceptarea comunicațiilor sau a oricărui tip de comunicare la distanță și realizarea supravegherii video, audio sau prin fotografiere, trebuie menționat că dispozițiile art. 143 alin. (4) C.pr.pen. nu se

vor aplica metodelor speciale de supraveghere a accesului la un sistem informatic, decât în măsura în care constituie modalitatea concretă de interceptare a comunicațiilor, și nici localizării sau urmăririi prin mijloace tehnice.

În cazul în care activitățile de supraveghere tehnică presupun interceptarea și înregistrarea de convorbiri, comunicări sau conversații, s-a considerat că mijlocul de probă scris va fi procesul-verbal în care sunt redate activitățile efectuate[1].

Potrivit reglementării anterioare, întreaga procedură în urma căreia rezulta procesul-verbal certificat de redare a convorbirilor sau comunicărilor interceptate se denumea „certificarea înregistrărilor" și includea selectarea și redarea integrală a acestora alături de certificarea propriu-zisă realizată de procuror. Ceea ce se va certifica este rezultatul supravegherii tehnice materializat într-un proces-verbal reglementat de art. 143 alin. (4) C.pr.pen., și nu a suporților de stocare[2].

Organul competent să procedeze la redarea convorbirilor, comunicațiilor sau conversațiilor va fi procurorul sau organul de cercetare penală, în funcție de normele generale de competență a organelor de urmărire penală, sens în care facem trimitere la explicațiile privind competența încheierii procesului-verbal de consemnare a activităților de supraveghere tehnică[3].

§1. Redarea integrală a convorbirilor, comunicărilor sau conversațiilor interceptate și înregistrate

Cea mai importantă condiție a respectării dreptului la apărare al persoanei care a fost supusă măsurilor de supraveghere tehnică este ca toate convorbirile, comunicările și conversațiile interceptate și înregistrate să fie redate în integralitatea lor. Prin aceasta nu înseamnă că vor trebui redate toate rezultatele de acest fel provenite din supravegherea tehnică, ci numai acele înregistrări care privesc cauza, în sensul dispozițiilor amintite mai sus. Într-un mod nefericit, legiuitorul a omis să mai precizeze expres că redarea se va face integral, dispozițiile legale actuale fiind considerate un regres față de legea procesuală penală anterioară[4]. Cu toate acestea, același autor consideră că, și în lipsa acestei mențiuni, interpretarea legală va trebui să fie în sensul unei redări integrale.

Importanța unei redări integrale a convorbirii este de necontestat, întrucât orice trunchiere sau omisiune de consemnare poate schimba înțelesul convorbirii și poate fi interpretat în mod greșit de organele judiciare. O situație ridicată în literatura de specialitate, prin analizarea unor practici discutabile ale procurorilor, a fost inversarea replicilor dintre interlocutori, pentru a fi relevate conotații penale[5].

În privința modalității de redare a conținutului convorbirilor, aceasta se va face într-o formă care să păstreze specificul vorbirii persoanei supuse măsurii de supraveghere tehnică, putând fi păstrate regionalismele, termenii argotici sau de jargon[6]. Transcrierea va trebui astfel să se realizeze cu cât mai mare fidelitate, pentru a nu fi denaturate sensurile specifice utilizate, trebuind să se interpreteze și tonul vocii, pentru a determina sensul real al cuvintelor folosite[7].

---

[1] *S. Grădinaru*, Supravegherea tehnică, 2014, p. 123; *Gh. Mateuț*, Procedură penală, 2019, p. 697.
[2] C. Ap. Suceava, s. pen., încheierea nr. 29 din 6 mai 2016.
[3] *V. supra*, Titlul III, Capitolul V.2.
[4] *Gh. Mateuț*, Procedură penală, 2019, p. 694.
[5] *S. Grădinaru*, Supravegherea tehnică, 2014, p. 125.
[6] *Ibidem*, p. 123.
[7] *M.V. Tudoran*, Teoria și practica interceptărilor, 2012, p. 193.

În măsura în care factorii externi convorbirii nu permit înțelegerea cuvintelor, se impune a se face o mențiune privind caracterul neinteligibil al vorbirii, nefiind permis a se intui respectivul cuvânt[1].

În situația în care nu se va utiliza limba română în interceptările și înregistrările care fac obiectul redării, potrivit art. 143 alin. (3) C.pr.pen., ele vor fi transcrise în limba română prin intermediul unui interpret care va fi obligat să păstreze confidențialitatea operațiunii. În această situație, procesul-verbal încheiat va fi semnat și de către interpret. Doctrina a criticat, pe bună dreptate, caracterul lacunar al dispozițiilor legale, arătând că, în traducere, trebuie avute în vedere: *i)* preschimbarea în limba română a capturilor audio din limba străină; *ii)* obligativitatea semnării de către interpret a fiecărei pagini a procesului-verbal de redare, pentru a se asigura oficialitatea preschimbării limbii; *iii)* realizarea măsurii de către traducători autorizați obiectivi (care să nu facă parte din organele care pun în executare măsura, precum era prevăzut în unele protocoale încheiate de Ministerul Public cu S.R.I.); *iv)* noțiunea de „interpret" prevăzută de cod trebuie să fie interpretată și în sensul de „traducător", în accepțiunea mai largă a noțiunii, pentru a permite redactarea în scris a traducerii[2].

În cazul înregistrărilor efectuate de părți, va exista o obligație de redare a acestora într-un proces-verbal în condițiile art. 143 alin. (4) C.pr.pen., chiar dacă acestea nu provin dintr-o măsură de supraveghere tehnică autorizată de judecătorul de drepturi și libertăți, deoarece vor avea o natură identică activităților de supraveghere tehnică. Mai mult, ele fiind prevăzute în cadrul măsurilor de supraveghere tehnică, nu sunt excluse expres de la obligația procurorului de a le reda integral într-un proces-verbal, legiuitorul nefăcând nicio distincție, în cuprinsul art. 143 alin. (4) C.pr.pen., care să conducă la o altă interpretare.

Pentru a fi complet, procesul-verbal de redare va trebui să conțină și elementele menționate în cuprinsul art. 143 alin. (4) C.pr. pen., respectiv: „*indicarea mandatului sau a ordonanței procurorului prin care s-a autorizat măsura de supraveghere tehnică, numerele posturilor telefonice, datele de identificare ale sistemelor informatice ori ale punctelor de acces, numele persoanelor care au efectuat comunicările, dacă sunt cunoscute, data și ora fiecărei convorbiri sau comunicări*". Aceste mențiuni cuprind mai multe ipoteze, astfel că se vor aplica în funcție de situația specifică, neputând fi cuprinse toate în același proces-verbal. În continuare vom prezenta numai acele elemente la care nu am făcut referire în secțiunea precedentă.

Numerele posturilor telefonice constituie o mențiune esențială în cazul interceptării comunicațiilor telefonice, deoarece permite identificarea persoanelor între care se realizează convorbirea. Acest element poate lipsi atunci când convorbirea se realizează prin alte mijloace tehnice – emițător radio – sau prin servicii de internet – Skype sau similare –.

Datele de identificare ale sistemelor informatice vor trebui menționate dacă convorbirile, comunicațiile ori conversațiile se realizează prin intermediul unor sisteme informatice. Cel mai des întâlnite situații sunt cele ale unor comunicații prin intermediul e-mailului, unde se vor introduce mai degrabă elementele unuia dintre sistemele informatice, întrucât, de regulă, va exista ca intermediar un server de e-mail între persoanele care comunică. În funcție de întinderea mandatului de supraveghere tehnică, este posibilă interceptarea ambelor puncte ale comunicării – trimitere și primire.

---

[1] *M. Udroiu*, Procedură penală, vol. I, 2019, p. 592.

[2] *M.V. Tudoran*, Teoria și practica interceptărilor, 2012, pp. 195-196; *E.-A. Iancu, G.M. Șinca, T. Șinca*, Considerații referitoare la folosirea interpreților și traducătorilor în activitățile de supraveghere tehnică, în Revista de Criminologie, Criminalistică și Penologie nr. 2/2018, pp. 38-40.

Datele de identificare ale punctului de acces reprezintă particularitățile de identificare ale echipamentului prin care se realizează conectarea unui sistem informatic la o rețea de comunicații publice.

Data și ora fiecărei convorbiri se impune a fi menționată ca o caracteristică obligatorie, însă apreciem că aceasta va trebui să privească nu numai convorbirile, ci și comunicările și conversațiile purtate de persoanele supuse măsurilor de supraveghere tehnică.

§2. Certificarea propriu-zisă a proceselor-verbale de redare a convorbirilor, comunicațiilor și conversațiilor interceptate și înregistrate

În mod similar cu legea procesuală penală anterioară, conform art. 143 alin. (4) C.pr.pen., procesele-verbale de redare a convorbirilor, comunicărilor sau conversațiilor interceptate și înregistrate sunt supuse certificării de către procuror. Codul de procedură penală nu a instituit o procedură clară privind modul de certificare și nici măcar nu a definit conceptul, fapt care a fost criticat în literatura de specialitate[1].

Certificarea servește la stabilirea autenticității datelor consemnate în procesul-verbal raportat la conținutul convorbirii sau comunicării interceptate și înregistrate[2]. S-a arătat că „*certificarea semnifică un act de confirmare, de întărire a exactității celor stabilite prin înscris (…) din punct de vedere juridic, se arată faptul că sunt respectate toate cerințele legii pentru valabilitatea catului juridic*”[3].

În esență, pentru ca procurorul să poată certifica procesele-verbale prevăzute de art. 143 alin. (4) C.pr.pen., se impune ca acesta să verifice corespondența dintre cele consemnate – transcrise – și convorbirile, comunicațiile și conversațiile interceptate și înregistrate, pe care va trebui să le asculte sau să le vizioneze personal, pentru a putea certifica autenticitatea proceselor-verbale. Nu vor fi supuse certificării înregistrările realizate de părți sau de alte persoane în temeiul art. 139 alin. (3) C.pr.pen., întrucât certificarea este strâns legată de existența unei autorizări a măsurii de supraveghere tehnică[4]. În practica judiciară s-a apreciat că lipsa certificării ar atrage nulitatea relativă a procesului-verbal de redare[5], motivându-se că nu există o vătămare și că o asemenea vătămare se poate înlătura dacă în procesul-verbal sunt indicate seriile suporților optici. Nu putem fi de acord cu această opinie, însăși procedura de certificare conferind valoare probatorie procesului-verbal, omisiunea acesteia neputând fi complinită în cursul cercetării judecătorești, contrar susținerii din speța amintită, întrucât, potrivit art. 143 alin. (4) C.pr.pen., certificarea este atributul exclusiv al procurorului.

Pentru ca certificarea să fie valabilă, este necesar ca actele desfășurate anterior acesteia să fie, la rândul lor, valabile, fiind greșită soluția instanței de a aprecia că certificarea de către procuror a unor procese-verbale de redare integrală întocmite ca urmare a interceptărilor puse în executare de către S.R.I. ar acoperi acest viciu[6].

Din punctul de vedere al formei, certificarea trebuie să constea într-o rezoluție a procurorului prin care se constată certificarea autenticității conținutului fiecărui proces-verbal, acesta

[1] *S. Grădinaru*, Supravegherea tehnică, 2014, p. 114.

[2] *M. Bulancea, R. Slăvoiu*, în M. Udroiu (coord.), Codul de procedură penală, 2017, p. 704.

[3] *S. Grădinaru*, Supravegherea tehnică, 2014, p. 100.

[4] *Ibidem*, p. 117; *M. Udroiu*, Procedură penală, vol. I, 2019, p. 592.

[5] Trib. Harghita, s. pen., încheierea din 18 noiembrie 2015, modificată prin încheierea nr. 3 din 19 ianuarie 2016 a C. Ap. Târgu Mureș, publicată în C. Moisă, op. cit., p. 104.

[6] C. Ap. Alba Iulia, încheierea nr. 77 din 7 iunie 2016.

semnând fiecare proces-verbal. Întrucât legea nu distinge, în situația în care procurorul este cel care realizează transcrierea convorbirilor și va semna procesul-verbal, este necesar ca acesta să facă mențiune distinctă asupra faptului că certifică autenticitatea respectivului proces-verbal. În sens contrar, s-a susținut că, deși Codul de procedură penală nu specifică în mod expres, nu ar trebui să se procedeze la certificarea pentru autenticitate de către procuror a proceselor-verbale în situația în care redarea este realizată de acesta, pentru că s-ar ajunge la situația absurdă în care procurorul să își certifice propriul act[1].

Secțiunea a 4-a. Realizarea suportului digital care conține rezultatele activităților de supraveghere tehnică

Deoarece nu se poate concepe ca o măsură de supraveghere tehnică să nu producă rezultatele într-o formă care să impună stocarea digitală a lor, pentru a permite contestarea sub aspectul veridicității a proceselor-verbale prevăzute de art. 143 alin. (1) și (4) C.pr.pen., rezultatele supravegherii tehnice vor trebui să fie inscripționate pe un suport care se va păstra la sediul parchetului, o copie atașându-se procesului-verbal prevăzut de art. 143 alin. (1) C.pr.pen.

Ținând seama de faptul că în cuprinsul art. 143 alin. (1) C.pr.pen. se consemnează numai activitățile efectuate care privesc fapta ce formează obiectul cercetării sau contribuie la identificarea ori localizarea persoanelor, suportul care va rezulta nu va conține integralitatea rezultatelor obținute din supravegherea tehnică, ci numai acea parte care a fost considerată de procuror ca fiind relevantă pentru cauză. Celelalte date care rezultă din supravegherea tehnică și care nu întrunesc condițiile art. 143 alin. (1) C.pr.pen. vor fi arhivate, conform art. 142 alin. (6) C.pr.pen. Consecința unei separări a rezultatelor de supraveghere tehnică prin trierea realizată de către procuror (sau de către organul de urmărire penală delegat) are importanță pentru stabilirea unor împrejurări privind existența unui suport original (în realitate, un suport inițial), despre care am vorbit într-o secțiune anterioară.

Pentru realizarea suportului de stocare inițial, datele și informațiile rezultate din supravegherea tehnică vor fi supuse analizei procurorului sau organului de cercetare și vor fi sortate în cele două categorii arătate. Ulterior sortării lor, se vor realiza suporți de stocare (CD/DVD/Blu-Ray, hard-diskuri, memorii flash, stick-uri USB etc.) distincți pentru fiecare dintre acestea. Suportul original va putea fi considerat acel suport inițial care rezultă din această triere și va întruni condițiile prevăzute de art. 143 alin. (1) C.pr.pen. Astfel cum am arătat într-o secțiune anterioară, toate rezultatele activităților de supraveghere tehnică care privesc fapta ce formează obiectul cercetării sau contribuie la identificarea sau localizarea persoanelor vor fi consemnate într-un proces-verbal, între acesta și suportul care conține rezultatul acestor activități fiind necesar să existe o corespondență perfectă privind activitățile conținute[2].

Conform art. 143 alin. (2) C.pr.pen., la procesul-verbal de consemnare a activităților de supraveghere tehnică se atașează, în plic sigilat, *o copie a suportului* care conține rezultatul activităților de supraveghere tehnică. În același timp, suportul inițial sau o copie certificată a acestuia se va păstra la sediul parchetului în plic sigilat și va putea fi pus la dispoziția instanței la solicitarea acesteia. Această reglementare pare surprinzătoare, dar credem că se poate explica din punct de vedere practic. Atașarea la procesul-verbal a unei copii a suportului care

[1] *V. Trif*, op. cit., p. 163.

[2] *Gh. Mateuț*, Procedură penală, 2019, p. 698.

conține activitățile de supraveghere tehnică are ca scop conservarea în bună stare tehnică a suportului care nu va fi folosit de organele de urmărire penală sau de instanță decât în situații speciale, precum în cazul contestării autenticității copiei suportului sau al pierderii sau deteriorării copiei transmise alături de procesul-verbal. Ținând cont că majoritatea suporților cu interceptări și înregistrări realizate în cauză sunt sub formă de mediu optic – CD-uri, întotdeauna există riscul ca, prin manipularea lor excesivă sau prin transportarea lor excesivă, supunerea lor la schimbări de temperatură, acțiunea unor raze UV, reacția cu unele substanțe sau chiar prin trecerea timpului, aceștia să se degradeze într-o măsură care nu va mai permite citirea informației. De aceea, legiuitorul a considerat că se impune ca suportul inițial să fie păstrat în condiții adecvate la sediul parchetului. Această soluție trebuie să fie privită ca una provenită din practică. În plus, păstrarea suportului original la sediul parchetului permite ca datele și informațiile obținute prin supraveghere tehnică să fie folosite și în alte cauze, potrivit art. 142 alin. (5) C.pr.pen., fără ca procurorul să fie nevoit să ceară o copie instanței.

Mențiunea legiuitorului privind păstrarea la sediul parchetului a suportului inițial sau a unei copii certificate are în vedere situația în care suportul va fi folosit în mai multe cauze penale, fiind necesar ca pentru fiecare cauză în care se folosesc rezultatele activităților de supraveghere tehnică să se realizeze câte o copie certificată a suportului inițial. Prin „copie certificată" se va înțelege o copie integrală a suportului inițial, care va conține toate datele rezultate în urma supravegherii tehnice[1].

Din punct de vedere tehnic, copia suportului va conține date informatice identice cu cele ale suportului inițial, trebuind să fie folosite metode de copiere care să conserve integritatea și autenticitatea datelor. În cazul suporților optici, aceasta nu reprezintă o problemă deosebită, fiind des răspândite cunoștințele privind copierea de suporți optici între cetățenii români. Totuși, se impune ca această copiere să fie realizată prin programe specifice și ulterior să se verifice dacă datele au fost copiate în mod fidel.

În plus față de dispozițiile arătate, Codul de procedură penală introduce și posibilitatea ca orice persoană autorizată să realizeze copii ale unui suport de stocare a datelor informatice pentru a putea verifica integritatea datelor incluse în suportul original și, după efectuarea copiei, să semneze datele incluse în copie prin utilizarea unei semnături electronice extinse[2]. Acest text legal introduce o facultate a persoanei autorizate, și nu o obligație, ca urmare a folosii expresiei „are posibilitatea". Pentru ca verificarea integrității datelor informatice de pe suportul original să poată avea loc, este necesar ca, în prealabil, odată cu realizarea activităților de supraveghere tehnică sau la transmiterea acestora, datele informatice conținute pe suportul original să fi fost semnate printr-o semnătură electronică extinsă. În absența acesteia, posibilitatea verificării nu va exista din punct de vedere tehnic, întrucât textul de lege limitează verificarea integrității numai la un procedeu care implică existența acestei semnături, conform art. 142[1] C.pr.pen.

În literatura de specialitate s-a susținută că, prin procedura prevăzută de art. 143 alin. (2[1]) C.pr.pen., „*copia trebuie să fie certificată pentru autenticitate de persoana autorizată*

[1] *Ibidem*, p. 697; *M. Bulancea, R. Slăvoiu*, în M. Udroiu (coord.), Codul de procedură penală, 2017, p. 704; *M. Udroiu*, Procedură penală, vol. I, 2019, p. 591.

[2] Conform art. 143 alin. (2[1]) C.pr.pen., „orice persoană autorizată care realizează copii ale unui suport de stocare a datelor informatice care conține rezultatul activităților de supraveghere tehnică are posibilitatea să verifice integritatea datelor incluse în suportul original și, după efectuarea copiei, să semneze datele incluse în aceasta, utilizând o semnătură electronică extinsă bazată pe un certificat calificat eliberat de un furnizor de servicii de certificare acreditat și care permite identificarea neambiguă a persoanei autorizate, aceasta asumându-și astfel responsabilitatea în ceea ce privește integritatea datelor".

prin intermediul unei semnături electronice extinse"[1]. Deși este de dorit să se procedeze așa, textul legal nu include o obligație în acest sens, ci o facultate a persoanei care realizează copia. Totodată, certificarea unei copii nu se va putea realiza prin intermediul unei semnături electronice extinse, întrucât aceasta se aplică pentru fiecare fișier în parte conținut de suportul de stocare, și nu asupra întregului suport[2]. Noțiunea de „certificare" din dreptul procesual penal nu are nicio legătură cu noțiunea de „certificat" folosită în Cod, deoarece termenul este preluat din argoul tehnologic, unde este folosit în contextul identificării digitale, a criptării și a transmisiei securizate de date. Desigur, se poate considera că certificarea unei copii s-ar putea face prin semnarea cu o semnătură electronică extinsă, dar cât timp Codul nu instituie o obligație în a folosi acest tip de semnătură, dar instituie obligația unei certificări a copiei, concluzia va trebui să fie una diferită. Ca atare, o copie certificată se va realiza prin mijloace care conservă integritatea datelor și certificarea se va face scriptic, persoana care realizează copia certificând că acțiunea de copiere s-a realizat astfel încât datele transferate pe suportul copie sunt autentice și și-au păstrat integritatea[3].

Cu privire la semnătura electronică extinsă, s-a considerat că, *„în cazul contestării înregistrărilor, expertizarea s-ar putea face numai asupra unor fișiere certificate cu semnătură electronică extinsă*"[4]. Nu putem fi de acord cu această opinie, întrucât lipsa unei semnături electronice nu influențează posibilitatea stabilirii autenticității înregistrării printr-o expertiză criminalistică care va determina dacă există modificări asupra fișierului, putând identifica inclusiv momentul la care s-a realizat înregistrarea contestată (dacă a fost simultan cu evenimentul înregistrat). Totodată, chiar și în lipsa semnăturii electronice, în momentul punerii în executare a supravegherii tehnice pot fi generate coduri hash de verificare pentru fiecare fișier în parte, tehnologia respectivă fiind preluată și în cadrul tehnologiei certificatelor digitale, oferind garanții privind integritatea datelor informatice[5].

După sesizarea instanței, potrivit art. 143 alin. (2) teza finală C.pr.pen., copia suportului care conține activitățile de supraveghere tehnică și copii de pe procesele-verbale se păstrează la grefa instanței, în locuri speciale, în plic sigilat, la dispoziția exclusivă a judecătorului sau completului învestit cu soluționarea cauzei. Această dispoziție este inclusă de legiuitor pentru ca suportul de stocare să nu fie expus unor manipulări excesive dacă ar fi cusut la dosarul cauzei ca orice act, în cazul unui suport optic, dar și pentru că, în situația în care suportul ar fi de un alt tip – hard-disk –, volumul acestuia ar putea genera riscuri suplimentare în avarierea sa, dacă s-ar încerca atașarea lui fizică la dosar. De altfel, cuvântul „atașare" folosit de legiuitor în cuprinsul art. 143 alin. (2) C.pr.pen. nu trebuie să fie înțeles ca o atașare fizică de procesul-verbal, ci o simplă anexare a suportului de stocare.

În ceea ce privește accesul părților și procurorului la copia suportului de stocare, aceasta nu va fi permisă în mod direct, în acest sens fiind interpretată dispoziția privind accesul exclusiv al judecătorului sau al completului învestit cu soluționarea cauzei. Pentru că părțile au dreptul să consulte întreg dosarul, inclusiv copia suportului de stocare, în practică se vor putea solicita copii ale copiei suportului de stocare, conforme cu acesta, ce vor fi remise părților din dispoziția instanței sau a judecătorului de cameră preliminară. Întrucât nu este obligatoriu ca

[1] *Gh. Mateuț*, Procedură penală, 2019, p. 697.

[2] Pentru explicații suplimentare privind modalitatea de semnare și considerații tehnice, a se vedea Titlul III, Capitolul V.

[3] *S. Grădinaru*, Supravegherea tehnică, 2014, p. 137.

[4] *C.M. Chiriță*, în N. Volonciu, A.S. Uzlău (coord.), Noul Cod, 2014, p. 325.

[5] *M.V. Tudoran*, Teoria și practica interceptărilor, 2012, p. 203.

suportul de stocare să fie un suport optic, ci un mediu de stocare care permite rescrierea (stick USB, hard-disk), este necesar ca părților să le fie restricționată consultarea nemijlocită a copiei suportului de stocare, pentru a se limita riscul ștergerii ori modificării datelor informatice. Aceasta nu o considerăm o limitare a dreptului la apărare, întrucât organele judiciare au dreptul să reglementeze modul concret în care se va exercita dreptul de a consulta dosarul.

Fiindcă, așa cum rezultă din art. 143 alin. (2^1) C.pr.pen., suportul de stocare va conține date informatice, o copiere a copiei suportului de stocare va prezenta aceleași caracteristici cu suportul inițial, în măsura în care copierea se realizează prin metode tehnice care să mențină autenticitatea și integritatea datelor informatice.

Copiile proceselor-verbale întocmite în temeiul art. 143 C.pr.pen. se vor transmite împreună cu copia suportului de stocare, pentru a facilita identificarea conținutului fiecărui suport de stocare prin raportare la activitățile de supraveghere consemnate.

Capitolul VI
Informarea persoanei supravegheate

Secțiunea 1. Dreptul persoanei supravegheate de a fi informată cu privire la măsură

Constituind o ingerință adusă vieții private, autorizarea supravegherii tehnice presupune un control strict asupra legalității autorizării sale de către o autoritate independentă sub controlul și supravegherea căreia se va pune în aplicare măsura. Caracterul secret al metodelor speciale reprezintă însăși natura lor, fiind unul dintre elementele de distincție față de procedeele probatorii clasice, alături de caracterul invaziv al lor, prin raportarea la drepturile fundamentale ale persoanei. În toate situațiile în care există o restrângere a drepturilor fundamentale ale unei persoane, ea trebuie să se realizeze conform legii, atât în lumina art. 8 par. 2 Conv.EDO, cât și a art. 53 alin. (1) din Constituție, astfel că nu se poate dispune decât în situația în care măsura este prevăzută de lege[1]. Respectarea legii și a principiilor statului de drept nu doar că este obligatorie, dar presupune ca restrângerea drepturilor să se facă în asemenea mod în care să fie proporțională cu scopul urmărit și să fie la intensitatea minimă necesară pentru a se îndeplini acest scop, trebuind să fie preferate măsuri mai puțin invazive. Întrucât caracterul secret al supravegherii tehnice nu permite, la momentul autorizării, ca persoana față de care se ia măsura să participe la procedura de autorizare pentru a se putea apăra și a putea invoca nelegalitatea unei eventuale autorizări a unei astfel de măsuri, se impune ca acest drept să îi fie acordat după realizarea supravegherii tehnice. Or, ține de caracterul efectiv al exercitării acestui drept ca persoana să fie încunoștințată de această posibilitate, fapt care impune ca ea să fie informată despre măsurile de supraveghere tehnică la care a fost supusă și să îi fie prezentate toate rezultatele activităților de supraveghere tehnică.

Legiuitorul român și-a respectat obligațiile numai pe jumătate, împrejurare constatată de către Curtea Constituțională[2], în sensul în care componenta de informare a persoanei supravegheate este numai o condiție pentru exercitarea efectivă a dreptului de a contesta *a posteriori* legalitatea măsurilor de supraveghere luate împotriva sa și de a obține anularea acestora. Textul art. 145 C.pr.pen. este criticabil sub acest aspect, deoarece reglementează o procedură formală care, după cum vom vedea în secțiunea următoare, poate fi considerată opțională pentru procuror, corect stabilindu-se în doctrină că „dreptul" persoanei de a fi informată este corelat cu „obligația" procurorului de a o informa, cu mențiunea că procurorul are și el „dreptul" de a amâna informarea[3]. Astfel, s-a arătat că, în reglementarea curentă, informarea persoanei supravegheate constituie un drept iluzoriu, nefiind vorba despre un drept concret și efectiv al persoanei în condițiile în care legea permite procurorului să amâne, pe considerente de oportunitate, informarea persoanei supravegheate, până la terminarea cauzei în urmărire penală[4]. Un drept presupune ca o persoană să beneficieze și de posibilitatea exercitării sale

[1] CEDO, cauza *Klass ș.a. c. Germania*, Hotărârea din 6 septembrie 1978, §43, pe *hudoc.echr.coe.int*
[2] CCR, Dec. nr. 244 din 6 aprilie 2017 (M. Of. nr. 529 din 6 iulie 2017).
[3] *Gh. Mateuț*, Procedură penală, 2019, p. 702.
[4] *Ibidem*.

efective, inclusiv sub aspectul obținerii unei protecții judiciare a acestuia, corelativ, o obligație nu poate fi concepută decât dacă efectiv leagă persoana obligată de îndeplinirea ei.

Ceea ce lipsește procedurii prevăzute de art. 145 C.pr.pen., considerat neconstituțional sub acest aspect, este componenta de contestare a legalității procedurii de autorizare și de punere în executare a supravegherii tehnice, orice ingerință adusă vieții private trebuind să fie protejată prin procedee judiciare care să ofere persoanei supravegheate posibilitatea reală de a contesta măsurile luate. În mod evident, sancționarea nelegalității privind autorizarea și punerea în executare a metodelor speciale de supraveghere tehnică poate avea consecințe de mai multe naturi – civile[1], penale, disciplinare –, ce se vor răsfrânge asupra persoanelor care au autorizat, respectiv pus în executare măsura. În mod evident, în cazul unei supravegheri tehnice realizate în mod nelegal, persoana ale cărei drepturi au fost restrânse are dreptul să obțină și dezdăunarea sa pe cale civilă[2], însă această situație nu poate avea influență asupra dreptului principal al persoanei, cel de a contesta legalitatea măsurii, care trebuie socotit a fi un drept separat[3].

O componentă deosebit de importantă a posibilității contestării legalității supravegherii tehnice va fi și posibilitatea persoanei de a obține, prin această procedură, distrugerea probelor rezultate[4], un drept limitat în dreptul procesual penal, întrucât nici în situația în care persoana care contestă măsura are calitate procesuală – de inculpat în faza camerei preliminare, tot nu va putea obține decât excluderea probei ca urmare a constatării nulității administrării probei, în condițiile art. 102 alin. (3) C.pr.pen.[5]. Acest aspect este cu atât mai nefiresc, întrucât, comparând cu situația procedurii de confirmare a autorizării provizorii emise de procuror în temeiul art. 141 C.pr.pen., legiuitorul a instituit obligația distrugerii probelor obținute ca urmare a nerespectării dispozițiilor legale pentru autorizare, textul actual neoferind persoanei posibilitatea de a obține, pe lângă declararea nelegală a supravegherii tehnice, și distrugerea rezultatelor acesteia.

Din punctul de vedere al protecției drepturilor fundamentale ale unei persoane, în stabilirea existenței unui drept de a fi informat asupra luării unor măsuri de supraveghere tehnică, Curtea Europeană a Drepturilor Omului s-a pronunțat în mod repetat asupra acestei obligații, corelativ cu dreptul de a putea contesta legalitatea unor asemenea măsuri.

Într-o cauză pilot în domeniu, Curtea a constatat, mai înainte de toate, că se impune ca măsura de supraveghere tehnică să fie prevăzută de lege[6] și că va constitui un drept al persoanei cel de a fi notificat despre măsura luată față de aceasta, deschizându-i-se calea pentru a formula acțiuni judiciare, prin care să conteste în fața unei instanțe legalitatea autorizării măsurii de supraveghere și dacă măsurile efectiv puse în executare s-au desfășurat conform legii[7].

Într-o altă cauză, Curtea a constatat că dreptul de a fi notificat cu privire la desfășurarea unei supravegheri tehnice față de o persoană este în mod indisolubil legat de dreptul la un recurs judiciar efectiv împotriva măsurii, în cazul în care s-ar considera ca fiind una abuzivă[8].

---

[1] *D. Ciuncan*, Supravegherea tehnică (I), în Revista Universul Juridic nr. 1/2015, p. 12.

[2] CEDO, cauza *Bălteanu c. România*, Hotărârea din 16 iulie 2013, §45, pe *hudoc.echr.coe.int*

[3] CEDO, cauza *Pruteanu c. România*, Hotărârea din 3 mai 2015, §55, pe *hudoc.echr.coe.int*

[4] CEDO, cauza *Sommer c. Germania,* Hotărârea din 27 iulie 2017, pe *hudoc.echr.coe.int*

[5] *S. Boțic*, Regula exclusiunii. Excluderea probelor obținute nelegal în procesul penal, Ed. Universul Juridic, București, 2016, p. 118.

[6] CEDO, cauza *Klass ș.a. c. Germania*, Hotărârea din 6 septembrie 1978, §43.

[7] *Ibidem*, §71.

[8] CEDO, cauza *Roman Zakharov c. Rusia*, Hotărârea din 4 decembrie 2015, §234, pe *hudoc.echr.coe.int*

Nu s-ar concepe posibilitatea de contestare în lipsa unei notificări cu privire la măsura de supraveghere nici dacă persoana nu ar avea dreptul de a contesta *a posteriori* măsura.

Mergând mai departe, jurisprudența Curții a recunoscut necesitatea reglementării în dreptul intern a unui recurs efectiv *a posteriori* cu privire la măsurile de supraveghere tehnică, reamintind constatările din cauza *Roman Zakharov c. Rusia* privind condiționarea posibilității de a exercita un recurs efectiv de informare a persoanei supravegheate[1]. Acest recurs efectiv nu trebuie să fie unul în sensul obținerii unor daune, ci trebuie să privească legalitatea măsurii și să deschidă posibilitatea concretă ca persoana supravegheată să obțină anularea măsurilor luate împotriva sa[2].

Nu se poate susține că nu s-ar impune un recurs efectiv cu privire la legalitatea măsurii, motivând că persoana care a dispus autorizarea măsurii ar avea calitatea de magistrat, această calitate neafectând regularitatea actului care este atacat, astfel că respingerea unei cereri pe temeiul acesta constituie o încălcare a art. 8 Conv.EDO. Această concluzie este deosebit de importantă, deoarece subliniază necesitatea ca orice control *a posteriori* să privească toate elementele care au stat la baza autorizării măsurii[3]. În dreptul procesual penal român, ar însemna un control asupra tuturor condițiilor prevăzute de art. 139 C.pr.pen.: competență, existența urmăririi penale începute în cauză, existența unei suspiciuni rezonabile, proporționalitatea măsurii, subsidiaritatea măsurii și autorizarea supravegherii tehnice într-o cauză care privește una dintre infracțiunile prevăzute de art. 139 alin. (2) C.pr.pen.

În cauza *Pruteanu c. România*, Curtea a analizat și caracterul efectiv al recursului judiciar, prin perspectiva solicitărilor reclamantului ca statul să dispună distrugerea rezultatelor supravegherii tehnice care îl priveau pe acesta[4]. Astfel, s-a mers mai departe decât în cauzele precedente, fără a se rezuma numai la nulitatea măsurilor de supraveghere tehnică. Totodată, prin raportare și la problemele incidente în cauză, Curtea a reținut că reclamantul avusese calitatea de avocat în cauză, însă această calitate de fost reprezentant legal nu îi permitea să exercite un drept procesual propriu și să intervină în cauză pentru a cere constatarea nulității supravegherii tehnice[5]. S-a mai reținut și faptul că la dosarul cauzei au fost depuse efectiv convorbiri purtate de acesta, apreciate ca fiind relevante de către organele de urmărire penală[6].

Deși cauza se referea la situația legislativă de sub imperiul Codului de procedură penală anterior, nici în prezent legiuitorul nu a reglementat o procedură de control *a posteriori*, care să ofere unei persoane posibilitatea exercitării unui recurs efectiv față de măsurile de supraveghere tehnică luate împotriva sa.

În ceea ce privește jurisprudența națională, Curtea Constituțională și-a exprimat punctul de vedere asupra problemei printr-o decizie din anul 2017, care, până în prezent, nu a condus la o modificare legislativă care să pună în acord legislația procesuală penală cu decizia Curții. Prin Decizia nr. 244 din 26 aprilie 2017, Curtea Constituțională a constatat că dispozițiile art. 145 C.pr.pen. sunt neconstituționale, întrucât nu permit contestarea legalității măsurii de supraveghere tehnică de către persoana vizată de aceasta, dacă nu are calitatea de inculpat. Chiar dacă o analiză în detaliu a acestei decizii o vom face într-o secțiune ulterioară[7], trebuie

[1] CEDO, cauza *Irfan Güzel c. Turcia*, Hotărârea din 7 mai 2017, §98, pe *hudoc.echr.coe.int*

[2] CEDO, cauza *Xavier Da Silveira c. Franța*, Hotărârea din 21 aprilie 2010, §48, pe *hudoc.echr.coe.int*

[3] CEDO, cauza *Matheron c. Franța*, Hotărârea din 29 iunie 2005, §40, pe *hudoc.echr.coe.int*

[4] CEDO, cauza *Pruteanu c. România*, Hotărârea din 3 mai 2015, pe *ier.gov.ro*

[5] *Ibidem*, §53.

[6] *Ibidem*, §52.

[7] *V. infra*, Titlul III, Capitolul VI.3.

subliniat că și jurisprudența Curții Constituționale este în sensul celor arătate de noi în secțiunea aceasta, respectiv că informarea persoanei supravegheate reprezintă doar o condiție pentru exercitarea dreptului la contestarea legalității supravegherii tehnice, acesta fiind dreptul care trebuie consacrat de legiuitor, și nu doar o informare formală care este opțională pentru procuror.

În concluzie, apreciem că legislația procesuală penală este deficitară în cazul dreptului persoanei de a putea contesta *a posteriori* legalitatea supravegherii tehnice dispuse față de aceasta, indiferent de calitatea sa procesuală, neputând obține o satisfacere a intereselor sale prin distrugerea rezultatelor activităților de supraveghere. În acest context, prevederea dreptului la informarea persoanei supravegheate – și acela efemer – nu poate reprezenta decât o încălcare a obligației pozitive a statului român de a reglementa o protejare efectivă împotriva abuzurilor dreptului la viață privată al persoanei.

Secțiunea a 2-a. Procedura informării persoanei supravegheate

Dreptul persoanei care a fost supusă supravegherii tehnice se corelează cu o obligație care incumbă procurorului de a o informa asupra măsurilor de supraveghere tehnică autorizate și puse în executare față de aceasta. Potrivit art. 145 alin. (1) C.pr.pen., procurorul este obligat să informeze în scris fiecare subiect al unui mandat de supraveghere tehnică despre măsura de supraveghere tehnică ce a fost luată împotriva sa.

Codul de procedură penală nu stabilește mai multe detalii despre conținutul informării pe care trebuie să o realizeze procurorul, menționând doar că aceasta trebuie să fie realizată în scris. Apreciem că, față de formularea folosită de legiuitor, cea de informare, se impune ca aceasta să conțină indicarea mandatului judecătorului de drepturi și libertăți prin care s-a luat măsura de supraveghere tehnică, indicarea măsurilor de supraveghere tehnică încuviințate și măsurile de supraveghere tehnică care au fost puse în executare față de persoană (uneori, mandatul de supraveghere tehnică nu se va executa în mod complet). Totodată, se impune ca informarea să conțină și mențiunea privind dreptul persoanei supravegheate de a lua la cunoștință, potrivit art. 145 alin. (2) C.pr.pen., de activitățile concrete de supraveghere tehnică desfășurate și de a avea acces nemijlocit la rezultatul acestora.

Termenul în care procurorul trebuie să emită informarea către persoana supravegheată este de cel mult 10 zile, care va curge de la încetarea măsurii de supraveghere tehnică luate cu privire la respectiva persoană. Acest termen a fost apreciat ca fiind un termen de recomandare[1], depășirea acestuia putând conduce numai la eventuale sancțiuni de natură civilă, ca urmare a introducerii unei acțiuni civile delictuale de drept comun[2]. În doctrină s-a evidențiat problema emiterii de mandate de supraveghere tehnică multiple, ca urmare a schimbării cartelelor SIM de către persoana supravegheată, apreciindu-se că, și în cazul în care vor exista mai multe mandate, se impune ca informarea să se realizeze pentru fiecare mandat în parte, chiar dacă toate privesc aceeași persoană, situație în care s-ar impune amânarea comunicării[3]. Nu considerăm a fi întemeiată această opinie, întrucât textul legal are în vedere încetarea măsurii de supraveghere tehnică dispuse față de o persoană, chiar dacă autorizarea vizează numai un

[1] *S. Grădinaru*, Supravegherea tehnică, 2014, p. 130.

[2] *M.V. Tudoran*, Considerații referitoare la nerespectarea dispozițiilor legale privind autorizarea interceptării și înregistrării de sunete și imagini, în Dreptul nr. 12/2010, p. 238.

[3] *V. Trif*, op. cit., p. 195.

anumit telefon mobil al acesteia, sens în care se va impune informarea acesteia în mod unitar la încetarea măsurii de supraveghere tehnică, iar nu la încetarea valabilității fiecărui mandat. În acest sens, dispozițiile art. 145 alin. (1) C.pr.pen. se referă la încetarea măsurii, și nu la expirarea mandatului de supraveghere tehnică.

Deoarece dreptul la informare este în legătură cu fiecare măsură de supraveghere tehnică, apreciem că pentru fiecare măsură va trebui să fie emisă câte o informare, cu excepția situației în care mai multe măsuri sunt dispuse prin același mandat. Ceea ce trebuie subliniat este că, la momentul la care realizează informarea, procurorul trebuie să fi finalizat deja consemnarea activităților rezultate din supravegherea tehnică, conform art. 143 alin. (1) și alin. (4) C.pr.pen., în caz contrar neputând pune la dispoziția persoanei care a făcut obiectul supravegherii tehnice rezultatele acesteia, conform art. 145 alin. (2) C.pr.pen.

Astfel cum am arătat și în secțiunea precedentă, dreptul persoanei de a fi informată, coroborat cu obligația procurorului de informare, are un caracter efemer, putând fi restrâns prin voința absolută a procurorului, față de care nu se poate exercita niciun control judiciar. Acest lucru se datorează posibilității procurorului de a dispune amânarea informării persoanei supravegheate, în conformitate cu dispozițiile art. 145 alin. (4) C.pr.pen. Potrivit acestor dispoziții legale, procurorul poate să amâne motivat efectuarea informării, dacă aceasta ar putea conduce la: *i)* perturbarea sau periclitarea bunei desfășurări a urmăririi penale în cauză; *ii)* punerea în pericol a siguranței victimei, a martorilor sau a membrilor familiilor acestora; *iii)* dificultăți în supravegherea tehnică asupra altor persoane implicate în cauză. În esență, legiuitorul a instituit procurorului oportunitatea de a alege oricare dintre aceste pretexte pentru a-și motiva amânarea informării persoanei care a fost supusă măsurilor de supraveghere tehnică. Din lecturarea dispozițiilor legale ale art. 145 alin. (4) C.pr.pen, s-ar putea considera că persoana care a fost supusă supravegherii tehnice ar prezenta un pericol, însă, după formularea art. 145 alin. (1) C.pr.pen., nu este necesar ca persoana care are dreptul de a fi informată să aibă vreo calitate procesuală ori să fie bănuită de săvârșirea vreunei infracțiuni. Mai mult, persoana care poate fi supusă supravegherii tehnice poate fi chiar persoana vătămată, la cererea acesteia, în condițiile art. 140 alin. (9) C.pr.pen. Nu credem că vreunul dintre cele trei temeiuri poate fi susținut ca fiind pertinent, pentru motivele pe care le vom expune mai jos.

Perturbarea sau periclitarea bunei desfășurări a urmăririi penale este privită de legiuitor ca un motiv generic care poate fi întrebuințat de procuror atunci când acesta socotește că ar fi oportun. Acest temei este instituit pentru ca procurorul să nu poată fi obligat să prezinte rezultatele activităților de supraveghere tehnică, sperând ca, prin această măsură, să asigure buna desfășurare a urmăririi penale. Modul în care este formulat acest temei legal ne amintește de art. 202 C.pr.pen. referitor la scopul și condițiile generale de aplicare a măsurilor preventive, ceea ce face ca amânarea informării să nu reprezinte o soluție eficientă în cazul în care ar exista un pericol pentru buna desfășurare a urmăririi penale. Dimpotrivă, prin menționarea acestui temei la informarea persoanei supravegheate, legiuitorul a instituit un pretext pentru ca procurorul să poată limita buna exercitare a dreptului la apărare al persoanelor care au calitate procesuală în cauză.

Punerea în pericol a siguranței victimei, a martorilor sau a membrilor familiilor acestora pare a fi un motiv serios pentru ca procurorul să ia măsuri concrete și eficiente pentru a împiedica persoana supravegheată să comită fapte de natură penală împotriva acestor persoane. Pentru acest motiv, nu înțelegem de ce, în această situație, procurorul nu ar putea propune luarea unei măsuri preventive față de persoana care a făcut obiectul supravegherii sau luarea unor măsuri

de protecție a persoanei vătămate sau a martorilor prevăzute de Codul de procedură penală. Motivul expus prin art. 145 alin. (4) lit. b) C.pr. pen. este unul artificial, deoarece metodele de supraveghere tehnică nu creează un pericol pentru persoanele amintite în cuprinsul acestuia, cel puțin nu unul mai mare decât ar putea fi generat prin consultarea dosarului de urmărire de către persoana supravegheată, caz în care ar putea afla toate declarațiile persoanei vătămate și a martorilor din cauză, plus adresa la care locuiesc, element care nu va fi conținut de procesul-verbal de consemnare a activităților de supraveghere tehnică.

Prin „dificultăți în supravegherea tehnică asupra altor persoane implicate în cauză", legiuitorul a introdus un temei generic la dispoziția procurorului, pentru a putea amâna informarea persoanei supravegheate, pe motiv că s-ar crea dificultăți în administrarea supravegherii tehnice în cauză. În esență, se consideră că dacă una dintre persoanele față de care a încetat supravegherea tehnică ar fi încunoștințată de faptul că a fost supusă unei asemenea măsuri, atunci aceasta ar putea informa și alte persoane față de care ar exista încă măsuri de supraveghere tehnică în executare. Dintre toate cele trei motive, acesta este singurul care ar putea fi de înțeles în contextul supravegherii tehnice, dar și cel care ar permite o limitare a obligației procurorului în a amâna informarea persoanei supravegheate. Întrucât metodele speciale de supraveghere sau cercetare au un caracter secret și eficacitatea lor depinde de acesta, toate persoanele care pun în executare măsurile sau își dau concursul sunt obligate să păstreze secretul operațiunii. De aceea, ar trebui să poată fi amânată informarea unor persoane care au făcut obiectul supravegherii tehnice în considerarea relațiilor pe care le au cu persoanele care încă sunt sub puterea unui mandat de supraveghere tehnică. Ceea ce trebuie subliniat este că acest temei va fi justificat numai până la momentul la care se va încheia supravegherea tehnică în cauză, neputându-se amâna informarea până la terminarea urmăririi penale sau până la clasarea cauzei, ci doar până la expirarea mandatelor de supraveghere tehnică dispuse față de alte persoane din cauză.

Amânarea informării persoanei supravegheate se va face prin ordonanță motivată, în care se vor arăta în mod concret care sunt motivele ce justifică amânarea, nefiind în spiritul legii motivarea acesteia doar prin reproducerea fidelă a unuia dintre cele trei cazuri prevăzute de legiuitor[1]. Asupra termenului până la care se poate dispune amânarea informării, legiuitorul a instituit o limită, prin art. 145 alin. (5) C.pr.pen., respectiv până cel târziu la terminarea urmăririi penale sau până la clasarea cauzei. Acest termen maximal nu va putea fi exploatat de procuror în defavoarea persoanei, fiind necesar ca ea să-și poată exercita efectiv dreptul de a consulta rezultatele activităților de supraveghere tehnică. Observăm că legiuitorul nu face nicio referire la situația în care se va dispune disjungerea cauzei, caz în care putem asista la o amânare *sine die* a efectuării informării persoanei supravegheate.

S-a exprimat și o propunere în literatura de specialitate prin care, în cazul în care se va proceda la amânarea informării persoanei supravegheate, acesteia să îi fie oferită posibilitatea consultării rezultatelor de supraveghere tehnică – procesele-verbale de consemnare a activităților de supraveghere tehnică și suporților de stocare aferenți înainte de finalizarea cauzei prin rechizitoriu[2]. O atare posibilitate exista sub imperiul Codului de procedură penală anterior și era denumită „prezentarea materialului de urmărire penală", procedură obligatorie și care preceda finalizarea urmăririi penale, permițând învinuitului sau inculpatului să consulte în întregime dosarul de urmărire penală și să propună probe în apărarea sa, mai înainte de a se

[1] *Ibidem*, p. 196.
[2] *Ibidem*, p. 197.

decide asupra emiterii rechizitoriului. Din nefericire, legiuitorul a considerat că este de preferat ca celeritatea terminării urmăririi penale să aibă prioritate față de respectarea dreptului la apărare al persoanei acuzate și astfel procedura a fost înlăturată din legislația actuală.

O omisiune flagrantă a legiuitorului este că nu se reglementează distinct situația informării persoanei în cazul în care s-ar decide trimiterea sa în judecată, caz în care nu trebuie confundat actul realizat de judecătorul de cameră preliminară – citarea și comunicarea unei copii certificate a rechizitoriului – cu cel realizat de procuror – informarea persoanei supravegheate. Întrucât nu se face nicio distincție, procurorul va fi ținut să informeze persoana supravegheată și dacă aceasta va avea calitatea de inculpat și s-a dispus trimiterea sa în judecată. Ceea ce va fi problematic este că, potrivit art. 145 alin. (2) C.pr.pen., se va impune ca persoana informată să poată consulta procesele-verbale în care sunt consemnate activitățile de supraveghere tehnică efectuate, însă, odată cu sesizarea instanței, acestea vor fi depuse la grefa instanței, conform art. 143 alin. (2) C.pr.pen. Într-o situație similară vor fi și celelalte persoane care au fost supuse măsurilor de supraveghere tehnică și informate după sesizarea instanței.

Odată informată cu privire la faptul că a fost supusă măsurilor de supraveghere tehnică, persoana vizată poate formula o cerere procurorului prin care poate cere, în conformitate cu art. 145 alin. (3) C.pr.pen., consultarea rezultatelor de supraveghere tehnică. Acest drept este limitat în timp, cererea putând fi formulată numai în termen de 20 de zile de la informare. În replică la solicitarea persoanei supuse măsurii de supraveghere tehnică, procurorul poate dispune amânarea prezentării suporților de stocare și a proceselor-verbale de consemnare a activităților de supraveghere tehnică, în aceleași condiții ca în cazul amânării informării persoanei care a făcut obiectul supravegherii tehnice. În doctrină s-a arătat că termenul de 20 de zile pentru formularea cererii este unul de decădere, astfel că, dacă cererea va fi formulată peste termen, procurorul o va respinge ca tardivă[1]. Nu putem decât să constatăm că reglementarea art. 145 C.pr.pen. a fost gândită doar în favoarea procurorului, nu și a persoanei ale cărei drepturi fundamentale au fost restrânse prin supravegherea tehnică, limitarea dreptului de a consulta rezultatele supravegherii tehnice fiind un abuz din partea legiuitorului.

Dacă va reuși să fie informată și mai apoi să i se încuviințeze cererea, persoana care a fost supusă măsurilor de supraveghere tehnică va putea lua cunoștință de conținutul proceselor-verbale în care sunt consemnate activitățile de supraveghere tehnică efectuate. Persoana supravegheată are și dreptul de a obține ascultarea convorbirilor, comunicărilor sau conversațiilor ori vizionarea imaginilor rezultate din activitatea de supraveghere tehnică. Nu se menționează nimic cu privire la datele informatice care pot rezulta din metoda specială a accesului la un sistem informatic. Totodată, legiuitorul nu a menționat nici posibilitatea ca persoana să poată obține copii ale suporților de stocare sau ale proceselor-verbale pentru ca, pe baza acestora, să își poată exercita drepturile, inclusiv să poată contesta legalitatea supravegherii tehnice.

Deși art. 145 alin. (2) C.pr.pen. nu prevede, nu se vor prezenta în integralitate rezultatele supravegherii tehnice, ci numai acelea care au fost selectate și consemnate în conformitate cu dispozițiile art. 143 alin. (1) C.pr.pen. Credem că se impune a se acorda un acces complet la toate activitățile de supraveghere tehnică, inclusiv cele care au fost arhivate potrivit art. 142 alin. (6) C.pr.pen. În plus, va exista și o limitare a dreptului de consultare, în sensul în care va trebui să îi fie prezentate persoanei numai activitățile de supraveghere tehnică ce au privit-o pe aceasta, dreptul prevăzut de art. 145 C.pr.pen. nefiind un drept de consultare a întreg dosarului

[1] *Ibidem*, p. 196.

sau a întregii supravegheri tehnice din cauză. Afirmăm acest lucru, deoarece persoana care va fi informată de supravegherea tehnică poate să nu aibă nicio calitate procesuală, astfel că nu se justifică accesul acesteia decât la propriile activități care au fost supuse supravegherii.

Secțiunea a 3-a. Contestarea legalității supravegherii tehnice în urma Deciziei Curții Constituționale nr. 244/2017 privind neconstituționalitatea dispozițiilor art. 145 C.pr.pen.

Reflectând asupra problemelor expuse mai sus, simpla informare a persoanei supravegheate nu constituie o garanție suficientă pentru respectarea dreptului la viață privată al persoanei, în condițiile în care acesteia nu îi este deschisă calea către contestarea legalității măsurii luate împotriva sa[1]. Este necesară și oferirea unei posibilități reale de a contesta legalitatea supravegherii printr-o procedură care să fie accesibilă nu doar persoanelor care au calitatea procesuală în respectiva cauză penală. În acest sens, art. 8 Conv.EDO privind dreptul la viață privată este legat de art. 13 Conv.EDO privind dreptul la un remediu efectiv. Ca urmare a omisiunii legiuitorului de a reglementa dreptul de contestare a măsurilor de supraveghere tehnică, a fost ridicată o excepție de neconstituționalitate a dispozițiilor art. 145 C.pr.pen. privind informarea persoanei supravegheate, întrucât acestea nu prevăd posibilitatea ca o persoană supusă măsurilor de supraveghere tehnică să aibă posibilitatea de a le contesta decât dacă ar deține calitatea procesuală de inculpat în cauză și numai în anumite proceduri judiciare.

Soluționarea problemei de drept deduse judecății Curții Constituționale s-a realizat prin Decizia nr. 244 din 6 aprilie 2017. În dispozitivul Deciziei Curții s-a constatat că soluția legislativă cuprinsă în dispozițiile art. 145 C.pr.pen., care nu permite contestarea legalității măsurii supravegherii tehnice de către persoana vizată de aceasta, care nu are calitatea de inculpat, este neconstituțională.

Astfel cum se arată și în cuprinsul deciziei, Curtea recunoaște că: „*prin însăși dispunerea măsurilor de supraveghere tehnică, persoana supravegheată suferă o ingerință în sfera dreptului său la viață privată, Curtea urmează să analizeze în ce măsură inexistența unui control a posteriori al legalității dispunerii măsurii supravegherii tehnice respectă condițiile prevăzute de Constituție și Convenție referitoare la restrângerea exercițiului dreptului de acces la o instanță, în scopul protejării dreptului unei persoanei la viață privată*"[2]. Această concluzie concordă cu poziția generală adoptată de noi prin prezenta lucrare, rezultând și din interpretarea întregii jurisprudențe a art. 8 Conv.EDO, care recunoaște universal caracterul de ingerință gravă a supravegherii tehnice față de viața privată a unei persoane.

În cursul analizei sale, Curtea Constituțională a observat că dispunerea întrebuințării unei metode speciale de supraveghere nu este condiționată de vreo calitate procesuală în cauză, putând fi dispusă și față de persoane care au calitatea de suspect sau inculpat[3]. În căutarea posibilității existenței unui recurs efectiv, Curtea a procedat la analizarea tuturor procedurilor judiciare în care se poate contesta legalitatea actelor efectuate în cursul urmăririi penale, inclusiv administrarea probelor.

[1] ICCJ, s. pen., încheierea nr. 287 din 6 aprilie 2016.
[2] CCR, Dec. nr. 244 din 6 aprilie 2017, §52 (M. Of. nr. 529 din 6 iulie 2017).
[3] *Ibidem*, §35.

Curtea a mai constatat faptul că, în cursul procedurii de cameră preliminară, formularea de cereri și excepții este rezervată numai inculpatului, celorlalte părți și persoanei vătămate, fără a fi incluse și persoanele care nu au această calitate procesuală[1]. Aceasta înseamnă că legalitatea supravegherii tehnice poate fi analizată numai prin prisma criticilor aduse de persoanele îndreptățite să formuleze cereri și excepții în procedura camerei preliminare. În mod similar, tot în atribuțiile judecătorului de cameră preliminară intră și soluționarea plângerilor împotriva soluțiilor de neurmărire și de netrimitere în judecată, sens în care Curtea a constatat că se pot invoca cereri și excepții cu privire la actele de procedură penală efectuate în cursul urmăririi penale, dar numai în măsura în care este pusă în mișcare acțiunea penală[2]. Dimpotrivă, în cadrul procedurii renunțării la urmărirea penală, nu se poate admite ca persoanele chemate în fața judecătorului de cameră preliminară să formuleze cereri și excepții cu privire la legalitatea măsurilor de supraveghere tehnică dispuse în cauză[3].

În privința recunoașterii dreptului persoanei de a-i fi respectate drepturile fundamentale, se impune ca aceasta să poată contesta legalitatea respectivului act, Curtea reținând că: „*în jurisprudența sa, a statuat cu valoare de principiu că, ori de câte ori se aduce o atingere unui interes legitim al unei persoane, această persoană trebuie să aibă posibilitatea să se poată adresa instanței cu o acțiune în care să pună în discuție încălcarea astfel suferită și să obțină, dacă este cazul, reparația corespunzătoare, chiar dacă, în unele cazuri, acțiunea exercitată îmbracă forma unei căi de atac împotriva unei hotărâri judecătorești*"[4].

Referindu-se direct la implicațiile cauzei *Pruteanu c. România*, Curtea mai reține că nu este suficientă calitatea de magistrat pe care o are persoana care autorizează măsura de supraveghere tehnică: „*pentru a fi necesară într-o societate democratică, ingerința în dreptul la viață privată al unei persoane trebuie să se bucure de garanții adecvate și eficiente împotriva abuzurilor, concretizate în proceduri destinate controlului adoptării și aplicării măsurii restrictive cu scopul de a limita ingerința care rezultă din legislația incriminată la ceea ce este necesar într-o societate democratică*"[5].

Recunoscând necesitatea unui control *a posteriori* asupra legalității măsurilor de supraveghere tehnică, Curtea a apreciat că acest control trebuie să vizeze toate aspectele care țin de autorizarea și de punerea în executare a acestora și că „*trebuie să se refere la analiza legalității măsurii supravegherii tehnice, indiferent dacă această verificare se realizează în cadrul procesului penal sau independent de acesta*"[6]. Din punctul nostru de vedere, în mod independent semnifică un control din partea unei instanțe penale care va fi sesizată direct de persoana supravegheată. Va rămâne la latitudinea legiuitorului cui îi va stabili competența să judece, în opinia noastră, aceasta trebuind să revină judecătorului de cameră preliminară.

Ținând seama că soluția Curții Constituționale de a găsi art. 145 C.pr.pen. neconstituțional nu contribuie la o mai bună protecție a drepturilor fundamentale ale persoanei, s-a impus ca, în considerentele deciziei, Curtea să instituie obligația legiuitorului de a lua măsuri în vederea legiferării unei proceduri de contestare a legalității măsurilor de supraveghere tehnică de către orice persoană, apreciind că sunt încălcate atât art. 8, cât și art. 13 Conv.EDO[7].

[1] *Ibidem*, §38.
[2] *Ibidem*, §40.
[3] *Ibidem*, §44.
[4] *Ibidem*, §56.
[5] *Ibidem*, §60, implicit și la cauza *Matheron c. Franța*.
[6] *Ibidem*, §63.
[7] *Ibidem*, §68.

În considerarea jurisprudenței Curții Europene a Drepturilor Omului, în cauza *Pruteanu c. România*, Curtea Constituțională a reținut că nu este suficientă posibilitatea contestării de către o persoană a măsurilor de supraveghere tehnică, ci, în urma pronunțării unei decizii în sensul constatării nelegalității acesteia, să se poată dispune distrugerea datelor interceptate prin punerea în executare[1]. Deși Curtea vorbește de datele interceptate, în realitate se impune distrugerea datelor rezultate din activitățile de supraveghere tehnică, fără a se ține cont de măsura concretă care a fost dispusă în cauză. Sub acest aspect, arătăm că măsura distrugerii nu poate fi luată chiar și dacă persoana ar formula o excepție de nelegalitate a supravegherii tehnice în procedura camerei preliminare în care acesta are calitatea de inculpat. Sub acest aspect, problemele ridicate de Decizia Curții au o întindere mai largă decât dispozițiile art. 145 C.pr.pen., deschizând posibilitatea discutării despre distrugerea fizică a unor mijloace de probă care, prin însăși existența lor, constituie o ingerință adusă vieții private, întrucât vor fi oricând expuse pericolului unei accesări neautorizate[2].

Până la acest moment, deși au trecut deja mai mulți ani de la Decizia Curții Constituționale, legiuitorul nu și-a îndeplinit obligațiile care îi reveneau ca urmare a pronunțării Deciziei nr. 244/2017. Cu toate că se consideră în mod corect că deciziile Curții Constituționale pronunțate în controlul *a posteriori* al constituționalității legilor nu instituie o obligație *per se* pentru legiuitor, această decizie constată de fapt o neîndeplinire a unor obligații pozitive ale legiuitorului care reies din art. 8 par. 2 Conv.EDO, sens în care se poate considera că statul român nu a luat nicio măsură pentru respectarea dreptului la viață privată al persoanei, prin oferirea unui remediu efectiv față de orice ingerință ce se aduce acestui drept.

În lipsa unei reglementări concrete, apreciem că s-ar impune recunoașterea judiciară a dreptului de a contesta măsurile de supraveghere tehnică în fața judecătorului de cameră preliminară, prin sesizarea directă de către persoana supravegheată, într-o procedură care ar trebui să fie guvernată de aceleași reguli precum cele ale camerei preliminare. Distincția ar trebui să o constituie posibilitatea obținerii de către persoană a distrugerii rezultatului activităților de supraveghere tehnică odată cu constatarea nulității acesteia. Menționăm că, în viziunea Curții Constituționale, numai o persoană care a făcut obiectul direct al supravegherii tehnice, prin emiterea mandatului de supraveghere tehnică față de aceasta, sau persoana care a dobândit calitate procesuală în cauză ulterior va putea contesta măsura, în contextul legislativ actual[3]. În practică au existat situații în care s-a încercat contestarea măsurilor de supraveghere tehnică în fața judecătorului de cameră preliminară, soluția fiind respingerea ca urmare a lipsei informării persoanei cu privire la supravegherea tehnică, apreciindu-se că numai după acest moment s-ar naște dreptul de a contesta măsura[4]. Această poziție o socotim vădit greșită, întrucât dreptul de contestare a legalității supravegherii tehnice se naște din momentul intruziunii în viața privată, informarea persoanei supravegheate fiind doar o garanție a exercitării efective a acestui drept.

Unul dintre neajunsurile actuale ale legii, pe care îl anticipăm în relație cu posibilitatea efectivă a persoanei supravegheate de a contesta legalitatea supravegherii tehnice desfășurate împotriva sa, constituie lipsa de acces la actele prin care s-a propus, dispus și pus în executare măsura de supraveghere. Astfel, chiar dacă legea îi recunoaște persoanei care a făcut obiectul unui mandat de supraveghere tehnică dreptul de a fi informată asupra măsurii și de a putea

[1] *Ibidem*, §71.

[2] CEDO, cauza *Craxi c. Italia (nr. 2)*, Hotărârea din 17 iulie 2003, §75 și §83, pe *hudoc.echr.coe.int*

[3] CCR, Dec. nr. 55 din 22 ianuarie 2019 (M. Of. nr. 417 din 28 mai 2019).

[4] Trib. Argeș, s. pen., încheierea nr. 117 din 22 martie 2018, pe *www.rolii.ro*

consulta procesele-verbale de consemnare a activităților de supraveghere tehnică și a suporților de stocare aferenți acestor activități, nu i se va permite accesul la actele procedurale în funcție de care se poate stabili legalitatea măsurii. Situația este una paradoxală, întrucât, prin Decizia Curții, se constată că se impune ca persoana supusă măsurii să poată contesta legalitatea ei, dar nu se amintește de necesitatea accesului la actele pe care le va contesta, fiind puțin probabil că o contestare a legalității să aibă vreun succes dacă se bazează numai pe aspectele ce țin de consemnarea activităților de supraveghere tehnică, și nu de legalitatea autorizării și punerii în executare. Cu toate acestea, Curtea amintește că posibilitatea contestării legalității include și îndeplinirea condițiilor prevăzute de lege pentru luarea măsurii, precum și a modalităților de punere în executare a mandatului de supraveghere tehnică, astfel că ar rezulta, prin interpretare, că și aceste acte trebuie puse la dispoziția persoanei informate cu privire la măsura luată împotriva sa[1].

De lege ferenda, apreciem că, pe lângă posibilitatea persoanei supravegheate de a contesta legalitatea măsurilor de supraveghere tehnică luate față de aceasta, se impune ca procurorul, în procedura informării, să îi permită accesul cel puțin la următoarele acte: propunerea de autorizare a măsurilor de supraveghere tehnică, încheierea judecătorului de drepturi și libertăți de încuviințare a măsurilor de supraveghere tehnică, mandatul de supraveghere tehnică, ordonanța procurorului de delegare a punerii în executare, procesul-verbal de consemnare a activităților de supraveghere tehnică și procesul-verbal de redare integrală a convorbirilor comunicațiilor și conversațiilor, precum și toți suporții de stocare privitori la activitățile de supraveghere tehnică realizate față de respectiva persoană.

În concluzie, procedura informării persoanei supravegheate constituie o reglementare incompletă, care nu își poate regăsi menirea, din punctul de vedere al Constituției și al Convenției, decât prin reglementarea de către legiuitor a unei proceduri distincte de contestare a legalității autorizării și punerii în executare a măsurilor de supraveghere tehnică. Această procedură trebuie să fie accesibilă oricărei persoane care a fost supusă unei măsuri de supraveghere tehnică, indiferent dacă are sau a avut o calitate procesuală în cauza penală în care s-a realizat supravegherea. Pentru a i se asigura dreptul la un recurs efectiv, este necesar ca procurorul să îi pună la dispoziție toate actele procedurale care au stat la baza autorizării și punerii în executare a măsurilor de supraveghere tehnică, pentru a-i permite să formuleze critici împotriva acestora și să obțină, într-un final, ulterior constatării nulității, distrugerea rezultatelor activităților de supraveghere tehnică.

[1] CCR, Dec. nr. 244 din 6 aprilie 2017, §63 (M. Of. nr. 529 din 6 iulie 2017).

Capitolul VII
Înregistrările care pot fi făcute fără autorizare

Alături de metodele speciale de supraveghere tehnică supuse autorizării judecătorului de drepturi și libertăți, legiuitorul a recunoscut posibilitatea utilizării în procesul penal și a înregistrărilor private, realizate în special de părți, în vederea protejării propriilor interese. Astfel de înregistrări sunt supuse unui regim mai puțin restrictiv, întrucât sunt prezentate voluntar de către o parte sau sunt realizate de către alte persoane în cadrul unor activități care nu privesc activități judiciare în respectiva cauză.

Sediul materiei pentru înregistrările private realizate fără autorizație este art. 139 alin. (3) C.pr.pen., în care se prevede că: „*înregistrările prevăzute în prezentul capitol, efectuate de părți sau de alte persoane, constituie mijloace de probă când privesc propriile convorbiri sau comunicări pe care le-au purtat cu terții. Orice alte înregistrări pot constitui mijloace de probă dacă nu sunt interzise de lege*".

Ca o delimitare a scopului textului legal arătat mai sus, trebuie să precizăm că nu orice metodă specială de supraveghere tehnică va putea fi folosită de un privat în vederea obținerii unor probe în procesul penal, ci numai *înregistrările*, astfel că va fi incidentă numai măsura de supraveghere tehnică prevăzută de art. 138 alin. (1) lit. c) C.pr.pen. Nu se vor încadra în prevederile legale interceptările comunicațiilor unei persoane, întrucât fapta ar constitui infracțiunea de violarea secretului corespondenței, prevăzută de art. 302 alin. (2) C.pen. Pe măsură ce tehnologia evoluează și devine accesibilă, există un pericol real ca un particular să realizeze interceptări[1]. Totodată, nu va fi justificat accesul la un sistem informatic realizat de o parte asupra unui sistem informatic, deoarece aceasta ar constitui infracțiunea de acces ilegal la un sistem informatic, prevăzută de art. 360 C.pen. În plus, nu putea va fi utilizată nici măsura specială a localizării sau urmăririi prin mijloace tehnice, întrucât aceasta ar constitui infracțiunea de hărțuire, prevăzută de art. 208 alin. (1) C.pen. Practic, un privat nu va putea niciodată să interfereze cu acele acte de administrare a probelor care pot fi realizate numai de către un organ de urmărire penală, tehnicile speciale de investigare fiind cele mai reprezentative pentru această regulă[2].

În doctrină s-a apreciat că vor intra în categoria înregistrărilor și e-mailurile sau înregistrările de imagini care surprind comunicări ale celui care a făcut înregistrarea[3]. Nu suntem de aceeași opinie, întrucât termenul „înregistrări" nu se referă la astfel de mijloace de comunicare, înregistrări trebuind să fie de sunet sau de imagine. Un e-mail reprezintă date informatice care pot fi puse la dispoziția organelor de urmărire penală în orice condiții, nu doar dacă prezintă comunicații proprii. Sub acest aspect, este relevant că, doar pentru obținerea unui e-mail stocat pe un sistem informatic, legea nu impune autorizarea accesului la un sistem informatic sau interceptarea comunicațiilor electronice ale unei persoane, putând fi folosit

[1] *K.R. Thompson*, Cell Phone Snooping: Why Electronic Eavesdropping Goes Unpunished, în The American Criminal Law Review, vol. 35, no. 1, fall 1997, pp. 139-140.

[2] *E. Grande*, Dances of Criminal Justice: Thoughts on Systemic Differences and the Search for the Truth, în J. Jackson, M. Langer, P. Tillers, Crime, Procedure and Evidence in a Comparative and International Context, Ed. Hart Publishing, Portland, Oregon, 2008, p. 161.

[3] *M. Bulancea, R. Slăvoiu*, în M. Udroiu (coord.), Codul de procedură penală, 2017, p. 667.

procedeul probatoriu al predării obiectelor, înscrisurilor sau a datelor informatice, care poate fi preferat ținând seama de condiția subsidiarității supravegherii tehnice[1]. Autorii citați anterior consideră că vor fi considerate înregistrări în sensul art. 139 alin. (3) C.pr.pen. și înregistrările de imagini care surprind comunicări, referindu-se, cel mai probabil, la capturile de ecran ale comunicărilor purtate de persoane prin dispozitive mobile sau chiar prin capturi de ecran ale comunicărilor de pe sisteme informatice. O captură de ecran sau *screenshot* nu va proba decât că pe ecranul dispozitivului există o comunicare, fiind o fotografie a ecranului realizată prin intermediul sistemului informatic (PC sau dispozitiv mobil), fără a fi diferită de o fotografie propriu-zisă a ecranului. Nu considerăm că va intra în sfera înregistrărilor realizate de părți sau de alte persoane o atare ipoteză, ea putând fi lesne un fals, care nu poate fi autentificat fără o expertiză informatică sau, cel puțin, prin prezentarea dispozitivului către organul de urmărire penală.

Legiuitorul a făcut o distincție între două situații care pot apărea în cazul înregistrărilor făcute fără autorizare: *înregistrările propriilor convorbiri sau comunicări* efectuate de părți sau de alte persoane ce *vor* constitui mijloace de probă și *orice alte înregistrări care nu sunt interzise de lege* care *pot* constitui mijloace de probă.

S-a arătat în literatura de specialitate că, deși nu sunt supuse autorizării, înregistrările realizate de părți sau de alte persoane nu pot fi exceptate de la un control de admisibilitate, sens în care legiuitorul le-a limitat doar la propriile convorbiri sau comunicări pe care le-au purtat cu terții[2]. Se impune a se face și o mențiune privind diferența gramaticală dintre înregistrările propriilor convorbiri și comunicări și orice alte înregistrări care nu sunt interzise de lege. În cazul înregistrării propriilor convorbiri și comunicări, legiuitorul a considerat că ele **constituie mijloace de probă**, nefiind supuse oricăror altor condiții de admisibilitate, neputând fi apreciate ca fiind ilegale în vreo situație. Ele vor putea fi administrate ca probă chiar dacă s-au realizat înainte de începerea urmăririi penale[3]. În schimb, în cazul *oricăror altor înregistrări*, ele *pot constitui mijloace de probă*, trebuind să fie supuse unor condiții de admisibilitate. S-a apreciat că, pentru a fi admisibile, acestea nu trebuie să fie interzise de lege, criteriu constituind un mijloc insuficient de protejare a dreptului la viață privată al persoanelor, în măsura în care nu se prevăd dispoziții legale care să interzică anumite tipuri de înregistrări[4].

Înregistrările realizate de părți sau de alte persoane privind propriile convorbiri nu prezintă probleme deosebite, rezultând din definiție că legiuitorul nu a condiționat ca înregistrarea să se realizeze de o persoană care să aibă vreo calitate procesuală în cauză[5]. Ceea ce s-a condiționat este ca înregistrările să privească propriile convorbiri sau comunicații, fiind de neconceput ca o persoană să realizeze o înregistrare a unei convorbiri la care nu a participat, respectiv înregistrarea unor terți, situație care cade sub incidența art. 226 C.pen.[6]. Nu este necesar ca persoana să participe efectiv la comunicare, fiind suficient ca prezența acesteia să fie la locul

[1] Simpla obținere a datelor informatice nu va presupune și posibilitatea organelor de urmărire penală de a le folosi în procesul penal, întrucât vizualizarea oricăror date conținut va constitui o ingerință în viața privată a unei persoane, fiind necesară o procedură în fața judecătorului de drepturi și libertăți pentru a se autoriza folosirea lor. *V. infra*, Titlul V, Capitolul IV.1.

[2] *Gh. Mateuț*, Procedură penală, 2019, p. 698.

[3] C. Ap. Iași, s. pen., încheierea din 5 septembrie 2016, publicată în C. Moisă, op. cit., pp. 113-115.

[4] *Gh. Mateuț*, Procedură penală, 2019, p. 698.

[5] *A. Barbu, G. Tudor, A.M. Șinc*, Codul de procedură penală adnotat cu jurisprudență națională și europeană, Ed. Hamangiu, București, 2016, p. 365.

[6] CCR, Dec. nr. 756 din 13 decembrie 2016 (M. Of. nr. 293 din 25 aprilie 2017).

realizării comunicării și ca persoana care realizează comunicarea să fie vizibilă interlocutorilor. Nu va constitui o înregistrare legală cea desfășurată de către o persoană ascunsă într-un dulap asupra discuțiilor purtate de persoanele dintr-o încăpere. Totodată, nelegală va fi și înregistrarea realizată de o persoană într-un bar sau restaurant privind discuțiile purtate la mese învecinate, în măsura în care presupune folosirea unor mijloace tehnice disimulate în masa la care se află interlocutorii.

Alte înregistrări pot constitui mijloace de probă dacă nu sunt interzise de lege, sens în care legiuitorul a prevăzut că înregistrările incidentale pot fi folosite în procesul penal dacă nu sunt interzise expres. O atare situație nu poate fi considerată decât ca fiind incomplet reglementată, prezentând riscul unor abuzuri în lipsa unor criterii legale cu privire la admisibilitatea unor astfel de probe. Propunem că unul dintre aceste criterii va trebui să fie caracterul incidental al înregistrării, neputând fi admisă înregistrarea intenționată a unei persoane în scopul obținerii de probe cu privire la săvârșirea unei infracțiuni determinate. Aceasta nu va însemna că nu vor putea fi realizate înregistrări în scop preventiv, sens în care trebuie să subliniem că acestea *pot* surprinde săvârșirea unei infracțiuni. O altă condiție care ar trebui să fie prevăzută este ca înregistrările să poată fi făcute numai prin mijloace tehnice ușor observabile de persoanele care intră în spațiile supravegheate, în acest sens fiind importantă respectarea caracterului de date cu caracter personal al înregistrărilor. Cu alte cuvinte, pentru ca „o altă înregistrare" să fie permisă, este necesar ca orice persoană să cunoască faptul că este înregistrată sau să poată prevedea în mod facil acest lucru, în cazul înregistrărilor prevăzute de art. 139 alin. (3) teza finală C.pr.pen. De pildă, un telefon mobil nu va îndeplini această condiție, dar o cameră de supraveghere montată pe un zid sau pe tavan o va putea îndeplini, mai ales dacă prezența ei este semnalizată prin afișe. Numai în cazul înregistrărilor realizate de părți sau de către alte persoane cu privire la propriile convorbiri sau comunicări cu terții, vor putea fi acceptate înregistrările realizate cu mijloace tehnice ascunse sau disimulate.

În legătură cu categoria altor înregistrări, s-a apreciat în mod corect că vor trebui avute în vedere în vedere dispozițiile cuprinse în Legea nr. 190/2018[1] și cele din Regulamentul (UE) nr. 2016/679, conform cărora înregistrările care vor fi realizate constituie date cu caracter personal[2]. În categoria datelor cu caracter personal, vor intra, potrivit art. 4 pct. 1 din Regulamentul (UE) nr. 2016/679, „*orice informații privind o persoană fizică identificată sau identificabilă («persoana vizată»); o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale*".

În categoria *oricăror alte înregistrări*, vor putea intra înregistrările realizate de camerele de supraveghere publice ale primăriilor, ale băncilor, bancomatelor, benzinăriilor ori cele realizate în spații deschise publicului, precum magazinele, restaurantele, barurile etc. sau cele realizate de camere purtate de lucrătorii de poliție[3]. Inclusiv spațiile private vor putea fi supuse unei

[1] Legea nr. 190 din 18 iulie 2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (M. Of. nr. 651 din 26 iulie 2018).

[2] *Gh. Mateuț*, Procedură penală, 2019, p. 698.

[3] *M.K. Wolf*, Anti-Wiretapping Statutes: Disregarding Legislative Purpose and the Constitutional Pitfalls of Using Anti-Wiretapping Statues to Prevent the Recording of On-Duty Police Officers, în Journal of Gender, Race and Justice no. 15/2012, p. 199.

supravegheri și vor conduce la obținerea de înregistrări, putând cădea în această categorie spațiile de birouri ale unei societăți comerciale. Desigur, va trebui să existe o limitare strictă și o justificare pentru respectiva înregistrare, fiind de neconceput înregistrarea angajaților în spații precum băile sau spațiile de odihnă și recreere[1]. Înregistrările nu se vor putea face și prin captarea sunetelor, o astfel de măsură fiind disproporționată față de scopul legitim urmărit[2].

S-a susținut în mod corect, prin raportare la jurisprudența Curții Europene a Drepturilor Omului, că înregistrările se vor putea realiza numai de persoane care nu vor fi „agenți ai statului" când aceștia înregistrează propriile convorbiri sub controlul statului sau cu asistență din partea organelor judiciare[3]. Autorilor amintiți li se raliază și jurisprudența recentă a Curții Constituționale, care a constatat că: „*dispozițiile art. 139 alin. (3) teza finală din Codul de procedură penală sunt constituționale în măsura în care nu privesc înregistrările rezultate ca urmare a efectuării activităților specifice culegerii de informații care presupun restrângerea exercițiului unor drepturi sau libertăți fundamentale ale omului desfășurate cu respectarea prevederilor legale, autorizate potrivit Legii nr. 51/1991*"[4]. În motivarea soluției sale, Curtea Constituțională reține că înregistrările efectuate în baza Legii nr. 51/1991 au o finalitate diferită față de cele prevăzute de Codul de procedură penală, acestea constând în „*cunoașterea, prevenirea și înlăturarea amenințărilor interne și externe cu scopul realizării securității naționale*"[5]. În plus, se ajunge și la situația neobișnuită ca o instanță inferioară, în cadrul controlului de legalitate desfășurat în procedura camerei preliminare, să verifice o hotărâre a Înaltei Curți de Casație și Justiție prin care s-au autorizat înregistrările conform legislației speciale. Strict sub aspectul caracterului neconstituțional al articolului de lege criticat, Curtea Constituțională apreciază că impedimentul real este dat de lipsa reglementării unui cadru clar, coerent și previzibil, prin care mijloacele de probă obținute potrivit Legii nr. 51/1991 să poată fi contestate, ceea ce echivalează cu lipsa de eficiență a posibilității de a le contesta[6]. În consecință, nu vor avea calitatea de mijloace de probă toate aceste procedee prevăzute de legea specială, până la momentul la care se va asigura posibilitatea contestării acesteia sub toate aspectele, inclusiv prin analizarea propunerii formulate de Procurorul General și a încheierii pronunțate de Președintele Înaltei Curți de casație și Justiție. În opinia noastră, Curtea Constituțională a deschis calea către eliminarea serviciilor de informații din domeniul judiciar, fiind puțin probabil ca legiuitorul să creeze un mecanism eficient de control judiciar al activităților desfășurate în baza unui mandat emis sub Legea nr. 51/1991.

În jurisprudența Curții Europene a Drepturilor Omului s-a constatat că o interferență din partea autorităților, și dacă se rezumă la furnizarea echipamentului de înregistrare a unor convorbiri telefonice, va constitui o încălcare a art. 8 Conv.EDO și în situația în care persoana care realizează înregistrarea este parte în cauză și o face voluntar, neputând fi eludate prin aceasta dispozițiile legale privind autorizarea măsurii de supraveghere tehnică[7]. În același sens,

[1] În acest sens, vor fi aplicabile dispozițiile art. 5 din Legea nr. 190/2018, care stabilesc condițiile utilizării unor sisteme de monitorizare în contextul relațiilor de muncă.

[2] *D.L. O'Mara*, How much covert is too much?, în Security, vol. 71, no. 12/2000, p. 35.

[3] *M. Bulancea, R. Slăvoiu*, în M. Udroiu (coord.), Codul de procedură penală, 2017, p. 666; *P. Ungureanu*, Aspects of human rights infringement by abusive use of technical surveillance measures, în Buletin Științific al Academiei Forțelor Terestre „Nicolae Bălcescu", Sibiu, vol. XX, nr. 1/2015, p. 112.

[4] CCR, Dec. nr. 55 din 4 februarie 2020 (M. Of. nr. 517 din 17 iunie 2020).

[5] *Ibidem*, §52.

[6] *Ibidem*, §61.

[7] CEDO, cauza *Van Vondel c. Olanda*, Hotărârea din 25 ianuarie 2008, §49, pe *hudoc.echr.coe.int*

s-a reținut că a sugera unei persoane să realizeze o înregistrare, dacă este făcută de organele de poliție sau de procuror, poate constitui o încălcare a art. 8 Conv.EDO dacă este asociată cu furnizarea unor mijloace de înregistrare, nefiind fondate susținerile statului, conform căruia persoana care a realizat înregistrarea putea acționa în același mod și singură[1].

În jurisprudența engleză, o situație aparte a fost expusă într-o cauză privind traficul ilicit de substanțe, atunci când un vecin a folosit o cameră pentru a-și supraveghea vecina în urma unor conflicte, îndreptând o cameră de supraveghere către proprietatea ei, cu posibilitatea de a se vedea în locuință. Pe fondul conflictelor, vecinul a prezentat poliției casete video din care rezulta că aceasta realiza trafic de droguri, organizându-se o percheziție domiciliară și descoperindu-se heroină, cocaină și crack. Curtea de Apel a Angliei și Țării Galilor a respins apelul inculpatei, apreciind că simpla folosire a materialului video înregistrat de un particular nu constituie o nelegalitate, întrucât acesta nu a fost încurajat sau ajutat în vreun mod de poliție. În plus, s-a reținut că mijlocul tehnic de supraveghere era unul ostentativ și că inculpata l-a observat și a recunoscut că știa că vecinul acesteia putea filma în casa ei, aspect care, în mod distinct, ar putea atrage consecințe civile, nu și excluderea probei[2]. Nu putem fi de acord cu o asemenea soluție, mai ales că instanța de apel a considerat că s-a respectat proporționalitatea măsurii în sensul art. 8 par. 2 Conv.EDO, prin aceea că scopul realizării înregistrărilor ar fi fost unul legitim – prevenirea săvârșirii unei infracțiuni – și că situația poate fi asemănată cu cea a unui trecător care privește printr-un geam și observă săvârșirea unei infracțiuni. Dimpotrivă, credem că nu se poate admite niciodată o supraveghere video a unei persoane cu caracter continuu și intenționat realizată de un privat. Mai mult, credem că instanța a procedat în mod greșit la un examen de proporționalitate atunci când a analizat această condiție prin raportare la probele obținute, și nu la interesul și scopul privat pentru care s-au realizat inițial înregistrările. Decizia Curții a fost criticată și de doctrina engleză, în special prin raportare la lipsa aplicării art. 8 Conv.EDO, o greșită considerare a tipului de înregistrare realizat (în spații private) și o eronată interpretare a colaborării dintre privat și organele de poliție, colaborare care s-a desfășurat pe parcursul mai multor luni, constituind în realitate complicitatea lor în efectuarea supravegherii inculpatei[3].

În literatura de specialitate s-a considerat că înregistrările realizate de persoane cu privire la propriile convorbiri sau comunicări trebuie supuse următoarelor condiții de admisibilitate: *i)* înregistrările trebuie să fie efectuate de părți (inculpat, parte civilă, parte responsabilă civilmente) sau de alte persoane (suspectul, persoana vătămată, martorii); *ii)* înregistrările trebuie să privească propriile convorbiri sau comunicări pe care cel care a făcut înregistrarea le-a purtat cu terții; *iii)* înregistrarea trebuie să aibă relevanță probatorie[4]. Credem că aceste condiții propuse nu pot fi considerate ca stabilind vreun criteriu de admisibilitate, ci constituie numai aprecieri asupra însăși definiției înregistrărilor realizate de părți, neavând valoarea unor criterii pe baza cărora să se poate încuviința administrarea probei.

În ceea ce ne privește, apreciem că legea procesuală penală instituie condiții de admisibilitate mult prea largi pentru ambele categorii de înregistrări, nefiind justificată exceptarea acestora de la condiția proporționalității, care trebuie să existe în cazul oricărei restrângeri a dreptului la viață privată al unei persoane, chiar dacă aceasta se realizează de un particular. Întrucât

[1] CEDO, cauza *M.M. c. Olanda*, Hotărârea din 24 septembrie 2003, §41, pe *hudoc.echr.coe.int*

[2] EWCA, cauza *Rosenberg c. R.*, Dec. din 20 ianuarie 2006, [2006] EWCA Crim 6, pe *www.bailii.org*

[3] *S. McKay*, Covert Policing, 2015, p. 360.

[4] *M. Bulancea, R. Slăvoiu*, în M. Udroiu (coord.), Codul de procedură penală, 2017, p. 667.

orice înregistrare, chiar și una privată, constituie o restrângere a dreptului la viață privată, chiar și atunci când înregistrarea se face în spații publice, admisibilitatea probei va trebui să fie condiționată de respectarea art. 8 par. 2 Conv.EDO. Chiar dacă Convenția ar părea că se aplică numai în relația dintre stat și persoanele private, în jurisprudența sa, Curtea a arătat că respectarea Convenției impune ca statul să adopte măsuri pentru respectarea drepturilor fundamentale. Sub acest aspect, există o obligație pozitivă a statelor de a prevedea condiții legale, clare și previzibile în sfera relațiilor particularilor cu privire la restrângerea dreptului la viață privată[1]. Comisia de la Veneția subliniază că orice supraveghere realizată de un privat în spații publice sau private va fi supusă condițiilor art. 8 par. 2 Conv.EDO, trebuind să existe o justificare în acest sens pentru ca supravegherea să fie considerată legitimă întocmai ca o înregistrare realizată de autoritățile publice[2].

În recomandările sale, Comisia de la Veneția evidențiază necesitatea proporționalității în materia supravegherii private, fiind justificate totodată interesele particularilor de a-și asigura siguranța proprietății private, a propriilor persoane sau pentru a se preveni săvârșirea de infracțiuni împotriva acestora. Se subliniază și că supravegherea – corelativ, și realizarea de înregistrări – trebuie să fie făcută într-un mod care permite persoanei supravegheate să sesizeze prezența unui mijloc tehnic de înregistrare ori să i se aducă la cunoștință existența acestuia. În cazul unei supravegheri secrete, aceasta se poate realiza de privați numai temporar și în măsura în care nu există alte măsuri mai puțin invazive (principiul subsidiarității). Codul de procedură penală este deficitar sub acest aspect, întrucât nu face nicio diferență între tipul de înregistrări care pot fi făcute de particulari, dacă acestea pot avea o durată limitată în timp, dacă spațiul trebuie să fie unul public sau privat, gravitatea infracțiunii care se poate dovedi etc.

Reflectând asupra unor eventuale condiții de admisibilitate care pot fi instituite de legiuitor, se impun a fi avute în vedere condițiile legale cuprinse de art. 139 alin. (1) C.pr.pen., care vor putea fi aplicabile numai în parte, astfel că apreciem că admisibilitatea probelor obținute de înregistrări private se va putea face dacă sunt îndeplinite următoarele condiții: *legalitatea înregistrării* și *proporționalitatea dintre interesul legitim urmărit de persoana care realizează înregistrarea și restrângerea dreptului la viață privată al persoanei înregistrate*.

Legalitatea înregistrării constituie o condiție generală care provine din imperativul stabilit de art. 1 alin. (3) și (5) din Constituție, dar și de art. 2 C.pr.pen. Ceea ce vrem să subliniem este că o înregistrare realizată de o persoană privată nu trebuie să aibă loc în condiții care sunt în mod expres interzise de lege sau care ar constitui o infracțiune. De pildă, nu vor putea fi acceptate probele care ar rezulta din înregistrările realizate în mod automatizat și ascuns în spațiile private ale unei persoane, prin instalarea unor dispozitive. În plus, tot în contextul legalității, vor trebui analizate condițiile prevăzute de art. 139 alin. (3) C.pr.pen. și dacă înregistrarea s-a făcut cu sprijinul sau la îndemnul unor autorități de stat, caz în care proba obținută va fi nelegală.

Proporționalitatea măsurii constituie corectivul necesar pentru a se asigura că înregistrările private vor putea fi folosite în procesul penal. Prin examenul de proporționalitate se impune ca persoana care realizează înregistrarea să fi urmărit un interes legitim prin efectuarea acesteia

[1] CEDO, cauza *Marckx c. Belgia*, Hotărârea din 13 iunie 1979, §31; cauza *Botta c. Italia*, Hotărârea din 24 februarie 1998, §33; cauza *Craxi c. Italia (nr. 2)*, Hotărârea din 17 iulie 2003, §73-76, pe *hudoc.echr.coe.int*

[2] Comisia de la Veneția, Opinie asupra supravegherii video realizate de operatori privați în public și în sfera privată și de autorități publice în sfera privată și protejarea drepturilor omului, adoptată în a 71-a Sesiune Plenară a Comisiei de la Veneția, 1-2 iunie 2007.

proporțional cu ingerința adusă dreptului la viață privată al persoanei supravegheate. Nu va constitui un interes legitim provocarea săvârșirii unei infracțiuni, fiind incidente aceleași reguli ca în cazul în care autoritățile ar fi cele care ar comite provocarea[1]. Va constitui un interes legitim supravegherea propriei locuințe prin dispozitive video pentru prevenirea și sancționarea oricăror infracțiuni care s-ar putea îndrepta împotriva patrimoniului persoanei. Pentru ca măsura să fie proporțională, se impune și ca interesul legitim urmărit să aibă o importanță care să justifice ingerința în viața privată a persoanei înregistrate. Prevenirea săvârșirii unei infracțiuni poate fi considerată un interes legitim suficient de important, însă trebuie să avem în vedere că, în examinarea proporționalității, suntem ținuți de prevederi similare celor pentru încuviințarea supravegherii tehnice. Este necesar ca gravitatea infracțiunii care se urmărește a fi dovedită să justifice nivelul de ingerință adus vieții private a unei persoane. De exemplu, nu va putea fi considerată proporțională urmărirea și înregistrarea video a tuturor mișcărilor în spații publice ale unei persoane pe o perioadă îndelungată de timp, chiar dacă s-ar justifica prin scopul arătat anterior. Într-o asemenea situație, persoana care realizează înregistrarea acționează cu rea-credință, în ipoteza existenței unei suspiciuni privind săvârșirea unei infracțiuni trebuind să sesizeze organele de urmărire penală.

Prin controlul de proporționalitate va trebui să se verifice dacă persoana care realizează înregistrările nu își asumă competențe de organ de urmărire penală și încearcă să realizeze o anchetă proprie prin înregistrările realizate. O situație care ridică probleme de proporționalitate a fost expusă în jurisprudența engleză, în care o angajată a suferit o vătămare la locul de muncă, necesitând îngrijiri și o perioadă de concediu medical, însă angajatorul ei a bănuit că își exagerează simptomele, angajând detectivi care au vizitat-o la domiciliu sub pretextul că realizează un sondaj de piață, descoperind că aceasta era sănătoasă și înregistrând-o în propria locuință[2]. Credem că instanțele naționale vor trebui să privească cu mare circumspecție realizarea unor înregistrări secrete în spații private, chiar dacă persoana care înregistrează este invitată în locuință. Instanța va trebui să acorde mare atenție dacă o atare înregistrare poate fi considerată proporțională și în acord cu art. 8 par. 2 Conv.EDO.

Până la modificarea legislației în privința înregistrărilor care pot fi realizate fără autorizarea judecătorului de drepturi și libertăți, apreciem că toate condițiile expuse mai sus vor putea fi aplicate prin raportare la obligația pozitivă a statului de a apăra dreptul la viață privată al persoanelor, judecătorul de cameră preliminară sancționând nelegalitatea probelor care ar fi obținute în dezacord cu condițiile arătate mai sus.

Referitor la procedeul probatoriu prin care se pot obține probele care rezultă din înregistrările realizate fără autorizare prealabilă, acestea vor fi procedeele probatorii clasice, fiind incident, în special, procedeul predării obiectelor, înscrisurilor sau a datelor informatice prevăzut de art. 170 C.pr.pen. În cazul în care înregistrările sunt realizate de părți, ele, de regulă, vor fi prezentate voluntar de acestea organelor de urmărire penală sub forma unor mijloace materiale de probă – suporți de stocare –, solicitând administrarea probei cu înregistrările respective.

Chiar dacă reprezintă înregistrări care provin dintr-o măsură de supraveghere tehnică realizată de o entitate privată, procurorul va fi obligat să procedeze, conform art. 143 alin. (4) C.pr.pen., la redarea integrală a convorbirilor și conversațiilor conținute de înregistrare,

[1] CEDO, cauza *Shannon c. Marea Britanie*, Hotărârea din 6 aprilie 2004; cauza *Teixeira de Castro c. Portugalia*, Hotărârea din 9 iunie 1998, pe *hudoc.echr.coe.int*

[2] EWCA, cauza *Jones c. University of Warwick*, Dec. din 4 februarie 2003, [2003] EWCA Civ 151, pe *www.bailii.org*

întrucât textul nu distinge asupra provenienței înregistrărilor. În schimb, procesul-verbal nu va fi certificat pentru autenticitate, deoarece înregistrările nu provin dintr-o supraveghere tehnică realizată de către procuror, organele de cercetare penală sau lucrătorii specializați din poliție[1]. Ca urmare a acestui fapt, nu se va încheia nici procesul-verbal de consemnare a activităților de supraveghere tehnică prevăzut de art. 143 alin. (1) C.pr.pen.[2].

[1] C. Ap. București, s. I pen., încheierea din 1 septembrie 2016, definitivă prin încheierea din 14 octombrie 2016 a ICCJ, s. pen., publicată în C. Moisă, op. cit., pp. 140-142.

[2] În sens contrar, C. Ap. Timișoara, s. pen., încheierea nr. 98 din 15 iunie 2016.

Capitolul VIII
Avocatul ca subiect al supravegherii tehnice

Secțiunea 1. Protejarea secretului profesional al avocatului din perspectiva Curții Europene a Drepturilor Omului

Dreptul unei persoane de a obține asistență juridică constituie fundamentul respectării drepturilor omului în contextul unei societăți democratice, prin rolul lor în apărarea justițiabililor. Astfel, interacțiunea dintre client și avocatul său în cadrul unei asistențe juridice cade sub imperiul art. 8 Conv.EDO privind dreptul la viață privată, întrucât astfel de interacțiuni au rolul de a permite persoanei să ia decizii informate asupra vieții sale. Comunicându-se adesea informații cu caracter intim, cu caracter personal sau probleme delicate, persoana care consultă un avocat trebuie să se aștepte ca interacțiunile sale să rămână confidențiale[1]. Secretul profesional a fost considerat ca fiind fundamentul relației și încrederii dintre avocat și clientul său[2].

Secretul profesional al avocatului trebuie să fie analizat din două perspective ce țin de respectarea dreptului la viață privată: *i)* obligația pozitivă a statului de a reglementa în sarcina avocatului obligația păstrării secretului profesional și *ii)* obligația statului de a proteja secretul profesional al avocatului față de ingerința unor terțe persoane, inclusiv a statului.

Prima problemă, cea a reglementării obligației păstrării secretului profesional, nu face obiectul prezentei lucrări, de altfel legislația națională prevăzând obligația păstrării secretului profesional de către avocat, cu includerea unor sancțiuni pentru încălcarea acestei obligații. Obligația păstrării secretului profesional se impune avocaților ca o datorie care decurge din funcția lor de apărare, fiind generală și absolută și însoțită de o garanție de confidențialitate cu privire la tot ceea ce avocatul ia cunoștință de la persoana apărată sau din procesul în care acesta o apără[3].

Cea de-a doua problemă, a protejării secretului profesional al avocatului față de ingerința unor alte persoane, inclusiv a statului, constituie subiectul pe care îl vom aborda, în contextul în care ingerința va fi adusă de stat. Unul dintre elementele esențiale într-o apărare efectivă din partea avocatului este să se permită comunicarea deschisă și neîngrădită dintre acesta și client, cu respectarea principiului confidențialității informațiilor, aceasta constituind o importantă garanție a dreptului la apărare[4].

Prezenta lucrare nu urmărește să stabilească situații în care un particular va lua măsuri care încalcă secretul profesional al avocatului, astfel de ingerințe nefiind permise și, prin modalitatea concretă de desfășurare, pot constitui și infracțiuni.

Supravegherea tehnică este un procedeu probatoriu cu caracter special și derogatoriu, trebuind să fie utilizat în situații în care probele nu pot fi obținute prin orice alt procedeu clasic

[1] CEDO, cauza *Altay c. Turcia (nr. 2)*, Hotărârea din 9 iulie 2019, §49, pe *hudoc.echr.coe.int*

[2] CEDO, cauza *André ș.a. c. Franța*, Hotărârea din 24 iulie 2008, §41, pe *hudoc.echr.coe.int*

[3] *Gh. Mateuț*, Unele considerații privind garantarea secretului profesional al avocatului în lumina noului Cod de procedură penală, publicat în vol. Avocatura în România. 150 de ani în linia întâi a luptei pentru Drept (coord. M. Livescu), Ed. Hamangiu, București, 2015, p. 418.

[4] CEDO, cauza *Apostu c. România*, Hotărârea din 6 iulie 2015, §96, pe *hudoc.echr.coe.int*

și numai cu respectarea proporționalității în restrângerea drepturilor și libertățile fundamentale ale persoanei. Folosirea supravegherii tehnice presupune întotdeauna o intruziune a statului în dreptul la viață privată al persoanei, această restrângere putând afecta și secretul profesional al avocatului. Caracterul tehnic al supravegherii presupune folosirea unor dispozitive apte să sprijine eforturile organelor de urmărire penală, dar permit și o descoperire automatizată, într-o oarecare măsură, a vieții private a unei persoane, care poate include și relația sa cu avocatul său.

Dreptul la păstrarea secretului profesional dintre client și avocat se va aplica atât în cazul unei conversații orale purtate cu apărătorul său, care trebuie să fie liberă și neinhibată de autoritățile statului[1], cât și în cazul corespondenței purtate cu avocatul său. În sensul acesta, în termenul de „corespondență" vor intra atât comunicările scrise transmise avocatului sau primite de la acesta, cât și apelurile telefonice ori orice alt fel de comunicări. Deși dreptul la protejarea secretului profesional este de o importanță deosebită, acesta poate cunoaște unele restrângeri, atunci când există o suspiciune rezonabilă că acest drept este exercitat abuziv sau contrar scopului său legal, putându-se proceda la verificarea corespondenței avocatului[2].

Întrucât prezenta secțiune analizează supravegherea tehnică a interacțiunilor cu avocatul, dar și interacțiunile avocatului, aspectele privind corespondența scrisă vor fi tratate într-o secțiune ulterioară, cu ocazia analizării măsurii speciale de cercetare a reținerii, predării și percheziționării corespondenței[3].

Trebuie avut în vedere că dreptul la viața privată este afectat atât în cazul clientului, cât și în cazul avocatului. Astfel, garanția secretului profesional trebuie să fie conferită amândurora, avocatul putând fi și el afectat de o ingerință adusă prin supravegherea tehnică a comunicărilor sale. Din acest punct de vedere, trebuie să ținem seama că un avocat va avea, de regulă, mai mulți clienți ale căror cauze le va instrumenta, caz în care supravegherea tehnică a avocatului va afecta însăși exercitarea profesiei sale, provocând o intruziune în viața privată a tuturor clienților săi.

Supravegherea tehnică a avocatului ori existența unei posibilități reale de a se realiza acest lucru, precum și inexistența unor garanții cu privire la desfășurarea unei asemenea supravegheri pot conduce implicit la încălcarea art. 6 par. 3 Conv.EDO privind dreptul unei persoane la un proces echitabil. Pentru a nu exista o restrângere a unei exercitări efective a dreptului la apărare, este necesară asigurarea cadrului pentru o comunicare liberă între avocat și client, fără ca acesta din urmă să aibă vreo reticență în a comunica, în urma fricii de a fi ascultat de organele de urmărire penală.

Întrucât există mai multe ipostaze în care se poate ajunge la supravegherea tehnică a unui avocat, vom analiza, din perspectiva jurisprudenței Curții Europene a Drepturilor Omului, cele mai des întâlnite situații, respectiv: *i)* interceptarea comunicațiilor dintre client și avocatul său; *ii)* supravegherea audio sau video a interacțiunilor dintre client și avocat la sediul cabinetului; *iii)* supravegherea audio sau video a interacțiunilor dintre client și avocat la locul de detenție.

[1] CEDO, cauza *Campbell c. Marea Britanie*, Hotărârea din 25 martie 1992, §46, pe *hudoc.echr.coe.int*

[2] *Ibidem*, §48 și §52. În cauză, restrângerea a fost privită din perspectiva deschiderii corespondenței cu avocatul a unei persoane aflate în stare de detenție, Curtea recunoscând statului posibilitatea deschiderii corespondenței atunci când există suspiciuni rezonabile privind un abuz al dreptului care ar pune în pericol siguranța închisorii, a altor persoane sau ar constitui o infracțiune.

[3] *V. infra*, Titlul XI, Capitolul VIII.

§1. Interceptarea comunicațiilor dintre client și avocatul său

După cum s-a stipulat de Curte în cauza *Iordachi ș.a. c. Moldova*, nu este legală interceptarea comunicațiilor unui avocat decât în măsura în care această restrângere este prevăzută de lege, în acest caz special fiind necesar ca în cuprinsul legislației să fie inserate dispoziții procesuale care să garanteze secretul profesional și să limiteze astfel de ingerințe aduse vieții private[1]. Astfel, legea moldoveană nu respecta condițiile art. 8 par. 2 Conv.EDO, întrucât interzicerea interceptării comunicațiilor dintre avocat și clientul său era prevăzută numai în Legea cu privire la avocatură din 13 mai 1999, unde se stipula că *„avocatului i se garantează taina convorbirii cu clientul său și se interzice interceptarea acestora"*[2]. Astfel, în toate cazurile, pentru a fi posibilă interceptarea comunicațiilor unui avocat, trebuie să existe dispoziții procesuale distincte și speciale față de cele comune și să se prevadă modul în care se vor putea folosi, dacă este cazul, probele din aceste interceptări, precum și reglementarea situației în care convorbirea este una accidentală (de exemplu, clientul supus măsurii își sună avocatul). Comunicațiile pot acoperi atât convorbirile telefonice, cât și pe cele prin sisteme informatice, ținând seama că toate datele informatice ce țin de activitatea avocatului sunt protejate, inclusiv metadatele[3].

În contextul supravegherii tehnice prin interceptarea comunicațiilor dintre client și avocatul său, una dintre principalele decizii jurisprudențiale a fost *Kopp c. Elveția*[4], în care domnului Kopp și societății sale de avocatură i-au fost ascultate toate convorbirile telefonice purtate prin liniile profesionale ale societății. În apărarea sa, guvernul elvețian a indicat faptul că interceptările telefonice au fost realizate în virtutea calității personale a domnului Kopp și nu aveau legătură cu activitatea sa de avocat, ci cu faptul că era soțul unui fost membru al Consiliului Federal și că, după ascultare, niciuna dintre înregistrări nu a fost folosită în cauza penală[5].

Un alt aspect interesant care rezultă din decizia *Kopp c. Elveția* este surprinderea Curții cu privire la punerea în executare a supravegherii tehnice de către un funcționar din cadrul Poștei, fără vreo supraveghere sau control din partea vreunui organ independent (de exemplu, un judecător)[6]. Or, un asemenea funcționar nu are competența funcțională de a determina care dintre convorbirile interceptate aparțin sau nu sferei secretului profesional.

Atunci când interceptarea comunicațiilor dintre client și avocat privesc aspecte ce țin de soluționarea propriei sale cauze, nu se va putea proceda la interceptarea și înregistrarea acestora, simplul fapt că s-au realizat aceste acțiuni fiind de natură a constitui o încălcare a art. 8 Conv.EDO și de a știrbi posibilitatea realizării unei apărări efective[7]. O atare măsură nu numai că este o încălcare a secretului profesional, dar constituie o ingerință adusă dreptului la apărare, ca o componentă a dreptului la un proces echitabil, întrucât nu permite o comunicare liberă între acuzat și apărătorul său. Pentru ca o persoană care caută consiliere din partea unui avocat să se destăinuie și să își poată expune problema cât mai liber, este necesar ca aceasta să se simtă liniștită și fără nicio frică de o posibilă interceptare a sa de

[1] CEDO, cauza *Iordachi ș.a. c. Moldova*, Hotărârea din 10 februarie 2009, §50, pe *hudoc.echr.coe.int*

[2] *Ibidem*, §14.

[3] *C.C. Steele*, Attorneys Beware: Metadata's impact on Privilege, Work Product, and the Ethical Rules, în The University of Memphis Law Review, vol. 25, no. 4/2005, p. 938.

[4] CEDO, cauza *Kopp c. Elveția*, Hotărârea din 25 martie 1998, pe *hudoc.echr.coe.int*

[5] *Ibidem*, §71.

[6] *Ibidem*, §74.

[7] CEDO, cauza *Zagaria c. Italia*, Hotărârea din 27 noiembrie 2007, §36, pe *hudoc.echr.coe.int*

către autoritățile statului, indiferent că utilizează o linie telefonică privată sau un sistem de videoconferință oferit de stat[1].

O situație aparte în jurisprudența Curții este posibilitatea folosirii probelor rezultate din interceptarea convorbirilor telefonice inițiate de clientul supus supravegherii tehnice cu avocatul său, din cele discutate de acesta din urmă reieșind săvârșirea de către avocat a unei infracțiuni. Astfel, în cauza *Versini-Campinchi și Crasnianski c. Franța*, Curtea a stabilit că este compatibilă cu Convenția Europeană a Drepturilor Omului folosirea într-un proces penal împotriva avocatului a convorbirii interceptate între acesta și clientul său, din care să rezulte, ca pentru o primă probă, săvârșirea de către avocat a unei infracțiuni de care organele de urmărire penală nu aveau cunoștință[2]. Această constatare a avut ca temei faptul că în legislația franceză există o prevedere expresă potrivit căreia vor putea fi redate convorbirile dintre avocat și client dacă rezultă că avocatul este implicat în săvârșirea unei infracțiuni, chiar dacă acestea nu aveau legătură cu cauza în care s-a dispus supravegherea tehnică[3]. Ceea ce contează într-o asemenea situație este dacă drepturile persoanei interceptate – clientul – au fost respectate, în speța arătată, Curtea constatând că discuțiile dintre acesta și avocatul său nu au fost folosite în cauza sa penală, ci au stat la baza tragerii la răspundere doar a avocatului[4].

În ceea ce privește avocatul și folosirea împotriva sa a înregistrărilor obținute din convorbirea cu clientul său, ca urmare a existenței unui mandat de supraveghere tehnică pe numele clientului, Curtea a reținut că „*această abordare este compatibilă cu jurisprudența amintită mai sus, întrucât se referă la păstrarea privilegiului de avocat-client, care se bazează pe respectarea drepturilor de apărare ale clientului, și care nu exclude transcrierea unei convorbiri între un avocat și clientul său în cadrul interceptării telefonice a celui de-al doilea, atunci când din conținutul acestei convorbiri se poate presupune participarea avocatului său la o infracțiune și în măsura în care această transcriere nu afectează drepturile de apărare ale clientului. Cu alte cuvinte, Curtea acceptă că, așa cum s-a precizat în mod restrictiv, această excepție de la principiul confidențialității schimburilor dintre avocat și clientul său conține în sinea ei o garanție adecvată și suficientă împotriva abuzului*”[5]. Analizând această concluzie a Curții, apreciem că ea pune în valoare necesitatea protejării secretului profesional din perspectiva intereselor clientului avocatului și că nu restrânge posibilitatea organelor de urmărire de a folosi convorbirea cu avocatul pentru tragerea la răspundere penală a acestuia din urmă, în măsura în care legislația permite acest lucru. În opinia noastră, legislația română nu ar putea permite folosirea probelor chiar și obținute incidental din discuțiile clientului cu avocatul său, întrucât probele obținute nu pot fi folosite în niciun proces penal, legea națională neadmițând excepția prevăzută de legislația franceză la care a făcut trimitere Curtea. În acest sens, dacă s-ar folosi împotriva unui avocat convorbirea sa cu propriul client, s-ar încălca art. 8 par. 2 Conv.EDO, întrucât ingerința nu ar fi prevăzută de lege.

În practica judiciară a organelor de urmărire penală române s-a observat practica ilegală de a cita, în calitate de martor, avocatul suspectului și de a-l audia în această calitate, ca urmare a interceptării comunicațiilor dintre acesta și suspect, în cadrul cărora acesta din urmă

[1] CEDO, cauza *Sakhnovskiy c. Rusia*, Hotărârea din 2 noiembrie 2010, §104; cauza *Gorbunov și Gorbachev c. Rusia*, Hotărârea din 1 martie 2016, §37, pe *hudoc.echr.coe.int*

[2] CEDO, cauza *Versini-Campinchi și Crasnianski c. Franța*, Hotărârea din 16 iunie 2016, §77, pe *hudoc.echr.coe.int*

[3] *Ibidem*, §27.

[4] *Ibidem*, §80.

[5] *Ibidem*, §78.

solicita avocatului să preia un nou caz pentru acesta, ținând seama de existența unui raport contractual precedent. În concret, organele de urmărire penală au folosit acest pretext pentru a exclude avocații care realizau apărări efective în cauzele penale, contrar legii, în acest sens pronunțându-se instanțele naționale prin constatarea nelegalității interceptării comunicațiilor dintre suspect și avocat și audierii în calitate de martor a avocatului[1], respectiva încălcare fiind sesizată și de către Curtea Europeană a Drepturilor Omului[2].

În ceea ce privește posibilitatea directă a avocatului de a contesta legalitatea măsurilor de supraveghere tehnică luate împotriva sa atunci când nu are nicio calitate procesuală în cauză, apreciem că sunt incidente explicațiile oferite într-o secțiune precedentă[3] în care am tratat problema și din perspectiva respectării art. 8 Conv.EDO, remarcându-se cauza *Pruteanu c. România*.

În concluzie, interceptarea comunicațiilor dintre avocat și clientul său constituie atât o ingerință adusă vieții private a unei persoane în componenta secretului profesional al avocatului, cât și din perspectiva exercitării unei apărări efective, fiind obligatoriu ca legislația națională să prevadă proceduri speciale care să confere garanții suplimentare împotriva arbitrariului privind această măsură de supraveghere tehnică, în contextul folosirii sale în relație cu un avocat.

§2. Accesul la un sistem informatic asupra avocatului și calitatea de corespondență a datelor informatice în interpretarea Curții Europene a Drepturilor Omului

Întrucât dispozițiile art. 139 alin. (4) C.pr.pen. nu limitează măsurile de supraveghere tehnică ce pot afecta activitatea avocatului prin încălcarea sau restrângerea secretului profesional, apreciem că și un acces la un sistem informatic poate conduce la o asemenea restrângere. În acest sens, trebuie avută în vedere interpretarea extensivă a Curții în privința noțiunii de „corespondență". Deoarece termenul de „corespondență" are un sens larg, în cadrul acesteia s-au inclus anumite componente ale sistemelor informatice ale avocatului, precum hard-diskurile[4] obținute în urma percheziților domiciliare realizate la domiciliul, dar și la sediul profesional al avocatului. În mod evident, în conținutul unui hard-disk nu pot fi regăsite decât date informatice.

Curtea a stabilit că intră în noțiunea extinsă de „corespondență" și sub incidența secretului profesional datele electronice[5], însemnând, în general, fișiere electronice care au fost extrase din sistemul informatic al avocatului, prin copierea lor pe un suport de stocare al organelor de urmărire penală. Într-o altă cauză, Curtea a subliniat faptul că va constitui o încălcare a dreptului la corespondență, ca o componentă a dreptului la viață privată, și o încălcare a secretului profesional al avocatului efectuarea unui percheziții informatice asupra unui sistem informatic deținut de acesta[6].

Din cele arătate mai sus, simpla natură a datelor informatice deținute de avocat este considerată ca fiind suficientă de către Curte pentru ca ele să constituie o corespondență între

[1] C. Ap. Oradea, încheierea pen. nr. 146/CCP din 21 decembrie 2015, nepublicată.

[2] CEDO, cauza *Mateuț c. România*, pe *hudoc.echr.coe.int*

[3] *V. supra*, Titlul III, Capitolul VI.

[4] CEDO, cauza *Petri Sallinen ș.a. c. Finlanda*, Hotărârea din 27 septembrie 2005, §71, pe *hudoc.echr.coe.int*

[5] CEDO, cauza *Wieser și Bicos Beteiligungen GmbH c. Austria*, Hotărârea din 16 octombrie 2007, §66-67, pe *hudoc.echr.coe.int*

[6] CEDO, cauza *Robathin c. Austria*, Hotărârea din 3 iulie 2012, §39, pe *hudoc.echr.coe.int*

acesta și client și să fie protejate de secretul profesional. Din acest punct de vedere, nu contează procedeul probatoriu prin care ele se obțin, fiind importantă numai natura acestora. Ca atare, folosirea metodei speciale a accesului la un sistem informatic nu va fi legală împotriva unui avocat decât dacă există suspiciuni rezonabile că acesta pregătește sau a săvârșit o infracțiune, între aceasta din urmă și respectivele date informatice existând o legătură.

Datele informatice pot fi de orice natură și deținute de orice persoană pentru a fi protejate de secretul profesional, sub acest aspect, ele putând fi simple fișiere sau chiar e-mailuri deținute de o persoană pe un sistem informatic și care țin de relația acesteia cu avocatul său[1]. În cauza citată, Curtea a statuat încălcarea art. 8 Conv.EDO prin aceea că a fost colectat un număr deosebit de mare de date informatice de la societățile percheziționate, în acestea existând și numeroase comunicări realizate cu avocați, precum și o disproporție între scopul urmărit și măsura impusă care a condus la încălcarea secretului profesional. Dacă, în cazul unei terțe persoane care poartă o corespondență cu avocatul său, există o limitare doar la informațiile respective, în situația în care sistemul informatic este al avocatului, apreciem că secretul profesional este strâns legat de toate informațiile conținute și astfel ar trebui să fie just apreciate motivele care impun luarea unei asemenea măsuri și o serioasă analiză de proporționalitate pentru realizarea accesului la un sistem informatic.

§3. Supravegherea audio sau video a interacțiunilor dintre client și avocat la sediul cabinetului

Una dintre garanțiile pentru protejarea secretului profesional al avocatului constă în regimul excepțional al desfășurării de activități de urmărire penală la sediul său profesional. Ținând seama că desfășurarea activității profesionale nu se realizează numai la sediul instanțelor, ci mai ales la sediul profesional, protejarea secretului profesional va viza două aspecte: *i)* protejarea secretului profesional al lucrărilor avocatului de la sediul profesional și *ii)* protejarea secretului profesional al conversațiilor și întâlnirilor care au loc la sediul profesional.

În ceea ce privește secretul profesional al lucrărilor avocatului, acesta privește protejarea sa împotriva ingerințelor care pot fi aduse prin intermediul procedeelor probatorii, precum perchiziția sediului profesional al avocatului, situație în care pot fi controlate lucrările acestuia în privința mai multor clienți. O atare situație, care aduce o maximă ingerință vieții private, nu va fi analizată în prezenta secțiune, întrucât nu prezintă relevanță prin raportare la supravegherea tehnică. Cu toate acestea, simpla pătrundere pentru instalarea sau dezinstalarea de mijloace tehnice de supraveghere (în sensul supravegherii video, audio sau prin fotografiere în spații private) va fi tratată tot sub aspectul aceleiași forme de ingerință, dar cu mențiunea că o sa fie una opțională raportată la mijloacele concrete prin care se poate realiza o astfel de supraveghere[2].

A doua problemă o constituie însăși supravegherea tehnică a cabinetului avocatului, prin instalarea dispozitivelor tehnice de captare a sunetelor și a imaginilor, aceasta constituind, potrivit legislației naționale, o supraveghere video, audio sau prin fotografiere, prevăzută de art. 138 alin. (1) lit. b) C.pr.pen.

---

[1] CEDO, cauza *Vinci Construction și GTM Génie Civil et Services c. Franța*, Hotărârea din 2 aprilie 2015, §69, pe *hudoc.echr.coe.int*

[2] Nu va fi necesară pătrunderea pentru realizarea unei supravegheri audio, sunetele putând fi captate prin mijloace tehnice, precum folosirea unor microfoane speciale îndreptate spre geamul cabinetului, ori prin folosirea sistemelor informatice din dotarea cabinetului pentru înregistrarea activităților desfășurate acolo (de pildă, o cameră de înregistrare video montată în interior).

Conceptul de „domiciliu" în sensul art. 8 par. 1 Conv.EDO se va extinde și asupra sediului unui cabinet de avocatură sau a unei societăți de avocatură, orice pătrundere în acestea fiind considerată o ingerință adusă vieții private[1]. După cum s-a statuat și în jurisprudența Curții Europene a Drepturilor Omului, încălcarea secretului profesional al avocatului prin percheziționarea sau numai pătrunderea în spațiul cabinetului se poate face numai atunci când există suspiciunea că avocatul a comis sau pregătește comiterea unei infracțiuni, o astfel de măsură neputând fi exercitată doar în vederea obținerii de probe cu privire la clienții avocatului[2]. Astfel, spre deosebire de situația interceptării comunicațiilor avocatului, care poate avea caracter accidental, în cazul percheziționării sediului avocatului, vom avea o încălcare voită a secretului profesional, care trebuie limitată la scopul unic de a trage la răspundere penală avocatul.

În ceea ce privește desfășurarea de activități la sediul avocatului, acestea trebuie să fie efectuate cu respectarea unor garanții procedurale speciale referitoare la secretul profesional și numai în situația în care există o suspiciune credibilă cu privire la participarea avocatului în săvârșirea unei infracțiuni. Legea română nu include suficiente garanții în privința măsurilor de supraveghere tehnică ce pot fi utilizate împotriva unui avocat, fiind prevăzute aceleași condiții de autorizare ca în cazul supravegherii unei alte persoane. Alături de acest neajuns, trebuie să menționăm imposibilitatea procedurală a contestării măsurii luate împotriva avocatului și de a obține distrugerea datelor rezultate din supraveghere[3] și lipsa unei notificări a decanului baroului din care face parte despre o asemenea măsură[4].

§4. Supravegherea audio sau video a interacțiunilor dintre client și avocat la locul de detenție

Pentru apărarea drepturilor unei persoane aflate în stare de detenție – atât preventivă, cât și ca urmare a executării unei pedepse privative de libertate –, acesteia i se permite să ia contact cu avocatul său prin orice mijloc – oral, telefonic sau în scris. Acest drept se aplică atât în cazul avocatului deja angajat, cât și în cazul avocatului care urmărește să angajeze cauza persoanei deținute[5]. Dreptul de a se consulta cu persoana pe care o apără, în condiții de confidențialitate, nu va reprezenta doar un drept care cade sub incidența art. 8 Conv.EDO, ci și unul care cade sub incidența art. 6 par. 3 Conv.EDO, numai prin comunicarea liberă și confidențială dintre avocat și client putând fi asigurată efectiva exercitare a dreptului la apărare.

În cauza *Altay c. Turcia (nr. 2)*, Curtea a stabilit că va constitui o ingerință adusă dreptului la viață privată – prin raportare la respectarea secretului profesional – prezența obligatorie a unei persoane din cadrul unei autorități publice la interacțiunile personale dintre avocat și client. În esență, reclamantul fusese condamnat la detențiune pe viață pentru subminarea ordinii constituționale a Turciei, în timpul detenției sale primind corespondență din partea avocatului său, inclusiv cărți sau reviste percepute de instanța națională ca neavând relevanță în apărarea persoanei. Ca o consecință, autoritățile naționale au impus ca fiecare întrevedere

[1] CEDO, cauza *Buck c. Germania*, Hotărârea din 28 aprilie 2005, §31-32; cauza *Niemietz c. Germania*, Hotărârea din 16 decembrie 1992, §30-33, pe *hudoc.echr.coe.int*

[2] CEDO, cauza *Smirnov c. Rusia*, Hotărârea din 7 iunie 2007, §46-47 și §49, pe *hudoc.echr.coe.int*

[3] CEDO, cauza *Heino c. Finlanda*, Hotărârea din 15 februarie 2011, §45, pe *hudoc.echr.coe.int*

[4] *Gh. Mateuț*, Unele considerații privind garantarea secretului profesional al avocatului în lumina noului Cod de procedură penală, în op. cit., p. 426.

[5] CEDO, cauza *Schönenberger și Durmaz c. Elveția*, Hotărârea din 20 iunie 1988, §29, pe *hudoc.echr.coe.int*

dintre persoana aflată în stare de detenție și avocatul său să se desfășoare numai în prezența unei persoane desemnate din cadrul penitenciarului. O atare situație reprezintă o ingerință adusă vieții private a unei persoane, întrucât împiedică posibilitatea ca aceasta să ia decizii informate care să privească viața sa[1]. În plus, în cazul corespondenței scrise, Curtea a stabilit că nu se poate delimita în mod absolut ce documente sau înscrisuri pot reprezenta o comunicare în legătură cu apărarea și una cu caracter general[2], situație aplicabilă cu atât mai mult în împrejurarea în care comunicarea are loc față în față[3]. Or, din cele relevate de Curte, nu este permisă prezența unei persoane la discuțiile dintre client și avocatul său, astfel încât acestea să poată fi auzite și cunoscute în mod nemijlocit, situație în care va fi încălcat dreptul la viață privată prin neasigurarea cadrului în care poate exista secretul profesional.

Numai în măsura în care întâlnirile dintre avocat și client rămân confidențiale, se poate considera că este protejat și dreptul la apărare al persoanei acuzate, în sensul art. 6 par. 3 Conv.EDO, fiind interzise imixtiunile organelor de urmărire penală[4]. În măsura în care nu s-ar asigura această confidențialitate, asistența juridică și-ar pierde din utilitate[5]. În acest sens, supravegherea convorbirilor nu poate avea loc fără o ingerință adusă și dreptului la apărare[6], Convenția interzicând autorităților de a percepe conținutul conversației prin ascultarea acesteia[7], nu neapărat acțiunile concrete care au loc între avocat și persoana aflată în locul de detenție[8]. Nu vor fi permise acțiuni, precum verificarea documentelor prezentate de către avocat clientului în timpul întâlnirilor sau ca acesta să fie percheziționat cu privire la tipul documentelor sau înscrisurilor pe care le are asupra sa la momentul la care își consultă clientul aflat în detenție[9], întrucât acestea ar face parte și din obiectul comunicării dintre cele două părți[10].

Interacțiunea dintre client și avocatul său nu poate face obiectul unei supravegheri tehnice a conținutului conversațiilor atunci când aceasta are loc într-un spațiu de detenție, fiind protejată în mod absolut comunicarea dintre aceștia atunci când are loc față în față și contactul fizic nu poate fi restricționat. În ceea ce ne privește, perspectiva Curții în materia confidențialității discuțiilor personale dintre client și avocat desfășurate la locul de detenție conduce la interzicerea absolută a oricărei forme de supraveghere tehnică prin care s-ar putea cunoaște conținutul conversației purtate între client și apărătorul său. Sub acest aspect, legislația română a consacrat acest principiu în cuprinsul art. 89 alin. (2) C.pr.pen., în care se arată că: „*persoana*

[1] CEDO, cauza *Altay c. Turcia (nr. 2)*, Hotărârea din 9 iulie 2019, §49-50.

[2] CEDO, cauza *Campbell c. Marea Britanie*, Hotărârea din 25 martie 1992, §48.

[3] *Ibidem*, §51.

[4] CEDO, cauza *Beuze c. Belgia*, Hotărârea din 9 noiembrie 2018, §133, pe *hudoc.echr.coe.int*

[5] CEDO, cauza *Lanz c. Austria*, Hotărârea din 30 aprilie 2002, §50; cauza *S. c. Elveția*, Hotărârea din 28 noiembrie 1991, §48; cauza *Brennan c. Marea Britanie*, Hotărârea din 16 octombrie 2001, §58, pe *hudoc.echr.coe.int*

[6] CEDO, cauza *Rybacki c. Polonia*, Hotărârea din 13 aprilie 2009, §56; cauza *Öcalan c. Turcia*, Hotărârea din 12 mai 2005, §135, pe *hudoc.echr.coe.int*

[7] CEDO, cauza *Sakhnovskiy c. Rusia*, Hotărârea din 2 noiembrie 2010, §97; cauza *Castraveț c. Moldova*, Hotărârea din 13 martie 2007, §49, pe *hudoc.echr.coe.int*

[8] Conform art. 62 alin. (3) din Legea nr. 254 din 19 iulie 2013 privind executarea pedepselor și a măsurilor privative de libertate dispuse de organele judiciare în cursul procesului penal, „consultarea cu avocatul, ales sau din oficiu, se face cu respectarea confidențialității vizitei, sub supraveghere vizuală". Supravegherea vizuală va permite numai împiedicarea transferului de bunuri interzise și asigurarea siguranței persoanelor în cursul vizitei.

[9] CEDO, cauza *Khodorkovskiy și Lebedev c. Rusia*, Hotărârea din 25 iulie 2013, §641, pe *hudoc.echr.coe.int*

[10] În mod evident, anumite reglementări trebuie să fie impuse pentru siguranța penitenciarului, inclusiv respectarea legii în privința obiectelor interzise a fi primite, cumpărate, păstrate și folosite de deținuți, cuprinse în Anexa nr. 2 a Regulamentului de aplicare a Legii nr. 254/2013, adoptat prin H.G. nr. 157/2016.

reținută sau arestată are dreptul să ia contact cu avocatul, asigurându-i-se confidențialitatea comunicărilor, cu respectarea măsurilor necesare de supraveghere vizuală, de pază și securitate, fără să fie interceptată sau înregistrată convorbirea dintre ei. Probele obținute cu încălcarea prezentului alineat se exclud". După cum rezultă din cuprinsul legislației naționale, aceasta se va aplica nu numai întrevederilor personale dintre client și avocat, dar și convorbirilor telefonice purtate cu acestea, sens în care este relevant termenul de „interceptare" folosit de legiuitor.

Secțiunea a 2-a. Limitele autorizării supravegherii tehnice față de avocat în legislația națională

Legiuitorul român a prevăzut anumite limitări în privința posibilității folosirii probelor obținute din supravegherea tehnică a unei persoane atunci când ele privesc raporturile dintre aceasta și avocatul său. În același timp, se prevede și o posibilitate a informării avocatului despre aceasta de către judecătorul de drepturi și libertăți.

În jurisprudență s-a susținut că dispozițiile art. 139 alin. (4) C.pr.pen. sunt menite să asigure apărarea efectivă a clientului avocatului, și nu a avocatului, opinie cu care nu putem fi de acord[1]. Interdicția supravegherii raportului profesional dintre client și avocat apără și avocatul, ca garant al exercitării efective a dreptului la apărare, ținând seama că un avocat va avea mai mulți clienți, iar o supraveghere tehnică îi poate afecta prestigiul profesional, dar și relațiile cu ceilalți clienți, care nu fac obiectul supravegherii tehnice.

Mai înainte de a trece la analiza legii procesuale penale, menționăm că secretul profesional al avocatului cunoaște o reglementare proprie în Legea nr. 51/1995[2], în care, la art. 34 alin. (3), se arată că: „*nu vor putea fi ascultate și înregistrate, cu niciun fel de mijloace tehnice, convorbirile telefonice ale avocatului și nici nu va putea fi interceptată și înregistrată corespondența sa cu caracter profesional, decât în condițiile și cu procedura prevăzute de lege*". Legea avocaturii nu reglementează în mod complet măsurile de supraveghere tehnică, legiuitorul omițând înregistrările în mediu ambiental, precum și accesul la un sistem informatic (decât dacă acceptăm, prin corespondență, sensul pe care îl are Convenția Europeană a Drepturilor Omului). Într-un mod cu totul neadecvat, legiuitorul mai include o copie a art. 139 alin. (4) C.pr.pen. pentru ca, în situația în care s-ar modifica Codul de procedură penală, să avem un paralelism legislativ complet și un conflict între Legea nr. 51/1995 și Codul de procedură penală. Era preferabil că Legea nr. 51/1995 să conțină garanții suplimentare față de Codul de procedură penală, pentru a proteja de abuzuri profesia.

În ceea ce privește dispozițiile incidente din cuprinsul Codului de procedură penală, potrivit art. 139 alin. (4) C.pr.pen., „*raportul dintre avocat și persoana pe care o asistă sau o reprezintă nu poate forma obiectul supravegherii tehnice decât dacă există date că avocatul săvârșește ori pregătește săvârșirea unei infracțiuni dintre cele prevăzute la alin. (2). Dacă pe parcursul sau după executarea măsurii rezultă că activitățile de supraveghere tehnică au vizat și raporturile*

[1] ICCJ, s. pen., încheierea nr. 155 din 3 iunie 2015, publicată în V.-I. Pușcașu, C. Ghigheci, Codul de procedură penală adnotat, vol. 1, Ed. Universul Juridic, București, 2019, p. 342. În respectiva cauză, clientul a fost cel care a realizat o înregistrare cu avocatul său, mai apoi organele de urmărire penală ridicând înregistrarea. Înregistrarea a fost folosită pentru formularea unor acuzații împotriva avocatului.

[2] Legea nr. 51 din 7 iunie 1995 pentru organizarea și exercitarea profesiei de avocat (republicată în M. Of. nr. 440 din 24 mai 2018).

dintre avocat și suspectul ori inculpatul pe care acesta îl apără, probele obținute nu pot fi folosite în cadrul niciunui proces penal, urmând a fi distruse, de îndată, de către procuror. Judecătorul care a dispus măsura este informat, de îndată, de către procuror. Atunci când apreciază necesar, judecătorul dispune informarea avocatului".

O primă constatare care se impune a fi făcută este că textul art. 139 alin. (4) C.pr.pen. se referă numai la raporturile avocatului cu suspectul sau inculpatul pe care acesta îl apără, textul trebuind să fie interpretat într-un sens extensiv, astfel încât să acopere orice persoană care primește asistență juridică din partea unui avocat, indiferent de calitatea sa în cauză. Cu alte cuvinte, legea nu apără relația avocat-parte, ci relația dintre avocat și clientul său, indiferent ce calitate ar avea unul sau altul în vreun proces penal[1].

După cum s-a observat în literatura de specialitate, limitarea adusă de legiuitor supravegherii tehnice privește numai raporturile dintre avocat și persoana pe care o asistă sau reprezintă în proces, nu și aspectele care depășesc acest cadru, care pot face obiectul supravegherii tehnice[2]. S-a reținut într-o opinie concurentă că o discuție dintre un inculpat și avocatul său, în care primul recunoaște fapta de care este acuzat, nu va putea fi folosită ca probă, însă nu vor exista restricții cu privire la folosirea comunicațiilor dacă pe parcursul acestora se discută despre participarea avocatului la săvârșirea unei infracțiuni. Totodată, s-a susținut că, din punct de vedere tehnic, la momentul interceptării, nu se va putea face o diferențiere între tipul de raport dintre persoana interceptată și avocatul său ori între persoanele angajate în discuții, aceste aspecte urmând să fie stabilite ulterior de organele de urmărire penală[3].

Față de toate aceste opinii de specialitate, alegem să ne exprimăm o opinie discordantă, atât sub aspectul definirii clare și previzibile a raportului dintre avocat și client, cât și cu privire la imposibilitatea interceptării comunicațiilor avocatului sau, în sens larg, la posibilitatea supravegherii tehnice incidentale ale avocatului.

În primul rând, apreciem că, pentru a se respecta necesitatea protejării caracterului confidențial al raportului dintre client și avocat, orice interacțiune pe care o are persoana supusă unei măsuri de supraveghere tehnică trebuie să fie protejată de supraveghere tehnică, indiferent de conținutul acestei interacțiuni. Cu alte cuvinte, ne opunem însăși întinderii efectelor supravegherii tehnice asupra avocatului. În susținerea acestui punct de vedere, trebuie să luăm în considerare că, la momentul autorizării unei măsuri de supraveghere tehnică, nu este previzibil pentru judecătorul de drepturi și libertăți că vor putea fi interceptate convorbirile dintre persoană și avocatul său – la acel moment nefiind cert dacă aceasta are un avocat.

În al doilea rând, interceptarea tuturor comunicațiilor, inclusiv ale celor cu avocatul nu prezintă suficiente garanții pentru protejarea drepturilor persoanei supravegheate, deoarece legea nu prevede o procedură eficientă prin care aceste comunicații să fie trecute printr-un filtru a cărei confidențialitate nu poate fi pusă la îndoială. Determinarea existenței unui raport profesional dintre client și avocat este o sarcină care incumbă procurorului, dar legea nu stabilește criterii prin care să se determine existența acestui raport, astfel că procurorul poate invoca necunoașterea existenței acestuia și să presupună că discuțiile au avut loc în baza unei relații de prietenie. În jurisprudență s-a apreciat că vor face obiectul interdicției numai

[1] *M.V. Tudoran*, Interceptările și înregistrările audio sau video efectuate asupra raportului avocat-client în procesul penal, în Curierul Judiciar nr. 5/2011, p. 289.

[2] *Gh. Mateuț*, Unele considerații privind garantarea secretului profesional al avocatului în lumina noului Cod de procedură penală, în op. cit., p. 422; *C.M. Chiriță*, în N. Volonciu, A.S. Uzlău (coord.), Noul Cod, 2014, pp. 316-317.

[3] *C.M. Chiriță*, în N. Volonciu, A.S. Uzlău (coord.), Noul Cod, 2014, p. 317.

discuțiile cu caracter profesional dintre avocat și client, nu și cele privind orice altă relație[1]. Nu putem fi de acord cu această opinie, deoarece ar presupune ascultarea tuturor convorbirilor dintre client și avocat pentru a determina conținutul discuțiilor, or, aceasta vine în contradicție cu dreptul la apărare și cu dreptul la viață privată, întrucât organele de urmărire penală vor putea afla aspecte despre apărarea unei persoane, chiar dacă nu vor putea obține probe în mod direct[2].

În al treilea rând, nu suntem de acord că la momentul interceptării nu există posibilitatea de a se delimita raportul dintre avocat și clientul său, întrucât această posibilitate există din punct de vedere tehnic în cazul interceptării comunicațiilor. Chiar dacă nu este implementată în sistemul informatic al C.N.I.C., interceptarea comunicațiilor cu un avocat poate fi evitată prin aceea că numerele de telefon de contact ale avocaților sunt publice, fiind înregistrate în aplicația Tabloului Național al avocaților[3] și pot fi utilizate pentru crearea unor filtre de interceptare a comunicațiilor care să excludă de la mandatul judecătorului de drepturi și libertăți respectivele numere de telefon.

În al patrulea rând, chiar dacă se interceptează comunicațiile persoanei supravegheate cu avocatul său, procurorul sau organul de cercetare penală nu va avea dreptul să le acceseze sau să le folosească, impunându-se distrugerea de îndată a tuturor, în măsura în care procurorul are date cu privire la identitatea avocatului care asistă sau reprezintă persoana supravegheată.

Din aceste motive, apreciem că supravegherea tehnică a avocatului poate avea loc numai dacă se va dispune față de acesta în mod direct și va exista o autorizare din partea judecătorului de drepturi și libertăți. O atare autorizare poate fi emisă numai dacă există o suspiciune rezonabilă din care rezultă că avocatul pregătește sau a săvârșit o infracțiune prevăzută de art. 139 alin. (2) C.pr.pen. și sunt îndeplinite și celelalte condiții prevăzute de art. 139 C.pr.pen.

Ținând seama că opinia expusă este una neîmpărtășită de literatura de specialitate, în continuare vom analiza aspectele relevate de doctrină în legătură cu problema analizată în prezenta secțiune.

S-a considerat că, pentru a opera interdicția supravegherii comunicărilor dintre client și avocat, se impun a fi îndeplinite trei condiții: *i)* să fie vorba de un avocat, o persoană care a dobândit această calitate în condițiile Legii nr. 51/1995; *ii)* comunicările supravegheate să privească raportul profesional al avocatului, existent ca urmare a încheierii unui contract de asistență juridică; *iii)* să nu existe date că, în cadrul raportului profesional, avocatul săvârșește ori pregătește săvârșirea unei infracțiuni dintre cele prevăzute de art. 139 alin. (2) C.pr.pen.[4].

În ceea ce privește calitatea de avocat, s-a susținut că reglementarea actuală este mult prea restrânsă, trebuind să fie inclusă în această categorie și consilierii juridici, dar și procurorii, judecătorii care ar putea pune concluzii în cauzele, inclusiv penale ale soțului, ascendenților și descendenților, potrivit art. 10 alin. (3) din Legea nr. 303/2004[5]. Nu putem fi de acord cu această interpretare lărgită a art. 139 alin. (4) C.pr.pen., deoarece niciuna dintre categoriile arătate nu îndeplinesc condițiile de pregătire profesională pentru exercitarea profesiei de avocat

[1] C. Ap. Iași, s. pen., încheierea din 5 septembrie 2016, publicată în C. Moisă, op. cit., pp. 113-115.

[2] Simpla ascultare a convorbirilor cu un avocat poate conduce la aflarea strategiei de apărare sau aflarea unor împrejurări esențiale pentru apărare. Nu este cu nimic diferită situația de cea constatată de CEDO în cauza *Altay c. Turcia (nr. 2)*, Hotărârea din 9 iulie 2019, unde era necesară prezența unui funcționar al statului la toate discuțiile dintre avocat și clientul său aflat în stare de detenție.

[3] *www.ifep.ro*

[4] *M. Bulancea, R. Slăvoiu*, în M. Udroiu (coord.), Codul de procedură penală, 2017, pp. 670-671.

[5] *Ibidem*, p. 670.

și astfel nu pot beneficia nici de privilegiile acordate exclusiv profesiei. În plus, este rizibilă susținerea că procurorii sau judecătorii pot pleda în cauzele penale ale soțului, ascendenților sau descendenților, întrucât legea procesuală penală nu le recunoaște această posibilitate, funcția de asistare și reprezentare convențională fiind atributul exclusiv al avocatului. Ceea ce pot exercita magistrații este apărarea în cauze civile a ascendenților și descendenților, a soților, precum și a persoanelor puse sub tutela sau curatela lor, în calitate de licențiați în drept, conform art. 83 alin. (2) C.pr.civ.

În practica judiciară s-a reținut că, pentru a fi atrasă nulitatea autorizării măsurilor de supraveghere tehnică dispuse față de avocat de către o instanță inferioară în grad celei competente (în speță, Tribunalul București), era necesar ca organele de urmărire penală și judecătorul de drepturi și libertăți să cunoască această calitate la momentul formulării, respectiv judecării propunerii de autorizare a măsurilor de supraveghere tehnică[1]. Nu putem fi de acord cu o asemenea soluție, întrucât cazurile de nulitate absolută nu presupun un element intențional în încălcarea legii și nici nu salvgardează actul dacă acesta a fost realizat cu bună-credință, impunându-se în toate cazurile constatarea nulității absolute, ca urmare a autorizării măsurii de către o instanță inferioară în grad celei competente.

Referitor la existența unui contract de asistență juridică, nu este necesar ca discuția interceptată să se refere la cauza care face obiectul urmăririi penale în care se realizează supravegherea tehnică, fiind suficient să se discute despre o cauză determinată pe care o are clientul avocatului[2]. În același timp, inexistența unui contract de asistență juridică în formă scrisă nu conduce la admisibilitatea supravegherii tehnice, acest contract putând fi încheiat și prin mijloace de comunicare la distanță, inclusiv telefonic, forma scrisă a contratului de asistență juridică fiind o condiție *ad probationem*[3]. Instanțele au recunoscut că nu este necesar ca acest contract să existe în formă scrisă la momentul interceptării, el putând fi încheiat și ulterior[4].

În ceea ce privește a treia condiție, respectiv lipsa unor suspiciuni că, în cadrul raportului profesional, avocatul pregătește săvârșirea sau săvârșește o infracțiune, aceasta este una obligatorie, întrucât altfel s-ar putea pune în discuție supravegherea tehnică a avocatului dacă vor fi îndeplinite celelalte condiții prevăzute de lege. Cu alte cuvinte, probele urmează a fi distruse numai în situația în care ele reflectă un raport profesional corect, și nu un abuz din partea avocatului care s-ar folosi de acest privilegiu în vederea comiterii de infracțiuni.

În doctrină s-a relevat că stadiul actual al legislației este deficitar, întrucât art. 139 alin. (4) C.pr.pen. nu oferă suficiente garanții, deoarece nu elimină riscul prejudicierii persoanei supravegheate în relația cu avocatul, organele de urmărire putând obține informații cu privire la fapta cercetată, conducând la administrarea altor procedee probatorii pentru dovedirea faptei[5]. Pericolul este unul real având în vedere ineficiența sancțiunilor aplicabile în cauză, ținând seama de exprimarea legiuitorului, potrivit căreia: „*probele obținute nu pot fi folosite în cadrul niciunui proces penal, urmând a fi distruse, de îndată, de către procuror*". Formularea a fost considerată una inexactă, întrucât ceea ce urmează a se distruge nu este proba, ci mijlocul de probă, acesta fiind transcrierea convorbirilor, procesul-verbal de interceptare, banda

[1] ICCJ, s. pen., încheierea nr. 3147 din 12 decembrie 2014.

[2] *V. Trif*, op. cit., p. 97.

[3] *Gh. Mateuț*, Unele considerații privind garantarea secretului profesional al avocatului în lumina noului Cod de procedură penală, în op. cit., pp. 424-425.

[4] C. Ap. Alba Iulia, încheierea nr. 77 din 7 iunie 2016.

[5] *Gh. Mateuț*, Unele considerații privind garantarea secretului profesional al avocatului în lumina noului Cod de procedură penală, în op. cit., p. 423.

sau suportul pe care s-a realizat înregistrarea[1]. Autorul a considerat că dacă înregistrarea se face pe un suport digital, simpla ștergere a informației nu ar avea ca efect distrugerea ei și imposibilitatea folosirii sale pe viitor. Constatarea este una care impune precizări tehnice pentru că este inexactă, distrugerea datelor informatice putându-se realiza nu numai prin ștergerea logică de pe un suport de stocare reinscriptibil (hard-disk, stick USB), dar și prin distrugerea fizică a suportului, prin operațiuni mecanice (ruperea, tocarea sa, lovirea cu ciocanul etc.) sau fizice (ardere, demagnetizare). Întrucât în practică suportul de stocare este de regulă un CD sau DVD, distrugerea sa va fi una facilă, majoritatea unităților de parchet deținând deja echipamente de distrugere a documentelor care includ și distrugătoare de suporți optici.

Distrugerea fizică a suportului de stocare trebuie să fie însoțită și de distrugerea copiei acestuia, care va fi realizată, potrivit art. 143 alin. (2) C.pr.pen., ca anexă la procesul-verbal de consemnare a activităților de supraveghere tehnică. Credem că acest proces-verbal va trebui să includă și activitatea desfășurată față de comunicarea dintre client și avocat, ceea ce nu va însemna și redarea acesteia, conform art. 143 alin. (4) C.pr.pen. S-a arătat în doctrină că redarea în cuprinsul unui proces-verbal al unor asemenea conversații este lovită de nulitate de ordine publică[2]. Este adevărat că sancțiunea va trebui să fie cea a nulității, însă apreciem că, raportat la limitările art. 281 C.pr.pen. privind nulitățile absolute, se va putea invoca numai nulitatea relativă a mijlocului de probă, vătămarea procesuală fiind una evidentă și constând în vătămarea dreptului la apărare, dar și a dreptului la viață privată.

În ceea ce privește folosirea probei în procesul penal, s-a considerat în doctrină că aceasta presupune numai utilizarea în procesul penal a înregistrării convorbirii dintre avocat și clientul său, nu și a folosirii probelor obținute ca urmare a audierii înregistrărilor și recurgerii la alte procedee probatorii[3]. Astfel, autorul a susținut că, deși suntem în situația unei probe derivate, nu vor fi aplicabile dispozițiile art. 102 alin. (4) C.pr.pen. Imposibilitatea folosirii probei nu se poate echivala cu obținerea ei în mod nelegal, apreciindu-se că ar fi necesară excluderea probei inițiale pentru a se exclude și proba derivată. Într-o altă opinie, s-a apreciat că folosirea informațiilor rezultate din convorbirile dintre client și avocat ar conduce la aplicarea art. 102 alin. (4) C.pr.pen., întrucât probele ar fi derivate din probe ilegale, trebuind să fie excluse dacă nu puteau fi obținute în alt mod[4].

În ceea ce ne privește, ambele opinii au valoare, însă apreciem că soluția care ar trebui adoptată în cauză este cea a nulității relative a mijloacelor de probă obținute în cauză prin prisma nerespectării dispoziției legale a *nefolosirii în cadrul niciunui proces penal a probelor*. În măsura în care se vor obține înregistrări ale raportului dintre avocat și clientul său, ele vor avea calitatea de mijloc de probă în cauză (atât sub forma de proces-verbal, cât și ca mijloc material de probă, constând în suportul de stocare pe care se află datele informatice rezultate din supravegherea tehnică), iar din acestea va rezulta proba[5]. La momentul administrării probei derivate, chiar dacă mijlocul de probă conținând rezultatele supravegherii tehnice a fost distrus, organul de urmărire penală se va folosi de proba obținută nelegal prin acestea în calitate de informație pentru administrarea de noi probe derivate, în acest sens, ceea ce a fost

[1] *C.M. Chiriță*, în N. Volonciu, A.S. Uzlău (coord.), Noul Cod, 2014, pp. 317-318.

[2] *Gh. Mateuț*, Unele considerații privind garantarea secretului profesional al avocatului în lumina noului Cod de procedură penală, în op. cit., p. 426.

[3] *Ibidem*.

[4] *M. Bulancea, R. Slăvoiu*, în M. Udroiu (coord.), Codul de procedură penală, 2017, p. 670.

[5] *A. Uzlău*, Considerații privind garanțiile procesual penale în materia respectării confidențialității relației avocat-client, în raport cu unele procedee probatorii, în Revista de Drept Penal nr. 3/2014, p. 107.

probă la un moment dat se va refolosi de organele de urmărire penală contrar dispozițiilor art. 139 alin. (4) C.pr.pen., determinând nulitatea relativă a oricărei probe derivate.

O situație care poate apărea în practică este atunci când față de avocat au fost autorizate măsuri de supraveghere în legătură sau nu cu exercitarea profesiei, printre care și interceptarea comunicațiilor acestuia. Aceasta va putea avea loc numai dacă există o urmărire penală începută față de fapta care se pretinde că s-ar săvârși sau s-a săvârșit de avocat, nefiind suficientă numai o simplă suspiciune față de acesta, fără a fi începută urmărirea penală, conform art. 305 alin. (1) C.pr.pen.

În mod evident, o atare măsură va afecta raporturile profesionale dintre avocat și clienții săi, situație care va fi cu atât mai sensibilă, întrucât ar presupune ascultarea rezultatelor supravegherii tehnice, putând fi aflate informații pentru alte cauze ale avocatului, în care își exercită în mod corect profesia[1]. În cadrul procedurii de autorizare, judecătorul de drepturi și libertăți va trebui să analizeze cu maximă rigoare caracterul suspiciunii rezonabile din cauză, nefiind permis organelor de urmărire penală să își justifice propunerea de autorizare a măsurilor de supraveghere tehnică pe simple presupuneri. În opinia noastră, ținând seama de importanța avocatului în apărarea drepturilor fundamentale ale persoanelor, s-ar impune ca standardul să fie unul mai ridicat față de cel prevăzut de art. 139 alin. (1) lit. a) C.pr.pen., trebuind ca suspiciunea rezonabilă să se întemeieze pe probe, și nu doar pe date și informații[2].

Sub aspectul proporționalității, trebuie subliniat că suficiența și concludența temeiurilor care justifică supravegherea tehnică vor trebui să fie mai mari atunci când, prin supravegherea avocatului, se vrea restrângerea secretului profesional[3]. Ele pot presupune restrângerea dreptului la apărare a mai multor persoane și numai o restrângere a dreptului la viață privată, ceea ce impune judecătorului de drepturi și libertăți să analizeze în mod complet dacă nu va exista o disproporție între măsură și ingerința adusă. Chiar și dacă măsura nu va fi considerată disproporționată, regula instituită de art. 139 alin. (4) C.pr.pen. va opera, neputând fi folosite probele rezultate din supravegherea tehnică a raportului dintre avocat și clienții care nu au legătură cu faptele care fac obiectul urmăririi penale.

În doctrină s-a considerat că interdicția folosirii probei în orice proces penal va fi incidentă în toate situațiile, mai puțin una, excepțională, respectiv tragerea la răspundere penală a avocatului. Astfel, s-a reținut această excepție atunci când: *„avocatul însuși săvârșește sau se pregătește să săvârșească o infracțiune din categoria celor enunțate la alin. (2) al aceluiași articol. În acest caz, proba poate fi folosită pentru dovedirea activității infracționale a unei persoane, care are doar față de clientul său calitatea de avocat*"[4]. Deși opinia concură cu jurisprudența recentă a Curții Europene a Drepturilor Omului[5], nu putem fi de acord cu concluziile literaturii de specialitate și nici cu practica judiciară[6], întrucât, în contextul legislației naționale, s-ar încălca art. 8 par. 2 Conv.EDO, posibilitatea folosirii probelor împotriva avocatului nefiind prevăzută de lege, or, în domeniul dreptului la viață privată, orice ingerință se impune a fi realizată numai în condițiile legii. Dimpotrivă, fiind un raport între un avocat și clientul său, se vor aplica dispozițiile art. 139 alin. (4) C.pr.pen., care prevăd imposibilitatea folosirii probei în nicio

[1] *S. McKay*, Covert Policing, 2015, p. 52.

[2] *V. supra*, Titlul III, Capitolul I.2.

[3] CEDO, cauza *Silver ș.a. c. Marea Britanie*, Hotărârea din 25 martie 1983, §105, pe *hudoc.echr.coe.int*

[4] *C.M. Chiriță*, în N. Volonciu, A.S. Uzlău (coord.), Noul Cod, 2014, p. 318; *M. Bulancea, R. Slăvoiu*, în M. Udroiu (coord.), Codul de procedură penală, 2017, p. 672.

[5] CEDO, cauza *Versini-Campinchi și Crasnianski c. Franța*, Hotărârea din 16 iunie 2016, §78.

[6] ICCJ, s. pen., încheierea nr. 1531 din 12 decembrie 2016.

cauză penală, prin aceasta înțelegându-se și o eventuală cauză penală împotriva avocatului. În opinia noastră, pentru a putea fi folosite vreodată probe obținute din supraveghere tehnică împotriva unui avocat, este necesar ca față de acesta să se fi dispus mai înainte încuviințarea supravegherii tehnice de către judecătorul de drepturi și libertăți.

Un ultim aspect care merită analizat este procedura ulterioară distrugerii probelor rezultate din supravegherea tehnică a raportului dintre avocat și clientul său. Conform art. 139 alin. (4) C.pr.pen., „*(…) judecătorul care a dispus măsura este informat, de îndată, de către procuror. Atunci când apreciază necesar, judecătorul dispune informarea avocatului*". Informarea judecătorului de drepturi și libertăți constituie o obligație, însă nu se include niciun termen în care aceasta trebuie realizată. În plus, în mod diferit față de art. 145 C.pr.pen. cu privire la informarea persoanei supravegheate, informarea avocatului supravegheat va fi facultativă, fiind lăsată la aprecierea judecătorului de drepturi și libertăți. O explicație pentru această diferență constă și în diferența de regim, întrucât se are în vedere doar o supraveghere tehnică accidentală a avocatului, nu situația în care față de acesta s-ar emite un mandat de supraveghere tehnică. O atare situație nu o considerăm a fi legală, deoarece îl pune pe avocat într-o situație inferioară față de clientul său, care va putea fi încunoștințat în cel mult 10 zile de încetarea supravegherii tehnice. În doctrină s-a arătat că, în cazul în care au fost surprinse elemente care țin de apărarea clientului, atunci informarea avocatului va fi obligatorie[1]. Considerăm că, în vederea respectării drepturilor proprii recunoscute de Codul de procedură penală avocatului, acesta va trebui să fie încunoștințat în mod separat, în condițiile art. 145 C.pr.pen., și să poată contesta, în nume personal, legalitatea măsurii de supraveghere tehnică care l-a afectat direct sau incidental.

[1] *S. Grădinaru*, Cazurile și condițiile de emitere a mandatului de supraveghere tehnică, în Curierul Judiciar nr. 1/2015, p. 39.

Capitolul IX
Valorificarea rezultatelor utilizării mijloacelor speciale de supraveghere tehnică

Secțiunea 1. Valoarea probatorie a mijloacelor de probă rezultate din supravegherea tehnică

În concepția legiuitorului, metodele speciale de supraveghere vor avea natura unor *procedee probatorii*, în sensul art. 97 alin. (3) C.pr.pen. Deși nu sunt amintite în cuprinsul acestui articol, ele cunosc o reglementare legală și conduc la obținerea de probe în procesul penal. În acest sens, supravegherea tehnică diferă de unele metode speciale de cercetare prin care nu se pot obține în mod direct probe, ci numai date și informații care pot sta la baza obținerii unor probe derivate. Cu toate acestea, scopul final al tuturor metodelor speciale de supraveghere sau cercetare este obținerea unei probe în procesul penal, fie direct, fie prin administrarea de probe derivate.

În ceea ce privește mijlocul de probă care poate rezulta din activitățile de supraveghere tehnică, acesta va fi, în principal, un proces-verbal întocmit de procuror sau de organul de cercetare, la dispoziția procurorului. Conform art. 143 alin. (1) C.pr.pen., acest proces-verbal se va întocmi pentru fiecare activitate de supraveghere tehnică. Întocmirea sa va avea loc în toate cazurile, indiferent de măsura de supraveghere tehnică concretă. Rolul său este atât de a proba împrejurările surprinse prin activitățile de supraveghere tehnică – din acesta reieșind proba în sensul art. 97 alin. (1) C.pr.pen., cât și de a proba desfășurarea supravegherii tehnice față de o persoană.

În funcție de specificul măsurii de supraveghere tehnice, legiuitorul a considerat că procesul-verbal prevăzut de art. 143 alin. (1) C.pr.pen. poate fi insuficient pentru a proba rezultatele supravegherii tehnice, sens în care nu va fi suficientă consemnarea activităților de supraveghere tehnică, fiind necesară întocmirea procesului-verbal de redare integrală a convorbirilor, comunicărilor sau conversațiilor interceptate și înregistrate, acesta urmând să fie certificat de procuror.

Într-o primă opinie s-a susținut că interceptările, înregistrările, localizările sau urmăririle reglementate de Cod nu sunt mijloace de probă, ci doar procedee probatorii, procesele-verbale constituind mijloacele de probă care pot fi folosite pentru stabilirea situației de fapt[1]. Într-o altă opinie, minoritară în literatura de specialitate, s-a susținut că procesul-verbal de redare integrală a convorbirilor, comunicărilor sau conversațiilor nu ar constitui mijlocul de probă, acesta fiind doar rezultatul a ceea ce a perceput organul de urmărire penală care l-a întocmit, mijloc de probă fiind însăși înregistrarea[2]. O altă opinie, cu care noi suntem de acord, este că vor constitui mijloace de probă atât procesul-verbal prevăzut de art. 143 C.pr.pen., cât și suportul de stocare pe care sunt înscrise rezultatele activităților de supraveghere tehnică[3].

[1] *M. Udroiu, R. Slăvoiu, O. Predescu*, Tehnici speciale, 2009, p. 193.
[2] *R. Slăvoiu*, Protecția penală a vieții private, Ed. Universul Juridic, București, 2016, pp. 322-323.
[3] *M. Udroiu*, Procedură penală, vol. I, 2019, p. 591.

Caracterul de mijloc de probă va fi acordat și suportului de stocare pe care se află rezultatele activităților de supraveghere tehnică, în doctrină considerându-se că acesta va constitui un mijloc material de probă[1]. El va avea un rol secundar, fiind folosit pentru verificarea veridicității proceselor-verbale de redare, precum și a autenticității și integrității acestuia, dacă acestea se contestă. După cum, în mod corect, s-a surprins în doctrină, acest suport de stocare care va fi anexat procesului-verbal prevăzut de art. 143 alin. (1) C.pr.pen. nu va fi suportul inițial, ci o copie a acestuia[2].

Raportat la configurația actuală a Codului de procedură penală, susținerea este corectă, însă apreciem că se impune redefinirea noțiunii de „mijloc de probă", prin includerea și a datelor informatice. Deja Codul de procedură penală recunoaște importanța datelor informatice, prevăzând procedee probatorii pentru obținerea lor, precum accesul la un sistem informatic, predarea obiectelor, înscrisurilor sau a datelor informatice sau percheziția informatică, fără a se preciza concret mijlocul de probă care rezultă din aceste procedee probatorii. De altfel, în prezent, și în cazul metodelor speciale de supraveghere, se recunoaște că rezultatele vor constitui date informatice, potrivit art. 143 alin. (2^1) C.pr.pen. În realitate, conceptul de „mijloc material de probă" este unul inadecvat pentru datele informatice, întrucât acordă un rol prea mare suportului de stocare al acestora, în condițiile în care nu se precizează ce fel de suport este sau care sunt caracteristicile sale. În plus, verificarea autenticității și integrității rezultatelor activităților de supraveghere tehnică nu se va face prin raportare la suportul de stocare – de pildă, pentru un CD sau DVD, alterarea sau adăugirea nu va fi constatată prin mijloace clasice, precum observarea sau compararea, examinarea sa sub microscop, identificarea urmelor de pe acesta etc. –, ci prin verificarea autenticității și integrității datelor informatice conținute.

Deși, în prezent, nici măcar Codul de procedură civilă nu recunoaște că noțiunea de „document" ar putea avea și caracter digital, insistând pe un act în formă materială[3], o abordare sistemică se impune pentru a recunoaște datelor informatice caracterul de mijloc de probă, alături de menținerea caracterului de mijloc de probă și al suportului de stocare pe care se află acestea. Întrucât procesul penal modern va presupune documente în format digital și accesarea dosarului cauzei prin intermediul unui sistem informatic, proba va putea fi administrată și prin intermediul unor mijloace de probă constând în date informatice. *De lege ferenda*, se impune ca, în cuprinsul Codului de procedură penală, să fie amintite ca mijloace de probă și datele informatice și să se prevadă un regim distinct pentru acestea. În același timp, vor trebui impuse noi proceduri pentru administrarea acestor probe digitale, plecând de la premisa că au o natură diferită față de probele tradiționale și presupun procedee probatorii adaptate acestora[4].

În ceea ce privește valoarea probantă a mijloacelor de supraveghere tehnică, Codul de procedură penală supune proba rezultată din acestea regulii liberei aprecieri a probelor, conform art. 103 alin. (1) C.pr.pen., potrivit căruia „*probele nu au o valoare dinainte stabilită prin lege și sunt supuse liberei aprecieri a organelor judiciare în urma evaluării tuturor probelor*

[1] *Gh. Mateuț*, Procedură penală, 2019, p. 697.

[2] *Ibidem*.

[3] Conform art. 282 alin. (1) C.pr.civ., „Când datele unui act juridic sunt redate pe un suport informatic, documentul care reproduce aceste date constituie instrumentul probator al actului, dacă este inteligibil și prezintă garanții suficient de serioase pentru a face deplină credință în privința conținutului acestuia și a identității persoanei de la care acesta emană".

[4] *O.S. Kerr*, Digital Evidence and the New Criminal Procedure, în Columbia Law Review, vol. 105, no. 1/2005, p. 317.

administrate în cauză". Conform dispozițiilor Codului de procedură penală, singura situație expres prevăzută de lege care impune caracter diminuat al valorii probante privește declarațiile investigatorilor, colaboratorilor ori martorilor protejați. În cazul investigatorilor sau colaboratorilor, declarațiile acestora vor constitui probe derivate în situația utilizării metodei speciale de cercetare a utilizării investigatorilor sub acoperire ori a colaboratorilor.

Neexistând nicio limitare asupra posibilității aprecierii probelor de către instanță, măsurile de supraveghere tehnică au un rol deosebit în dovedirea faptelor ce fac obiectul procesului penal, putând conduce la obținerea de probe directe[1] privind săvârșirea unei infracțiuni.

Totodată, prin metodele speciale de supraveghere tehnică pot fi obținute și înregistrări în care persoanele recunosc săvârșirea faptelor de care sunt acuzate sau urmează a fi acuzate, obținându-se o probă determinantă care va fi foarte greu de combătut. Aceasta va constitui o mărturisire care nu va fi supusă regulii stabilite în cazul declarației suspectului sau inculpatului de a fi condiționată de coroborarea cu alte probe în cauză și nici nu va fi posibilă retragerea sa[2], întrucât nu a fost obținută prin audiere. Acest efect este dat de caracterul special și derogatoriu al măsurilor speciale de supraveghere tehnică prin care se permite surprinderea tuturor interacțiunilor persoanei într-un mod ascuns, astfel că aceasta nu își poate formula o apărare, neștiind că poate face obiectul unei asemenea măsuri. Fiind surprinsă, persoana se va destăinui unor prieteni apropiați cu privire la săvârșirea faptei, probele obținute putând fi folosite împotriva sa. În cazul audierii unei persoane, dacă aceasta mărturisește săvârșirea unei fapte, va exista întotdeauna o posibilitate ca această mărturisire să nu fie una spontană, ci să provină din presiunile psihologice sau chiar fizice la care poate fi supusă[3].

Nu în toate cazurile vor fi obținute probe directe în procesul penal prin supravegherea tehnică, de cele mai multe ori fiind obținute doar probe indirecte[4], care singure nu au aptitudinea de a conduce la pronunțarea unei soluții de condamnare decât în măsura în care acestea se coroborează între ele[5]. De pildă, într-o cauză privind infracțiunea de omor, o localizare a făptuitorului prin mijloace tehnice va putea să probeze deplasarea sa la locuința victimei, dar și prezența sa la acea locație în perioada de timp în care a avut loc decesul victimei, fiind interceptate anterior omorului convorbiri cu victima pe un ton amenințător, precum și cu alte persoane de la care a procurat același tip de armă cu care a fost ucisă victima, iar ulterior omorului fiind surprinse convorbiri în care făptuitorul manifestă o stare de panică nejustificată sau este localizat deplasându-se în afara țării imediat după comiterea faptei. La acestea putem adăuga eventuale camere de supraveghere montate în zone publice din apropierea locuinței victimei (sau din scara de bloc, montate de asociația de proprietari), care îl surprind pe făptuitor intrând și ieșind din locuința victimei. Într-o asemenea situație, apreciem că ar exista suficiente probe din supravegherea tehnică pentru a pronunța o soluție de condamnare.

Distinct față de probele obținute în procesul penal prin supravegherea tehnică, legiuitorul a inclus, în cuprinsul art. 139 alin. (3) C.pr.pen., posibilitatea obținerii de către părți a unor probe

---

[1] *Gh. Mateuț*, Tratat, vol. II, 2012, p. 35.

[2] Retractarea declarației suspectului sau inculpatului este posibilă numai atunci când a avut loc o audiere propriu-zisă a sa, retractarea trebuind să fie una justificată pentru a fi luată în seamă. A se vedea *Gr.Gr. Theodoru*, op. cit., p. 314.

[3] *M. Damaška*, Evaluation of Evidence. Pre-modern and Modern Approaches, Cambridge University Press, Cambridge, 2019, p. 69.

[4] *Gh. Mateuț*, Tratat, vol. II, 2012, pp. 34-36.

[5] *I. Neagu*, Tratat de procedură penală. Partea generală, ed. a III-a, revăzută și adăugită, Ed. Universul Juridic, București, 2013, pp. 441-442; ICCJ, s. pen., dec. nr. 3927 din 29 noiembrie 2012, nepublicată.

prin înregistrările făcute de acesta atunci când privesc propriile convorbiri sau comunicări. În doctrină s-a susținut că acest tip de înregistrări nu pot fi utilizate în scopul obținerii de probe, motivat de faptul că nu au fost efectuate cu urmărirea penală legal începută, deci în cadrul procesului penal, ci, dimpotrivă, în scopul începerii procesului penal[1]. Același autor susține că dispozițiile art. 139 alin. (3) C.pr.pen. nu ar fi constituționale, contrazicând art. 26 alin. (1) din Constituție, deoarece proba poate fi obținută prin provocare. Nu putem fi de acord cu niciuna dintre aceste opinii. Textul legal nu include necesitatea ca, în cazul înregistrărilor realizate de părți, să fie începută urmărirea penală, stabilind pe cale de excepție că orice înregistrare va constitui mijloc de probă atunci când este realizată în condițiile art. 139 alin. (3) C.pr.pen., fără alte condiționări. Faptul că la acel moment nu este începută urmărirea penală sau că prin înregistrare s-ar urmări obținerea de probe nu este de natură a face inaplicabile dispozițiile legale arătate. Dimpotrivă, dacă s-ar admite ca aceste dispoziții să fie aplicabile numai în situația propusă de autor – în cursul unei urmăriri penale, ar însemna ca partea sau persoana vătămată să aibă posibilitatea de a se substitui rolului organelor de urmărire penală sau, mai grav, de a propune ori de a accepta realizarea de înregistrări în cursul urmăririi penale, contrar dispozițiilor legale care ar impune o autorizare din partea judecătorului de drepturi și libertăți. Suntem de acord cu o altă opinie din literatura de specialitate, conform căreia legiuitorul chiar a urmărit să permită folosirea ca mijloace de probă a unor înregistrări valoroase din punct de vedere probatoriu, instituind o regulă simplă de admisibilitate, respectiv ca acestea să privească propriile convorbiri sau comunicări pe care le-au purtat cu terții[2]. În ceea ce privește provocarea la comiterea unei infracțiuni, autorul citat nu distinge cine realizează provocarea în cuprinsul art. 101 alin. (3) C.pr.pen., astfel că va constitui o provocare realizată de un privat dacă acesta ia inițiativa și procedează la provocarea unei infracțiuni în vederea tragerii la răspundere penală a unei persoane[3]. Cu toate acestea, meritele opiniei doctrinare criticate[4] constau în reflectarea existenței unei lipse de reglementare în privința înregistrărilor realizate de părți, aspect care reiese cu prisosință din lipsa limitărilor acestor înregistrări și din lipsa unui control asupra proporționalității acestora, sens în care facem trimitere la secțiunea din prezenta lucrare dedicată înregistrărilor care pot fi realizate fără autorizare[5].

În ceea ce privește valoarea probantă pe care o au metodele speciale de supraveghere tehnică în alte cauze decât cea în care s-au administrat, facem trimitere la secțiunea următoare, unde va fi analizată această problemă.

Secțiunea a 2-a. Utilizarea în altă cauză a materialului probatoriu rezultat din supraveghere tehnică

În vederea valorificării cât mai complete a rezultatelor activităților de supraveghere tehnică, legiuitorul a instituit posibilitatea ca acestea să fie folosite și într-o altă cauză penală, atunci când prezintă o asemenea relevanță. Astfel se poate ajunge ca nu numai o singură cauză – cea în care s-au autorizat mijloacele speciale de supraveghere – să beneficieze de pe urma restrângerii

[1] *S. Grădinaru*, Supravegherea tehnică, 2014, p. 188.
[2] *V. Trif*, op. cit., p. 175.
[3] *V. infra*, Titlul XIII, Capitolul V.
[4] *S. Grădinaru*, Supravegherea tehnică, 2014, p. 188.
[5] *V. supra*, Titlul III, Capitolul VII.

dreptului la viață privată al persoanelor supravegheate. Folosirea în altă cauză a rezultatelor activităților de supraveghere tehnică este prevăzută de art. 142 alin. (5) C.pr.pen., în care se arată că: „*datele rezultate din măsurile de supraveghere tehnică pot fi folosite și în altă cauză penală dacă din cuprinsul acestora rezultă date sau informații concludente și utile privitoare la pregătirea ori săvârșirea unei alte infracțiuni dintre cele prevăzute la art. 139 alin. (2) C.pr.pen.*". Dispozițiile art. 142 alin. (5) C.pr.pen. vor trebui coroborate cu dispozițiile art. 142 alin. (6) C.pr.pen., de unde rezultă că datele și informațiile provenite din activitățile de supraveghere tehnică vor fi arhivate numai în măsura în care nu sunt folosite într-o altă cauză, ceea ce reflectă că nu va fi necesar ca supravegherea să fi produs probe în cauza în care au fost dispuse măsurile[1] sau ca acestea să privească obiectul respectivei cauze.

Mai înainte de a analiza dacă prevederile legale reprezintă o ingerință suplimentară adusă vieții private sau reprezintă o metodă de obținere a probelor legitimă și loială, va trebui să analizăm ce înseamnă folosirea în altă cauză a rezultatelor supravegherii tehnice.

Prin expresia „folosirea în altă cauză", apreciem că legiuitorul a avut intenția de a se reglementa întrebuințarea rezultatelor supravegherii tehnice într-o cauză penală diferită față de cea în care s-a dispus supravegherea tehnică. Prin „cauză diferită" nu vom înțelege numai o infracțiune diferită de cea care face obiectul urmăririi penale, ci o altă cauză constituită într-un alt dosar de urmărire penală. Considerăm că nu vor fi aplicate dispozițiile art. 142 alin. (5) C.pr.pen. în situația în care rezultatele supravegherii tehnice se folosesc în aceeași cauză, chiar dacă din acestea se constată săvârșirea unor infracțiuni care nu făceau obiectul inițial al urmăririi penale. Într-o atare situație, procurorul va fi în măsură să extindă urmărirea penală cu privire la noua infracțiune constatată și apoi să dispună, după caz, disjungerea cauzei, situație în care probele care rezultă din supravegherea tehnică vor fi în mod valabil administrate în cauza disjunsă. Credem că, pentru a fi considerată legală o asemenea folosire a măsurilor de supraveghere tehnică, se impune ca infracțiunea constatată să fie una flagrantă, să fie dintre cele prevăzute de art. 139 alin. (2) C.pr.pen. și ca din supravegherea tehnică să rezulte probe directe cu privire la săvârșirea sa. Sub acest aspect, reglementarea de la art. 293 C.pr.pen. privind constatarea infracțiunii flagrante poate justifica o obținere de probe în afara procesului penal, într-o asemenea situație constituind o excepție de la prevederile art. 97 alin. (2) C.pr.pen.[2]. În alte cazuri, astfel cum vom vedea mai jos, datele și informațiile obținute vor putea fi folosite numai în vederea sesizării organelor de urmărire penală.

O ipoteză interesantă reflectată de doctrină este posibilitatea folosirii unor probe rezultate din supravegherea tehnică pentru dovedirea unor infracțiuni pentru care nu se poate dispune autorizarea supravegherii tehnice atunci când fie cauza privește atât infracțiuni care intră sub incidența art. 139 alin. (2) C.pr.pen., cât și infracțiuni care nu intră, precum și situația în care se descoperă infracțiuni care nu ar putea fi cercetate prin supravegherea tehnică[3]. S-a considerat că, într-o astfel de situație, organele de urmărire penală nu ar putea proceda la folosirea probelor, întrucât s-ar face cu încălcarea dispozițiilor art. 139 alin. (2) C.pr.pen., care nu ar fi permis supravegherea tehnică în cauză dacă obiectul acesteia ar fi fost numai infracțiunea care nu intra sub incidența acestui text de lege. Opinia arătată a fost acceptată și de alți autori[4],

[1] *Gh. Mateuț*, Procedură penală, 2019, p. 705.

[2] *M. Bulancea, A. Șinc*, în M. Udroiu (coord.), Codul de procedură penală, 2017, p. 1322.

[3] *M.V. Tudoran*, Teoria și practica interceptărilor, 2012, pp. 68-69.

[4] *M. Bulancea, R. Slăvoiu*, în M. Udroiu (coord.), Codul de procedură penală, 2017, p. 695.

în opinia noastră, ea fiind corectă față de caracterul excepțional și derogatoriu al metodelor speciale de supraveghere tehnică[1].

O situație aparte este dacă prin supravegherea tehnică se descoperă săvârșirea unei infracțiuni flagrante pentru care legea prevede sesizarea la plângerea prealabilă a organelor de urmărire penală, caz în care caracterul secret al operațiunii vine în contradicție cu obligația organelor de urmărire penală de a se sesiza asupra infracțiunii flagrante și a de a chema, în temeiul art. 298 alin. (2) C.pr.pen., persoana vătămată pentru a declara dacă formulează plângere prealabilă. Situația prezentată este directa urmare a lipsei de prevedere din partea legiuitorului de a exclude din sfera supravegherii tehnice infracțiunile urmărite, la plângere prealabilă, nefiind suficient criteriul limitelor de pedeapsă. De pildă, infracțiunea de viol în formă simplă prevăzută de art. 218 C.pen. se va urmări la plângere prealabilă, deși limitele de pedeapsă sunt de la 3 ani la 10 ani. Față de modalitățile concrete pe care le poate îmbrăca infracțiunea de viol, este posibilă situația în care victima să nu cunoască persoana care a comis infracțiunea sau să cunoască săvârșirea acesteia, probele putând rezulta, de pildă, din înregistrările în mediu ambiental dispuse în cauză.

În literatura de specialitate au fost aduse argumente cu privire la folosirea unor înregistrări obținute din supravegherea tehnică într-o cauză civilă, susținându-se că, potrivit dispozițiilor Codului de procedură civilă, astfel de probe ar fi admisibile în conformitate cu art. 341 alin. (2) C.pr.civ.[2]. O atare situație nu poate fi concepută, fiind încălcate dispozițiile legale menționate, întrucât legea procesuală penală limitează folosirea rezultatelor activităților de supraveghere tehnică numai în cauze penale. A considera altfel ar însemna deturnarea scopului pentru care s-a autorizat măsura, ceea ce ar invalida iremediabil proporționalitatea sa prin raportare la scopul procesului civil. Ținând seama de acesta, instanța civilă ar trebui să constate că probele au fost obținute prin încălcarea legii, contrar art. 341 alin. (2) C.pr.civ.[3]. Alta va fi situația în cazul în care probele reies din înregistrări private, fără autorizare, realizate în temeiul art. 139 alin. (3) C.pr.pen.

O *folosire într-o altă cauză* este condiționată de gravitatea și natura infracțiunii săvârșite, potrivit art. 142 alin. (5) C.pr.pen., putând fi folosite datele sau informațiile obținute numai dacă privesc pregătirea ori săvârșirea unei infracțiuni dintre cele prevăzute la art. 139 alin. (2) C.pr.pen.[4]. Condiționarea este dată numai de unul dintre criteriile de autorizare prevăzute de art. 139 C.pr.pen., în situația folosirii datelor și informațiilor într-o altă cauză, nemaifiind analizate celelalte condiții legale pentru autorizarea supravegherii tehnice. În sensul celor

[1] *Gh. Mateuț*, Procedură penală, 2019, p. 705.

[2] *V. Trif*, op. cit., p. 173.

[3] Potrivit art. 341 alin. (2) C.pr.civ., „sunt, de asemenea, mijloace materiale de probă și fotografiile, fotocopiile, filmele, discurile, benzile de înregistrare a sunetului, precum și alte asemenea mijloace tehnice, dacă nu au fost obținute prin încălcarea legii ori a bunelor moravuri".

[4] Reamintim că dispozițiile legale ale art. 139 alin. (2) C.pr.pen. prevăd: „Supravegherea tehnică se poate dispune în cazul infracțiunilor contra securității naționale prevăzute de Codul penal și de legi speciale, precum și în cazul infracțiunilor de trafic de droguri, de efectuare de operațiuni ilegale cu precursori sau cu alte produse susceptibile de a avea efecte psihoactive, infracțiunilor privind nerespectarea regimului armelor, munițiilor, materialelor nucleare și al materiilor explozive și al precursorilor de explozivi restricționați, de trafic și exploatarea persoanelor vulnerabile, acte de terorism, de spălare a banilor, de falsificare de monede, timbre sau de alte valori, de falsificare de instrumente de plată electronică, în cazul infracțiunilor care se săvârșesc prin sisteme informatice sau mijloace de comunicare electronică, contra patrimoniului, de șantaj, de viol, de lipsire de libertate în mod ilegal, de evaziune fiscală, în cazul infracțiunilor de corupție și al infracțiunilor asimilate infracțiunilor de corupție, infracțiunilor împotriva intereselor financiare ale Uniunii Europene ori în cazul altor infracțiuni pentru care legea prevede pedeapsa închisorii de 5 ani sau mai mare".

arătate, se reține în literatura de specialitate că: „*menținerea prevederii care înfățișează extinderea rezultatelor supravegherii numai pentru infracțiunile predeterminate de legiuitor nu credem că este suficientă pentru a elimina riscul utilizării lor abuzive, în detrimentul drepturilor și libertăților fundamentale ale persoanei interesate*"[1]. Același autor a arătat că, alături de elementul de gravitate, legiuitorul a mai instituit o condiție ca datele și informațiile obținute să fie concludente și utile, condiție care ține de posibilitatea lor de a contribui la stabilirea elementelor de fapt[2].

În doctrină s-a constatat că folosirea într-o altă cauză a datelor și informațiilor rezultate din supravegherea tehnică reprezintă o problemă deosebită, deoarece pune serioase semne de întrebare cu privire la asigurarea proporționalității dintre ingerința adusă dreptului la viață privată și scopul urmărit[3]. În opinia noastră, este evident că, în ipoteza prevăzută de art. 142 alin. (5) C.pr.pen., folosirea rezultatelor activităților de supraveghere tehnică într-o altă cauză nu va trece printr-un filtru al judecătorului de drepturi și libertăți, neexercitându-se un control de legalitate privind existența unei suspiciuni rezonabile, proporționalitate și subsidiaritate. Fără un atare control, nu există niciun motiv pentru a crede că o astfel de măsură ar fi fost autorizată în mod independent de către judecătorul de drepturi și libertăți. Încheierea inițială a judecătorului de drepturi și libertăți nu poate justifica decât îndeplinirea condițiilor legale cu privire la obținerea probelor în cauza inițială, nu și într-o altă cauză. Ca atare, procedura instituită de art. 142 alin. (5) C.pr.pen. poate fi privită ca un mijloc pentru ca procurorul să poată eluda dispozițiile legale privind autorizarea supravegherii tehnice. Într-o opinie cu care nu suntem de acord, s-a apreciat că probele pot fi folosite valabil într-o altă cauză, fără limitări, problema existenței unei autorizări în respectiva cauză fiind nefondată și că aceasta ar constitui o pierdere de timp[4]. Tocmai aceasta este gândirea pragmatică și polițienească față de care nu putem să ne exprimăm decât rezerve grave, întrucât motivele de eficiență vor veni în contradicție cu respectarea drepturilor omului, dar și a legii, ignorându-se scopul autorizării inițiale.

O soluție pe care o propune doctrina este instituirea unei proceduri prealabile folosirii rezultatelor supravegherii tehnice într-o altă cauză, prin acordarea unui rol judecătorului de drepturi și libertăți în acest sens, care va decide asupra admisibilității lor într-o altă cauză printr-un control de proporționalitate[5]. În esență, autorul citat propune ca, mai înainte de a fi folosite în altă cauză, procurorul va trebui să obțină o autorizare în acest sens de la judecătorul de drepturi și libertăți, constituindu-se o garanție în plus pentru respectarea dreptului la viață, în condițiile insuficienței controlului *a posteriori*, care se va desfășura în camera preliminară, chiar și dacă acesta va avea loc în cauza în care au fost transferate rezultatele supravegherii tehnice[6]. Deși considerăm că propunerea autorului identifică probleme valide și ar fi preferabilă situației reglementării actuale, nu putem fi de acord cu soluția propusă. Atât timp cât judecătorul de drepturi și libertăți are acces direct asupra datelor rezultate în urma supravegherii tehnice, el poate fi tentat să autorizeze folosirea lor într-o altă cauză, bazându-se pe o evaluare a valorii lor probante. Întotdeauna când se va evalua legalitatea unei măsuri de supraveghere tehnică, este necesar ca judecătorul să se pună în situația inițială și să verifice dacă la acel moment erau îndeplinite condițiile legale, altfel percepția sa poate fi afectată de un

[1] *Gh. Mateuț*, Procedură penală, 2019, p. 705.

[2] *Ibidem*.

[3] *S. Grădinaru*, Supravegherea tehnică, 2014, p. 186.

[4] *S. Șerb, P. Ungureanu*, Considerations on the use of technical surveillance in criminal proceedings, în Acta Universitatis George Bacovia, vol. 5, no. 2/2016, p. 4.

[5] *Gh. Mateuț*, Procedură penală, 2019, p. 706.

[6] CCR, Dec. nr. 855 din 14 decembrie 2017 (M. Of. nr. 150 din 16 februarie 2018) (decizie de respingere).

rezultat amplu al supravegherii tehnice și să aprecieze că măsura era proporțională numai prin raportare la rezultatul obținut.

Nu considerăm că o autorizare prealabilă ar putea fi una eficientă în condițiile arătate mai sus, impunându-se ca dispozițiile art. 142 alin. (5) C.pr.pen. să fie abrogate pentru a se împiedica o ingerință sporită în viața privată a unei persoane care nu poate fi supusă unui control prealabil de proporționalitate, în același sens fiind și unele opinii din literatura de specialitate[1]. Într-o opinie contrară, cu care nu suntem de acord, s-a susținut că dispozițiile art. 142 alin. (5) C.pr.pen. nu încalcă dreptul la apărare al inculpatului care nu poate invoca faptul că ar fi fost în imposibilitate de a demonstra că înregistrările sunt nejustificate sau neîntemeiate[2]. Problema reflectată în această din urmă opinie confirmă cele enunțate mai sus, întrucât instanțele vor avea o tendință de a conduce analiza rezultatelor supravegherii tehnice din perspectiva temeiniciei ori acest lucru este nelegal, întrucât filtrul va trebui să fie unul de legalitate, nefiind importantă semnificația și relevanța probelor obținute atât timp cât nu se asigură garanții suficiente privind proporționalitatea și subsidiaritatea obținerii lor. Bunăoară, art. 8 par. 2 Conv.EDO limitează posibilitatea legală de autorizare a mijloacelor de supraveghere tehnică de condițiile afirmate de noi, și nu de caracterul temeinic al probelor care pot rezulta.

Analizând mai departe art. 142 alin. (5) C.pr.pen., observăm că legiuitorul se referă la folosirea în alte cauze penale a *datelor și informațiilor* rezultate din activitățile de supraveghere tehnică. În literatura de specialitate s-a exprimat opinia potrivit căreia modul de exprimare al legiuitorului nu poate conduce la ideea că aceste date și informații ar trebui să poată fi considerate probe, putând eventual sta la baza unei sesizări din oficiu a organelor de urmărire penală, existând o diferență fundamentală între cele două noțiuni[3]. Din acest punct de vedere, considerăm că se poate admite ca valoarea rezultatelor supravegherii tehnice să fie una diminuată, fiind utilă doar sesizării organelor de urmărire penală, ulterior putând fi administrate probe cu privire la respectiva infracțiune, dar se impune ca legiuitorul să prevadă în mod clar că ele nu vor putea fi folosite ca probe. Avem suspiciunea că, prin formularea neadecvată a art. 142 alin. (5) C.pr.pen., legiuitorul a urmărit, în realitate, ca datele și informațiile rezultate din supravegherea tehnică să fie folosite ca probe în alte cauze penale, o situație care, după cum am arătat mai sus, ar fi în disonanță cu respectarea dreptului la viață privată al unei persoane, sens în care apreciem în continuare că se impune, *de lege ferenda*, abrogarea dispozițiilor legale criticate. Până la acel moment, în vederea respectării drepturilor fundamentale ale persoanelor supuse măsurilor de supraveghere tehnică, se impune ca datele și informațiile rezultate din supravegherea tehnică să poate constitui doar simple informații care vor putea sta la baza doar a sesizării din oficiu a organelor de urmărire penală.

Secțiunea a 3-a. Contestarea legalității administrării probelor obținute prin supravegherea tehnică

Pentru a se asigura desfășurarea în mod legal a actelor de urmărire penală și a administrării probelor în cursul urmăririi penale, legiuitorul a prevăzut o fază distinctă a procesului, denumită „camera preliminară", având menirea de a pregăti cauza în vederea exercitării funcției

[1] *S. Grădinaru*, Supravegherea tehnică, 2014, p. 186.
[2] Trib. Cluj, s. pen., încheierea nr. 63/CP/2016, *apud V. Trif*, op. cit., p. 172.
[3] *Gh. Mateuț*, Procedură penală, 2019, p. 705.

de judecată, urmând ca, în exercitarea acesteia, instanței să îi rămână să se preocupe numai de aspectele de fond ale acuzației[1]. În acest scop stau atât avantajele, cât și dezavantajele reglementării procedurii camerei preliminare. Ca avantaj, teoretic, aducea celeritate desfășurării procesului penal. Ca dezavantaj, punea părțile în imposibilitatea contestării legalității actelor de urmărire penală sau a administrării probelor după un anumit moment procesual. Ambele sunt dovedite ca fiind neadevărate în prezent, camera preliminară a prelungit în mod nepermis toate procesele penale, dezideratul de la art. 343 C.pr.pen. privind durata maximă de 60 de zile nu poate fi atins, mai ales în condițiile motivelor de nelegalitate invocate în privința supravegherii tehnice.

În ceea ce privește contestarea actelor de urmărire penală și a probelor administrate în cursul urmăririi penale, tocmai aspectele privind nelegalitatea metodelor speciale de supraveghere au dovedit caracterul insuficient al fazei camerei preliminare pentru a putea proteja părțile de consecințele unei urmăriri penale viciate.

Insuccesul reglementării camerei preliminare a fost subliniat de practica judiciară care a fost pusă în situația de a pronunța hotărâri, ținând seama, în mod obligatoriu, de probe obținute cu încălcarea separației puterilor în stat și ca urmare a implicării serviciilor de informații în activitatea de punere în executare a mandatelor de supraveghere tehnică[2]. Abia după pronunțarea Deciziei Curții Constituționale nr. 302/2017 privind neconstituționalitatea dispozițiilor art. 281 alin. (1) lit. b) din Codul de procedură penală care nu includeau necompetența materială și personală a organelor de urmărire penală între cazurile de nulitate absolută, instanțele au putut cenzura aceste nelegalități, ulterior fazei camerei preliminare.

În prezenta secțiune nu ne vom referi la posibilitatea contestării legalității supravegherii de către persoanele care nu au calitate procesuală în cauză și care au făcut obiectul unui mandat de supraveghere, această problemă fiind tratată anterior în prezenta lucrare prin prisma efectelor Deciziei nr. 244/2017 a Curții Constituționale[3].

§1. Contestarea legalității supravegherii tehnice în camera preliminară

Conform art. 342 C.pr.pen., „*obiectul procedurii camerei preliminare îl constituie verificarea, după trimiterea în judecată, a competenței și a legalității sesizării instanței, precum și verificarea legalității administrării probelor și a efectuării actelor de către organele de urmărire penală*", din perspectiva metodelor speciale de supraveghere, fiind de interes faptul că în această fază se va putea invoca nelegalitatea administrării probelor prin acest procedeu probatoriu. Nelegalitatea probelor poate fi invocată pe calea *cererilor și excepțiilor* în procedura de cameră preliminară, judecătorul de cameră preliminară având competența de a verifica legalitatea administrării probelor, conform art. 54 lit. b) C.pr.pen.

În faza camerei preliminare se va putea proceda inclusiv la contestarea legalității încheierii prin care judecătorul de drepturi libertăți a dispus autorizarea măsurilor de supraveghere tehnică, chiar dacă aceasta are un caracter definitiv[4]. La această concluzie se poate ajunge prin prisma atât a obiectului camerei preliminare prevăzut de art. 342 C.pr.pen. (verificarea

[1] *I. Kuglay*, în M. Udroiu (coord), op. cit., p. 1413.

[2] *I. Bălan*, Efectuarea supravegherii tehnice. Proba neconstituțională. Studiu de jurisprudență, în Pandectele Române nr. 4/2019, p. 27.

[3] *V. supra*, Titlul III, Capitolul VI.3.

[4] *R.M. Pintea*, Unele aspecte controversate privind legalitatea probelor obținute prin supravegherea tehnică, în Revista Themis nr. 2/2018, p. 37, pe *inm-lex.ro/revista-themis*

legalității administrării probelor), cât mai ales ca urmare a dezlegărilor Curții Constituționale prin Decizia nr. 244/2017. În acest sens s-a pronunțat și instanța supremă într-o cauză[1], chiar înainte de a se pronunța Curtea Constituțională. Înainte de pronunțarea Deciziei nr. 244/2017 a Curții Constituționale, unii judecători de cameră preliminară au respins posibilitatea atacării încheierii de autorizare pronunțată de judecătorul de drepturi și libertăți, apreciind că aceasta depășește obiectul camerei preliminare[2]. Chiar și la momentul respectivei soluții, se impunea aplicarea jurisprudenței obligatorii a Curții Europene a Drepturilor Omului pentru ca judecătorul de cameră preliminară să constate că se impune analizarea în cameră preliminară a încheierii de autorizare[3].

Totodată, se va putea contesta caracterul legal atât al actelor prin care s-a dispus punerea în executare, cât și în privința efectivei puneri în executare, care va trebui să fie exercitată în limitele mandatului judecătorului de drepturi și libertăți sau ordonanței de autorizare provizorie a procurorului.

Vor putea fi invocate și cereri și excepții privind activitatea de consemnare a rezultatelor supravegherii tehnice, însă numai cu privire la legalitatea acestora[4]. Conținutul acestora nu va putea fi contestat în faza camerei preliminare, presupunând un control de temeinicie care nu poate fi exercitat decât de instanță, prin verificarea veridicității celor consemnate față de rezultatele supravegherii tehnice de pe copia suportului de stocare prin audierea sau vizualizarea acestora[5].

§2. Contestarea legalității supravegherii tehnice în cursul judecății în primă instanță și în apel

Codul de procedură penală prevede anumite limitări privind contestarea legalității administrării probelor în afara camerei preliminare. Dacă la intrarea în vigoare a Codului, instanțele erau reticente în a permite un control de legalitate asupra probelor după parcurgerea fazei camerei preliminare, în jurisprudența recentă, mai ales ca urmare a consecințelor Deciziei nr. 51/2016 și a Deciziei nr. 302/2017 pronunțate de Curtea Constituțională, jurisprudența instanțelor s-a schimbat, soluțiile menționate permițând invocarea nulităților și în afara camerei preliminare.

Ținând cont de regimul nulităților, în faza de judecată în primă instanță, dar și în faza apelului vor putea fi invocate numai încălcări ale dispozițiilor legale ce vor atrage nulitatea absolută, întrucât textul art. 282 alin. (4) lit. a) C.pr.pen. limitează invocarea nulității relative a unui act realizat în cursul urmăririi penale până la închiderea procedurii camerei preliminare. Dincolo de acest moment procesual, orice nulitate relativă invocată ar urma să se considere ca fiind acoperită ca urmare a neinvocării ei în termenul legal, potrivit art. 282 alin. (5) lit. a) C.pr.pen.

Motivul cel mai des întâlnit pentru invocarea nulității absolute în cursul judecății îl reprezintă necompetența organului care a pus în executare supravegherea tehnică, contrar dispozițiilor

[1] ICCJ, s. pen., dec. nr. 3147 din 12 decembrie 2014, nepublicată.

[2] C. Ap. București, s. a II-a pen., încheierea din 4 martie 2016, menținută prin încheierea nr. 726 din 18 martie 2016 a ICCJ, s. pen.

[3] CEDO, cauza *Matheron c. Franța*, Hotărârea din 29 iunie 2005, §40.

[4] *R. Slăvoiu*, Verificarea legalității procedeelor probatorii în camera preliminară, în Dreptul nr. 1/2018, pp. 151-152.

[5] *S. Grădinaru*, Supravegherea tehnică, 2014, p. 146.

art. 142 alin. (1) C.pr.pen., ca urmare a realizării acestui act de procedură de către *„alte organe specializate ale statului*".

În privința posibilității invocării nulității absolute în cursul cercetării judecătorești, această posibilitate a fost recunoscută de instanțe, pronunțându-se prin admiterea unor asemenea cereri formulate de apărare cu rezultatul înlăturării probelor obținute în urma supravegherii tehnice[1]. O atare abordare o apreciem ca fiind corectă, întrucât permite apărării să cunoască dacă probele adunate împotriva sa de către acuzare vor putea fi folosite în cursul judecății la soluționarea fondului cauzei.

În funcție de consecințele pe care le poate avea constatarea nulității absolute a măsurilor de supraveghere desfășurate în cursul urmăririi penale – în special atunci când probele care rezultă sunt determinante sau cel puțin considerate ca fiind determinante de către acuzare[2], o să difere hotărârea prin care se va constata nelegalitatea lor. Dacă ele vor avea caracter determinant, instanțele vor fi tentate să constate nelegalitatea probelor odată cu pronunțarea asupra fondului cauzei. Nu considerăm că o astfel de abordare este una în spiritul garantării dreptului la apărare al acuzaților, întrucât forțează apărarea să își formeze concluziile și cererile pe probe a căror eliminare din cadrul procesului penal este incertă până la soluția pronunțată în cauză, mai ales în situația în care cauza se află în cale de atac. Într-o interpretare a Deciziei Curții Constituționale nr. 250/2019[3], considerăm că argumentele reținute de Curte în privința schimbării încadrării juridice a faptelor se pot aplica și în această situație, întrucât cunoașterea în întregime a probelor care se rețin ca dovedind vinovăția unei persoane are un rol determinant în modul în care își va exercita apărarea și asupra poziției procesuale pe care o va adopta.

În concluzie, posibilitatea invocării nelegalității supravegherii tehnice își găsește plenitudinea de aplicare în faza camerei preliminare, iar, în cazul fazei de judecată, posibilitatea de contestare se restrânge numai la încălcările care vor atrage sancțiunea nulității. În următoarea secțiune, vom aborda problema sancțiunilor incidente în privința supravegherii tehnice și vom realiza o analiză a posibilelor ipoteze care pot apărea în procesul penal și a efectelor pe care le produce nulitatea asupra mijloacelor de probă.

Secțiunea a 4-a. Sancțiunile procesuale în cazul obținerii probelor în mod nelegal

De la debutul prezentului proiect de cercetare, legislația română a cunoscut mai multe modificări legislative cauzate de pronunțarea unor decizii ale Curții Constituționale, prin care au fost constatate ca fiind neconstituționale dispoziții legale ori interpretări ale legii, cu influență deosebită privind sancțiunile procesuale.

În literatura de specialitate, sancțiunea procesuală a fost definită ca fiind mijlocul legal care lipsește de efecte juridice actele procesuale și procedurale, precum și măsurile efectuate ori,

[1] Jud. Baia Mare, s. pen., încheierea din 23 septembrie 2019, pronunțată în dosar nr. 3879/337/2015, nepublicată.

[2] C. Ap. Oradea, s. pen. și pentru cauze cu minori, dec. nr. 703 din 20 decembrie 2019, pronunțată în dosar nr. 4630/83/2006**, nepublicată; C. Ap. București, s. a II-a pen., dec. nr. 1123/A din 18 septembrie 2019, pronunțată în dosar nr. 18875/3/2012, nepublicată.

[3] CCR, Dec. nr. 250 din 16 aprilie 2019 (M. Of. nr. 500 din 20 iunie 2019).

după caz, dispuse în mod ilegal sau care se aplică în cazul comiterii unei abateri judiciare[1]. Ea va avea ca efect imposibilitatea folosirii în procesul penal a probelor obținute în mod nelegal, ca urmare a excluderii acestora.

În literatura de specialitate străină au fost identificate mai multe abordări în privința regulilor de excludere a probelor obținute în mod nelegal. O primă abordare a regulilor de excludere este cea disciplinară, funcționând potrivit principiului prevenirii unei viitoare încălcări a legii de către organele de urmărire penală, mizând pe ideea că excluderea unei probe în urma constatării nelegalității ei, prin prisma gravității sancțiunii, va preveni încălcări viitoare[2]. Acest sistem este întrebuințat în S.U.A., unde excluderea probelor obținute în mod nelegal sau neloial are scop preventiv. Această abordare se bazează pe noțiunea unei excluderi automate, asigurând organul care încalcă legea în administrarea probei că nu va putea vreodată să folosească proba împotriva unei persoane, fiind determinată prin aceasta să respecte legea[3]. Reguli de excludere automată cu acest scop pot fi întâlnite în mai multe state, precum: Irlanda, Italia, Germania, Grecia, Spania, Rusia, Ungaria și Turcia[4].

A doua abordare o constituie cea prin care sancțiunea este văzută ca un remediu, în care instanțele urmăresc ca, prin excluderea probelor obținute în mod nelegal, persoana acuzată să fie pusă înapoi în poziția inițială, în care nu erau încălcate drepturile sale[5]. Excluderea în scop de remediu și excluderea în scop disciplinar-preventiv constituie abordări diferite, prima operând în funcție de lezarea drepturilor apărării, iar cea de-a doua operând și prin raportare la buna-credință a organelor de urmărire penală, în cel din urmă caz putând fi menținute probe ca urmare a faptului că încălcarea nu s-a comis cu rea-credință[6]. Sancțiunea remediului și excluderea probelor obținute în mod nelegal ca un remediu este abordarea aflată în conformitate cu legea română și cu abordările doctrinare naționale.

A treia abordare posibilă este specifică sistemului englez ca soluție, dar subliniază necesitatea ca justiția să fie văzută ca legitimă și integră în fața publicului. Argumentul expus este că dacă o instanță se va folosi de probele obținute în mod nelegal, își va submina statutul moral de a-l putea judeca pe acuzat. În esență, dacă instanța ar permite folosirea probelor obținute în mod nelegal și persoana acuzată ar fi condamnată, s-ar ajunge ca, prin același act, instanța să condamne încălcarea legii (de către acuzat), dar să și ierte o încălcare a ei (în cazul probelor obținute în mod nelegal)[7]. Sub imperiul acestei gândiri, în unele situații de obținere a probelor în mod nelegal (precum provocarea la săvârșirea unei infracțiuni), sistemul englez include și o soluție care blochează desfășurarea unui proces penal împotriva acuzatului (*stay of process*), întrucât: *i)* procesul ar aduce atingere simțului de justiție și corectitudine al instanței; *ii)* desfășurarea procesului ar submina încrederea publică în sistemul de justiție și l-ar dezonora; *iii)* refuzul unui *stay of process* ar conduce la degradarea legalității administrării actului de justiție[8]. În principiu, suntem de acord cu aceste consecințe, însă sistemul român este reglementat într-un mod diferit, nepermițând o asemenea putere judecătorului de cameră

[1] *Gh. Mateuț*, Procedură penală, 2019, p. 991.

[2] *A. Ashworth, M. Redmayne*, The Criminal Process, 2014, p. 344.

[3] *K.-H. Hsieh*, The Exclusionary Rule of Evidence. Comparative Analysis and Proposals for Reform, Ed. Ashgate, Farnham, 2014, p. 56.

[4] *A. Ashworth, M. Redmayne*, The Criminal Process, 2014, p. 57.

[5] *Ibid*em, p. 345.

[6] *Ibidem*.

[7] *Ibidem*, p. 346.

[8] *C. Wells*, op. cit., p. 8.

preliminară care, de pildă, are posibilități extrem de limitate în a împiedica procedura desfășurată împotriva inculpatului de a nu continua prin începerea judecății, chiar în situația insuficienței probelor legal administrate.

În dreptul român, sancțiunea incidentă în cazul nerespectării dispozițiilor legale privind autorizarea, punerea în executare și consemnarea supravegherii tehnice este nulitatea. Aceasta va putea afecta procedeul probatoriu, actele efectuate în cadrul acestuia și mijloacele de probă obținute. Proba, în conformitate cu art. 102 alin. (3) C.pr.pen., va fi exclusă în urma constatării nulității actului prin care s-a autorizat administrarea ei sau prin care s-a administrat.

Alături de nulitate, mai poate fi incidentă și sancțiunea decăderii, în situația nerespectării obligației procurorului de a supune confirmării judecătorului de drepturi și libertăți, în termen de 24 de ore, măsura autorizării provizorii a supravegherii tehnice, conform art. 141 alin. (3) C.pr.pen. Întrucât această procedură, precum și sancțiunea specifică au fost deja analizate într-o secțiune precedentă, facem trimitere la explicațiile care au fost date anterior[1].

O altă potențială sancțiune procesuală poate fi cea incidentă în cazul supravegherii tehnice a raportului profesional dintre avocat și persoana pe care o asistă sau reprezintă (clientul său), dispozițiile art. 139 alin. (4) C.pr.pen. stabilind că *probele obținute nu pot fi folosite în cadrul niciunui proces penal, urmând a fi distruse*. Această sancțiune nu are o reglementare juridică concretă, în plus, aparent, afectează proba, și nu actul procedural. Credem că această situație este incomplet reglementată, actul procedural trebuind să fie lovit de nulitate relativă, după cum am arătat într-o secțiune anterioară[2].

În jurisprudența sa, Curtea Constituțională a constatat că: „*nulitatea este definită ca fiind acea sancțiune procesuală constatată și aplicată de un organ judiciar, care atrage nevalabilitatea actelor procesuale și procedurale efectuate cu încălcarea dispozițiilor legale care reglementează desfășurarea procesului penal, dacă s-a produs o vătămare dovedită sau prezumată de lege, ce nu poate fi înlăturată decât prin desființarea actului, organul judiciar dispunând refacerea acestuia atunci când este necesar și dacă este posibil*"[3].

Rolul nulității este unul deosebit în procesul penal, reprezentând o garanție privind respectarea dispozițiilor legale, prevenind încălcarea lor prin caracterul distructiv față de actul nelegal al sancțiunii. După cum se spunea în literatura de specialitate, „*fără sancțiunea nulității, regulele procesuale ar fi simple recomandări, fără forță coercitivă de aplicațiune sau de remediere a consecințelor neobservării lor*"[4]. În jurisprudența Curții Constituționale, s-a subliniat acest rol și scop al nulităților, reținându-se că „*nulitățile actelor procesuale și procedurale ocupă un loc important în sfera garanțiilor ce asigură efectivitatea principiului legalității procesului penal și a principiului aflării adevărului, fiind menite să înlăture încălcările normelor de procedură care au intervenit cu ocazia dispunerii unui act procesual sau a ducerii la îndeplinire a unui act procedural, precum și consecințele negative pe care aceste încălcări le-au produs în procesul penal. Nulitățile îndeplinesc astfel un scop preventiv – de preîntâmpinare a încălcării legii, un rol sancționator – de desființare a actelor efectuate cu încălcarea legii, precum și un scop reparator – de refacere a actelor procesuale și procedurale desființate, dacă este necesar și posibil*"[5].

---

[1] *V. supra*, Titlul III, Capitolul II.3.

[2] *V. supra*, Titlul III, Capitolul VIII.2.

[3] CCR, Dec. nr. 554 din 19 septembrie 2017, §15 (M. Of. nr. 1013 din 21 decembrie 2017).

[4] *Tr. Pop*, Drept procesual penal. Partea generală, Vol. III, Tipografia Națională Cluj S.A., reeditare anastatică Ed. Universul Juridic, București, 2019, p. 60.

[5] CCR, Dec. nr. 554/2017, §14.

În prezenta secțiune vom analiza formele nulități care pot interveni ca urmare a nerespectării dispozițiilor legale în privința măsurilor de supraveghere tehnică.

§1. Nulitatea absolută a măsurilor de supraveghere tehnică

Nulitatea absolută constituie o sancțiune care va interveni în cazul încălcării unor dispoziții legale care au o importanță deosebită în desfășurarea procesului penal[1], spre deosebire de nulitățile relative, vătămarea procesuală fiind prezumată *iuris et de iure*[2].

Din perspectiva incidenței cazurilor de nulitate absolută, în privința supravegherii tehnice, vor fi operante numai unele dintre acestea, ținând cont de caracteristicile procedeului probatoriu. Astfel, nu vor putea fi incidente cazurile de nulitate absolută prevăzute de art. 281 alin. (1) lit. c), e) sau f) C.pr.pen. Procedura de autorizare a supravegherii tehnice se judecă, potrivit art. 140 alin. (3) C.pr.pen., în camera de consiliu (astfel nu este un caz de publicitate al ședinței de judecată)[3], fiind realizată fără citarea sau participarea părților, nu este un caz de prezență obligatorie a suspectului sau inculpatului și nici nu se va asigura asistența juridică obligatorie a părților (care nu pot fi prezente).

În ceea ce privește art. 281 alin. (1) lit. a) C.pr.pen. privind compunerea completului de judecată, apreciem că acest caz de nulitate absolută poate fi incident și față de judecătorul de drepturi și libertăți care dispune asupra propunerii de autorizare a măsurilor de supraveghere tehnică[4]. Cazul de nulitate poate fi incident atunci când nu se poate determina care a fost componența completului care s-a pronunțat asupra supravegherii tehnice, întrucât încheierea prin care s-a autorizat măsura este nesemnată sau nu s-a întocmit minuta conform art. 140 alin. (4) teza finală C.pr.pen. Sub acest aspect vor fi aplicabile, prin analogie, dezlegările Înaltei Curți de Casație și Justiție cuprinse în Decizia nr. 17/2005[5], în care s-a statuat că omisiunea întocmirii minutei de către judecătorul care se pronunță asupra măsurilor preventive se va sancționa cu nulitatea absolută a actului. După cum se arată în cuprinsul deciziei citate: „*minuta leagă instanța și constituie o garanție că la redactarea încheierii nu se va omite, adăuga sau schimba ceva privind soluția și, de aceea, în special în cazul încheierilor care pot fi atacate separat cu recurs, cum sunt cele mai multe dintre încheierile prin care judecătorul sau instanța se pronunță asupra măsurilor preventive, se impune ca rezultatul deliberării să fie consemnat într-o minută*".

În același timp, nesemnarea mandatului de supraveghere va atrage tot nulitatea absolută a acestui act, întrucât nu se poate proceda la verifica existenței unei autorizații din partea unui judecător de drepturi și libertăți în lipsa acestei mențiuni și nici nu se poate dovedi care a fost constituirea completului (judecătorul de drepturi și libertăți care s-a pronunțat asupra autorizării). O atare omisiune va atrage nulitatea absolută nu numai a mandatului de supraveghere, dar și nelegalitatea procedeului probatoriu realizat în temeiul respectivului mandat.

În cazul nulității absolute prevăzute de art. 281 alin. (1) lit. b) C.pr.pen., sunt incidente două situații posibile: *i)* necompetența materială și personală a judecătorului de drepturi și libertăți care încuviințează măsurile de supraveghere tehnică; *ii)* necompetența materială sau

[1] *Gh. Mateuț*, Procedură penală, 2019, p. 1003.

[2] CCR, Dec. nr. 302 din 4 mai 2017, §32.

[3] În sens contrar, *M.V. Tudoran*, Teoria și practica interceptărilor, 2012, p. 131. S-a susținut că desfășurarea procedurii de autorizare în ședință publică ar conduce la nulitatea absolută a actului de autorizare.

[4] *Gh. Mateuț*, Procedură penală, 2019, p. 1004.

[5] ICCJ, Secțiile Unite, Dec. nr. 17 din 21 noiembrie 2005 (M. Of. nr. 119 din 8 februarie 2006).

personală a organului de urmărire penală care pune în executare supravegherea tehnică sau consemnează rezultatele activităților de supraveghere tehnică.

Judecarea propunerii de autorizare a măsurilor de supraveghere tehnică de către un judecător de drepturi și libertăți de la o instanță inferioară celei legal competente va atrage nulitatea absolută a încheierii pronunțate și nulitatea derivată a tuturor actelor îndeplinite în baza acestei încheieri, conform art. 280 alin. (2) C.pr.pen.[1]. Cazul de nulitate prevăzut de art. 281 alin. (1) lit. a) C.pr.pen. va opera numai dacă se va pronunța un judecător de drepturi și libertăți de la o instanță inferioară în grad celei competente, nu aceeași fiind consecința dacă judecătorul de drepturi și libertăți va fi din cadrul unei instanțe superioare în grad celei competente. În această din urmă ipostază, va putea fi incidentă o nulitate relativă, în doctrină arătându-se că nu se poate identifica o vătămare a drepturilor procesuale prin judecarea unei cauze de o instanță superioară în grad[2]. Este adevărat că o astfel de vătămare va fi greu de probat, însă nu trebuie să fie exclusă, fapt subliniat și de Curtea Constituțională, care, la rândul ei, apreciază că ar putea fi incidentă o nulitate relativă[3] și că judecarea cauzei de o instanță superioară celei competente îndeplinește prima condiție a nulității relative, respectiv încălcarea unei dispoziții legale.

S-a apreciat că vom fi în situația necompetenței materiale a judecătorului de drepturi și libertăți și atunci când acesta se va pronunța asupra propunerii de autorizare, în sensul admiterii ei, dar infracțiunile care fac obiectul urmării penale nu sunt dintre cele prevăzute de art. 139 alin. (2) C.pr.pen.[4]. Această sancțiune se va întinde asupra tuturor mijloacelor de probă, ele neputând fi folosite într-o altă cauză penală[5].

În ceea ce privește nulitatea absolută ca sancțiune a nerespectării dispozițiilor privind competența organelor de urmărire penală, ea va opera în temeiul art. 281 alin. (1) lit. b) C.pr.pen., în interpretarea dată de Curtea Constituțională prin Decizia nr. 302/2017, prin care s-a stabilit că îndeplinirea unui act de urmărire penală de către un organ inferior celui competent material sau după calitatea persoanei se sancționează cu nulitatea absolută. În mod similar cu cele învederate în cazul competenței instanțelor, desfășurarea urmăririi penale de către un organ de urmărire penală superior celui competent va putea determina, dacă sunt întrunite toate condițiile legale, nulitatea relativă a actului.

O situație des întâlnită în practică este cea a punerii în executare a mandatului de supraveghere tehnică de către un organ necompetent, contrar regulii stabilite de art. 142 alin. (1) C.pr.pen., potrivit căreia punerea în executare a supravegherii tehnice se realizează de către procuror, acesta putând dispune (prin ordonanță) ca punerea în executare să se realizeze de către organele de cercetare penală sau de către lucrătorii specializați din cadrul poliției[6]. Această situație a apărut în practică din două motive: *i)* punerea în executare s-a făcut de către „*alte organe specializate ale statului*", expresie care a fost constatată ca fiind neconstituțională prin Decizia nr. 51/2016 a Curții Constituționale; *ii)* punerea în executare s-a realizat de către S.R.I., contrar dispozițiilor legale prevăzute în art. 91[2] C.pr.pen. anterior, sau alte servicii secrete similare, în temeiul protocoalelor secrete încheiate între aceste servicii și organele de urmărire

[1] *M.V. Tudoran*, Teoria și practica interceptărilor, 2012, p. 121.

[2] *M. Mareș*, Nulitățile în procesul penal, Ed. Hamangiu, București, 2019, p. 182.

[3] CCR, Dec. nr. 554/2017, §22.

[4] *M.V. Tudoran*, Teoria și practica interceptărilor, 2012, p. 124.

[5] *Ibidem*, p 126.

[6] *C. Ghigheci, V. Neagoe*, Supravegherea tehnică în lumina noilor soluții ale Curții Constituționale –interpretarea și aplicarea deciziilor în materie ale instanței constituționale, în Caiete de Drept Penal nr. 3/2019, p. 44.

penală (P.I.C.C.J. și P.N.A./D.N.A.)[1]. În cazul unor asemenea situații, deși actul de autorizare va rămâne valabil, punerea în executare va fi lovită de nulitate absolută, cu consecința nulității tuturor mijloacelor de probă obținute – procese-verbale, dar și mijloace materiale de probă (suporții de stocare), precum și a excluderii probelor. Anterior Deciziei nr. 302/2017 a Curții Constituționale, se putea invoca doar o nulitate relativă, sens în care instanțele rețineau lipsa unei vătămări procesuale, respingând excepțiile[2]. Într-un mod paradoxal, nici instanța supremă nu vedea o problemă în acest sens, apreciind că nu poate constitui o vătămare faptul că punerea în executare s-a realizat de către un „ofițer de servicii secrete"[3].

În cazul lipsei competenței organelor de urmărire penală în consemnarea rezultatelor activităților de supraveghere tehnică, conform art. 143 C.pr.pen., activitățile de supraveghere tehnică vor rămâne valabile, dar actele încheiate referitoare la acestea nu vor mai putea fi folosite ca mijloace de probă în procesul penal. O asemenea situație este incidentă în cazul în care nu va exista delegarea din partea procurorului competent pentru consemnarea activităților de supraveghere tehnică sau în cazul în care se redau de un organ necompetent, de pildă, de un lucrător specializat al poliției care are doar posibilitatea de a pune în executare mandatul de supraveghere tehnică, dar niciodată nu va putea încheia procesele-verbale de consemnare a activităților de supraveghere tehnică sau de redare integrală a convorbirilor, comunicărilor ori a conversațiilor, chiar dacă acestea din urmă ar fi, mai apoi, certificate de procuror conform art. 143 alin. (4) C.pr.pen.

O situație particulară care merită câteva mențiuni va fi aceea în care va lipsi în totalitate actul de autorizare a supravegherii tehnice. Într-o astfel de situație, întreaga supraveghere va fi una nelegală, însă sancțiunea care va interveni, în mod aparent, ar fi nulitatea relativă a actelor de urmărire penală, întrucât nu este incident vreunul dintre cazurile prevăzute de art. 281 C.pr.pen. O atare situație este paradoxală, întrucât, după cum am arătat mai sus, în cazul punerii în executare a mandatului de supraveghere tehnică de către un organ necompetent, va fi incidentă sancțiunea nulității absolute, însă va fi mai grav să se realizeze activități de supraveghere tehnică fără existența unei autorizări legale. În realitate, omisiunea autorizării supravegherii tehnice va trebui să atragă nulitatea absolută a întreg procedeului probatoriu, în considerarea faptului că, prin punerea în executare a supravegherii tehnice fără autorizarea ei de către judecătorul de drepturi și libertăți, procurorul va încălca separația funcțiilor judiciare prevăzută de art. 3 C.pr.pen., fiind incident cazul prevăzut de art. 281 alin. (1) lit. b) C.pr.pen. Incidența acestui caz de nulitate absolută este dată de faptul că autorizarea supravegherii tehnice se va suprapune cu actul de punere în executare al acesteia, act care va fi realizat de procuror, or, acesta va trebui să fie considerat nul, întrucât este emis sau realizat de procuror ori din dispoziția acestuia. Realizarea unei supravegheri tehnice, în lipsa unei autorizări, poate atrage și sancțiuni de altă natură, inclusiv penale, pentru procurorul care se va substitui judecătorului de drepturi și libertăți în autorizarea supravegherii tehnice.

O situație similară celei mai sus menționate va fi în cazul depășirii limitelor autorizației, în acest sens practica reținând în mod eronat existența doar a nulității relative în cauză, chiar

[1] Pentru detalierea aspectelor privind legalitatea încheierii unor asemenea protocoale, precum și conținutul acestora, *v. infra*, Titlul IV, Capitolul IV.

[2] C. Ap. Bacău, s. pen., încheierea nr. 33 din 13 mai 2016, definitivă prin încheierea nr. 919 din 22 iunie 2016 a ICCJ, s. pen., publicată în C. Moisă, op. cit., p. 72; Trib. Iași, s. pen., sent. nr. 18 din 15 februarie 2017, pe *portal.just.ro*; C. Ap. București, s. I pen., sent. nr. 278 din 13 iulie 2016, pe *portal.just.ro*

[3] ICCJ, s. pen., dec. nr. 416/A/2016 din 27 octombrie 2016, pe *www.scj.ro*

într-o situație gravă, precum depășirea intervalului de timp pentru care s-a autorizat măsura[1]. Pentru identitate de motive, apreciem că sancțiunea va trebui să fie nulitatea absolută[2].

Cel de-al treilea caz de nulitate absolută care poate fi incident cu privire la supravegherea tehnică este cel prevăzut de art. 281 alin. (1) lit. d) C.pr.pen., respectiv lipsa procurorului atunci când participarea sa este obligatorie, potrivit legii. Acest caz de nulitate absolută se poate aplica numai în etapele supravegherii tehnice care prevăd o procedură în fața judecătorului de drepturi și libertăți: *i)* judecarea propunerii de încuviințare a supravegherii tehnice; *ii)* judecarea confirmării supravegherii tehnice autorizate provizoriu de procuror.

În privința judecării propunerii de încuviințare a măsurilor de supraveghere tehnică, situația amintită nu prezintă probleme semnificative, întrucât, potrivit art. 140 alin. (3) teza finală C.pr.pen., participarea procurorului la judecarea propunerii este obligatorie. Din acest punct de vedere, se reflectă necesitatea ca procedura să fie una efectivă și să permită judecătorului de drepturi și libertăți să lămurească în camera de consiliu orice aspecte ce țin de îndeplinirea condițiilor legale pentru încuviințarea măsurilor cerute.

Cea de-a doua ipoteză amintită prezintă o problemă, întrucât art. 141 C.pr.pen. nu face nicio referire la obligativitatea prezenței procurorului la judecarea cererii de confirmare a măsurilor speciale de supraveghere tehnică autorizate provizoriu, pe o durată de maximum 48 de ore. Omisiunea legiuitorului nu trebuie interpretată în sensul în care va putea fi incidentă numai o eventuală nulitate relativă, ci în sensul în care procedura confirmării va trebui să respecte și condițiile art. 140 C.pr.pen. Potrivit art. 141 alin. (3) C.pr.pen., procurorul are obligația de a *sesiza* judecătorul de drepturi și libertăți, sens în care trebuie să observăm că acest termen este folosit de legiuitor numai în situațiile în care se impune ca procurorul să propună sau să remită judecarea unei cereri sau propuneri către un alt organ judiciar. Sesizarea va fi astfel diferită față de o declinare, unde cauza se trimite unui organ judiciar de aceeași natură, și față de trimiterea cererii pe cale administrativă, care nu presupune decât o operațiune material tehnică, și nu un act procedural. Prin termenul de „sesizare" înțelegem că procurorul își menține obligația de a participa la judecarea cererii, întrucât el va fi obligat să pună concluzii cu privire la propunerea sa, în mod similar exercitării funcției acuzării în cursul judecății[3]. În ceea ce privește procedurile în care nu va fi obligatorie prezența procurorului, observăm că legiuitorul a inclus și situații în care judecătorul de cameră preliminară este doar informat de procuror [art. 139 alin. (4) C.pr.pen. privind supravegherea tehnică realizată față de avocat-client, art. 142 alin. (4) C.pr.pen. privind încetarea supravegherii tehnice] sau în care se solicită judecătorului de drepturi și libertăți să realizeze o procedură ulterior soluționării cauzei (conservarea materialelor rezultate din supravegherea tehnică).

Un alt argument pentru a susține obligativitatea participării procurorului la confirmarea supravegherii tehnice dispuse prin ordonanță este și dispoziția legală aferentă art. 141 alin. (7) C.pr.pen., care prevede posibilitatea procurorului de a cere, alături de confirmarea supravegherii tehnice, luarea măsurii supravegherii tehnice *în condițiile art. 140 C.pr.pen.*, într-o asemenea situație, judecătorul de cameră preliminară urmând a se pronunța prin aceeași încheiere.

În afară de cele două situații expuse mai sus, nu pot fi identificate alte situații în care să fie invocat cazul de nulitate absolută privind lipsa participării procurorului, întrucât acesta se va aplica numai cazurilor în care va exista o judecată a cauzei.

---

[1] Trib. Gorj, s. pen., încheierea din 13 ianuarie 2016, definitivă prin încheierea din 28 martie 2016 a C. Ap. Craiova, publicată în C. Moisă, op. cit., p. 97.

[2] În același sens, *M.V. Tudoran*, Teoria și practica interceptărilor, 2012, pp. 128-129.

[3] *Tr. Pop*, op. cit., p. 78.

În măsura în care vor exista alte încălcări ale dispozițiilor legale incidente în autorizarea sau punerea în executare a metodelor speciale de supraveghere, va putea fi incidentă o nulitate relativă, în cazul în care vor fi îndeplinite și celelalte condiții prevăzute de lege.

§2. Nulitatea relativă a măsurilor de supraveghere tehnică

Potrivit art. 282 alin. (1) C.pr.pen., formularea condițiilor nulității relative este următoarea: „*încălcarea oricăror dispoziții legale în afara celor prevăzute la art. 281 determină nulitatea actului atunci când prin nerespectarea cerinței legale s-a adus o vătămare drepturilor părților ori ale subiecților procesuali principali, care nu poate fi înlăturată altfel decât prin desființarea actului*".

În privința persoanelor care pot invoca nulitatea relativă, textul legal limitează această sferă numai la părțile sau subiecții procesuali principali. În doctrină s-a considerat că posibilitatea invocării nulității relative trebuie să fie corelată cu existența unui interes procesual propriu în invocarea ei[1]. Din acest punct de vedere, credem că interpretarea dispoziției din Codul de procedură penală trebuie să se facă și prin prisma Deciziei Curții Constituționale nr. 244/2017 referitoare la excepția de neconstituționalitate a dispozițiilor art. 145 din Codul de procedură penală, care privește posibilitatea persoanei care nu participă la procedura de cameră preliminară de a contesta legalitatea supravegherii tehnice. Nu se face nicio referire la nulitățile care pot fi invocate într-o asemenea contestație, fiind necesar ca orice persoană care justifică un interes procesual propriu să poată invoca nulitatea relativă, în orice procedură judiciară.

Condiția existenței unei vătămări suscită unele interpretări doctrinare largi cu privire la semnificația acestui concept, la natura vătămării și la drepturile la care se va raporta aceasta. Problema esențială este dacă vătămarea care trebuie să fie dovedită va trebui să afecteze caracterul echitabil al procesului penal, punând persoana care o suferă într-o poziție de inferioritate față de acuzare sau va fi suficient să constea într-o vătămare adusă unui drept sau interes legitim larg recunoscut de lege. Potrivit Codului de procedură penală, formularea existenței vătămării este următoarea: „*s-a adus o vătămare drepturilor părților ori ale subiecților procesuali principali, care nu poate fi înlăturată altfel decât prin desființarea actului*". Deși doctrina și jurisprudența vorbesc despre existența unei vătămări procesuale, va trebui să analizăm cele două puncte de vedere în privința întinderii vătămării.

Într-o primă opinie, mai restrânsă, vătămarea procesuală trebuie să fie circumscrisă sferei procedurale, trebuind să aducă atingere unui drept sau interes procesual al părții sau subiectului procesual principal[2]. Într-o altă opinie din doctrina națională se arată că noțiunea de „vătămare procesuală" este mai largă, cuprinzând și încălcări ale unor drepturi și libertăți fundamentale ale cetățeanului, și nu doar încălcări care produc consecințe în planul procedural[3]. Autorul citat se referă expres și la supravegherea tehnică în argumentarea poziției sale, subliniind că modalitatea de dispunere și punere în aplicare a unor astfel de măsuri atrage automat încălcări ale drepturilor și libertăților substanțiale, întrucât ingerința adusă acestora trebuie să se producă în cadrul limitelor legale[4]. Într-o altă opinie concurentă se arată că „*prin «vătămare» înțelegem atingerea adusă bunei desfășurări a procesului penal, echitabilității procedurilor ori drepturilor și*

[1] *Ibidem*, p. 80; *Gh. Mateuț*, Procedură penală, 2019, p. 1012.

[2] *V. Dongoroz (coord.), C. Bulai, S. Kahane, N. Iliescu, G. Antoniu, R. Stănoiu*, Explicații teoretice ale Codului de procedură penală român. Partea generală, vol. I, Ed. Academiei Republicii Socialiste România, București, 1975, p. 412.

[3] *M. Mareș*, op. cit., p. 216.

[4] *Ibidem*, pp. 216-217.

libertăților fundamentale ale părților ori subiecților procesuali principali"[1]. Acest din urmă autor detaliază sfera vătămărilor, considerând că pot fi vătămate atât drepturi substanțiale, precum demnitatea umană, viața privată, secretul profesional, cât și drepturi procesuale, precum dreptul la apărare, dreptul de a fi informat cu privire la acuzație, dreptul la tăcere[2].

În opinia noastră, vătămarea nu va trebui să conducă neapărat la punerea părții sau subiectului procesual principal într-o poziție de inferioritate care să afecteze echitabilitatea procedurii, fiind suficient, potrivit art. 282 alin. (1) C.pr.pen., să se producă o vătămare a drepturilor părților sau subiecților procesuali în legătură cu desfășurarea procesului penal.

În doctrina străină s-a susținut că, în situația în care vătămarea ar consta în încălcarea art. 8 Conv.EDO, s-ar impune aplicarea sancțiunii *excluderii automate a probei obținute* fără a fi nevoie de o analiză distinctă asupra caracterului echitabil al procedurii prin raportare la vătămare[3]. O atare interpretare este acceptabilă, din punctul nostru de vedere, și ca urmare a naturii măsurilor de supraveghere tehnică, problema existenței unei vătămări nefiind pusă la îndoială. Caracterul intruziv al măsurilor de supraveghere fac ca această vătămare să existe, fiind legată în această situație și de imposibilitatea înlăturării sale în orice alt mod decât desființarea actului.

Astfel, o problemă esențială este dacă vătămarea constând în încălcarea dreptului persoanei la viață privată poate fi înlăturată prin anulare sau va putea exista o alternativă la desființarea actului prin care vătămarea să fie înlăturată. În doctrină s-a arătat că înlăturarea vătămării produse se impune a se realiza numai pe parcursul procesului, în situație contrară impunându-se anularea actului vătămător[4]. Particularitatea supravegherii tehnice este că niciodată nu va putea fi înlăturată complet vătămarea, chiar și prin constatarea nulității actului, întrucât legiuitorul nu a prevăzut și distrugerea mijloacelor de probă nelegale, sens în care nu este suficientă doar excluderea probelor de la dosarul cauzei. Conform jurisprudenței Curții Constituționale[5] cu privire la art. 102 alin. (3) C.pr.pen., este necesară nimicirea fizică a mijlocului de probă, ținând cont de caracterul vătămător al menținerii acestuia la dosarul cauzei, putând fi expus unui acces abuziv în detrimentul vieții private a persoanei[6].

În cazul nulităților relative a măsurilor de supraveghere tehnică, o problemă care suscită interes este necesitatea desființării actului prin raportare la condiția existenței unei vătămări care nu poate fi înlăturată în alt mod. Ținând seama de caracterul intruziv al tuturor măsurilor de supraveghere tehnică, va exista întotdeauna o restrângere a drepturilor fundamentale ale unei persoane, în special a dreptului la viață privată, astfel că încălcarea dispozițiilor procesuale penale privind o asemenea măsură va conduce la transformarea acestei ingerințe într-o vătămare a dreptului la viață al persoanei, în sensul art. 282 C.pr.pen.

§3. Efectele constatării nulității supravegherii tehnice

În urma constatării nulității absolute sau relative, va fi atras efectul retroactiv al nulității ce constă în desființarea actului atacat, ceea ce prezintă mai multe consecințe care au fost în mod corect împărțite de doctrină în următoarele categorii principale: *i)* lipsirea de efecte juridice a

[1] *M. Udroiu*, Procedură penală, vol. II, 2019, p. 1151.

[2] *Ibidem*, p. 1168.

[3] *D. Ormerod*, ECHR and the exclusion of evidence: trial remedies for Article 8 breaches, în Criminal Law Review no. 61/2003, London.

[4] *I. Kuglay*, în M. Udroiu (coord.), Codul de procedură penală, 2017, p. 1296.

[5] CCR, Dec. nr. 22 din 18 ianuarie 2018 (M. Of. nr. 177 din 26 februarie 2018).

[6] CEDO, cauza *Craxi c. Italia (nr. 2)*, Hotărârea din 17 iulie 2003, §75 și §83, pe *hudoc.echr.coe.int*

actului efectuat cu încălcarea legii; *ii)* iradierea la actele subsecvente aflate în legătură directă cu actul nul; *iii)* refacerea actelor anulate de către organul judiciar; *iv)* retragerea din dosar a actelor anulate[1].

Prima consecință va fi cea directă, asupra actului juridic lovit de nulitate, constând în desființarea acestuia, considerat a fi ineficient și lipsit de orice efecte juridice pe care altfel le-ar fi putut produce. Se va considera că actul anulat a fost de la început lipsit de aptitudinea de a produce efecte juridice din momentul realizării lui (*ex tunc*), iar nu numai de la momentul constatării nulității (*ex nunc*)[2].

A doua consecință va fi cea indirectă, constând în extinderea efectelor nulității și asupra actelor subsecvente, dacă acestea au legătură cu actul nul, potrivit art. 280 alin. (2) C.pr.pen. Aceasta va fi denumită „nulitate derivată", de o importanță deosebită, mai ales în cazul supravegherii tehnice. Afirmăm acest lucru, deoarece realizarea acestui procedeu probatoriu presupune o procedură etapizată în care se pot produce încălcări ale legii în mai multe momente, de regulă, sancțiunea nulității derivate intervenind pentru toate actele subsecvente, întrucât fiecare este condiționat de actul anterior. De pildă, odată cu constatarea nulității actului de autorizare, se va constata nulitatea tuturor activităților de punere în executare, dar și a mijloacelor de probă care au fost obținute, între toate acestea existând o legătură directă.

Alături de consecința desființării actului nelegal, constatarea nulității presupune și remedierea încălcării prin refacerea actului atunci când este necesar și posibil[3]. Referitor la posibilitatea refacerii actului după constatarea nulității sau la readministrarea probei, trebuie să avem în vedere și faza procesuală în care s-ar afla cauza, întrucât supravegherea tehnică este strict legată de faza de urmărire penală, neputând fi realizată în cursul fazelor ulterioare.

Ca urmare a naturii supravegherii tehnice, odată ce a trecut momentul la care s-a realizat evenimentul surprins, el nu poate fi supus din nou metodelor speciale pentru ca proba să se readministreze în mod legal. Cu alte cuvinte, va fi imposibilă readministrarea probei obținute prin supraveghere tehnică. Contrar acestei situații, vor fi procedeele probatorii care cunosc repetabilitate, precum audierea persoanelor. Consecința va fi imposibilitatea refacerii supravegherii tehnice ca procedeu probatoriu, putând fi refăcute anumite acte procedurale ce compun procedeul probatoriu.

În ceea ce privește efectele nulității actului prin care s-a autorizat supravegherea tehnică, acest act nu se va putea reface în niciuna dintre fazele procesuale, nulitatea acestui act impunând constatarea unei nulități derivate a tuturor actelor subsecvente, inclusiv a proceselor-verbale de consemnare a activităților rezultate din supravegherea tehnică și a proceselor-verbale de redare integrală prevăzute de art. 143 alin. (4) C.pr.pen.[4].

Nulitatea punerii în executare a supravegherii tehnice nu va afecta legalitatea actului de autorizare, dar va conduce la nulitatea tuturor mijloacelor de probă obținute prin supravegherea tehnică. În măsura în care numai anumite activități de supraveghere tehnică au fost puse în executare în mod nelegal, atunci nulitatea va afecta numai aceste acte, putând fi menținute celelalte. De exemplu, prin același mandat de supraveghere tehnică se autorizează interceptarea comunicațiilor unei persoane, dar și supravegherea video, audio sau prin fotografiere. În cazul în care se va constata nulitatea punerii în executare a interceptării comunicaților, întrucât au fost

[1] *Gh. Mateuț*, Procedură penală, 2019, pp. 1017-1020.
[2] *S. Kahane*, în V. Dongoroz (coord.), op. cit., p. 412.
[3] CCR, Dec. nr. 554/2017, §15.
[4] C. Ap. Timișoara, s. pen., încheierea din 19 mai 2016, pe *portal.just.ro*

realizate de către un organ de urmărire penală necompetent (situație des întâlnită în practică pentru interceptările realizate mai înainte de pronunțarea Deciziei Curții Constituționale nr. 51/2016), aceasta nu va afecta supravegherea video realizată de un organ de cercetare penală legal desemnat conform art. 142 alin. (1) C.pr.pen.

Referitor la refacerea actului de procedură penală lovit de nulitate, această posibilitate va putea exista numai în condiții restrânse, putând fi incidentă numai în privința proceselor-verbale întocmite în condițiile art. 143 C.pr.pen. și doar dacă întocmirea lor s-a realizat cu încălcarea legii, și nu ca urmare a unei nulități a autorizării sau punerii în executare a supravegherii tehnice. O atare situație poate fi incidentă în situația în care procurorul nu a certificat procesul-verbal de redare integrală a convorbirilor, comunicărilor sau conversațiilor, prevăzut de art. 143 alin. (4) C.pr.pen. Cu toate acestea, există o limitare în timp a posibilității refacerii acestor acte de procedură, aceasta putându-se realiza numai până la desesizarea procurorului după terminarea urmăririi penale, nefiind posibilă refacerea lor după acest moment. Acest lucru se datorează faptului că, ulterior acestui moment, administrarea oricăror probe se va realiza de către judecătorul de cameră preliminară (limitat la obiectul acestei faze) și de către instanță, or, din cuprinsul art. 143 alin. (4) C.pr.pen. reiese posibilitatea procurorului de a efectua procedura de certificare, aceasta neputând fi realizată de către instanță sau la dispoziția instanței. În mod corect s-a reținut în practică atributul exclusiv al procurorului de a realiza certificarea procesului-verbal de redare integrală a convorbirilor interceptate[1], neexistând nicio dispoziție privind posibilitatea realizării unei astfel de operațiuni de către orice alt organ judiciar. Ceea ce va rămâne astfel la dosarul cauzei este copia suportului de stocare inițial, pe care se vor regăsi rezultatele supravegherii tehnice, din acestea putând rezulta proba numai prin audierea, vizionarea sau prezentarea lor în mod nemijlocit judecătorului de cameră preliminară și instanței.

O ultimă problemă în cazul efectelor sancțiunii nulității o reprezintă imperativul din doctrină al retragerii din dosar a actelor sau pieselor anulate, pentru a evita posibilitatea folosirii pentru viitor, dar și pentru a evita distrugerea documentului[2]. În acest sens este și jurisprudența Curții Constituționale, care, prin Decizia nr. 22/2018[3], a statuat că, odată cu excluderea probei, se impune și înlăturarea de la dosar a mijlocului de probă. În situația măsurilor de supraveghere tehnică, numai înlăturarea fizică a mijlocului de probă va fi insuficientă în opinia noastră, fiind necesară distrugerea acestuia – atât ca proces-verbal întocmit conform art. 143 C.pr.pen., cât mai ales ca mijloc material de probă – suportul de stocare a rezultatelor activităților de supraveghere tehnică – suport inițial și copia realizată, conform art. 143 alin. (2) C.pr.pen. Această obligație rezultă din caracterul vătămător al prezenței la dosarul cauzei a rezultatelor supravegherii tehnice, în special când acestea constau în interceptarea comunicațiilor sau supravegherea video, audio sau prin fotografiere a unor persoane. În sensul necesității distrugerii lor, este și jurisprudența Curții Europene a Drepturilor Omului, unde s-a arătat că se impune ca persoana care contestă legalitatea supravegherii tehnice să poată obține și distrugerea acestora[4], astfel că se impune, *de lege ferenda*, ca sancțiunea nulității să fie urmată de excluderea probei obținute în mod nelegal și distrugerea tuturor mijloacelor de probă rezultate din supravegherea tehnică.

[1] *S. Grădinaru*, Supravegherea tehnică, 2014, p. 117.
[2] *Gh. Mateuț*, Procedură penală, 2019, p. 1019.
[3] CCR, Dec. nr. 22/2018 (M. Of. nr. 177 din 26 februarie 2018).
[4] CEDO, cauza *Pruteanu c. România*, Hotărârea din 3 mai 2015, §52, pe *ier.gov.ro*

Capitolul X
Concluzii

Supravegherea tehnică reprezintă categoria cea mai importantă de metode speciale de supraveghere sau cercetare prevăzută de Codul de procedură penală. În cazul supravegherii tehnice, legea română prevede anumite condiții legale care trebuie să fie respectate, condiții de fond și condiții procedurale.

În primul rând, trebuie să fie începută urmărirea penală, ca o condiție prealabilă, nefiind posibilă administrarea vreunei probe, decât după emiterea unei ordonanțe de începere a urmăririi penale, conform art. 305 alin. (1) C.pr.pen. Procesul penal nu mai cunoaște o fază a actelor premergătoare în care să poată fi realizate anumite acte în vederea începerii urmăririi penale, astfel că nu se vor putea autoriza măsuri de supraveghere tehnică înainte de începerea urmăririi penale.

Prima condiție de fond este cea a existenței unei suspiciuni rezonabile privind săvârșirea unei infracțiuni, termenul reprezentând un împrumut legislativ din dreptul american și britanic. O suspiciune rezonabilă presupune atât existența unui element obiectiv – informații privind săvârșirea unei infracțiuni, cât și a unui element subiectiv – ca organul care constată existența suspiciunii rezonabile să poată concluziona, pe baza experienței sale, că din elementele obiective există o astfel de suspiciune. Acest element va fi analizat atât de procurorul care întocmește propunerea de autorizare a supravegherii tehnice, cât și de judecătorul de drepturi și libertăți, prin raportare la dosarul cauzei. Nu va fi posibilă autorizarea unor măsuri de supraveghere tehnică decât dacă există un minim de date sau informații care rezultă din actele de cercetare sau din administrarea de probe. În cazul unui control *a posteriori*, judecătorul de cameră preliminară va verifica dacă la momentul autorizării a existat o suspiciune rezonabilă, fără a ține seama de rezultatele supravegherii tehnice. Astfel, sunt interzise anchetele făcute abuziv pentru a descoperi comiterea de infracțiuni denumite *fishing expeditions*, prin care organele de urmărire penală demarează o urmărire penală în căutare de fapte ilicite nedeterminate. Pe o scară graduală, mai presus de aceste *fishing expeditions*, va fi numai provocarea la săvârșirea de infracțiuni.

Suspiciunea rezonabilă va trebui să privească o infracțiune de o gravitate considerabilă, fiind definită de legiuitor o listă în cuprinsul art. 139 alin. (2) C.pr.pen. În afara infracțiunilor prevăzute expres, nu va fi posibilă autorizarea supravegherii tehnice, reflectând aplicarea Recomandării (2005) 10 a Comitetului de Miniștri, prin care tehnicile speciale de investigare trebuie limitate numai la infracțiuni grave, precum terorismul sau criminalitatea organizată. Critica ridicată de noi cu privire la această problemă este că lista stabilită de legiuitor este mult prea permisivă, prin criteriul subsidiar al pedepsei de 5 ani sau mai mare, fiind incluse și infracțiuni des întâlnite în societate, dar de o gravitate care nu poate justifica astfel de măsuri (infracțiuni contra siguranței circulației pe drumurile publice).

Proporționalitatea măsurii se impune a fi respectată în toate cazurile în care se autorizează supravegherea tehnică, presupunând ca judecătorul de drepturi și libertăți să evalueze importanța probelor care ar putea fi obținute și gravitatea intruziunii în viața privată a unei persoane. Pentru a se realiza acest control, este necesar ca procurorul să explicitеze în propunerea formulată măsurile de supraveghere tehnică solicitate, trebuind să detalieze, de asemenea, modul și

limitele în care vor fi puse în executare. În realizarea controlului de proporționalitate, judecătorul de drepturi și libertăți va autoriza expres măsuri concrete și nu va putea autoriza generic una dintre măsurile prevăzute de art. 138 alin. (1) lit. a)-d) C.pr.pen., prin simpla referire la textul de lege, fără a stabili limitele concrete ale autorizării.

Subsidiaritatea supravegherii tehnice este o condiție esențială, strâns legată de proporționalitate, însă legiuitorul a introdus elemente suplimentare care nu au nicio legătură cu acest criteriu, respectiv *existența unui pericol pentru siguranța persoanelor sau a unor bunuri de valoare*. Acest din urmă criteriu se impune a fi înlăturat, lăsând loc de abuz și nici nu ar dovedi vreo eficiență, întrucât strângerea de probe nu va proteja respectivele persoane sau bunuri, presupunând o intervenție directă a organelor de urmărire penală. Subsidiaritatea va însemna că vor trebui preferate alte procedee probatorii mai puțin intruzive decât supravegherea tehnică.

Propunerea de autorizare va putea fi realizată numai de către procuror, acesta având competența exclusivă de a sesiza judecătorul de drepturi și libertăți. Propunerea va trebui că conțină elementele cuprinse în art. 140 alin. (2) C.pr.pen., iar procurorul va trebui să motiveze în mod temeinic, prin raportare la condițiile legale expuse mai sus. Din punctul de vedere al suspiciunii rezonabile, procurorul va trebui să motiveze existența acesteia, textul legal fiind criticabil prin referirea numai la *indicarea probelor ori a datelor din care rezultă suspiciunea rezonabilă*, care va trebui dovedită. Procurorul va trebui să expliciteze și fiecare măsură pe care o solicită, dar și să indice, în concret, după caz, cum se va realiza pătrunderea în spații private pentru instalarea și dezinstalarea tehnicii operative, de câte ori se va realiza aceasta, de câte persoane și unde vor fi montate dispozitivele.

Autorizarea supravegherii tehnice se va face prin încheierea judecătorului de drepturi și libertăți, care va verifica îndeplinirea tuturor condițiilor legale, emițând de îndată un mandat de supraveghere tehnică și întocmind obligatoriu minuta. În cazul respingerii propunerii, aceasta nu va fi supusă niciunei căi de atac. O nouă propunere nu va putea fi formulată de procuror decât dacă se întemeiază pe descoperirea de fapte noi.

În cazuri urgente, Codul de procedură penală actual a menținut instituția autorizării provizorii de către procuror, procedură pe care o considerăm a fi neconstituțională și contrară introducerii competenței judecătorului de drepturi și libertăți în soluționarea urgentă a unor astfel de cauze. Apreciem că textul art. 141 C.pr.pen. este susceptibil de abuzuri, întrucât procurorul nu este o autoritate independentă, ci are un interes procesual – administrarea de probe în procesul penal, în special în defavoarea persoanei supravegheate. Ar fi de neconceput realizarea unei supravegheri tehnice pentru a administra probe în favoarea persoanei supravegheate. Mai mult, procedura confirmării autorizării provizorii nu prezintă garanții suficiente, judecătorul de drepturi și libertăți putând fi tentat ca, pe baza importanței probelor obținute, să confirme ordonanța procurorului.

Punerea în executare a supravegherii tehnice a cunoscut critici numeroase, fiind punctul de discordie în practica judiciară, cauzată de implicarea ilicită a organelor din domeniul securității statului în punerea în executare a supravegherii tehnice, cu complicitatea Ministerului Public. Această practică a început în anul 2003 și s-a extins până la pronunțarea Deciziei nr. 51/2016 a Curții Constituționale, decizii subsecvente subliniind amploarea fenomenului. Ca regulă, punerea în executare se va realiza de către procuror, acesta putând să dispună ca organele de cercetare penală sau lucrătorii specializați din poliție să realizeze acest act. Codul de procedură penală limitează în mod expres organele care pot fi delegate cu o astfel de sarcină. În cursul punerii în executare, procurorul va realiza un control și o supraveghere continuă a măsurii,

aceasta reprezentând, în ceea ce ne privește, o situație criticabilă, întrucât acest rol ar trebui să fie al judecătorului de drepturi și libertăți. Apreciem că s-ar impune ca toate rezultatele supravegherii tehnice să fie trecute prin filtrul judecătorului de drepturi și libertăți, care ar trebui să fie informat în timp real asupra desfășurării supravegherii tehnice. Dacă vor înceta să subziste temeiurile care au condus la autorizarea măsurii, procurorul va fi obligat să dispună încetarea măsurii, încunoștințând judecătorul de drepturi și libertăți.

Dacă din punerea în executare a măsurii vor rezulta date care nu privesc cauza sau care nu contribuie la identificarea ori localizarea persoanelor, ele vor fi arhivate, în măsura în care nu vor fi folosite în alte cauze. Este criticabilă alegerea legiuitorului de a pretinde ca folosirea lor în cursul judecății să fie limitată la situația în care există noi probe din care ar rezulta că ele sunt utile cauzei, punând apărarea într-o situație inechitabilă, întrucât nici nu are acces la aceste rezultate ale supravegherii tehnice și trebuie să dovedească instanței că acestea pot fi utile soluționării cauzei.

Codul de procedură penală a instituit o procedură facultativă de semnare electronică a rezultatelor activităților de supraveghere tehnică, prin utilizarea de semnături electronice extinse pe bază de certificate calificate. Prin aceasta se exploatează faptul că rezultatele activităților de supraveghere tehnică au natura de date informatice și pot fi semnate electronic, asigurându-se autenticitatea acestora și împiedicându-se modificări care să nu poată fi lesne observate. Se impune ca legiuitorul să stabilească un caracter obligatoriu al semnării digitale a rezultatelor supravegherii tehnice, însă, în prealabil, vor trebui emise dispozitive de semnare și certificate calificate pentru toate organele judiciare, ceea ce va presupune costuri suplimentare.

Informarea persoanei supravegheate prezintă neajunsuri legislative, constatate și de Curtea Constituțională, întrucât legiuitorul a omis să introducă în lege cel mai important element legat de informare, și anume contestarea legalității și temeiniciei supravegherii tehnice. Din jurisprudența Curții Europene a Drepturilor Omului, rezultă că acest drept este unul esențial pentru orice persoană supravegheată, informarea nefiind un drept autonom, ci doar o condiție pentru a permite contestarea supravegherii. La momentul actual, dreptul român este încă deficitar, fiind întrevăzute soluții judiciare întemeiate pe Decizia Curții Constituționale nr. 244/2017. Acestea ar consta numai în formularea unei contestații în fața judecătorului de cameră preliminară de către persoana care se consideră vătămată prin intruziunea în viața sa privată, cauzată de supravegherea tehnică.

O problemă aparte ce ține de supravegherea tehnică este posibilitatea obținerii unor probe fără autorizare, aceasta fiind stabilită de legiuitor prin art. 139 alin. (3) C.pr.pen. numai în favoarea înregistrărilor realizate de particulari cu privire la propriile înregistrări. Nu va fi admisă nicio interferență din partea organelor de urmărire penală, acțiunea particularului fiind una independentă, în sens contrar, jurisprudența Curții Europene a Drepturilor Omului stabilind că ar fi încălcat dispozițiile art. 8 Conv.EDO. Orice intervenție din partea organelor de urmărire penală ar transforma o supraveghere privată într-una publică, fiind necesară o autorizare din partea unei autorități independente. Ceea ce lipsește în Codul de procedură penală este necesitatea ca orice probă obținută prin înregistrările realizate fără autorizare să fie trecută printr-un filtru al proporționalității și subsidiarității, reflectându-se, în lucrare, situații în care un privat a depășit flagrant proporționalitatea măsurii și a încălcat dreptul la viață privată al unei alte persoane în realizarea de înregistrări. În jurisprudența recentă a Curții Constituționale a fost atinsă și problema justificării, prin intermediul dispozițiilor art. 139 alin. (3) C.pr.pen., a folosirii rezultatelor obținute în urma activităților specifice culegerii de

informații, prin Decizia nr. 55 din 4 februarie 2020, Curtea Constituțională stabilind că acestea nu pot fi socotite ca *alte înregistrări care nu sunt interzise de lege*.

Avocatul poate fi un subiect al supravegherii tehnice, legea procesuală penală neacordând o protecție adecvată acestuia, neexistând garanții care să împiedice supravegherea accidentală a raporturilor dintre avocat și client. Chiar dacă o astfel de supraveghere a avut loc, probele ar urma să fie distruse de îndată de procuror, dar nu se poate evita ca acesta să dobândească cunoștințe despre conținutul convorbirilor. Mai mult, lipsa unor garanții efective este evidențiată și prin caracterul facultativ al încunoștințării avocatului despre faptul că au fost supravegheate convorbirile sale cu clientul în mod accidental. Gradul de protecție oferit avocatului este unul scăzut, acesta putând fi supus direct măsurilor de supraveghere tehnică în aceleași condiții ca orice altă persoană, prin aceasta putând fi afectată relația sa profesională cu orice client pe care l-ar avea.

Valoarea probantă a supravegherii tehnice este una deosebită și a fost avută în vedere în această lucrare atât datorită importanței, cât și naturii probelor obținute în cauza în care s-a dispus folosirea tehnicilor speciale de investigare. Deseori, prin supravegherea tehnică se pot obține probe directe privind săvârșirea unei infracțiuni, în special în cauzele care au ca obiect infracțiuni de corupție, a căror săvârșire se poate realiza prin mijloace de comunicare la distanță. Chiar și în cazul altor tipuri de infracțiuni, măsurile de supraveghere tehnică vor avea o importanță mare, putând stabili legăturile dintre anumite persoane și structura unui grup de criminalitate organizată ori putând dezvălui pregătirea săvârșirii unor infracțiuni. Rezultatele supravegherii tehnice vor putea fi utilizate nu numai în cauza în care au fost autorizate, dar și în alte cauze derivate. În acest din urmă caz, rezultatele activităților de supraveghere tehnică nu vor putea fi folosite ca probe într-o altă cauză, dar vor putea sta la baza sesizării organelor de urmărire penală, cu excepția situației constatării infracțiunii flagrante și numai dacă fapta s-ar încadra în infracțiunile prevăzute de art. 139 alin. (2) C.pr.pen.

Ținând seama de modificările legislative și de deciziile obligatorii ale Curții Constituționale, înainte de momentul intrării în vigoare a Codului de procedură penală, vor exista mai multe posibilități în contestarea legalității supravegherii tehnice, putând fi sancționate nelegalitățile ce țin de autorizarea, punerea în executare și consemnarea rezultatelor atât în faza de cameră preliminară, cât și în faza de judecată. Vor putea fi aplicate mai multe sancțiuni procedeelor probatorii, nulitatea absolută fiind cea mai prevalentă. În cazul nulității relative, apreciem că, prin raportare la jurisprudența Curții Europene a Drepturilor Omului și la dispozițiile art. 282 C.pr.pen., existența unei vătămări a drepturilor persoanei și dovedirea vătămării nu prezintă probleme, întrucât supravegherea tehnică restrânge dreptul la viață privată al unei persoane, restrângere care devine ilicită în momentul în care măsura se desfășoară nelegal, astfel că o vătămare va exista întotdeauna.

Titlul IV
Interceptarea comunicațiilor ori a oricărui tip de comunicare la distanță

Capitolul I
Aspecte generale

Secțiunea 1. Utilitatea metodei de supraveghere tehnică

Interceptarea comunicațiilor ori a oricărui tip de comunicare este o metodă de supraveghere tehnică, cu origini care datează de la inventarea comunicațiilor la distanță, fie ele scrise, telegrafice sau audio, fiind recunoscută importanța metodei pentru aflarea informațiilor confidențiale. Importanța sa este una istorică, metoda fiind recunoscută ca un mijloc de asigurare a siguranței statului, prin spionajul desfășurat împotriva oricărui alt stat care ar avea planuri dușmănoase față de acesta[1]. Ca metodă de culegere de informații, interceptarea comunicațiilor și măsura sa predecesoare – interceptarea corespondenței – sunt cunoscute din vechi timpuri ca fiind atributul serviciilor secrete ale unui stat[2]. În scopuri judiciare, interceptarea este recunoscută ca o metodă care poate fi pusă în practică încă din prima jumătate a secolului al XX-lea, fiind recunoscută sub imperiul legislației române încă din acele timpuri[3].

În ultimele două decenii, societatea a cunoscut o folosire intensă a acestei măsuri de supraveghere tehnică, în special pentru combaterea terorismului ca urmare a atentatelor din S.U.A. ce au avut loc la 11 septembrie 2001[4]. La nivel global s-a încercat combaterea acestui fenomen prin implementarea unor activități de supraveghere tehnică în masă, conducând la autorizarea de activități de acest gen împotriva a zeci de mii de persoane deodată, printr-un singur act de autorizare, fără existența niciunei suspiciuni că persoanele respective au fost implicate în săvârșirea vreunei infracțiuni[5]. Reverberațiile acestor măsuri s-au simțit mai recent, ca urmare a dezvăluirilor făcute de particulari, precum Edward Snowden, privind programele desfășurate pentru supravegherea în masă a persoanelor[6]. La nivel internațional, dezvăluirile au dus la o mișcare împotriva ideii de supraveghere în masă a persoanelor, considerându-se că „*societățile democratice trebuie să respingă ideea că este admisibil ca executivul să înregistreze*

[1] *S. McKay*, Blackstone's Guide to The Investigatory Powers Act 2016, Oxford University Press, Oxford, 2017, p. 46.

[2] *Idem*, Covert Policing, 2015, p. 66.

[3] *Tr. Pop*, op. cit., p. 474.

[4] *A. Ashworth, L. Zedner*, op. cit., p. 171.

[5] *L.K. Donohue*, The Future of Foreign Intelligence, 2016, p. 95; *R. Jeffreys-Jones*, op. cit., p. 173.

[6] *M.E. Moon*, How America Lost its Secrets: Edward Snowden, The Man and The Theft, în Journal of Strategic Security, vol. 10, no. 1/2017, pp. 143-145; *R. Shimonski, J. Zenir, A. Bishop*, Cyber Reconnaissance, Surveillance and Defense, Ed. Elsevier, Waltham, 2015, pp. 8-10.

toate comunicațiile prin Internet și activitățile telefonice cu sau fără o autorizare"[1]. Corelativ, tot ca urmare a dezvăluirilor lui Snowden, guvernele naționale au început să recunoască activitățile de supraveghere în masă desfășurate, subliniindu-se în literatura de specialitate că problema interceptării comunicațiilor a dobândit o preeminență globală, reprezentând o îngrijorare la nivel general a societății, și nu doar a organizațiilor care apără drepturile fundamentale ale persoanelor[2]. Această interdicție a fost observată în jurisprudența Curții de Justiție a Uniunii Europene, care a sancționat în mod repetat forme de supraveghere în masă prin colectarea metadatelor privind toate persoanele care dețineau dispozitive mobile, inclusiv telefoane[3].

În țara noastră, interceptările comunicațiilor au avut un rol deosebit în combaterea criminalității, în special a fenomenului corupției, care ar fi reprezentat și încă reprezintă o problemă majoră a țării noastre[4]. Dincolo de factorul politic european care exagerează fenomenul corupției în România și îl prezintă ca un stigmat al acestei țări, omițând să aibă în vedere propriile cazuri de corupție[5], mai grave decât orice s-ar fi descoperit în țara noastră[6], supravegherea tehnică a avut un rol determinant în descoperirea unor fapte de corupție la noi în țară. Evidentă în cazul țării noastre a fost folosirea excesivă a măsurilor de supraveghere tehnică, inclusiv a interceptărilor în cazuri de corupție mai puțin importante, bună parte având un element de ridicol asociat cu ele[7]. Doar recent s-a dezvăluit că activitatea organelor de urmărire penală era susținută de serviciile secrete prin aplicarea unor protocoale, secrete bineînțeles, prin care organele de urmărire penală colaborau cu serviciile secrete, inclusiv prin echipe comune de anchetă. Fenomenul a avut o asemenea amploare încât, potrivit unui raport parțial al Comisiei comune permanente a Camerei Deputaților și Senatului pentru exercitarea controlului asupra activității S.R.I., în perioada 2005-2016 au fost emise și puse în executare 311.825 de mandate de supraveghere tehnică și mandate de securitate națională, doar în anul 2015 fiind emise 51.248 de mandate. Ținând seama de faptul că un astfel de mandat poate privi un număr mai mare de persoane, a fost de o importanță istorică Decizia nr. 51/2016 a Curții Constituționale, care a determinat scăderea numărului de mandate la 12.992, în anul 2016[8]. Situația României era similară cu cea a Moldovei, unde Curtea Europeană a Drepturilor Omului a constatat că autorizarea unor măsuri de supraveghere tehnică se făcea într-un mod aproape automat, aproape toate solicitările fiind încuviințate de instanțe[9].

---

[1] *N.M. Richards*, The Dangers of Surveillance, în Harvard Law Review, vol. 126, 1934, par. 1959 (2013), pe *harvardlawreview.org*

[2] *S. McKay*, Covert Policing, 2015, p. 65; *P.B. Heymann*, An Essay on Domestic Surveillance, în Journal of National Security Law & Policy, vol. 8:421, 2015, p. 433.

[3] CJUE, cauzele reunite C-293/12 și C-594/12, *Digital Rights Ireland și alții*, Hotărârea din 8 aprilie 2014; cauzele reunite C-203/15 și C-698/15, *Tele2 Sverige AB, Secretary of State for the Home Department și alții*, Hotărârea din 21 decembrie 2016.

[4] Raportul Comisiei Europene privind evoluția situației din România în cadrul mecanismului de cooperare și de verificare din 22 octombrie 2019 (raportul MCV pentru anul 2019), IP/19/6135, pe *ec.europa.eu*

[5] De exemplu, punerea sub acuzare a fostului președinte al Franței, Nicolas Sarkozy, pe *www.theguardian.com*

[6] Un alt exemplu recent îl constituie cazul Airbus, companie care va plăti suma de 3,6 miliarde de euro ca urmare a unor acuzații de dare de mită și alte fapte de corupție în Franța, Marea Britanie și S.U.A., pe *www.euronews.com*

[7] Ne referim la dosarul fostului ministru Decebal Traian Remeș, condamnat pentru că a primit, între altele, caltaboși și țuică, pe *www.hotnews.ro*

[8] Comisia comună permanentă a Camerei Deputaților și Senatului pentru exercitarea controlului asupra activității Serviciului Român de Informații, Raportul parțial reprezentând activitatea comisiei în perioada septembrie 2017 - prezent, referitor la mandatele de securitate națională, mandatele de supraveghere tehnică și la ordonanțele procurorilor pe 48 de ore, 3 octombrie 2018, p. 10, pe *www.cdep.ro*

[9] CEDO, cauza *Iordachi ș.a. c. Moldova*, Hotărârea din 10 februarie 2009, §51-52, pe *hudoc.echr.coe.int*

Considerăm că numărul excesiv de mandate emise poate fi un exces din partea judecătorilor, prin evaluarea în mod superficial a condițiilor legale de autorizare, dar și o neglijență flagrantă din partea controlului parlamentar al S.R.I. Acest din urmă aspect a fost subliniat de Curtea Constituțională prin Decizia nr. 26/2019, unde a reținut că, deși era cunoscut numărul total al mandatelor emise și puse în executare de S.R.I., comisia parlamentară a constatat că „*Serviciul Român de Informații, în 2014, și-a desfășurat activitatea cu respectarea strictă a prevederilor constituționale, a reglementărilor naționale în materie, precum și a normelor naționale, comunitare și internaționale referitoare la protecția drepturilor și libertăților fundamentale ale cetățeanului (...)*"[1], ceea ce reflectă un dezinteres total al Parlamentului față de respectarea dreptului la viață privată al cetățenilor ori o influență a serviciilor de informații și asupra factorului politic.

Astfel cum s-a arătat în doctrină, măsurile de supraveghere tehnică, precum interceptarea comunicațiilor, aduc un grad mare de fidelitate și de certitudine cu privire la probele obținute prin acestea, însă ridică multe probleme privind respectarea drepturilor omului[2].

Conceptul de „interceptare a comunicațiilor" implică mai multe procedee concrete, pe care le vom detalia în cuprinsul lucrării, importantă fiind caracteristica principală ce constă în intruziunea în canalul de comunicații, astfel că probele vor fi obținute fără ca oricare dintre persoanele interceptate să cunoască acest lucru și, de regulă, fără a exista o interferență din punct de vedere tehnic asupra dispozitivelor folosite de acestea. Interceptarea comunicațiilor prezintă similarități cu supravegherea video, audio sau prin fotografiere, întrucât ambele pot presupune înregistrarea de conversații purtate de persoanele vizate, fiind uneori mai dificil să se stabilească diferențe între cele două măsuri. În literatura de specialitate engleză s-a arătat că, în trecut, folosirea unui dispozitiv pentru ascultarea în timp real a unei conversații în mediu ambiental (autorul citat dă exemplul unui polițist care „trage cu urechea") ar constitui o interceptare a comunicațiilor, necesitând o autorizare distinctă în asemenea situații[3]. O altă situație problematică o poate reprezenta o comunicație video între două persoane, capturându-se, prin interceptare, imagini și sunet de la ambele persoane. Deși prezintă similarități cu supravegherea audiovideo, aceasta va rămâne tot o interceptare a comunicațiilor prin modul în care se realizează – interceptarea semnalului celor două dispozitive –, atât emițător, cât și receptor.

Ca orice metodă specială de supraveghere, interceptarea comunicațiilor va avea un caracter tehnic, ceea ce semnifică că este necesară utilizarea unor dispozitive apte pentru realizarea scopului măsurii. Aceasta va include interceptarea atât a convorbirilor telefonice clasice, cât și orice alte comunicări realizate la distanță de o persoană prin mijloace electronice[4]. Caracterul electronic nu este menționat expres de legiuitor, însă a fost prevăzută o măsură de cercetare alternativă în cazul comunicărilor în scris – reținerea, predarea și percheziționarea trimiterilor poștale în care comunicările se realizează în scris. Nu vom putea aplica metoda specială de supraveghere dacă comunicarea la distanță s-ar realiza prin semne, semnale acustice specifice, luminoase sau chiar semnale cu fum, aceste activități putând fi supuse supravegherii audio, video sau prin fotografiere. Deocamdată, comunicațiile se pot realiza numai prin mijloace electronice, însă nu este de exclus posibilitatea ca, în viitorul apropiat, să se realizeze comunicări prin alte mijloace.

[1] CCR, Dec. nr. 26 din 16 ianuarie 2019, §81 (M. Of. nr. 193 din 12 martie 2019).
[2] *A. Ashworth, M. Redmayne*, The Criminal Process, 2014, p. 125.
[3] *S. McKay*, Covert Policing, 2015, p. 67.
[4] *O.S. Kerr*, op. cit., p. 296.

Relevanța metodei speciale de supraveghere a interceptării comunicațiilor ca procedeu probatoriu este una deosebită, întrucât permite obținerea de probe directe în procesul penal, putând contribui determinant la tragerea la răspundere penală a infractorilor. Printr-o interceptare a comunicațiilor poate fi surprins momentul săvârșirii infracțiunii, în cazul în care executarea acesteia se face prin mijloace verbale[1], fiind probă suficientă pentru a se dovedi existența infracțiunii, constituind și o probă foarte greu de combătut pentru apărare. Măsura de supraveghere tehnică va putea fi utilizată și pentru obținerea de probe indirecte în procesul penal, în special când este folosită pentru a stabili activitățile unor persoane sau relațiile dintre acestea. În cazul infracțiunii de constituirea unui grup infracțional organizat, prevăzută de art. 367 C.pen., se va putea stabili componența grupului infracțional, dar și structura și rolul fiecărui membru[2].

Prin posibilitatea utilizării sale pe o scară largă asupra unui număr nelimitat de persoane, interceptarea comunicațiilor este aptă să producă o gravă ingerință drepturilor fundamentale ale multor persoane prin restrângerea dreptului la viață privată. Caracterul social al ființei umane și comoditatea utilizării unor mijloace electronice de comunicare la distanță fac din interceptarea comunicațiilor o metodă specială propice pentru supravegherea ascunsă a unei persoane. Această împrejurare o face și metoda cea mai puțin previzibilă cu privire la numărul persoanelor ale căror drepturi vor fi restrânse în mod colateral, fiindcă nu se poate anticipa numărul, durata, frecvența și natura convorbirilor pe care le va avea persoana supravegheată. Nu doar persoana care va face obiectul măsurii de supraveghere tehnică va cunoaște o restrângere a drepturilor sale, ci toate persoanele cu care aceasta intră în contact. Consecința este că, la consemnarea rezultatelor activităților de supraveghere tehnică, va trebui să existe o selectare riguroasă a convorbirilor și comunicărilor obținute, precum și înlăturarea acelora care nu au relevanță cu cauza pentru ca, în final, acestea să fie distruse cu scopul de a preveni accesarea lor abuzivă.

În mod evident, interceptarea comunicațiilor este măsura de supraveghere tehnică cu gradul cel mai scăzut de toleranță la divulgarea secretului operațiunii, persoana supravegheată putând sista orice comunicație. Dreptul la viață privată al acesteia va fi incontestabil restrâns, chiar și libertatea de conștiință va fi afectată, întrucât vor putea fi interceptate și înregistrate toate nemulțumirile, credințele și opiniile unei persoane, mai ales cele pe care nu și le-ar exprima public, dar pe care le poate expune atunci când are o convorbire cu o persoană de încredere.

Din punct de vedere legal, reglementarea unei astfel de măsuri de supraveghere tehnică era necesară pentru a justifica ingerința care poate fi adusă dreptului la viață privată. Lipsa unei atare prevederi, dată fiind utilitatea interceptării comunicațiilor în unele cauze, ar fi constituit o ingerință nelegală în viața privată a unei persoane, prin raportare la art. 8 par. 2 Conv.EDO. O atare situație a fost constatată în repetate rânduri de către Curtea Europeană a Drepturilor Omului, atunci când autoritățile din domeniul judiciar au procedat la folosirea interceptării comunicațiilor (ori măsuri de supraveghere tehnică, în general) fără a fi prevăzute expres de lege.

[1] De exemplu, prin acțiunea de amenințare care intră în latura obiectivă a infracțiunii de șantaj, acceptarea în cazul infracțiunii de luare de mită etc.

[2] *G. Buftea*, Măsuri eficiente împotriva Criminalității Organizate Transnaționale, în Revista de investigare a criminalității, vol. 8, nr. 2/2015, pp. 12-13.

În sistemul englez, cauza *Malone c. Marea Britanie*[1] a avut impact deosebit, întrucât, până la pronunțarea hotărârii, nu exista nicio reglementare a interceptării comunicațiilor, ca urmare a acesteia adoptându-se o legislație specială pentru această măsură (Interception of Communications Act 1985), în vederea acoperirii lipsei unui cadru legal clar și previzibil pentru realizarea interceptărilor[2] și ca urmare a obligațiilor pozitive ale statelor în protejarea dreptului la viață privată[3].

În cauza *Kruslin c. Franța* s-a mers mai departe cu raționamentul din cauza *Malone c. Marea Britanie*, întrucât, deși dreptul francez prevedea posibilitatea folosirii interceptării comunicațiilor, legea era una deficitară, nedetaliind elementele esențiale și fiind în dezacord cu art. 8 Conv.EDO[4]. În concret, Curtea a reținut că nu există garanții suficiente cuprinse în lege ca urmare a existenței următoarelor aspecte: lipsa mențiunilor privind categoriile de persoane care pot fi ascultate, natura infracțiunilor care pot justifica o astfel de măsură, prevederea unei limite temporale a interceptărilor, procedura de certificare a convorbirilor interceptate, a posibilității controlului judecătorului asupra acestora, dar și condițiile în care înregistrările trebuie șterse sau distruse[5].

În mod similar, s-a stabilit o lipsă a caracterului complet al legislației în cauza *Govell c. Marea Britanie*[6], în care Curtea a constatat că supravegherea s-a desfășurat prin încălcarea dreptului la viață privată, întrucât legislația nu prevedea o reglementare, existând numai ghiduri polițienești ale Home Office care nu erau obligatorii sau opozabile *erga omnes*. Ulterior, în cauza *Khan c. Marea Britanie*[7], Curtea a constatat că, în cauza *Govell c. Marea Britanie*, nu numai că nu exista un cadru legal pentru supraveghere, dar acesta trebuia să fie în concordanță cu statul de drept, astfel că era necesar să ofere o protecție contra arbitrariului prin caracterul previzibil și clar al legii, iar pentru un eventual acuzat, ingerința în viața sa privată să fie una previzibilă.

În concluzie, utilitatea interceptării comunicațiilor constituie o metodă specială de supraveghere care poate conduce la obținerea de probe determinante în cursul urmăririi penale, dar cu restrângerea drepturilor la viață privată a persoanei. Pentru ca aceasta să se realizeze în acord cu Convenția Europeană a Drepturilor Omului, este necesar ca măsura să fie reglementată prin lege, aceasta din urmă să aibă un caracter clar și previzibil în special cu privire la modalitățile în care măsura se va desfășura, asupra modului în care se vor consemna activitățile, limitarea ei în timp și, în general, asigurarea unor garanții efective împotriva abuzurilor autorităților.

[1] CEDO, cauza *Malone c. Marea Britanie*, Hotărârea din 2 august 1984, §68, pe *hudoc.echr.coe.int*; a se vedea și *A. Băcăuanu*, Technical Surveillance in the European Union Judicial System. Aspects of Comparative Law, în Acta Universitatis Danubius, vol. 10, no. 1/2018, p. 76.

[2] *S. McKay*, Covert Policing, 2015, p. 88.

[3] *A. Ashworth*, op. cit., pp. 199-200.

[4] CEDO, cauza *Kruslin c. Franța*, Hotărârea din 24 aprilie 1990, §36, pe *hudoc.echr.coe.int*

[5] *Ibidem*, §35.

[6] CEDO, cauza *Govell c. Marea Britanie*, Hotărârea din 14 ianuarie 1998, §62, pe *hudoc.echr.coe.int*

[7] CEDO, cauza *Khan c. Marea Britanie*, Hotărârea din 4 octombrie 2000, §26, pe *hudoc.echr.coe.int*

Secțiunea a 2-a. Interceptarea comunicațiilor ori a oricărui tip de comunicare la distanță înainte de intrarea în vigoare a Codului de procedură penală

Metoda specială de supraveghere a interceptării comunicațiilor ori a oricărui tip de comunicare la distanță nu constituie o noutate pentru procesul penal român, posibilitatea folosirii acesteia existând și în cuprinsul Codului de procedură penală anterior, în care era denumită „interceptarea și înregistrarea convorbirilor sau comunicărilor efectuate prin telefon ori prin orice mijloc electronic de comunicare". În doctrină s-a arătat că formularea curentă a denumirii acestui procedeu este una defectuoasă, întrucât nu acoperă și activitatea de înregistrare, fiind preferabilă denumirea veche instituită de legiuitor[1]. În opinia noastră, credem că denumirea este oricum prea lungă prin includerea „comunicărilor la distanță", fiind preferabilă o denumire simplificată, alături de definirea completă a terminologiei folosite de legiuitor, astfel cum se face și în cuprinsul art. 138 alin. (2) C.pr.pen. De altfel, soluția este aceeași în legislația franceză, unde art. 100 din Codul de procedură penală francez are denumirea marginală „Des interceptions de correspondances émises par la voie des communications électroniques"[2], o situație similară fiind și în legislația engleză, unde denumirea prevăzută în Investigatory Powers Act 2016 este „Interception of communications"[3].

Până la pronunțarea Deciziei nr. 51/2016, interceptarea și înregistrarea convorbirilor sau comunicărilor era o metodă de supraveghere folosită regulat în cercetarea cazurilor de corupție.

Potrivit art. 91[1] alin. (1) C.pr.pen. anterior, „*interceptarea și înregistrarea convorbirilor sau comunicărilor efectuate prin telefon ori prin orice mijloc electronic de comunicare se realizează cu autorizarea motivată a judecătorului, la cererea procurorului care efectuează sau supraveghează urmărirea penală, în condițiile prevăzute de lege, dacă sunt date ori indicii temeinice privind pregătirea sau săvârșirea unei infracțiuni pentru care urmărirea penală se efectuează din oficiu, iar interceptarea și înregistrarea se impun pentru stabilirea situației de fapt ori pentru ca identificarea sau localizarea participanților nu poate fi făcută prin alte mijloace ori cercetarea ar fi mult întârziată*". Din acest text legal nu rezulta o definiție propriu-zisă a metodei speciale de supraveghere, ci, mai degrabă, numai condițiile legale ale acesteia. Legiuitorul făcea referire numai la interceptarea și înregistrarea convorbirilor efectuate prin telefon – o categorie limitată de comunicări, prin raportare la situația tehnologică actuală, dar și la cele privind orice mijloc electronic de comunicare. Din acest punct de vedere, menționea că mijlocul de comunicare trebuie să fie electronic era preferabilă reglementării actuale, care nu mai include această condiție în mod expres, trebuind să fie dedusă. Desigur, se subînțelege că mijlocul de comunicare va trebui să fie unul electronic, altfel putând fi aplicabile alte procedee probatorii prevăzute de lege.

Observăm că există unele asemănări cu procedura de autorizare prevăzută în Codul de procedură penală în vigoare. Din punctul de vedere al condițiilor legale, mai puțin cea privind infracțiunile a căror urmărire poate justifica autorizarea măsurilor de supraveghere tehnică, care presupune explicații suplimentare, Codul de procedură penală actual stabilește în mod expres condițiile de suspiciune rezonabilă, proporționalitate și subsidiaritate. Expunerea în Codul de procedură penală anterior se limita la existența de date ori indicii temeinice privind săvârșirea

[1] *Gh. Mateuț*, Procedură penală, 2019, p. 674.

[2] trad. *Interceptarea corespondenței transmise prin comunicații electronice.*

[3] trad. *Interceptarea comunicațiilor.*

unei infracțiuni și necesitatea autorizării interceptărilor și înregistrărilor față de insuficiența măsurilor alternative, lipsind condiția proporționalității cu desăvârșire. „Existența unor date sau indicii temeinice privind pregătirea sau săvârșirea unei infracțiuni" este o altă expresie pe care o considerăm inferioară celei actuale, care, ținând seama de întinsa jurisprudență străină privind conceptul de „suspiciune rezonabilă" (împrumutat din dreptul american și englez), poate permite judecătorilor să înțeleagă mai bine acest standard.

În privința infracțiunilor pentru care se puteau autoriza mijloacele de supraveghere tehnică, acestea erau prevăzute la art. 91[1] alin. (2) C.pr.pen.[1] și erau similare cu cele din legislația actuală, legiuitorul enumerând limitativ o serie de infracțiuni considerate a fi suficient de grave pentru a justifica folosirea unor procedee probatorii intruzive și derogatorii.

Procedura de autorizare a interceptărilor și înregistrărilor prevăzută de art. 91[1] alin. (3) C.pr.pen. anterior[2] era similară actualei, desfășurându-se în camera de consiliu, autorizația fiind emisă de președintele instanței sau, în lipsa acestuia, de judecătorul desemnat de acesta, pentru o durată care nu putea depăși 30 de zile. Spre deosebire de reglementarea actuală, durata totală de autorizare a măsurii speciale de supraveghere era de 120 de zile, un termen care a fost prelungit, în prezentul Cod, la 6 luni.

În ceea ce privește punerea în executare a interceptărilor și înregistrărilor, aceasta se putea realiza de către procuror, potrivit art. 91[2] alin. (1) C.pr.pen. anterior, sau se putea dispune de către acesta să se realizeze de către organele de cercetare penală, lipsind cu desăvârșire posibilitatea ca punerea în executare să se realizeze de „lucrători specializați ai poliției sau de alte organe specializate ale statului". În realitate, toate interceptările erau puse în executare de către S.R.I., organele de urmărire penală neavând nicio implicare și neavând nici posibilitatea de a realiza ele însele aceste acte, deoarece S.R.I. deținea tehnica necesară realizării interceptărilor. Mai înainte de pronunțarea Deciziei nr. 51/2016 a Curții Constituționale, site-ul S.R.I. chiar conținea o mențiune publică asupra atribuției lor exclusive de a realiza în cadrul urmăririi penale interceptările și înregistrările autorizate de judecător. Desigur, vina era a sistemului judiciar că a acceptat și apoi a devenit complice în a permite unui serviciu secret să se substituie organelor de urmărire penală și să dobândească acces la informații cu caracter nepublic. Astfel, chiar dacă am fi fost tentanți, anterior deciziei Curții Constituționale menționate, să considerăm superioară vechea reglementare , adevărul este că, deși era clară și previzibilă în sensul jurisprudenței Curții Europene a Drepturilor Omului, sistemul judiciar a fost cel care a decis să ignore legea sub imperiul vechiului Cod.

Un progres al legii, prin raportare la Codul de procedură penală anterior, îl constituie instituirea unei proceduri unitare de autorizare a măsurilor de supraveghere tehnică, în care rolul principal îl are judecătorul de drepturi și libertăți. Din punctul de vedere al sistematizării,

[1] Conform art. 91[1] alin. (2) C.pr.pen. anterior, „interceptarea și înregistrarea convorbirilor sau comunicărilor efectuate prin telefon ori prin orice mijloc electronic de comunicare pot fi autorizate în cazul infracțiunilor contra siguranței naționale prevăzute de Codul penal și de alte legi speciale, precum și în cazul infracțiunilor de trafic de stupefiante, trafic de arme, trafic de persoane, acte de terorism, spălare a banilor, falsificare de monede sau alte valori, în cazul infracțiunilor prevăzute de Legea nr. 78/2000 pentru prevenirea, descoperirea și sancționarea faptelor de corupție, cu modificările și completările ulterioare, în cazul unor alte infracțiuni grave ori al infracțiunilor care se săvârșesc prin mijloace de comunicare electronică".

[2] Conform art. 91[1] alin. (3) C.pr.pen. anterior, „autorizația se da pentru durata necesară interceptării și înregistrării, dar nu pentru mai mult de 30 de zile, în camera de consiliu, de președintele instanței căreia i-ar reveni competența sa judece cauza în prima instanța sau de la instanța corespunzătoare în grad acesteia, în a cărei circumscripție se afla sediul parchetului din care face parte procurorul care efectuează sau supraveghează urmărirea penala. În lipsa președintelui instanței autorizația se da de către judecătorul desemnat de acesta".

Codul în vigoare este superior, deoarece nu transpune procedura interceptărilor și înregistrărilor la alte măsuri de supraveghere tehnică, ci prevede că va trebui ca, pentru fiecare dintre măsuri, să se procedeze la o analiză distinctă, prin raportare la criteriile generale prevăzute de art. 139 C.pr.pen.

Secțiunea a 3-a. Forma actuală a interceptării comunicațiilor ori a oricărui tip de comunicare la distanță

În prezent, interceptarea comunicațiilor ori a oricărui tip de comunicare la distanță constituie o metodă de supraveghere tehnică, amintită expres în cuprinsul art. 138 alin. (13) C.pr.pen. Fiind o astfel de metodă, autorizarea acesteia va trebui să se realizeze cu îndeplinirea tuturor condițiilor legale prevăzute de art. 139 C.pr.pen., a procedurii autorizării, dar și cea a punerii în executare a măsurii. O importanță deosebită o va avea consemnarea activităților de supraveghere tehnică obținute prin această metodă, procesele-verbale de redare integrală a convorbirilor telefonice fiind cel mai des întâlnite mijloace de probă ce pot rezulta din supravegherea tehnică. Întrucât face parte din supravegherea tehnică, prin folosirea acestei metode speciale, se vor obține probe în procesul penal, și nu doar date și informații, precum în cazul altor metode speciale de cercetare.

Dincolo de definiția legală a măsurii, nu poate fi contestat caracterul de măsură de supraveghere tehnică al acesteia, întrucât reprezintă un procedeu probatoriu prin care sunt restrânse drepturile fundamentale ale persoanei, are un caracter secret și pentru viitor, se poate dispune numai în cursul urmăririi penale și autorizarea ei se va face de judecătorul de drepturi și libertăți, în condițiile legii.

Potrivit art. 138 alin. (2) C.pr.pen., măsura de supraveghere specială este definită: „*prin «interceptarea comunicațiilor ori a oricărui tip de comunicare» se înțelege interceptarea, accesul, monitorizarea, colectarea sau înregistrarea comunicărilor efectuate prin telefon, sistem informatic ori prin orice alt mijloc de comunicare*".

Prin „comunicație" vom înțelege o conversație purtată printr-un mijloc de comunicare la distanță, care va permite transmiterea sunetului persoanelor participante la convorbire printr-un canal de comunicație electronic. Alături de sunetele transmise – conversația în sine –, vom considera convorbire și un dialog purtat prin sisteme care transmit și imagini video la distanță în timp real. O convorbire va putea fi realizată atât prin intermediul unui telefon, cât și prin intermediul unui sistem informatic. Nu va fi necesar ca, pentru realizarea convorbirii, interlocutorii să dețină sau să folosească numere de telefon, fiind posibilă existența unei convorbiri și prin internet sau prin folosirea unor echipamente de radiotransmisie care să comunice direct (de exemplu, *walkie-talkie*).

Prin „comunicare" vom înțelege transmiterea unei informații către o altă persoană, altele decât sunete sau imagini, în timp real, acestea putând fi e-mailuri[1], SMS-uri, mesaje transmise prin alte aplicații sau servicii, precum Signal, Whatsapp, Facebook, Viber etc. Vom include în acest tip de comunicări și datele informatice transmise.

Pentru a face o diferență între cele două concepte, apreciem că un criteriu care se impune a fi folosit este *simultaneitatea comunicării bilaterale dintre persoane*, astfel că o comunicație va avea loc numai atunci când atât emițătorul, cât și receptorul vor putea avea acest rol în mod

[1] *D.E. Hall*, op. cit., p. 408.

simultan, evident și în timp real. De pildă, va fi o comunicație o convorbire telefonică, în timp ce transmiterea unui mesaj către căsuța vocală a unei persoane va constitui o comunicare. După cum s-a arătat în doctrină, va avea o influență deosebită natura conținutului datelor transmise și destinația acestora[1]. În ceea ce ne privește, apreciem că o comunicație poate exista numai prin raportare la o persoană și în timp real, însă o comunicare poate avea loc și față de un sistem informatic, precum situația unui server de e-mail, pe care ulterior îl va putea accesa destinatarul mesajului.

În literatura de specialitate se încearcă o diferențiere între *comunicație* și *comunicare*, considerându-se, pe de o parte, că prin „comunicare" se înțelege acțiunea de a comunica și rezultatul acestei acțiuni, iar, pe de altă parte, prin „comunicație" se înțelege un mijloc de comunicare între puncte diferite ori un sistem tehnic folosit pentru realizarea acțiunii de a comunica[2]. O altă opinie este în sensul în care prin „comunicare" trebuie înțeles orice schimb de informații, fie că aceasta este de tip text, imagine, audio, video, audio-video etc., iar prin „comunicație" trebuie să înțelegem orice transmitere de informații, chiar dacă aceasta nu vizează ca destinație o altă persoană[3].

Autorii menționați operează de la premisa că termenul de „comunicare" va fi cel definit de art. 2 lit. d) din Legea nr. 506/2004: „*orice informație schimbată sau transmisă între un număr determinat de participanți prin intermediul unui serviciu de comunicații electronice destinat publicului; aceasta nu include informația transmisă publicului printr-o rețea de comunicații electronice ca parte a unui serviciu de programe audiovizuale, în măsura în care nu poate fi stabilită o legătură între informația în cauză și abonatul sau utilizatorul identificabil care o primește*". Un atare argument nu poate fi primit, întrucât autorii omit faptul că Legea nr. 506/2004[4] reprezintă transpunerea în dreptul național a Directivei (UE) 2002/58/CE[5], fapt care rezultă din art. 15 din lege, ceea ce impune interpretarea prin prisma textului original. Contrar susținerilor autorilor, din traducerea în română a directivei menționate, termenul de „comunicare" definit prin Legea nr. 506/2004 este înlocuit de termenul „comunicație" în cuprinsul art. 2 lit. d) din Directiva (UE) 2002/58/CE[6]. Mergând mai departe, în forma sa din limba engleză, directiva nu cunoaște nicio distincție între comunicare și comunicație, dat fiind faptul că, în toate cazurile în care traducerea în limba română folosește termenul de „comunicare", traducerea în limba engleză prevede termenul de *communication*.

În consecință, termenul folosit de ambii autori – „comunicare" – este, de fapt, o comunicație în sensul Directivei, care trebuia transpusă obligatoriu în legislația națională, relevând faptul că argumentele expuse nu pot fi pertinente, deoarece nici măcar legislația specială nu face această distincție. Rămânem la opinia că diferențierea dintre cele două concepte trebuie să rămână una doctrinară. De altfel, vedem o importanță practică redusă a stabilirii naturii de comunicație și

[1] *M. Bulancea, G. Zlati, R. Slăvoiu*, în M. Udroiu (coord.), Codul de procedură penală, 2017, p. 637.

[2] *M. Udroiu, R. Slăvoiu, O. Predescu*, Tehnici speciale, 2009, p. 12.

[3] *M. Bulancea, G. Zlati, R. Slăvoiu*, în M. Udroiu (coord.), Codul de procedură penală, 2017, pp. 637-638.

[4] Legea nr. 506 din 17 noiembrie 2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice (M. Of. nr. 1101 din 25 noiembrie 2004).

[5] Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 (J. Of., seria L, nr. 201/37).

[6] Conform art. 2 lit. d) din Directiva 2002/58/CE, „«comunicație» înseamnă orice informație trimisă sau transmisă între un număr finit de părți prin intermediul unui serviciu public de comunicații electronice. Această categorie nu include informațiile transmise în cadrul unui serviciu de radiodifuziune pentru public prin intermediul unei rețele de comunicații electronice, în măsura în care aceste informații nu pot fi relaționate cu un abonat sau cu un utilizator identificabil care primește informația".

comunicare, mai ales în situația similarității celor doi termeni. Menținerea celor doi termeni poate fi utilă, deoarece, din punct de vedere evolutiv, pot exista schimbări care să conducă la o distincție mai puternică între aceștia, precum dezvoltarea unor moduri de comunicare la distanță neelectronice, precum teleportarea cuantică, care nu presupune o legătură electronică între emițător și receptor[1], fapt care a fost dovedit prin rezultatele unei cercetări recente[2].

Acțiunea de interceptare nu este definită de legiuitor, însă presupune ca o convorbire sau o comunicare să fie captată concomitent cu realizarea ei de către un terț care se interpune între emițător și receptor și care va putea să constate conținutul mesajului dintre cei doi. Interceptarea va presupune întotdeauna o intervenție din partea unui organ de urmărire penală, neputând fi realizată de un particular[3]. Interceptarea se va putea realiza prin diverse metode, de la cele mai vechi (precum cele electrice: atașarea unor dispozitive de cablul de telefonie fixă care vor capta semnalul, releuri, creare de derivații etc.), până la cele mai moderne [electronice: folosirea sistemului informatic al C.N.I.C. (din cadrul S.R.I.), folosirea unor dispozitive denumite Stingray prin care se simulează un turn de emisie-recepție GSM la care se conectează, fără știrea persoanei supravegheate și prin care se interceptează comunicațiile sale etc.].

În ceea ce privește acțiunea de accesare a comunicărilor, s-a apreciat în doctrină că reprezintă „*vizualizarea (fișiere tip text, video, imagine etc.) ori ascultarea (fișiere audio) prin acțiune cu datele informatice stocate într-un sistem informatic ori mijloc de stocare a datelor informatice. (…) accesarea comunicării reprezintă și un acces la sistemul informatic ori la mijlocul de stocare*"[4]. O atare interpretare o considerăm greșită, întrucât relevă un alt procedeu probatoriu incident, un acces la un sistem informatic sau o percheziție informatică, ceea ce nu corespunde cu specificul interceptării comunicațiilor, descriind o metodă prin care sunt accesate date informatice deja obținute. Or, aceasta este caracteristică măsurii de supraveghere tehnică a accesului la un sistem informatic, nefiind permisă înglobarea unei alte măsuri de supraveghere tehnice în alta, ele trebuind să aibă sfere de activitate diferite[5]. Sub acest aspect, s-a pronunțat și doctrina străină, accesarea unei comunicații deja stocate sau obținute de o altă persoană decât organele de urmărire penală neputând fi realizată printr-un procedeu probatoriu obișnuit (de exemplu, predarea obiectelor, înscrisurilor sau datelor informatice)[6].

Credem că, în realitate, *accesul* nu constituie decât încercarea legiuitorului de a caracteriza modalitatea în care se realizează cel mai des interceptările, respectiv prin sistemul informatic aflat în proprietatea S.R.I. Astfel, accesul ține de modalitatea concretă de realizare a interceptării, nefiind necesară în unele dintre situațiile arătate. Lămuririle necesare le putem descoperi în Protocolul încheiat între Ministerul Public și S.R.I.[7] cu privire la folosirea judiciară de către

[1] Pentru explicarea conceptului, a se vedea *www.nature.com* și, pentru prima demonstrație a conceptului, *www.sciencealert.com*

[2] *D. Llewellyn, Y. Ding, I.I. Faruque ș.a.*, Chip-to-chip quantum teleportation and multi-photon entanglement in silicon, în Nature Physics, vol. 16, 2020, pp. 148-153, pe *doi.org*

[3] *C. Olaru*, op. cit., p. 22.

[4] *M. Bulancea*, *G. Zlati*, *R. Slăvoiu*, în M. Udroiu (coord.), Codul de procedură penală, 2017, p. 639.

[5] Aceasta nu va însemna că nu se vor putea autoriza mai multe măsuri de supraveghere tehnică, folosite în paralel, pentru realizarea unor operațiuni complexe, precum interceptarea comunicațiilor prin intermediul unui software instalat la distanță pe sistemul informatic al persoanei față de care s-a autorizat supravegherea tehnică.

[6] *C. Fehr*, The Constitutionality of Using Production Orders to Obtain Stored Communications Content, în Canadian Criminal Law Review (2018), 23:2, pp. 173-176.

[7] Protocol privind cooperarea între Serviciul Român de Informații și Ministerul Public pentru stabilirea condițiilor concrete de acces la sisteme tehnice ale Centrului Național de Interceptare a Comunicațiilor,

procuror și organele de cercetare penală a sistemului informatic de interceptare al C.N.I.C., în care, la art. 2, se arată: „*Serviciul Român de Informații asigură Ministerului Public, structurilor sale centrale sau teritoriale, precum și organelor de cercetare penală delegate de procuror,* ***accesul direct, nemijlocit și independent la sisteme tehnice deținute și administrate de acesta, prin Centrul Național de Interceptare a Comunicațiilor****, pentru punerea în aplicare a actelor de autorizare emise în temeiul prevederilor Codului de procedură penală sau a legii speciale (…)*" (s.n.). Este relevant că termenul „acces" se repetă în cuprinsul protocolului menționat, reflectând că sensul avut în vedere de legiuitor trebuie interpretat în acest sens. Mai mult, trebuie avut în vedere faptul că accesarea reprezintă numai prima etapă în interceptare.

După cum am amintit mai sus, art. 138 alin. (2) C.pr.pen. indică într-un mod progresiv și etapele în care se poate realiza interceptarea prin sistemul informatic al S.R.I. Accesarea este prima etapă în interceptare și presupune ca procurorul sau organul de cercetare delegat de procuror să folosească echipamentul (sistem informatic) din sediul parchetului dedicat exclusiv pentru conectare la C.N.I.C. și să acceseze sistemul informatic, dobândind control asupra sistemului național de interceptare. Simplul acces la Centru nu va însemna acces la un sistem informatic în sensul art. 138 alin. (1) lit. b) C.pr.pen., ci prin „acces" trebuie să înțelegem acces la comunicații, asta presupunând folosirea sistemului informatic al S.R.I. pentru implementarea tehnică a mandatului de supraveghere tehnică în vederea interceptării de către acest sistem informatic a comunicațiilor. Comunicațiile interceptate vor fi *înregistrate în sistemul informatic al S.R.I.*, la dispoziția exclusivă a organului de urmărire penală care a implementat în sistem mandatul de supraveghere tehnică[1].

Înregistrarea constituie componenta interceptării care conduce la crearea rezultatelor activităților de supraveghere tehnică sub formă de date informatice. Întrucât metodele speciale de supraveghere reprezintă procedee probatorii, prin înregistrarea comunicațiilor sau comunicărilor interceptate se poate realiza scopul pentru care a fost instituit acest procedeu probatoriu. În doctrină se apelează la noțiunea de „captare" referitor la înregistrare, aceasta din urmă constituind copierea comunicărilor „captate" la momentul interceptării propriu-zise[2]. Credem că explicația dată în doctrină presupune niște precizări de ordin tehnic. Modalitatea prin care se realizează interceptările de către sistemul informatic al S.R.I. se bazează pe conectarea sistemului la infrastructura informatică a furnizorilor de rețele publice de comunicații electronice și a furnizorilor de servicii de comunicații electronice destinate publicului prin dispozitive speciale care permit captarea semnalelor de la nivelul furnizorului și transmiterea acestora către C.N.I.C., unde se va realiza înregistrarea lor. Nu credem că vom vorbi despre o copiere propriu-zisă, ci mai degrabă de o îmbinare a semnalelor și o procesare a lor de către un sistem informatic și apoi transmiterea lor, de către furnizori, către C.N.I.C., unde vor fi înregistrate și stocate în vederea colectării lor de către organele de urmărire penală. Credem că prin această metodă se asigură autenticitatea modalității de interceptare a comunicării, o atare cerință fiind subliniată în doctrină drept esențială[3].

încheiat sub nr. 2440/C din 08.12.2016 și nr. 9331 din 07.12.2016, între Ministerul Public prin Parchetul de pe lângă Înalta Curte de Casație și Justiție și Serviciul Român de Informații.

[1] Conform art. 2 lit. a) din Protocol, Serviciul Român de Informații: „asigură Ministerului Public sau organelor de cercetare penală delegate de acesta **accesul direct, nemijlocit și independent** la sistemul tehnic de interceptare, în scopul punerii în aplicare, în sistem centralizat, a mandatelor de supraveghere tehnică" (s.n.).

[2] *M. Bulancea, G. Zlati, R. Slăvoiu*, în M. Udroiu (coord.), Codul de procedură penală, 2017, p. 639.

[3] *D.E. Hall*, op. cit., p. 409.

Colectarea comunicărilor constituie valorificarea rezultatelor obținute prin implementarea mandatului de supraveghere tehnică în sistemul informatic al C.N.I.C. Tehnic, sistemul informatic realizează o înregistrare care va fi la dispoziția organelor de urmărire penală, în serverele S.R.I., până la momentul la care acestea vor fi colectate. „Colectarea" înseamnă, din punct de vedere informatic, mutarea datelor informatice de pe serverele S.R.I. pe sistemul informatic aflat la sediul parchetului, în condiții care să asigure autenticitatea și integritatea datelor informatice. Prin colectare se pune în evidență caracterul automat al interceptării comunicațiilor, organul de urmărire penală trebuind doar să colecteze rezultatele atunci când consideră că este necesar. Deși S.R.I. oricum nu are acces la datele informatice respective[1], credem că, la momentul colectării datelor informatice, acestea trebuie să fie distruse de pe sistemul informatic al S.R.I., ceea ce pare a fi situația la momentul actual, potrivit rapoartelor de control desfășurate de președintele Înaltei Curți de Casație și Justiție la C.N.I.C.

Monitorizarea comunicațiilor presupune supravegherea acestora în timp real, fără a fi obligatorie și obținerea unei copii a informației interceptate[2]. O atare monitorizare credem că implică atât folosirea unui sistem informatic, precum cel aflat în proprietatea S.R.I., cât și posibilitatea folosirii unor mijloace specifice de interceptare, precum dispozitivele Stingray pentru dispozitive mobile. În plus, s-a arătat în mod corect în doctrină[3] că monitorizarea poate presupune analizarea în timp real a pachetelor wireless transmise. Deși este adevărată afirmația, credem că se va impune și înregistrarea acestora ca date informatice pentru a fi ulterior analizate în mod complet[4]. De pildă, și în situația în care comunicațiile s-ar realiza prin intermediul unor căi de comunicații criptate prin internet (inclusiv folosirea rețelei TOR), datele informatice sau cel puțin destinația acestora se vor putea determina pe baza dimensiunii fiecărui pachet transmis.

[1] Sub acest aspect, încă avem anumite îndoieli până la momentul la care S.R.I. va face publice minime informații tehnice care să permită o transparență în această privință. Tehnic, este posibil ca datele informatice să nu fie accesibile S.R.I., putând fi criptate automat cu o cheie asimetrică ce permite decriptarea informațiilor numai de către sistemul informatic aflat în incinta parchetului.

[2] *M. Bulancea, G. Zlati, R. Slăvoiu*, în M. Udroiu (coord.), Codul de procedură penală, 2017, p. 639.

[3] *Ibidem*, p. 640.

[4] *M. Vondráček*, *J. Pluskal*, *O. Ryšavý*, Automated Man-in-the-Middle Attack Against Wi-Fi Networks, în Journal of Digital Forensics, Security and Law, vol. 13, no. 1/2018, p. 60.

Capitolul II
Autorizarea interceptării comunicațiilor ori a oricărui tip de comunicare la distanță

Secțiunea 1. Condițiile legale pentru autorizarea interceptării comunicațiilor ori a oricărui tip de comunicare la distanță

Interceptarea comunicațiilor ori a oricărui tip de comunicare la distanță presupune o restrângere a drepturilor și libertăților persoanei vizate de acest procedeu probatoriu, motiv pentru care legea condiționează folosirea acestuia numai când sunt îndeplinite anumite condiții și cu garantarea respectării proporționalității între interesul public și interesul individului. Aceste condiții sunt cele comune, avute deja în vedere la analiza capitolului destinat autorizării metodelor de supraveghere tehnică, astfel că în această secțiune vom relua doar unele aspecte esențiale și vom face completări care țin de această metodă specială de cercetare[1].

Organul competent să dispună asupra folosirii metodei speciale de supraveghere este *judecătorul de drepturi și libertăți*, ca regulă. În mod excepțional, *procurorul,* potrivit art. 141 C.pr.pen., va putea dispune limitat, pentru o durată de maximum 48 de ore și cu controlul ulterior al judecătorului de drepturi și libertăți, interceptarea convorbirilor ori comunicațiilor.

Metoda specială de supraveghere tehnică se va putea încuviința numai dacă sunt îndeplinite condițiile cumulative prevăzute de art. 139 C.pr.pen. O condiție implicită constă în necesitatea începerii urmăririi penale pentru o faptă prevăzută de legea penală. Această condiție reiese din faptul că începerea urmăririi penale este actul procesual care creează întreg cadrul pentru desfășurarea activităților de urmărire penală, inclusiv administrarea probelor, întrucât Codul de procedură penală actual nu mai recunoaște faza actelor premergătoare din Codul de procedură penală anterior. În doctrină s-a arătat că, sub imperiul Codului de procedură penală anterior, desfășurarea interceptărilor în faza actelor premergătoare era inadmisibilă[2]. Abordarea avea în vedere împrejurarea că interceptările și înregistrările aveau ca finalitate obținerea unor mijloace de probă în procesul penal care să conducă la stabilirea adevărului în mod obiectiv[3], or, în faza actelor premergătoare nu se putea administra probe, ci numai obține date și informații în vederea începerii urmăririi penale.

O particularitate a acestei măsuri de supraveghere tehnică este strânsa sa corelație cu autorizarea măsurilor de supraveghere tehnică, la cererea motivată a persoanei vătămate, prevăzută de art. 140 alin. (9) C.pr.pen.[4]. În opinia noastră, o lecturare a acestor dispoziții legale face trimitere tocmai la această metodă specială de supraveghere, întrucât particularii nu pot

[1] *V. supra*, Titlul III, Capitolul I.

[2] *S. Grădinaru*, Supravegherea tehnică, 2014, pp. 197-198.

[3] *Gh. Mateuț*, În legătură cu noua reglementare privind înregistrările audio sau video în probațiunea penală, în Dreptul nr. 8/1997, p. 70.

[4] Conform art. 140 alin. (9) C.pr.pen., „la cererea motivată a persoanei vătămate, procurorul poate solicita judecătorului autorizarea interceptării comunicațiilor ori înregistrării acestora, precum și a oricăror tipuri de comunicări efectuate de aceasta prin orice mijloc de comunicare, indiferent de natura infracțiunii ce formează obiectul cercetării. Dispozițiile alin. (1)-(8) se aplică în mod corespunzător".

deține tehnica necesară pentru realizarea unor asemenea interceptări[1], posibilitățile deținerii sale fiind restrânse prin lege. Această particularitate are drept consecință imposibilitatea aplicării dispozițiilor art. 139 alin. (3) C.pr.pen. în această cauză, întrucât activitatea de interceptare nu se poate realiza de către o persoană particulară, fără a aduce o ingerință dreptului la viață privată al altuia, care nu poate fi acceptată într-o societate democratică. În concret, dacă o persoană va utiliza mijloace tehnice (hardware sau software) pentru a înregistra o convorbire telefonică proprie, aceasta nu va putea fi considerată o interceptare, ci o înregistrare în sensul art. 138 alin. (1) lit. c) C.pr.pen., întrucât se va realiza numai prin dispozitivul aflat la persoana vătămată [sau orice altă persoană, conform art. 139 alin. (3) C.pr.pen.], și nu printr-un dispozitiv situat între cele două dispozitive.

Prima condiție de autorizare a acestui procedeu probatoriu este existența unei *suspiciuni rezonabile cu privire la pregătirea sau săvârșirea unei infracțiuni* de o anumită gravitate dintre cele indicate la art. 139 alin. (2) C.pr.pen. Față de cele analizate anterior cu privire la această condiție, comună tuturor metodelor speciale de supraveghere, precizăm că nu considerăm că legiuitorul a conferit suficientă atenție caracterului invaziv al măsurii de supraveghere tehnică. Facem referire în special la infracțiunile contra patrimoniului. În plus, nu se face nicio distincție între infracțiunile care se vor urmări din oficiu și cele care se urmăresc numai la plângere prealabilă, ultimele având un caracter mai puțin grav, chiar dacă nu se reflectă în limitele de pedeapsă. Sub acest aspect, legislația anterioară era superioară, întrucât limita sfera faptelor care putea justifica interceptarea și înregistrarea numai la cele care se urmăreau din oficiu, conform art. 91[1] alin. (1) C.pr.pen. anterior[2]. Totodată, nu credem că se impunea menținerea, în cazul acestei măsuri de supraveghere tehnică, a criteriului subsidiar al aplicării măsurii și unor *infracțiuni pentru care legea prevede pedeapsa închisorii de 5 ani sau mai mare*. Ținând seama de această dispoziție, pot fi incluse și majoritatea infracțiunilor împotriva siguranței pe drumurile publice, fapte des întâlnite în practică și care nu pot fi considerate de o gravitate deosebită. *De lege ferenda*, se impune ca legiuitorul să stabilească un criteriu subsidiar al prevederii de către legea penală a pedepsei închisorii de cel puțin 7 ani, alături de eliminarea infracțiunilor contra patrimoniului și a celor care se vor urmări la plângerea prealabilă a persoanei vătămate din categoria infracțiunilor care pot justifica autorizarea măsurii de supraveghere tehnică.

Măsura de supraveghere poate fi întrebuințată numai în cursul urmăririi penale, împrejurare comună cu toate metodele speciale de supraveghere sau cercetare, întrucât va trebui să aibă un caracter secret, incompatibil cu orice altă fază procesuală[3].

A doua condiție care se impune a fi îndeplinită pentru autorizarea măsurii este cea privitoare la *proporționalitatea acesteia cu restrângerea drepturilor și libertăților fundamentale*. Această condiție este prevăzută de art. 139 alin. (1) lit. b) C.pr.pen. și se impune a fi analizată de judecătorul de drepturi și libertăți prin prisma criteriilor prevăzute de textul de lege: „*particularitățile cauzei*, *importanța informațiilor ori a probelor ce urmează a fi obținute sau gravitatea infracțiunii*". Acest criteriu este cel mai important pentru autorizarea oricărei

[1] Potrivit art. 302 alin. (6) C.pen., va constitui infracțiunea de violarea secretului corespondenței: „deținerea sau confecționarea, fără drept, de mijloace specifice de interceptare ori de înregistrare a comunicațiilor se pedepsește cu închisoare de la 3 luni la 2 ani sau cu amendă".

[2] *I. Neagu*, *M. Damaschin*, Audio and video interceptions and recordings in criminal law in Romania, în Lex et Scientia International Journal (LESIJ), vol. 1, no . XVI/2009, p. 206.

[3] A se vedea și *A.C. Lionte*, Aspecte generale cu privire la activitatea de interceptare și înregistrare a comunicațiilor și comunicării în cadrul procesului penal, în Revista de Investigare a Criminalității nr. 1/2016, p. 1098.

metode speciale de supraveghere și este cel care trebuie analizat cu cea mai mare seriozitate de către judecătorul de drepturi și libertăți. În cadrul analizei de proporționalitate, se va impune raportarea măsurii la inviolabilitatea corespondenței și a convorbirilor telefonice ca o componentă a dreptului la viață privată al persoanei[1].

Proporționalitatea este un criteriu complex, în care toate subcriteriile sale se află într-o legătură directă, influențându-se reciproc. De pildă, în analiza judecătorului se poate stabili că, prin particularitățile cauzei, interceptarea convorbirilor telefonice ale infractorului va conduce la dovedirea săvârșirii unei infracțiuni de furt, importanța informațiilor obișnuite va fi deosebită, putând consta în probe directe privind vinovăția, dar gravitatea concretă a faptei nu va justifica folosirea unor metode speciale de supraveghere. Din acest punct de vedere, interceptarea convorbirilor este cea mai susceptibilă de a fi folosită în mod abuziv, întrucât va permite descoperirea facilă a unui număr deosebit de mare de interacțiuni între persoane, fiind folosită în trecut de unele organe de urmărire penală ca o nouă „regină a probelor". Întrucât interceptările se vor realiza prin mijloace automatizate, fără vreo limită asupra numărului persoanelor care pot fi supuse măsurii[2], se vor putea obține deosebit de multe probe, fără niciun efort inițial din partea organelor de urmărire penală.

Prin „particularitățile cauzei" vom înțelege acele împrejurări specifice unei anumite cauze penale care vor impune utilizarea metodelor speciale de supraveghere sau cercetare pentru soluționarea cauzei, deoarece un altfel de mijloc nu ar fi propice pentru a stabili starea de fapt. Sub acest aspect, trebuie să fie evaluat modul în care supravegherea poate să furnizeze probe în procesul penal prin prisma modalităților concrete în care se pregătește fapta sau în care a fost săvârșită fapta[3]. Ceea ce se impune a se analiza este și natura infracțiunii prin raportare la mijloacele de comitere. Unele infracțiuni pot fi probate numai prin anumite metode speciale de supraveghere sau cercetare, iar altele pot fi dovedite și prin procedee probatorii obișnuite. În cazul infracțiunilor de corupție, modul în care se realizează luarea de mită poate să determine ca interceptarea convorbirilor să fie necesară prin raportare la natura infracțiunii și la modul în care se comite, respectiv prin primirea directă a unei sume de bani. Prin interceptări se poate descoperi dacă persoanele au stabilit o întâlnire, dacă a existat o înțelegere privind primirea unei sume de bani, putând fi obținute probe directe, dar și probe indirecte, care pot fi completate prin organizarea unui flagrant cu ocazia primirii mitei.

Prin „importanța informațiilor ori a probelor ce urmează a fi obținute" înțelegem contribuția pe care o pot avea informațiile sau probele obține pentru stabilirea împrejurărilor esențiale ale cauzei. Judecătorul trebuie să găsească un just echilibru, întrucât cu cât este mai invazivă metoda de supraveghere, cu atât este mai capabilă să furnizeze o probă determinantă în procesul penal.

„Gravitatea infracțiunii" presupune o analiză a pericolului social concret pe care îl presupune săvârșirea infracțiunii care face obiectul urmăririi penale. Acest criteriu de gravitate este unul judiciar și ține de intima convingere a judecătorului dacă se impune încuviințarea supravegherii tehnice, chiar dacă vor fi îndeplinite condițiile prevăzute de art. 139 alin. (2) C.pr.pen., care sunt criterii legale privind gravitatea faptei.

[1] *C. Olaru*, op. cit., p. 14.

[2] Recordul pentru asemenea măsuri a fost stabilit în anul 2014, în S.U.A., când s-a autorizat interceptarea a 89.138 de persoane prin același mandat, în *L.K. Donohue*, The Future of Foreign Intelligence, 2016, p. 59.

[3] *Gh. Mateuț*, Procedură penală, 2019, p. 681.

A treia condiție impusă de Codul de procedură penală pentru încuviințarea măsurii de cercetare este *necesitatea procedeului probatoriu* pentru obținerea probei. Cu alte cuvinte, condiția se referă și la *subsidiaritatea* măsurilor speciale de supraveghere sau cercetare față de orice alt procedeu probatoriu. Această condiție este prevăzută în cuprinsul art. 139 alin. (1) lit. c) C.pr.pen. și restrânge folosirea supravegherii tehnice numai în situația în care „*probele nu ar putea fi obținute în alt mod sau obținerea lor ar presupune dificultăți deosebite ce ar prejudicia ancheta ori există un pericol pentru siguranța persoanelor sau a unor bunuri de valoare*". Această condiție de fond este comună cu celelalte măsuri de supraveghere tehnică, măsura specială analizată nu prezintă caracteristici particulare, astfel că facem trimitere la cele expuse mai devreme în prezenta lucrare[1].

Secțiunea a 2-a. Autorizarea interceptării comunicațiilor ori a oricărui tip de comunicare la distanță

Întrucât măsura face parte din supravegherea tehnică, vor fi incidente dispozițiile art. 140 C.pr.pen., sens în care în prezenta secțiune vom face scurte considerații privind particularitățile autorizării interceptării comunicațiilor ori a oricărui tip de comunicare la distanță, care se vor completa cu explicațiile pe care le-am dat odată cu analizarea unitară a procedurii de autorizare a măsurilor de supraveghere tehnică[2].

Pentru a se putea autoriza metoda specială de supraveghere tehnică, este necesar ca procurorul să întocmească o *propunere* în acest sens, în care să fie cuprinse toate elementele prevăzute de art. 140 alin. (2) C.pr.pen., pe care să o transmită judecătorului de drepturi și libertăți. Aceasta se va realiza și în situația în care propunerea procurorului va fi la cererea persoanei vătămate, în condițiile art. 140 alin. (9) C.pr.pen.

Competența de judecare a propunerii revine judecătorului de drepturi și libertăți din cadrul instanței competente să judece cauza în primă instanță sau din cadrul instanței corespunzătoare în grad acesteia în a cărei circumscripție se află sediul parchetului din care face parte procurorul care a formulat cererea.

Pentru încuviințarea interceptării comunicațiilor ori a oricărui tip de comunicare la distanță de către *judecătorul de drepturi și libertăți*, se impune, mai întâi, verificarea de către acest organ judiciar a respectării condițiilor prevăzute de art. 139 C.pr.pen. la care am făcut referire într-o secțiune anterioară[3]. Această verificare se face prin analizarea propunerii formulate de procuror și a dosarului cauzei, care va fi înaintat de către procuror împreună cu propunerea de autorizare a măsurii speciale de supraveghere tehnică. Transmiterea dosarului cauzei asigură o verificare efectivă, de fond, a argumentelor procurorului pentru care formulează propunerea și asigură un control judiciar *ex ante* asupra supravegherii tehnice. În cuprinsul propunerii, procurorul trebuie să includă toate elementele prevăzute de art. 140 alin. (2) C.pr.pen.[4], aceasta trebuind să fie detaliată și sub aspectul modalității concrete de punere în executare

[1] *V. supra*, Titlul III, Capitolul I.4.

[2] *V. supra*, Titlul III, Capitolul II.2.

[3] *V. supra*, Titlul III, Capitolul I.

[4] Conform acestui articol, cererea trebuie să cuprindă: „(...) numele sau alte date de identificare a persoanei împotriva căreia se dispune măsura, dacă sunt cunoscute, indicarea probelor ori a datelor din care rezultă suspiciunea rezonabilă cu privire la săvârșirea unei infracțiuni, indicarea faptei și a încadrării juridice, (...) motivarea caracterului proporțional și subsidiar al măsurii (...)".

a măsurii, întrucât indicarea concretă a modului în care va fi pus în executare mandatul va avea implicații asupra proporționalității măsurii. În concret, se va impune să se indice dacă se va realiza o interceptare a *convorbirilor telefonice* ale unei persoane (realizată prin C.N.I.C. din cadrul S.R.I.) sau ale unor convorbiri realizate prin *servicii informatice alternative de comunicare* – Whatsapp, Signal (deși, tehnic improbabil), Viber, Facebook Messenger, Skype ori vor fi vizate interceptări de comunicări, precum e-mail, SMS sau comunicări realizate prin serviciile informatice alternative de comunicare menționate deja. Credem că dacă procurorul va propune măsura și nu va indica modalitatea concretă, judecătorul de drepturi și libertăți va trebui să respingă cererea ca fiind nefondată, întrucât o autorizare a acestei măsuri fără nicio limitare va constitui o ingerință disproporționată asupra vieții private a persoanei.

Judecarea propunerii procurorului are loc în aceeași zi cu formularea ei, în camera de consiliu, fără citarea părților și cu prezența obligatorie a procurorului. Soluțiile pe care le poate pronunța judecătorul de drepturi și libertăți sunt fie respingerea cererii, fie admiterea ei. Respingerea cererii se va dispune conform art. 140 alin. (6) C.pr.pen., atunci când judecătorul de drepturi și libertăți va respinge în totalitate cererea procurorului, fie ca inadmisibilă, fie ca nefondată.

În cazul oricăreia dintre soluțiile adoptate de către judecătorul de drepturi și libertăți, aceasta nu va putea fi supusă niciunei căi de atac, însă procurorul va fi îndreptățit să formuleze o nouă cerere de încuviințare în cazul respingerii, dacă vor fi îndeplinite cerințele prevăzute de art. 140 alin. (8) C.pr.pen.[1].

După admiterea cererii procurorului, judecătorul de drepturi și libertăți emite, conform art. 140 alin. (5) C.pr.pen., un mandat care trebuie să cuprindă mai multe elemente regăsite și în încheierea de admitere a cererii. Întocmirea minutei va fi obligatorie.

Elementele comune care nu pun probleme deosebite sunt cele privind *denumirea instanței*, *data, ora și locul emiterii*, *numele, prenumele* și *calitatea persoanei care a dat încheierea și a emis mandatul*, *semnătura judecătorului și ștampila instanței*. Față de obiectul măsurii de supraveghere tehnică, nu va fi necesară indicarea numărului de cont. Un alt element comun care nu ridică probleme este perioada maximă pentru care se dispune supravegherea tehnică, aceasta putând fi de maximum 30 de zile.

În schimb, în cazul măsurii interceptării comunicațiilor ori a oricărui tip de comunicare la distanță, vor trebui indicate, după caz, *elementele de identificare a fiecărui telefon*, *a punctului de acces la un sistem informatic* sau *datele de identificare a căii de comunicare*.

Prin „elementele de identificare a fiecărui telefon", legiuitorul a vrut să indice nu doar numărul de telefon, ci și posibilitatea ca judecătorul de drepturi și libertăți să dispună autorizarea măsurii de supraveghere tehnică prin raportare la identificatorul unic al fiecărui terminal sau dispozitiv. Aceasta se poate realiza prin numărul IMEI (International Mobile Equipment Identity), însă nu este legat neapărat de un telefon, putând fi orice dispozitiv mobil. Prin termenul de „telefon" folosit de legiuitor nu va trebui să înțelegem doar echipamentul clasic cunoscut ca atare – telefon fix sau mobil –, ci orice dispozitiv care va avea un cod IMEI și capacitatea de a se conecta la o rețea de comunicații electronice destinate publicului. Codul acesta nu va putea fi substituit și, chiar dacă se va schimba cartela telefonică, interceptarea tot va putea avea loc. În S.U.A., instanțele au adoptat ca o soluție pentru schimbarea cartelelor telefonice, emiterea unor mandate de supraveghere prin interceptare, numite *rolling wiretap*[2],

[1] Cu privire la formularea unei noi cereri de autorizare, *v. supra*, Titlul III, Capitolul II.2.

[2] En., *interceptare rostogolită*.

prin care mandatul se va extinde automat și altor terminale, ca urmare a schimbării lor de către persoana supravegheată[1]. O atare măsură nu o vedem posibilă în legislația română, prin raportare la necesitatea precizării elementelor de identificare a fiecărui telefon, și nici nu o considerăm oportună, întrucât prezintă riscuri crescute de abuz din partea organelor de urmărire penală. Ea prezintă și o posibilitate ridicată ca mandatul de supraveghere tehnică să fie extins față de persoane care nu au făcut obiectul procedurii de autorizare, fapt care ar contraveni imperativului respectării dreptului la viață privată și a standardului impus de art. 8 par. 2 Conv.EDO.

În privința indicării numărului de telefon interceptat, o asemenea mențiune se va impune de cele mai multe ori, deoarece o persoană nu își va schimba des numărul de telefon de-a lungul timpului decât dacă întreprinde activități infracționale grave care să îi dea temerea că ar putea fi interceptată. În jurisprudența Curții Europene a Drepturilor Omului s-a subliniat necesitatea identificării în mandat a numărului de telefon, fiind insuficientă menționarea acestuia în cuprinsul proceselor-verbale redactate după înregistrarea convorbirilor[2]. Ceea ce a criticat Curtea a fost lipsa de precizie a mandatului de supraveghere tehnică, apreciind că menționarea dispunerii măsurii asupra anumitor persoane nu este suficientă, trebuind să fie indicate și elemente ce țin de telefonul sau numărul de telefon interceptat[3]. În opinia noastră, mandatul de supraveghere tehnică nu va trebui să conțină în mod obligatoriu numărul de telefon în situația în care există date și informații că persoana își schimbă regulat numărul de telefon, dar păstrează același echipament, măsura fiind autorizată legal dacă se motivează în cuprinsul încheierii de autorizare acest lucru și se indică, potrivit art. 140 alin. (5) lit. g) C.pr.pen., elementele de identificare a fiecărui telefon.

Prin „punctul de acces la un sistem informatic" se desemnează echipamentul prin care dispozitivul sau telefonul se conectează la un sistem informatic, precum o rețea. Un exemplu de astfel de punct de acces poate fi echipamentul folosit de un client al unui furnizor de servicii de comunicații electronice pentru a se conecta la internet – router sau modem, la nivelul căruia se vor putea intercepta comunicațiile care trec prin acesta.

Prin „datele de identificare a căii de comunicare" vom înțelege orice alte date decât cele arătate mai sus, prin care se poate stabili modalitatea de comunicare la distanță. O atare situație poate apărea când se folosesc căi de comunicații mai puțin utilizate de publicul larg, precum emițătoare radio pe frecvențe civile sau comunicații radio pe frecvențe militare sau alte frecvențe interzise folosirii publice. Ar putea intra, într-o categorie de comunicații pentru care se impune precizarea căii de comunicații, folosirea stațiilor radio tip CB, des întâlnite la autocamioane (TIR) și la unele autovehicule, adeseori utilizate pentru comunicarea în trafic a unor împrejurări relevante (accidente, echipaje de poliție cu radar etc.), dar care pot transmite convorbiri private între participanți.

Alături de mențiunile arătate mai sus, în cuprinsul art. 140 alin. (5) lit. e) teza a II-a C.pr.pen., legiuitorul a prevăzut că este obligatorie menționarea *scopului* pentru care s-a încuviințat măsura. Întrucât, în cazul supravegherii tehnice, vom fi în situația autorizării unui procedeu probatoriu, scopul va fi obținerea de probe cu privire la săvârșirea unei infracțiuni, pregătirea săvârșirii unei infracțiuni sau a descoperirii și identificării persoanelor care au participat sau participă la săvârșirea respectivelor infracțiuni.

[1] *D.E. Hall*, op. cit., p. 113.

[2] CEDO, cauza *Calmanovici c. România*, Hotărârea din 1 iulie 2008, §124, pe *hudoc.echr.coe.int*

[3] *Ibidem*.

În privința *indicării concrete a măsurii încuviințate*, judecătorul de drepturi și libertăți va trebui să detalieze care sunt modalitățile concrete de realizare a supravegherii, numai cele menționate expres putând fi puse în executare de procuror. Sub acest aspect, punerea în executare a interceptării comunicațiilor ori a oricărui tip de comunicare la distanță va fi abordată într-o secțiune ulterioară[1].

Numele persoanei supuse măsurii nu va trebui indicat decât dacă vor fi cunoscute datele de identificare ale acestei persoane, în caz contrar trebuind să se arate că nu se cunoaște persoana. Există situații des întâlnite în practică în care nu se va putea cunoaște numele persoanei care deține un anumit telefon, întrucât cartela SIM folosită este din categoria celor preplătite, astfel că nu va exista un abonament pe numele persoanei prin care să fie identificată.

În ceea ce privește prelungirea măsurii de supraveghere tehnică și a duratei maxime de autorizare a acesteia, facem trimitere la explicațiile generale privind autorizarea supravegherii tehnice[2].

[1] *V. infra*, Titlul V, Capitolul III.
[2] *V. supra*, Titlul III, Capitolul II.2.

Capitolul III
Punerea în executare a interceptării comunicațiilor ori a oricărui tip de comunicare la distanță

Secțiunea 1. Particularități privind punerea în executare a interceptării comunicațiilor ori a oricărui tip de comunicare la distanță

Alături de aspectele generale privind punerea în executare a mandatului de supraveghere tehnică pe care le-am tratat în context general, se impun a fi formulate câteva mențiuni particulare privind punerea în executare a interceptării comunicațiilor ori a oricărui tip de comunicare la distanță.

Punerea în executare a interceptării comunicațiilor sau a altor tipuri de comunicări la distanță a constituit obiectul mai multor decizii cu privire la legalitatea interferenței serviciilor de informații în activitatea organelor de urmărire penală. În prezent, față de modificările legislative avute, punerea în executare se va face potrivit art. 142 alin. (1) C.pr.pen., respectiv de către procuror sau, în urma delegării, de către organul de urmărire penală sau de către un lucrător specializat din poliție.

Modalitatea concretă de punere în executare variază în funcție de specificul infracțiunii urmărite și a particularităților cauzei, dar, de regulă, va consta în interceptarea automatizată a unor comunicații sau comunicări telefonice realizate de persoanele care vor face obiectul mandatului de supraveghere tehnică. Supravegherea va fi una continuă, menținându-se pe toată durata mandatului sau până la momentul la care procurorul dispune încetarea măsurii, mai înainte de expirare.

Cu caracter continuu va fi și supravegherea comunicațiilor sau comunicărilor făcute printr-un sistem informatic de către o persoană, sub acest aspect fiind diferit doar mijlocul tehnic prin care se poate realiza măsura. Acesta va fi tot unul automatizat, dar va fi diferit de cel utilizat în interceptarea comunicațiilor telefonice. În plus, acesta va trebui să fie instalat de către organele de urmărire penală într-un mod în care poate intra în legătură cu punctul de acces al persoanei la internet. Era oportun ca legiuitorul să includă și posibilitatea de a se pătrunde în spații private pentru instalarea și dezinstalarea unor asemenea dispozitive, în mod similar cazului prevăzut pentru măsura supravegherii video, audio sau prin fotografiere. Astfel, un dispozitiv specializat poate fi atașat la rețeaua internă a persoanei și să capteze datele care se transmit prin rețea. În situația în care dispozitivul va permite și accesarea sistemelor informatice din rețea, se va impune și autorizarea accesului la un sistem informatic.

Supravegherea prin interceptare va putea fi și secvențială în cazul în care se folosesc dispozitive prin care se simulează un turn de recepție GSM (dispozitivele Stingray despre care am făcut vorbire). Tot secvențială va fi și în cazul în care comunicațiile se realizează prin alte mijloace radio, precum stații de emisie-recepție (*walkie-talkie*), dispozitivul de interceptare trebuind să fie în raza lor de acțiune (care poate fi pe o suprafață de câțiva km^2). De regulă, astfel de dispozitive se folosesc în zonele unde nu există semnal de telefonie, fiind des utilizate în domeniul exploatărilor forestiere pentru comunicațiile dintre persoanele aflate pe teren sau între acestea și bază. Întrucât adeseori nu sunt criptate și presupun folosirea unor frecvențe comerciale, interceptarea lor poate

fi lesne realizată printr-o stație de emisie recepție, iar înregistrarea se va realiza prin racordarea acesteia la un dispozitiv de înregistrare, precum un reportofon.

Rezultatele activităților de supraveghere tehnică vor trebui amplasate pe suporți de stocare apți să conțină cantitatea de date informatice obținute (CD, DVD, Blu-Ray, hard-diskuri, în funcție de spațiul de stocare necesar). Deși nu constituie la acest moment o obligație, în măsura în care organele de urmărire penală dețin un certificat calificat, vor putea semna prin semnătură electronică extinsă datele informatice conținute de suporții de stocare.

Sub aspectul valorificării probelor obținute din interceptarea comunicațiilor ori a oricărui tip de comunicare la distanță, mijlocul de probă principal care va rezulta din punerea în executare a măsurii va fi un proces-verbal. Alături de acesta, vor rezulta și suporții optici pe care se vor regăsi înregistrările audio, audiovideo sau video care au făcut obiectul interceptării. Facem mențiunea că nu doar clasicele interceptări audio vor putea fi obținute, deși ele reprezintă cea mai mare parte a obiectului măsurii speciale de supraveghere, în majoritatea situațiilor. În cazul în care se va proceda la interceptarea unor comunicări realizate prin mijloace tehnice, precum internetul, se vor putea obține inclusiv date informatice conținut care variază foarte mult sub aspectul categoriilor – e-mailuri, imagini, înregistrări audio, video. Într-adevăr, legiuitorul nu a limitat expres natura comunicărilor[1], ci, mai degrabă, *modalitatea prin care ele sunt obținute de către organele de urmărire penală*.

Rezultatele supravegherii tehnice vor fi cuprinse, în conformitate cu art. 143 alin. (1) C.pr.pen., într-un proces-verbal de consemnare a activităților de supraveghere tehnică. Întrucât există similarități cu alte măsuri de supraveghere tehnică, vor fi necesare unele mențiuni suplimentare privind rezultatele activităților de supraveghere tehnică pentru a nu se depăși limitele măsurii prin modalitatea concretă de punere în executare. Revenind asupra exemplului anterior, va fi o interceptare a unei comunicări captarea datelor informatice transmise prin internet între o persoană și un server de e-mail dacă aceasta se realizează la nivelul punctului de acces la internet prin interpunerea unui dispozitiv al organelor de urmărire penală, dar va constitui un acces la un sistem informatic dacă se va realiza o pătrundere în sistemul informatic care primește sau care transmite acel e-mail. Apreciem că această constatare se raliază tezei susținute de noi prin prezenta lucrare, în sensul existenței unei distincții între procesul-verbal prevăzut de art. 143 alin. (1) C.pr.pen., în cazul tuturor măsurilor de supraveghere tehnică, și cel prevăzut de art. 143 alin. (4) C.pr.pen., în care se vor reda convorbirile, comunicările sau conversațiile[2].

Dacă sunt surprinse convorbirile, comunicările sau conversațiile unor persoane, apreciem că acestea vor trebui redate integral, în conformitate cu dispozițiile art. 143 alin. (4) C.pr.pen. Procesele-verbale vor trebui să conțină redarea integrală a tuturor convorbirilor constatate, comunicărilor sau conversațiilor și va fi obligatorie certificarea lor de către procuror. Facem trimitere la secțiunea dedicată din lucrare, unde am tratat mai amănunțit problema consemnării și certificării rezultatelor supravegherii tehnice în aceste situații[3].

Nu va fi necesar ca procesul-verbal întocmit să fie singular, rezultatele supravegherii tehnice putând fi consemnate în mai multe procese-verbale. Acest lucru îl găsim a fi acceptabil și legal, dar numai în măsura în care din cuprinsul procesului-verbal va reieși faptul că acesta a fost întocmit pe o perioadă mai lungă de timp, consemnându-se în mod concret perioada în care a fost întocmit. În practică au fost întâlnite situații în care procesele-verbale de redare prevăzute

[1] *M. Bulancea*, *G. Zlati*, *R. Slăvoiu*, în M. Udroiu (coord.), Codul de procedură penală, 2017, p. 637.

[2] *V. supra*, Titlul III, Capitolul V.2.

[3] *V. supra*, Titlul III, Capitolul V.3.

de art. 143 alin. (4) C.pr.pen. cuprindeau sute de pagini de transcrieri, fiind imposibil ca acestea să fie redate de organul de urmărire penală în decursul aceleiași zi. O atare împrejurare ridică suspiciuni privind obținerea acestor redări de la organe specializate ale statului, precum S.R.I., în perioada anterioară Deciziei Curții Constituționale nr. 51/2016, serviciile secrete asigurând, la cerere, inclusiv realizarea unor note de redare care erau preluate de organele de urmărire penală, însușite și cuprinse în procese-verbale.

În cazul în care se vor realiza comunicațiile și au și o componentă video – apeluri video, videoconferințe etc. –, atunci se va impune, după caz, descrierea în procesul-verbal a acțiunilor persoanelor. Spre deosebire de supravegherea video, audio sau prin fotografiere, în cazul interceptărilor, persoanele care comunică prin mijloace video cunosc faptul că se adresează unei alte persoane și vor fi concentrate asupra discuțiilor, componenta video fiind doar o preferință de familiaritate. Nu apreciem că va fi nevoie de o planșă fotografică în asemenea situații, decât dacă reies anumite elemente de interes, precum prezentarea unor obiecte care pot avea însemnătate pentru cauză (bani, droguri etc.).

Secțiunea a 2-a. Modalități de realizare a interceptării comunicațiilor ori a altor mijloace de comunicare la distanță

§1. Interceptarea comunicațiilor în sistem centralizat

Cea mai des întâlnită formă a punerii în executare a interceptărilor o constituie interceptarea comunicațiilor prin intermediul C.N.I.C. din cadrul S.R.I. Ca urmare a efectelor Deciziei nr. 51/2016 a Curții Constituționale, s-a inițiat și, până la acest moment, finalizat un program de dotare a unităților de parchet cu tehnică necesară utilizării în sistem centralizat a echipamentelor S.R.I. pentru interceptarea comunicațiilor. Aceste echipamente sunt interconectate cu furnizorii de rețele publice de comunicații electronice și cu furnizorii de servicii de comunicații electronice destinate publicului și au posibilitatea de a intercepta semnalele care trec prin respectivele sisteme informatice și de a le redirecționa în copie, pentru a nu întrerupe comunicarea, la C.N.I.C.

Pentru realizarea interceptării, un terminal securizat aflat la sediul Parchetului și racordat exclusiv la C.N.I.C. va permite controlarea de la distanță a operațiunii de interceptare a comunicațiilor. Practic, procurorul sau organul de cercetare penală va accesa prin acest terminal (un computer) o aplicație a S.R.I., pe bază de utilizator și parolă, echipamentul S.R.I. și va putea iniția punerea în executare a mandatului de supraveghere tehnică prin introducerea sa în sistemul informatic. În acest sistem informatic se introduc toate datele esențiale ale mandatului și se stabilesc persoanele (țintele) interceptării comunicațiilor, precum și durata pentru care poate opera măsura. Comandând sistemul informatic, procurorul sau organul de cercetare penală rămâne în control deplin asupra măsurii într-un mod independent, care nu presupune intervenția S.R.I.

Sistemul informatic al C.N.I.C. va intercepta automat toate comunicațiile și le va stoca pe serverul său într-o formă criptată și accesibilă numai organului care a pus în executare mandatul, transmițând rezultatele în mod automat către terminalul din sediul parchetului printr-un canal criptat, ulterior operațiunii distrugând automat și în mod ireversibil informația conținută inițial pe server. Pentru a se păstra secretul operațiunii, personalul S.R.I. nu are posibilitatea de a accesa informația din server, aceasta fiind criptată și accesibilă numai organului de urmărire penală.

Folosind terminalul din sediul parchetului, procurorul va colecta rezultatele interceptării comunicațiilor și va proceda la înscrierea acestora pe suporți de stocare, procedând în continuare, conform art. 143 C.pr.pen., la selectarea comunicațiilor relevante și la consemnarea lor într-un proces-verbal. Desigur, selectarea lor poate fi făcută și pe terminalul din cadrul parchetului, în funcție de capacitățile logistice ale organelor de urmărire penală și de numărul mandatelor de supraveghere tehnică de pus în executare.

Din cuprinsul Protocolului încheiat între Ministerul Public și S.R.I. privind cooperarea concretă în vederea permiterii accesului la C.N.I.C.[1] nu rezultă o limitare tehnică privind interceptarea comunicațiilor telefonice, nefiind clare, la acest moment, capacitățile tehnice ale sistemului. În acest sens, nici ultimul raport întocmit de președintele Înaltei Curți de Casație și Justiție în temeiul art. 30[1] din Legea nr. 304/2004 nu este suficient de clar[2]. Cu alte cuvinte, nu știm exact ce fel de interceptări se pot realiza prin tehnologia deținută de S.R.I. Cu toate acestea, din protocol rezultă că S.R.I. va acorda sprijin necesar pentru identificarea soluției tehnice în cazul operatorilor care nu au activată funcția de interceptare, existând la momentul semnării protocolului anumite limitări în posibilitatea interceptării comunicațiilor.

Considerăm că, la momentul formulării propunerii de autorizare a măsurilor de supraveghere tehnică, procurorul va trebui să precizeze și metoda concretă de interceptare, indicând dacă aceasta se va realiza în sistem centralizat prin C.N.I.C. sau prin alte metode pe care le vom analiza în prezenta secțiune.

§2. Interceptarea comunicațiilor prin dispozitive mobile tip Stingray

Dispozitivele de tip Stingray sunt o formă de IMSI-catcher, dispozitive care simulează identitatea unui turn GSM și păcălesc dispozitivele mobile că ar reprezenta un echipament de rețea real, forțându-le să se conecteze direct la acestea în locul turnului GSM adevărat. Dispozitivele de acest tip sunt cu caracter local, neavând o rază mare de acțiune, dar permițând interceptarea tuturor comunicațiilor din respectiva zonă. Modul de funcționare se bazează pe intermedierea transmiterii semnalului, dispozitivul copiind datele interceptate și transmițându-le mai departe unui turn GSM real.

Unul dintre avantaje este obținerea în teren și în timp real a locației și conținutului comunicațiilor unei persoane supravegheate, aflate într-o anumită zonă, fără a fi nevoie de implementarea într-un terminal aflat la sediul parchetului a unor date privind mandatul de autorizare. Dezavantajul este că interceptarea se va face cu privire la toate dispozitivele mobile din zonă, dispozitivul Stingray forțându-le să se conecteze la acesta. Desigur, acest lucru nu înseamnă că este obligatorie și înregistrarea conținutului fiecărei comunicații, acestea putând fi retransmise în mod automat, cu excepția comunicațiilor persoanei supravegheate. Un alt dezavantaj îl constituie faptul că sunt limitate la comunicațiile purtate prin operatorii de telefonie, neputând intercepta și decripta transmiterea de informații prin internet.

[1] Protocol privind cooperarea între Serviciul Român de Informații și Ministerul Public pentru stabilirea condițiilor concrete de acces la sisteme tehnice ale Centrului Național de Interceptare a Comunicațiilor, înregistrat sub nr. 2440/C din 08.12.2016 la P.I.C.C.J. și sub nr. 9331 din 07.12.2016 la S.R.I. Documentul este nesecret și poate fi accesat online pe *www.mpublic.ro*

[2] ICCJ, Raport privind verificarea efectuată de președintele Înaltei Curți de Casație și Justiție în temeiul art. 30[1] din Legea nr. 304/2004 privind organizarea judiciară, republicată, cu modificările și completările ulterioare, înregistrat sub nr. 11 din 7 ianuarie 2020, pe *www.scj.ro*

Existența acestor dispozitive este cunoscută la nivel internațional, însă nu este menționată în vreunul dintre protocoalele secrete încheiate de Ministerul Public cu Serviciul Român de Informații. De pildă, în S.U.A., circa 75 de agenții guvernamentale dețin și folosesc astfel de dispozitive, între care F.B.I., N.S.A., D.E.A., inclusiv organe fiscale, precum I.R.S.[1]. Cu toate acestea, în Protocolul încheiat cu S.R.I. se menționează folosirea unei tehnici operative portabile de localizare a dispozitivelor mobile, aceasta constituind și o funcție a unui dispozitiv de tip Stingray, fiind posibil ca serviciul să dețină și acest tip de mijloace tehnice.

[1] *www.aclu.org*

Capitolul IV
Problema protocoalelor de cooperare care permiteau participarea serviciilor de informații la efectuarea urmăririi penale

Secțiunea 1. Conflictul de natură constituțională constatat prin Decizia nr. 26/2019 a Curții Constituționale privind încheierea de către Ministerul Public și Serviciul Român de Informații a unor protocoale de colaborare

Metoda specială de supraveghere a interceptării comunicațiilor a fost punctul de plecare pentru o întreagă suită de decizii ale Curții Constituționale, pornind de la implicarea serviciilor secrete în activitatea de punere în executare, aceasta fiind cea mai des utilizată formă a supravegherii tehnice. În acest context, Ministerul Public a încheiat mai multe protocoale de colaborare, cu caracter secret sau strict secret, care reglementau, contrar legii procesuale penale, punerea în aplicare a mandatelor emise de autoritățile judiciare care puteau autoriza măsura. Am ales să tratăm problema protocoalelor de colaborare în această parte a lucrării, deoarece influența lor a fost cea mai amplă prin raportare la această metodă specială de supraveghere, pentru care S.R.I. a creat o structură internă, care a avut ca scop și a obținut monopolul național în interceptarea comunicațiilor.

În urma Deciziei Curții Constituționale nr. 51/2016 și a altor decizii mergând pe aceeași linie, a sporit interesul publicului în activitatea desfășurată de S.R.I. în domeniul combaterii criminalității, ridicându-se suspiciuni privind implicarea acestora dincolo de atribuțiile lor, uzurpând competența procurorului de a efectua urmărirea penală și, mai ales, cea de a pune în executare mandatele de supraveghere tehnică.

Prin demersul Camerei Deputaților, Curtea Constituțională a fost sesizată cu soluționarea conflictului juridic de natură constituțională dintre Ministerul Public – P.I.C.C.J., Parlamentul României, Înalta Curte de Casație și Justiție și celelalte instanțe judecătorești. Această problemă de natură constituțională a fost soluționată prin Decizia nr. 26/2019[1], stabilindu-se că a existat la acel moment un conflict juridic de natură constituțională ca urmare a semnării a două protocoale secrete, astfel în dispozitiv s-au consemnat următoarele: „*se constată existența unui conflict juridic de natură constituțională între Ministerul Public – Parchetul de pe lângă Înalta Curte de Casație și Justiție și Parlamentul României, pe de-o parte, și Înalta Curte de Casație și Justiție și celelalte instanțe judecătorești, pe de altă parte, generat de încheierea între Ministerul Public – Parchetul de pe lângă Înalta Curte de Casație și Justiție și Serviciul Român de Informații a Protocolului nr. 00750 din 4 februarie 2009, precum și de exercitarea, în mod necorespunzător, a controlului parlamentar asupra activității Serviciului Român de Informații*". Aceleași concluzii le are Curtea și cu privire la Protocolul nr. 09472 din 8 decembrie 2016, doar cu referire la dispozițiile art. 6 alin. (1), art. 7 alin. (1) și art. 9 din acesta, constatându-se conflictul de natură constituțională.

[1] CCR, Dec. nr. 26 din 16 ianuarie 2019 (M. Of. nr. 193 din 12 martie 2019).

Prin sesizarea formulată, președintele Camerei Deputaților a susținut că, prin semnarea a două protocoale, în anii 2009 și 2016, cu S.R.I., Ministerul Public – P.I.C.C.J. și-a încălcat propriile competențe constituționale și, uzurpând competențele Parlamentului, a învestit S.R.I. cu competența de a desfășura activități specifice organelor de cercetare penală, fapt interzis în mod expres de legiuitor prin Legea nr. 14/1992 privind organizarea și funcționarea S.R.I. Aceste protocoale având caracter secret nu au putut fi aduse la cunoștința publicului și au condus la: desfășurarea urmăririi penale și strângerea de probe de către lucrătorii S.R.I. și parchete pe baza unor norme/reguli secrete, care, din punct de vedere juridic, sunt inexistente, atât timp cât Constituția reglementează strict și expres modul de adoptare și intrare în vigoare a legilor și condiționează existența acestora de publicarea în Monitorul Oficial; imposibilitatea persoanelor acuzate de a invoca, pe durata urmăririi penale sau a judecății, excepțiile nulităților prevăzute de Codul de procedură penală privind modul nelegal de administrare a probelor, nulități pe care legiuitorul le-a prevăzut în lege în vederea protejării dreptului constituțional al persoanei la apărare, la un proces echitabil și la acces efectiv la justiție; imposibilitatea instanțelor de a se pronunța efectiv pe legalitatea acestor probe, de a le cenzura, din moment ce, în afara Ministerului Public și a S.R.I., conținutul protocoalelor era necunoscut nu doar celorlalte părți din proces, ci și judecătorilor[1].

Din punct de vedere constituțional, problema principală care a fost dedusă judecății a fost dacă Ministerul Public și-a asumat rolul de legiuitor, subrogându-se rolului Parlamentului și adăugând la lege prin protocoale de colaborare, care au condus la înfăptuirea justiției în temeiul acestora[2]. Consecințele procesuale pentru persoana care ar fi contestat legalitatea unor acte îndeplinite prin aplicarea protocoalelor de colaborare era gravă, aceasta trebuind să se lupte cu o paradigmă juridică instituționalizată de 9 ani, ce acorda un rol prevalent protocoalelor de colaborare în fața legii[3]. Deși Curtea Constituțională se referă la o paradigmă juridică de 9 ani, în realitate, după cum vom vedea, aceasta datează cel puțin din anul 2003, mărind la 15 ani starea de nelegalitate cauzată prin implicarea serviciilor secrete în realizarea actelor de urmărire penală.

Incidente în cauză au fost dispozițiile Constituționale privind rolul Ministerului Public și statutul procurilor, în special art. 131 alin. (1) și art. 132 alin. (1) din Constituție, care stabilesc atât rolul și atribuțiile Ministerului Public în mod distinct față de alte autorități ale statului[4], cât și modul în care își desfășoară atribuțiile procurorii[5].

În analiza realizată de Curte, instanța s-a referit numai la protocoalele încheiate cu S.R.I., în anii 2009, respectiv 2016. Sub aspectul naturii lor, acestea nu aveau natura unui act în legătură cu activitatea judiciară, întrucât, în cursul urmăririi penale, măsurile sau actele procurorului se iau sau se emit în condițiile normelor de procedură penală[6], acestea neprevăzând ca procurorii

[1] *Ibidem*, §7.

[2] *Ibidem*, §131.

[3] *Ibidem*, §132.

[4] Conform art. 131 alin. (1)-(2) din Constituție:

„(1) În activitatea judiciară, Ministerul Public reprezintă interesele generale ale societății și apără ordinea de drept, precum și drepturile și libertățile cetățenilor.

(2) Ministerul Public își exercită atribuțiile prin procurori constituiți în parchete, în condițiile legii".

[5] Conform art. 132 alin. (1) din Constituție: „Procurorii își desfășoară activitatea potrivit principiului legalității, al imparțialității și al controlului ierarhic, sub autoritatea ministrului justiției".

[6] CCR, Dec. nr. 26/2019, §143.

să aibă atribuția de a încheia „protocoale de colaborare" în legătură cu o anumită cauză, astfel că aceste protocoale nu sunt acte procesuale care să poată fi dispuse de procuror[1].

În privința primului protocol analizat, Curtea a reținut: „*în ceea ce privește Protocolul nr. 00750 din 4 februarie 2009, încheiat între Ministerul Public – Parchetul de pe lângă Înalta Curte de Casație și Justiție și Serviciul Român de Informații, Curtea reține că art. 2, art. 3 lit. g), art. 6 alin. (1), art. 7, art. 9, art. 16, art. 17 alin. (1) și (2) și art. 33 alin. (1) din protocol cuprind dispoziții care excedează sferei de cuprindere a unui act administrativ normativ, realizând, sub aspect substanțial, o modificare implicită a Constituției*"[2]. Un prim element de critică însușit de Curte este lipsa de claritate și previzibilitate privind noțiunea de „infracțiune gravă", a cărei combatere ar fi putut face parte din scopul încheierii Protocolului, terminologia permițând o largă apreciere a incidenței de aplicare a actului, o asemenea măsură suplimentând infracțiunile care formează sfera de competență a S.R.I. (infracțiunile împotriva securității naționale, cele de terorism și infracțiunile ce au corespondent în amenințările la adresa securității naționale). Astfel, încheierea Protocolului a adăugat la lege și a condus la crearea unei norme juridice primare cu conținut flexibil, care a putut fi apreciată, de la caz la caz, de parchet sau S.R.I.[3].

O altă problemă identificată de Curte a fost posibilitatea constituirii de echipe comune de anchetă care să acționeze în baza unor planuri comune de acțiune, reținând că din modul în care era formulat Protocolul se înțelegea că efectuarea urmăririi penale se realiza în comun de procurori și reprezentanții serviciului secret, iar, prin raportare la noțiunea vagă de „infracțiune gravă", s-au creat premisele pentru ca S.R.I. să exercite atribuții de cercetare penală în orice domeniu[4]. Această situație nu putea fi considerată în acord cu Constituția, întrucât submina rolul procurorului, printr-o intruziune a unui serviciu secret în modul de desfășurare al urmăririi penale. Prin modul în care erau reglementate planurile de acțiune pe baza cărora acționau echipele operative comune, decizia se împărțea între procuror și factorul decizional din S.R.I.; practic, procurorul nu mai avea un control exclusiv asupra modului în care se efectuau actele de urmărire penală.

Cea mai importantă constatare a Curții s-a referit la punerea în executare a actelor de autorizare emise de instanțe în conformitate cu art. 91[1]-91[5] C.pr.pen. anterior prin echipamentele proprii ale S.R.I. Reiterând Decizia nr. 51/2016, punerea în aplicare a unor măsuri de supraveghere tehnică intră în sfera de competență a organelor de urmărire penală, suportul tehnic putând fi oferit și de alte organe, ceea ce nu ar putea fi cazul în privința Protocolului S.R.I., care, pe lângă suportul tehnic, se referă expres la punerea în executare a actelor de autorizare. Caracterul deosebit de grav al acestei situații care contrazicea dispozițiile procesuale penale a fost subliniat de Curte: „*Protocolul a reglementat competența Serviciului Român de Informații de a pune în executare mandatul de supraveghere tehnică în cadrul procesului penal, fără să fie organ de urmărire penală. Astfel, deși Codul de procedură penală nu a acordat serviciului secret această competență, Ministerul Public, din proprie inițiativă, îi transferă acestuia o competență proprie procurorului. Practic, acest protocol operează, în mod indirect, o adăugire la prevederile Codului de procedură penală, competența dispunerii unei măsuri procesuale fiind transferată de către chiar titularul său – Ministerul Public – unui serviciu secret*"[5].

[1] *Ibidem*, §145.
[2] *Ibidem*, §151.
[3] *Ibidem*, §153.
[4] *Ibidem*, §156.
[5] *Ibidem*, §165.

Alături de punerea în executare a mandatelor de supraveghere tehnică, Curtea a constatat că S.R.I. îi revenea și competența de a realiza supravegherea audio și video a unei persoane, în baza acelorași tipuri de acte de autorizare[1]. În plus, cooperarea dintre cele două instituții era una strânsă prin punerea la dispoziție, mutuală, de informații și documente cu privire la infracțiunile din protocol, inclusiv „infracțiunile grave" care nu sunt definite.

În Constituție, activitatea procurorilor este reglementată în cuprinsul art. 131, astfel că atribuțiile acestora sunt stabilite într-un mod în care nu se poate face derogare de la acestea printr-o formă de delegare precum cea a semnării unui protocol de colaborare, Curtea constatând că: „*dispozițiile art. 2, art. 3 lit. g), art. 6 alin. (1), art. 7, art. 9, art. 16, art. 17 alin. (1) și (2) și art. 33 alin. (1) din Protocolul nr. 00750 din 4 februarie 2009, încheiat între Ministerul Public – Parchetul de pe lângă Înalta Curte de Casație și Justiție și Serviciul Român de Informații, dispoziții esențiale în economia acestuia, stabilesc norme juridice diferite față de cele cuprinse în cadrul Codului penal (cu referire la noțiunea de infracțiune gravă) sau Codului de procedură penală (competențele acordate Serviciului Român de Informații), norme care, în esența, lor contravin art. 131 din Constituție*"[2].

Consecința, din punctul de vedere al încălcării separației puterilor în stat, este că se diminuează rolul procurorului în procesul penal, prin sporirea rolului serviciilor secrete, pe de o parte, și conduce, pe de altă parte, la diminuarea în mod nepermis a garanțiilor privind respectarea drepturilor și libertăților fundamentale ale persoanei, prin substituirea unui serviciu secret în locul organului de urmărire penală. În cazul oricărui act realizat de procuror sau de un organ de cercetare penală, legea procesuală penală prevede un remediu care să conducă la posibilitatea persoanei vătămate să obțină repararea vătămării. Sub acest aspect, în domeniul măsurilor de supraveghere tehnică, acesta trebuie să constea și în posibilitatea de a contesta legalitatea măsurii sau a punerii în executare a acesteia. Or, lipsa oricărui control care să poată fi exercitat de o instanță asupra unei activități a unui serviciu secret plasează întreaga procedură de punere în executare în afara legii, prin nerespectarea dreptului la viață privată al persoanei[3]. Totodată, scopul punerii în executare a măsurilor de supraveghere tehnică constă în obținerea de probe în cadrul procesului penal, acest scop putând fi deturnat de un serviciu secret în propriile sale interese, iar rezultatele obținute să fie folosite și în alte scopuri decât cele avute în vedere de organele judiciare.

Din perspectiva consecințelor asupra instanțelor, Protocolul încheiat a determinat aplicarea, de către acestea, fără a cunoaște existența Protocolului, a unor dispoziții care veneau în contradicție cu Constituția, primind ca legale probele obținute cu încălcarea competenței funcționale a organelor de urmărire penală, Curtea reținând că „*protocolul încheiat a determinat punerea instanțelor în situația de a nu mai putea înfăptui justiția în numele legii, contrar art. 124 din Constituție, cu nesocotirea rolului acestora în ordinea constituțională, prevăzut de art. 126 din același act*"[4].

În privința celui de-al doilea Protocol de colaborare dintre P.I.C.C.J. și S.R.I., încheiat în anul 2016, acesta cunoaște o oarecare evoluție ca urmare a Deciziei Curții Constituționale nr. 51/2016, fiind eliminate dispozițiile privind măsurile de supraveghere tehnică puse în executare de serviciu, cu excepția celor care pot fi puse în executare de ofițerii serviciului, în

[1] *Ibidem*, §169.
[2] *Ibidem*, §170.
[3] *Ibidem*, §175-176.
[4] *Ibidem*, §189.

calitate de organe de cercetare penală speciale. După cum se reține și de Curte, „*încheierea acestui protocol s-a realizat în contextul în care paradigma juridică promovată prin Protocolul nr. 00750 din 4 februarie 2009 a devenit inaplicabilă, ca urmare a unei sancțiuni de drept constituțional rezultate din Decizia Curții Constituționale nr. 51 din 16 februarie 2016*"[1].

Cu toate acestea, anumite dispoziții ale acestui protocol au fost considerate ca fiind contrare dispozițiilor art. 131 alin. (1) și art. 132 alin. (1) din Constituție, respectiv cele privitoare la: *i)* comunicarea de informații către S.R.I. cu privire la modalitatea în care au fost valorificate sesizările primite de la serviciu [art. 6 alin. (1) din Protocol]; *ii)* asigurarea de consultanță din partea parchetului, prin specialiști, în beneficiul S.R.I. în ceea ce privește activitățile ce fac obiectul cooperării [art. 7 alin. (1) din Protocol]; *iii)* obligarea parchetului să pună la dispoziția S.R.I., la cerere sau din oficiu, date și informații de interes pentru contracararea și prevenirea unor amenințări la securitatea națională (art. 9 din Protocol). Prezența acestor prevederi în cuprinsul Protocolului „*generează presupuneri privind o ingerință a serviciului secret în desfășurarea activității de urmărire penală și creează premisele subordonării acestuia și, prin urmare, a activității de urmărire penală structurilor unui serviciu secret, ceea ce, pe plan constituțional, pune în discuție relația dintre parchete și serviciile de informații*"[2]. Astfel, se reține, în mod similar cu cele avute în vedere în cazul Protocolului încheiat în anul 2009, că se realizează o redimensionare a atribuțiilor Ministerului Public, care contravine cu dispozițiile constituționale anterior menționate.

În concluzia considerentelor, Curtea face trimitere la Decizia nr. 302/2017 a Curții Constituționale privind neconstituționalitatea dispozițiilor art. 281 alin. (1) lit. b) C.pr.pen., care nu reglementează nulitatea absolută în cazul organelor de urmărire penală, stabilind, în contextul celor două protocoale secrete nelegale, că: „*revine Înaltei Curți de Casație și Justiție și celorlalte instanțe judecătorești, precum și Ministerului Public – Parchetul de pe lângă Înalta Curte de Casație și Justiție și unităților subordonate să verifice în cauzele pendinte, în ce măsură s-a produs o încălcare a dispozițiilor referitoare la competența materială și după calitatea persoanei a organului de urmărire penală, și să dispună măsurile legale corespunzătoare*"[3].

În urma deciziei arătate, instanțele s-au poziționat împotriva folosirii în procesul penal a rezultatelor obținute în baza aplicării protocoalelor secrete, stabilindu-se ca fiind nelegale acte, precum: constituirea de echipe operative comune; transmiterea de informații obținute din derularea activităților operative care prezentau relevanță și care ar putea fi valorificate în cadrul procesului penal; acordarea de sprijin prin efectuarea de activități de investigații și supraveghere operativă; punerea la dispoziție de informații și documente care puteau sprijini documentarea faptelor; încheierea unui plan comun de acțiune; furnizarea de informații cu privire la persoanele menționate, pe parcursul anchetei penale; oferirea de sprijin tehnic pentru punerea în executare a unor acte de autorizare a supravegherii tehnice – resurse umane sau materiale, transcriere trafic brut rezultat din exploatarea actelor de autorizare, transmitere convorbiri transcrise, întocmire de procese-verbale de transcriere[4]. Ținând seama de imperativul din cuprinsul deciziei analizate în prezenta secțiune, instanțele au obligația de a cercetata, în fiecare caz, dacă, în cursul urmăririi penale, actele care au fost realizate în cauză

[1] *Ibidem*, §195.

[2] *Ibidem*, §200.

[3] *Ibidem*, §211.

[4] C. Ap. București, s. a II-a pen., dec. nr. 1123/A din 18 septembrie 2019, pronunțată în dosar nr. 18875/3/2012, nepublicată.

au constat inclusiv în aplicarea protocoalelor menționate, caz în care vor trebui să sancționeze cu nulitatea absolută orice imixtiune a serviciilor secrete în realizarea unui act procesual sau procedural în cauză.

În concluzie, încheierea protocoalelor de colaborare dintre Ministerul Public și S.R.I. a determinat formarea unei practici contrare dispozițiilor Codului de procedură penală, în cazul punerii în executare a măsurilor de supraveghere tehnică, conducând, contrar rolului procurorului și principiului separației puterilor în stat, la atribuirea rolului de organ de punere în executare a acestor măsuri unui serviciu secret. În secțiunile care urmează, vom analiza atât protocoalele de colaborare declasificate până la acest moment, cât și stadiul actual al implicării S.R.I. în punerea în executare a interceptării comunicațiilor.

Secțiunea a 2-a. Protocoalele de cooperare dintre organele de urmărire penală și serviciile de informații

Subiectul protocoalelor de cooperare este unul care prezintă dificultăți în abordare, întrucât accesul la acestea nu este unul facil, chiar dacă au fost declasificate. O observație generală este că toate protocoalele semnate înainte de pronunțarea Deciziei nr. 51/2016 a Curții Constituționale aveau caracter nepublic, fiind clasificate ca documente secrete sau strict secrete. Ca atare, ieșirea lor din vigoare odată cu încheierea unui nou protocol, de regulă, nu conducea la declasificarea lor. Dimpotrivă, declasificarea acestora a fost realizată ca urmare a inițiativei Ministerului Public sau la inițiativa instanțelor. Chiar și așa, nu toate aceste documente au fost declasificate și, chiar dacă au fost, sunt greu de obținut. Din studierea unor astfel de protocoale, putem constata că ele se încheiau în mod distinct între instituții, precum P.I.C.C.J. și S.R.I., dar și între instituții aflate în subordine, precum multiplele protocoale încheiate de D.N.A. (anterior Parchetul Național Anticorupție și Departamentul Național Anticorupție) cu S.R.I. Acest din urmă serviciu de informații nu era privit exclusiv, existând protocoale similare și cu alte servicii secrete, precum D.G.P.I. a Ministerului Afacerilor Interne. Totodată, fără a face obiectul prezentei lucrări, organele de urmărire penală au încheiat protocoale cu alte instituții ale statului, precum Inspectoratul General al Poliției de Frontieră, Agenția Națională de Administrare Fiscală sau chiar Academia Română.

Considerăm că o cooperare instituțională se poate realiza mai bine prin protocoale care să detalieze anumite proceduri administrative între instituții ale statului, însă acestea nu pot privi aspecte precum desfășurarea de acte de urmărire penală, chiar și dacă nu se referă expres la acestea. Admitem și că protocoalele trebuie să fie uneori secrete, dar secretizarea lor, atunci când presupune modalitatea de lucru cu organele de urmărire penală, nu poate fi acceptată dacă influențează actele de urmărire penală și impietează exercitarea dreptului la apărare.

După cum vom vedea în protocoalele pe care le vom analiza, instituțiile care le-au încheiat s-au ferit, de regulă (cu excepția P.N.A./D.N.A.), la a menționa expres că interceptarea și înregistrarea comunicațiilor se va realiza în mod concret de către serviciile secrete, făcând trimiteri generice la respectarea dispozițiilor Codului de procedură penală. În special în privința Codului de procedură penală anterior, competența organelor de urmărire penală era încălcată de fiecare dată, acesta fiind și scopul Protocolului – de a deturna normala aplicare a legii. Reglementarea secretă a unei norme, care să fie considerată cu putere mai mare decât legea, nu poate fi concepută într-o societate democratică, cu atât mai mult cu cât norma era emisă

de instituții prin uzurparea atribuțiilor Parlamentului. Tocmai din aceste motive, protocoalele erau ținute secrete, deoarece adăugau la lege în mod nepermis și stabileau proceduri paralele cu legea și care erau contrare respectării separației puterilor în stat.

În cele ce urmează vom analiza sumar prevederile protocoalelor secrete încheiate între organele de urmărire penală și serviciile secrete, relevând principalele dispoziții criticabile atât în privința implicării serviciilor secrete în activitatea de urmărire penală, cât și în ceea ce privește punerea în executare a metodelor speciale de supraveghere tehnică.

§1. Protocolul privind organizarea cooperării între Serviciul Român de Informații și Parchetul Național Anticorupție din 28.01.2003[1]

Scopul încheierii Protocolului dintre S.R.I. și P.N.A a fost cel al „organizării și realizării sarcinilor comune" ale celor două instituții, menționându-se că unul dintre scopurile P.N.A. era de a descoperi și sancționa faptele de corupție sesizate de S.R.I. Așadar, se observă încă din primul articol al Protocolului că organele de urmărire penală erau sesizate ca urmare a unor informări din partea serviciilor secrete, situație care poate părea a fi acceptabilă în cazul unor infracțiuni precum cele privind securitatea națională, însă competența P.N.A. era în domeniul infracțiunilor de corupție, astfel că întrevedem prima imixtiune nelegală în realizarea actului de justiție.

Al doilea scop al Protocolului era, potrivit art. 1 alin. (2) pct. 2, „*punerea în aplicare de către Serviciul Român de Informații a autorizațiilor emise de Parchetul Național Anticorupție în baza dispozițiilor art. 91¹-91⁵ din Codul de procedură penală*". Cu alte cuvinte, obiectivul Protocolului consta în stabilirea competenței S.R.I. în punerea în executare a mandatelor de supraveghere tehnică. Nici măcar nu se încerca, prin acest protocol, să se ascundă faptul că S.R.I. realiza punerea în executare, stabilindu-se o regulă cu caracter derogatoriu de la lege.

Sprijinul S.R.I. se manifesta și prin „*documentarea preliminară începerii urmăririi penale, **în comun**, a cauzelor sesizate de Serviciul Român de Informații, aflate pe rolul Parchetului Național Anticorupție*" (s.n.), potrivit art. 4 din Protocol. Nu numai că sesizarea se făcea de către S.R.I., dar acest serviciu participa împreună cu procurorul la realizarea actelor premergătoare în vederea începerii urmăririi penale. Acest articol întrevede menținerea unui interes al S.R.I. în cercetarea infracțiunilor sesizate, ceea ce este nefiresc și neadecvat și constituie o încălcare a principiului separației puterilor în stat.

Nu numai că imixtiunea S.R.I. avea loc la nivelul desfășurării urmăririi penale, dar aceasta influența și cariera procurorilor din cadrul P.N.A., potrivit art. 5 din Protocol, unde se arăta ca scop al Protocolului: „*schimbul de materiale documentare, de lucrări și date utile recrutării și pregătirii pe profil a personalului Parchetului Național Anticorupție*". Cu alte cuvinte, S.R.I. furniza P.N.A. informații despre persoanele care ar putea fi recrutate în cadrul unității de parchet. Trecând peste faptul că „recrutarea" nu este un cuvânt bine ales pentru cariera unui procuror în relația cu S.R.I., putem să avem în vedere că, prin aceste documente și lucrări realizate, serviciul putea influența numirea în funcție a procurorilor P.N.A., ceea ce, din nou, pune la îndoială independența sistemului de justiție față de ramura executivului.

În cazul S.R.I., erau prevăzute și responsabilități specifice, precum completarea investigațiilor din teren, desfășurarea de investigații și supraveghere operativă, dar și alte activități

[1] Protocol privind organizarea cooperării între Serviciul Român de Informații și Parchetul Național Anticorupție, înregistrat sub nr. 002128 din 28.01.2003 la S.R.I. și sub nr. 00112 din 28.01.2003 la P.N.A. Declasificat sub nr. 7516 din 11.09.2018 la S.R.I. și 2657/C/662 din 21.09.2018 la D.N.A.

care implică folosirea de surse tehnice secrete în cauze cu grad mare de complexitate. Cu alte cuvinte, se realiza filaj și supraveghere video, audio sau prin fotografiere. În orice caz, S.R.I. acorda, potrivit art. 10 din Protocol, sprijin și asistență pentru obținerea probelor și mijloacelor de probă necesare soluționării temeinice a cauzelor în lucru.

Chiar și organele de urmărire penală aveau responsabilități, acestea trebuind, potrivit art. 14 din Protocol, să acorde sprijin S.R.I. „*în analiza unor cazuri concrete*". Suplimentar, organele de urmărire penală eliberau „*autorizațiile necesare întreprinderii de măsuri speciale în conformitate cu dispozițiile art. 91[1]-91[5] din Codul de procedură penală*". Practic, analiza la comun a dosarului între P.N.A. și S.R.I. nu era o posibilitate, ci o obligație, iar, în privința supravegherii tehnice, Protocolul implica încălcarea dispozițiilor Codului de procedură penală prin transferarea punerii în executare către S.R.I., procurorul transmițând numai actul de autorizare.

Ca dovadă a sprijinului deosebit și a importanței combaterii corupției, S.R.I. și P.N.A. colaborau „frățește" în cauzele complexe, potrivit art. 22 din Protocol, unde se arăta că „*în cazurile complexe, cooperarea efectivă se realizează pe baza unor planuri comune, cu precizarea misiunilor ce revin fiecărei instituții*".

§2. Nota anexă din 02.03.2004 la Protocolul privind organizarea cooperării între Serviciul Român de Informații și Parchetul Național Anticorupție din 29.01.2003[1]

În continuarea colaborării interinstituționale dintre S.R.I. și P.N.A., la începutul anului 2004 a fost încheiată o notă anexă, care aducea anumite completări și modificări Protocolului, cu influență deosebită în realizarea activităților de supraveghere tehnică.

Astfel, se stabilește că U.M. 0894 București din cadrul S.R.I. va avea competență exclusivă în punerea în aplicare a actelor de autorizare vizând interceptarea comunicațiilor, toate actele de autorizare obținute de P.N.A. fiind trimise către această unitate militară. Observăm că s-a omis indicarea formală a respectării dispozițiilor Codului de procedură penală, în care se stabilea că procurorul, și nu o unitate militară a S.R.I., are competența de punere în executare a interceptării și înregistrării comunicațiilor.

În ceea ce privește rezultatul supravegherii tehnice, redarea urma să se facă de procurori și ofițeri de poliție judiciară ai P.N.A., însă, în cazul în care ar fi fost nevoie, „*U.M. 0894 București va acorda sprijin, în limita posibilităților, Parchetului Național Anticorupție în exploatarea unor posturi în limbi străine și pentru traducerea unor materiale*". Întrucât Nota anexă se referea la activități de supraveghere tehnică, materialele traduse puteau fi numai notele de redare.

În privința altor forme de supraveghere tehnică, decât interceptarea comunicațiilor telefonice, prin art. 15 alin. (1) din Nota anexă se prevedea: „*constituirea unor echipe mixte formate din personalul tehnic din cele două instituții, conduse de procurorul anume desemnat, care vor acționa în baza unui «Plan comun de acțiune»*". Aceste situații implică și supravegherea audio și video sau localizarea prin mijloace tehnice. O atare prevedere subliniază caracterul de implicare nepermisă a S.R.I. în activitatea de urmărire penală. Ceea ce este mai grav se observă din alineatele care succed acestuia. Potrivit art. 15 alin. (2) din Nota anexă: „*planul comun de acțiune se întocmește pe baza analizei situației operative și a soluției tehnice stabilite prin studiul*

[1] Nota anexă la Protocolul privind organizarea cooperării între Serviciul Român de Informații și Parchetul Național Anticorupție din 29.01.2003, înregistrată sub nr. 44/C din 01.03.2004 la P.N.A. și 002461 din 02.03.2004 la S.R.I. Declasificată sub nr. 7517 din 11.09.2018 la S.R.I. și sub nr. 2657/C/662 din 21.09.2018 la D.N.A.

de specialitate, se aprobă de reprezentanții autorizați ai celor două instituții și stabilește măsurile și responsabilitățile concrete de desfășurare a activităților tehnic-operative, în scopul prevenirii deconspirării acțiunii și producerii unor evenimente contrainformative". Nu numai că planul comun de acțiune era obligatoriu, dar conducerea activităților de către procuror era anulată, întrucât planul urna a fi aprobat atât de către P.N.A., cât și de S.R.I., ceea ce contrazice rolul procurorului, în faza de urmărire penală, de a fi singurul care poate decide asupra modului în care se efectuează urmărirea penală.

O ultimă mențiune care reflectă colaborarea nelegală dintre P.N.A. și S.R.I. o constituie necesitatea „legendării" de către organele de urmărire penală a operațiunilor desfășurate, potrivit art. 15 alin. (3) din Nota anexă, în care se arată că: „*Parchetul Național Anticorupție răspunde de întreprinderea măsurilor organizatorice necesare legendării, în toate situațiile, atât a acțiunilor specifice de instalare și recuperare a mijloacelor tehnice utilizate, cât și a sursei de proveniență a informațiilor obținute din acestea, respectiv asigurarea protecției mijloacelor tehnice instalate, până la recuperarea lor*". Termenul de „legendare" desemnează construirea unei povești, unei ficțiuni privind o situație de fapt, o minciună care să fie inventată de organul de urmărire penală pentru a permite instalarea și recuperarea mijloacelor tehnice ale S.R.I.[1]. Ceea ce este mai grav este obligația legendării provenienței informațiilor, aceasta semnificând obligarea organului de urmărire penală să mintă în cursul efectuării urmăririi penale privind sursa reală a informațiilor obținute. Această mențiune încalcă flagrant dreptul la un proces echitabil, prin faptul că anulează posibilitatea ca apărarea să cunoască toate împrejurările esențiale în care s-au realizat măsurile de supraveghere tehnică în cauză și nu oferă posibilitatea nici măcar a invocării încălcării dreptului la viață și să obțină, în conformitate cu art. 8 par. 2 Conv.EDO, anularea măsurilor luate împotriva sa și distrugerea rezultatelor activităților de supraveghere tehnică.

§3. Protocolul de cooperare dintre Parchetul de pe lângă Înalta Curte de Casație și Justiție și Serviciul Român de Informații pentru îndeplinirea sarcinilor ce le revin în domeniul securității naționale din 30.06.2005[2]

Într-un mod similar cu protocoalele amintite, și la nivelul P.I.C.C.J. au fost încheiate protocoale de colaborare cu S.R.I., cu influență asupra modului în care erau puse în executare măsurile de supraveghere tehnică. Deși după titlul Protocolului se poate înțelege o colaborare limitată, în realitate, acesta era una general aplicabilă în cazul unor „infracțiuni grave". Potrivit art. 2 din Protocol, „*părțile cooperează, potrivit competențelor și atribuțiilor prevăzute de lege, în activitatea de valorificare a informațiilor din domeniul prevenirii și combaterii infracțiunilor împotriva securității naționale, a actelor de terorism și a altor infracțiuni grave, precum corupția, criminalitatea organizată, macro-criminalitatea economică și criminalitatea informatică*". Întrucât categoriile de infracțiuni grave erau menționate exemplificativ, nu era definit în mod clar și previzibil conceptul de „infracțiune gravă", în realitate desemnând colaborarea cu S.R.I. în orice cauză considerată gravă de către procuror.

[1] *M.V. Tudoran*, Teoria și practica interceptărilor, 2012, p. 179.

[2] Protocol de cooperare între Parchetul de pe lângă Înalta Curte de Casație și Justiție și Serviciul Român de Informații pentru îndeplinirea sarcinilor ce le revin în domeniul securității naționale, înregistrat sub nr. 003222 din 28.06.2005 la S.R.I. și sub nr. 002349 din 30.06.2005 la P.I.C.C.J. Declasificat sub nr. 1949/C1 din 03.08.2018 la P.I.C.C.J.

Unul dintre obiectivele cooperării dintre cele două instituții îl constituia *punerea la dispoziție pe bază de reciprocitate a informațiilor, datelor, documentelor și materialelor relevante și utile pentru îndeplinirea atribuțiilor specifice părților*, aceasta desemnând o cooperare cu date și documente de ambele părți, inclusiv comunicarea, de către organele de urmărire penală, a unor acte de procedură către serviciul secret.

Asemenea colaborării cu D.N.A., exista posibilitatea constituirii de echipe operative comune care, potrivit art. 3 lit. d) din Protocol, „*să acționeze în baza unor planuri de acțiune pentru documentarea preliminară începerii urmăririi penale și pentru transformarea informațiilor în probe în cadrul procesului penal*". O atare prevedere încălca în mod flagrant competența funcțională a organelor de urmărire penală de a proceda la administrarea probelor în procesul penal, prin implicarea S.R.I. în procesul penal, pentru obținerea de probe. Totodată, documentarea preliminară a începerii urmăririi penale se referă la etapa actelor premergătoare, practic, serviciul secret putând să sprijine începerea urmăririi penale în cauză prin informații obținute din surse proprii (neverificabile de organele de urmărire penală, instanță sau de viitoare părți, evident) care să stea la baza acestui act procesual.

În domeniul supravegherii tehnice, Protocolul prevede, conform art. 3 lit. g), „*acordarea de către experții SRI, în condițiile legii, a asistenței tehnice de specialitate procurorilor care efectuează urmărirea penală, pentru aplicarea prevederilor art. 91[1]-91[5] Cod procedură penală privind interceptările și înregistrările audio sau video, în conformitate cu autorizațiile emise în acest scop*". Credem că conceptul de „asistență tehnică" folosit desemnează cu totul altceva, sens în care ne referim la mențiunile privind actul de autorizare. Un asemenea act nu trebuie să fie cunoscut de S.R.I. pentru a oferi un simplu sprijin tehnic procurorului, numai în cazul în care respectivul act este necesar pentru a stabili limitele punerii în executare a supravegherii tehnice, sens în care, credem că, înclină dispozițiile din protocol. În plus, simpla mențiune a expresiei „în condițiile legii" nu schimbă caracterul nelegal al procedeului, întrucât nu exista nicio lege care să prevadă sprijinul S.R.I. în modalitatea în care se realiza în concret.

Trebuie amintit și art. 13 din Protocol, în care se detaliază activitatea concretă a S.R.I. în sprijinul organelor de urmărire penală, aceasta fiind mai mult decât un sprijin tehnic. Potrivit art. 13 din Protocol S.R.I., „*acordă sprijin, prin compartimentele specializate, pentru completarea informațiilor «din teren», în cauzele cu grad mare de complexitate, aflate pe rolul Parchetului, scop în care desfășoară activități de investigații și supraveghere operativă, precum și alte activități necesare punerii în aplicare a prevederilor art. 91[1]-91[5] Cod procedură penală, care implică utilizarea mijloacelor tehnice de interceptare*". Activitățile din teren, constând în activități de investigații și supraveghere operativă, reprezintă una sau mai multe forme de supraveghere video, audio sau prin fotografiere, ceea ce intră în contradicție cu dispozițiile Codului de procedură penală în vigoare la acel moment, care permiteau numai procurorului sau organului de cercetare penală delegat să pună în executare această metodă specială de supraveghere. În mod egal, erau contrar legii și activitățile de punere în aplicare a mandatelor de supraveghere tehnică în privința interceptărilor. Chiar dacă se vorbește numai de activități necesare care implică utilizarea mijloacelor tehnice de interceptare, lipsa de claritate a Protocolului permite o interpretare foarte largă a acestuia, în sensul punerii în executare de către S.R.I. a interceptării comunicațiilor.

O ultimă mențiune care se impune a fi făcută, legat de acest protocol de cooperare, este posibilitatea sprijinirii activităților procurorilor în instanță prin asistență tehnică de specialitate. Potrivit art. 3 lit. h) din Protocol, era posibilă „*acordarea de către experții S.R.I., în*

condițiile legii, a asistenței tehnice de specialitate procurorilor care pun concluzii în cauzele complexe aflate pe rolul instanțelor judecătorești, în cazurile în care prezentarea mijloacelor de probă impune cunoștințe tehnice specifice". Cu alte cuvinte, S.R.I. sprijinea activ procurorul în cursul judecății în care Ministerul Public exercita acțiunea penală împotriva unor cetățeni. O atare contribuție nu este numai o imixtiune secretă în actul de justiție, ci și o încălcare a dreptului la un proces echitabil, fiindcă procurorul avea un sprijin de specialitate de care apărarea nu putea niciodată beneficia și nici nu avea căile legale prin care să solicite respectivul sprijin. În plus, S.R.I. trebuie să adopte un rol neutru în privința activităților desfășurate în fața instanței, prin sprijinul acordat procurorilor putându-se încălca și prezumția de nevinovăție a persoanei trase la răspundere penală. Rămâne să ne întrebăm: de ce s-a considerat că S.R.I. ar fi avut un interes propriu în condamnarea unor persoane?

Chiar dacă Protocolul mai sus arătat nu expune la fel de clar colaborarea ilicită a S.R.I. cu organele de urmărire penală, reiese suficient de clar că acestea realizau acte de urmărire penală prin punerea în executare a supravegherii tehnice în cauze, substituindu-se procurorului în această privință. În plus, nu putem crede că activitatea S.R.I. era de o altă natură față de colaborarea cu P.N.A., ulterior D.N.A., sau că, în cauzele privind securitatea națională, ar fi acționat cu mai puțin zel decât în cauzele de corupție.

§4. Protocolul de cooperare dintre Parchetul de pe lângă Înalta Curte de Casație și Justiție și Serviciul Român de Informații pentru îndeplinirea sarcinilor ce le revin în domeniul securității naționale din 04.02.2009[1]

Ținând seama de protocoalele tratate deja în prezenta secțiune, arătăm că, în anul 2009, toate acestea au ieșit din vigoare și au fost înlocuite cu un protocol unitar pentru toate unitățile de parchet, inclusiv pentru D.N.A., urmând să analizăm în cele ce urmează caracteristicile acestui protocol din punctul de vedere al metodelor speciale de supraveghere sau cercetare.

Cel mai îndelung aplicat protocol, cel mai complex și cel mai abuziv dintre toate acestea, Protocolul de cooperare dintre Parchetul de pe lângă Înalta Curte de Casație și Justiție și Serviciul Român de Informații pentru îndeplinirea sarcinilor ce le revin în domeniul securității naționale din 04.02.2009 și-a încetat aplicabilitatea treptat, potrivit celor relatate de Ministerul Public. Potrivit paginii de internet a Ministerului Public, referitor la acest protocol, se reține: „*cap. III-VI din protocol și-au încetat efectele la data intrării în vigoare a Deciziei Curții Constituționale nr. 51/2016, iar restul dispozițiilor și-au încetat efectele la data de 8 decembrie 2016, în mod expres prin abrogare, dispusă prin acordul părților semnatare. Aspectele privind încetarea aplicabilității protocolului și denunțarea acestuia au fost reconfirmate ulterior, prin acordul părților semnatare, la data de 13 martie 2017*".

Spre deosebire de protocoalele anterioare, actul are un caracter complex, fiind împărțit în două părți – Partea generală și Partea specială, aidoma unui cod. În cuprinsul Protocolului, în Partea specială, se regăsesc aspecte privind: soluționarea propunerilor de emitere a mandatelor, în baza art. 3 din Legea nr. 51/1991 privind siguranța națională a României, republicată – mandate de siguranță națională –, punerea lor în executare (Capitolul I), punerea în executare a mandatelor de supraveghere tehnică (Capitolul III), o secțiune specială privind punerea în

[1] Protocol de cooperare între Parchetul de pe lângă Înalta Curte de Casație și Justiție și Serviciul Român de Informații pentru îndeplinirea sarcinilor ce le revin în domeniul securității naționale din 04.02.2009, înregistrat sub nr. 003064 din 04.02.2009 la S.R.I. și sub nr. 00750 din 04.02.2009 la P.I.C.C.J. Declasificat sub nr. 884/C din 29.03.2018 la P.I.C.C.J.

executare a mandatelor de supraveghere tehnică emise în cauze aflate în urmărirea penală a procurorilor D.N.A. (Capitolul IV), supravegherea audiovideo pe momente operative – corespunzând art. 138 alin. (1) lit. c) C.pr.pen. (Capitolul V), desfășurarea de activități de supraveghere operativă și investigații operative – echivalente filajului, tot sub incidența art. 138 alin. (1) lit. c) C.pr.pen. (Capitolul VI). Practic, acest Protocol conținea o reglementare paralelă și contrară dispozițiilor Codului de procedură penală, urmărindu-se eludarea dispozițiilor legale și conferirea de atribuții de organ judiciar Serviciului Român de Informații. Există numeroase dispoziții privind conlucrarea dintre instituții, informarea reciprocă, sesizarea de către S.R.I. a organelor de urmărire penală, transmiterea de informații sau documente clasificate către organele de urmărire penală pentru a fi folosite în cauză în mod secret, cu obligația de a solicita declasificarea lor pentru a fi introduse oficial în dosarele de urmărire penală.

În privința dispozițiilor privind realizarea supravegherii tehnice prin interceptarea comunicațiilor, cuprinse în Capitolul III din Protocol, se prevăd următoarele: *i)* posibilitatea solicitării S.R.I. de a verifica starea tehnică, identitatea titularului postului telefonic, starea sa de funcțiune, existența condițiilor pentru realizarea interceptării; *ii)* punerea în executare, la dispoziția procurorului, a activităților dispuse prin autorizațiile emise de instanțele competente, potrivit art. 91[1]-91[5] C.pr.pen. anterior[1]; *iii)* S.R.I. urma să realizeze înregistrarea comunicărilor sau convorbirilor pe suporți optici și să **transcrie comunicările și convorbirile considerate de serviciu relevante în cauză, putând realiza, la cererea procurorului, și alte transcrieri**[2]; *iv)* S.R.I. putea apela la tehnică specială mobilă pentru identificarea și localizarea persoanelor urmărite ce utilizează terminale mobile[3].

Referitor la supravegherea video, audio sau prin fotografiere (Capitolele V și VI din Protocol), se prevăd următoarele: *i)* efectuarea de operațiuni tehnice, pe baza actului de autorizare emis de instanță, pe momente operative (supraveghere secvențială – n.n.); *ii)* supravegherile

[1] Conform art. 33 din Protocol:

„(1) Punerea în executare a activităților dispuse prin autorizațiile emise de instanțele competente potrivit dispozițiilor art.91[1]-91[5] Cod procedură penală va fi realizată de către Serviciu, pe echipamentele proprii, în baza solicitării scrise a procurorului.

(2) Adresa de solicitare a punerii în executare a activităților autorizate va fi însoțită de actul de autorizare (autorizație, încheiere sau ordonanță motivată), în original și copie certificată de emitent sau de procuror, și de suporții de date necesari, înseriați.

(3) Adresa va avea caracter „secret de serviciu" și va cuprinde precizări privind modul de transmitere și transcriere a rezultatelor obținute și modalitățile de legătură operativă, precum și cu privire la categoriile de date și informații relevante pentru cauză".

[2] Conform art. 34 din Protocol:

„(1) Serviciul va asigura înregistrarea comunicărilor sau convorbirilor rezultate din interceptare pe suporți de date înseriați, puși la dispoziție de procuror, precum și trimiterea acestora Parchetului sau parchetelor teritoriale.

(2) În vederea sprijinirii activităților specifice desfășurate de Parchet sau parchetele teritoriale Serviciul va asigura transcrierea comunicărilor sau convorbirilor considerate relevante în cauză.

(3) Ulterior, la solicitarea scrisă a procurorului, Serviciul poate asigura redarea altor convorbiri, selectate din traficul înregistrat. Solicitarea trebuie să conțină numărul actului de autorizare, criteriul de interceptare (număr post telefonic, serie IMEI a terminalului mobil, adresă IP, frecvență radio), data și ora efectuării convorbirii sau comunicării. În vederea desfășurării acestor activități, Parchetul sau parchetele teritoriale vor transmite Serviciului suporții de date conținând înregistrările menționate la alin. (1)".

[3] Conform art. 36 din Protocol: „(1) Pentru utilizarea pe momente operative a echipamentelor mobile din dotare, în vederea identificării și localizării persoanelor urmărite, ce utilizează terminale mobile, Parchetul sau parchetele teritoriale transmit unității specializate a Serviciului actele de autorizare emise potrivit legii, ce vor cuprinde și dispoziția de interceptare și înregistrare a convorbirilor".

audio-video se realizau în aceleași condiții ca interceptarea comunicațiilor, din punct de vedere procedural (potrivit acelorași dispoziții din Protocol); *iii)* supravegherea video, audio sau prin fotografiere se realiza în baza unui plan comun de acțiune întocmit de procuror și un reprezentant S.R.I., aprobat de conducerea S.R.I. (procurorul nu mai are un rol de a conduce urmărirea penală, acesta revenind S.R.I. – n.n.)[1]; *iv)* activitățile de supraveghere operativă și investigații informative (forme de filaj – n.n.) se puteau realiza cu aprobarea adjunctului directorului care organiza activitatea de profil din S.R.I. și numai pentru o durată operativă de maximum 24 de ore, ce putea fi extinsă până la 3 zile.

Concluzionând cu privire la conținutul Protocolului de colaborare din anul 2009, încheiat între P.I.C.C.J. și S.R.I., se observă caracterul vădit nelegal al activităților desfășurate de serviciu, acesta uzurpând atribuțiile procurorului în procesul penal și, în special, în privința punerii în executare a metodelor speciale de supraveghere tehnică. Din acest punct de vedere, gravitatea ingerințelor este incomensurabilă, permițându-se ca un serviciu de informații, fără nicio garanție privind respectarea drepturilor omului, să procedeze la realizarea supravegherii tehnice în mod automatizat și necontrolat. Cu atât este mai flagrantă ilegalitatea atunci când avem în vedere că anumite măsuri de supraveghere tehnică nu erau puse în executare din dispoziția procurorului, ci ele trebuiau să fie aprobate de către conducerea S.R.I.

Din cele arătate mai sus, rezultă că, la momentul pronunțării Deciziei nr. 51/2016, sistemul de punere în executare a măsurilor de supraveghere tehnică ajunsese la un apogeu al abuzurilor instituționale comise de S.R.I., cu cunoștința și complicitatea Ministerului Public.

§5. Protocolul privind organizarea cooperării între Serviciul Român de Informații și Parchetul de pe lângă Înalta Curte de Casație și Justiție pentru îndeplinirea sarcinilor ce le revin, potrivit legii, din 08.12.2016[2]

Primul protocol încheiat după pronunțarea Deciziei nr. 51/2016 a Curții Constituționale a reflectat unele modificări în privința activității desfășurate de S.R.I. în cursul urmăririi penale, stabilindu-se condițiile și modalitățile în care ofițerii din cadrul serviciului urmau să pună în executare mandatele de supraveghere tehnică, potrivit legii, în calitate de organe de cercetare penală speciale.

La nivel de principiu, s-a menținut ideea de informare reciprocă între S.R.I. și organele de urmărire penală, prin datele și informațiile care rezultau din activitatea specifică fiecăruia

[1] Conform art. 46-48 din Protocol:

„Art. 46. (1) La cererea scrisă a Parchetului sau parchetelor teritoriale, Serviciul efectuează operațiuni tehnice audio/video, în baza actului de autorizare emis de instanța de judecată sau de procuror, pe momente operative, în cazuri concrete, numai prin intermediul ofițerilor de legătură desemnați de Serviciu.

(2) Activitățile menționate la alin. (1) vor fi realizate de unitatea specializată, cu aprobarea directorului Serviciului și numai în cazurile prevăzute în art. 2 al prezentului protocol.

Art. 47. Dispozițiile art. 34, art. 35 și art. 36 din prezentul protocol se aplică și în cazul înregistrărilor rezultate din efectuarea activităților prevăzute la art. 46 alin. (1), precum și în cazul supravegherii audio-video.

Art. 48. Acțiunile audio/video vor fi executate de unitatea specializată a Serviciului sau de direcțiile județene de informații, sub coordonarea procurorului de caz, în baza unui «Plan comun de acțiune» întocmit de reprezentanți desemnați ai celor două părți și aprobat de șeful unității specializate a Serviciului sau de șefii direcțiilor județene de informații".

[2] Protocol privind organizarea cooperării între Serviciul Român de Informații și Parchetul de pe lângă Înalta Curte de Casație și Justiție pentru îndeplinirea sarcinilor ce le revin, potrivit legii, înregistrat sub nr. 03656 din 07.12.2016 la S.R.I. și sub nr. 09472 din 08.12.2016 la P.I.C.C.J. Declasificat sub nr. 2104/C1 din 30.08.2018 la P.I.C.C.J.

dintre acestea, ceea ce încă făcea posibilă cooperarea lor. Din acest punct de vedere, s-a menținut și obligativitatea informării S.R.I. în privința modului de valorificare a sesizărilor primite, de organele de urmărire penală, de la S.R.I. În plus, se admite ca informațiile obținute de la S.R.I. să poată fi introduse în dosarele penale, în conformitate cu art. 61 C.pr.pen., prin declasificarea acestora.

În continuare, din motive necunoscute până în prezent, se menține în cadrul Protocolului posibilitatea solicitării din partea parchetului a traducerii unor „materiale de interes" sau realizarea unor „activități de translație" prin traducători autorizați.

În cuprinsul Protocolului se prevede o secțiune specială dedicată desfășurării activităților prevăzute de art. 138-144 C.pr.pen., de către S.R.I., în calitate de organ de cercetare penală specială. Potrivit art. 13 alin. (1) din Protocol, aceste activități de punere în executare a actelor de autorizare emise de instanțele competente, potrivit art. 138-144 C.pr.pen. (implicit și autorizarea provizorie a procurorului), se vor realiza în baza solicitării Parchetului. Într-o interpretare firească, va trebui să existe o ordonanță de delegare a punerii în executare a supravegherii tehnice dispuse de procuror. În realitate, numai interceptarea comunicațiilor se va putea realiza, existând o limitare în acest sens prin art. 8 alin. (2) din Legea nr. 14/1992, întrucât atât această lege, cât și Protocolul au în vedere Centrul Național de Interceptare a Comunicațiilor. Dincolo de aspectele tehnice care preiau din dispozițiile Codului de procedură penală, se arată, prin art. 15 alin. (2) din Protocol, că „*în vederea sprijinirii activităților specifice desfășurate de Parchet, Serviciul va asigura transcrierea comunicărilor sau convorbirilor considerate relevante în cauză*". O atare dispoziție va fi nelegală, întrucât intră în contradicție cu dispozițiile art. 143 C.pr.pen., care prevăd competența procurorului în această privință, fiind necesar ca acesta să dispună ca ofițerii din cadrul S.R.I. să realizeze aceste procese-verbale, în calitate de organe de cercetare penală speciale și numai în cazul infracțiunilor limitativ indicate în Legea nr. 14/1992.

Observăm și faptul că prin protocol se stabilește că ar exista mijloace tehnice mobile pentru identificarea și localizarea de dispozitive mobile, ceea ce ne conduce la ideea că, în curând, vom putea avea implementate și turnuri de recepție mobile tip Stingray (I.M.S.I. catcher)[1]. Măsurile vor putea fi puse în executare numai în acele cauze în care S.R.I. poate avea calitatea de organ de cercetare specială. Astfel, potrivit art. 16 alin. (1) din Protocol, „*Parchetul poate solicita unităților specializate ale Serviciului, pe momente operative, utilizarea echipamentelor mobile din dotare, în scopul identificării și localizării terminalelor mobile sau pentru efectuarea de înregistrări audio-video ale persoanelor ce fac obiectul măsurilor de supraveghere tehnică legal autorizate*". Din dispozițiile citate rezultă și posibilitatea punerii în aplicare a metodei speciale de supraveghere video, audio sau prin fotografiere, aceasta putând fi pusă în executare de S.R.I. numai prin dispoziția procurorului.

În concluzie, din acest protocol, observăm că au existat anumite îmbunătățiri privind respectarea legalității punerii în executare a supravegherii tehnice, având în vedere mențiunile pe care le-am exprimat deja. Acest protocol nu se mai află în vigoare, însă, la momentul la care a intrat în vigoare, a fost încheiat și un protocol public privind modalitatea în care se realizează colaborarea organelor de urmărire penală cu C.N.I.C., protocol pe care îl vom analiza într-o secțiune viitoare[2].

[1] *R. Saini, M. Wadhwa, M. Khari*, Vulnerabilities and Attacks in Global System for Mobile Communication (GSM), în International Journal of Advanced Research in Computer Science, vol. 2, no. 3/may-june 2011, p. 140.

[2] *V. infra*, Titlul IV, Capitolul V.

§6. Protocolul de cooperare dintre Parchetul de pe lângă Înalta Curte de Casație și Justiție și Departamentul de Informații și Protecție Internă a Ministerului Afacerilor Interne din 07.08.2015[1]

După cum am menționat și la începutul prezentei secțiuni, încheierea protocoalelor secrete nu s-a rezumat numai la relația dintre organele de urmărire penală și S.R.I., existând și alte instituții – servicii secrete – care au încheiat astfel de protocoale cu Ministerul Public. Din acest punct de vedere, Departamentul de Informații și Protecție Internă a acționat întocmai ca S.R.I. în unele cauze, realizând activități care intrau sub incidența supravegherii tehnice, cu încălcarea dispozițiilor legale privind competența organelor de urmărire penală.

Deși D.I.P.I. constituie o direcție în cadrul poliției române, aceștia nu pot fi considerați a fi lucrători specializați, în sensul art. 142 alin. (1) C.pr.pen., întrucât această direcție a Poliției Române nu are și nu poate dobândi atribuții în domeniul urmăririi penale, ei neputând fi delegați în vederea punerii în executare a mandatelor de supraveghere tehnică. Observăm că prin protocolul secret s-a realizat o deturnare de la atribuțiile poliției judiciare, în acest caz a Direcției Generale Anticorupție, care era singura direcție care avea atribuții în domeniul realizării actelor de urmărire penală (implicit punerea în executare a supravegherii tehnice) în cazul infracțiunilor săvârșite de personalul Ministerului Afacerilor Interne.

În privința domeniilor cooperării cu organele de urmărire penală, Protocolul menționează că personalul D.I.P.I. va putea coopera în: *i)* domeniul acordării asistenței tehnice de specialitate, respectiv pentru efectuarea unor activități prevăzute de Codul de procedură penală; *ii)* realizarea altor sarcini ce le revin potrivit dispozițiilor Codului de procedură penală; *iii)* constituirea de echipe operative comune. Niciuna dintre aceste modalități de cooperare nu este lipsită de critici, întrucât problema supravegherii tehnice nu este prevăzută în mod expres – Protocolul putând sta la baza punerii în executare în cazul oricărei cauze penale –, iar, în privința altor sarcini stabilite de Codul de procedură penală, expresia este neclară și lipsită de previzibilitate, dat fiind faptul că această instituție nu are sarcini stabilite prin Cod.

Sub aspectul asistenței tehnice specifice, la art. 10 alin. (1) lit. b) din Protocol se detaliază această responsabilitate, prin aceea că Departamentul acordă sprijin pentru „*desfășurarea activităților necesare punerii în aplicare a prevederilor Codului de procedură penală care implică utilizarea mijloacelor tehnice specifice*". Cu alte cuvinte, într-un mod aparent lacunar și lipsit de claritate, dar ușor interpretabil pentru un jurist, Protocolul se referă chiar la punerea în executare a măsurilor de supraveghere tehnică. În mod similar, prin art. 10 alin. (1) lit. a) din Protocol se vor putea desfășura activități de investigații sau supraveghere operativă, ceea ce semnifică punerea în executare a metodei speciale de supraveghere prevăzută de art. 138 alin. (1) lit. b) C.pr.pen.

Desigur, cea din urmă chestiune privind constituirea unor echipe operative comune între procurori și reprezentanții unui serviciu secret considerăm că este neadecvată într-un stat de drept, pentru motive pe care nu le vom repeta. Mergând mai departe cu posibilitatea conlucrării, la art. 7 din Protocol se stabilește că: „*în cauze complexe sau ori de câte ori părțile apreciază necesar, cooperarea efectivă se realizează pe baza unor planuri comune, cu precizarea sarcinilor concrete ce revin fiecăreia*". Din nou, modalitatea aceasta de colaborare nu respectă rolul procurorului de a dispune cu privire la efectuarea urmăririi penale prin aceste planuri de acțiune.

[1] Protocol de cooperare din 07.08.2015 între Parchetul de pe lângă Înalta Curte de Casație și Justiție și Departamentul de Informații și Protecție Internă a Ministerului Afacerilor Interne înregistrat sub nr. 0020 din 07.08.2015 la D.I.P.I. și sub numărul 009726 din 06.08.2015 la P.I.C.C.J. Declasificat sub nr. 1590/C1 din 21.06.2018 la P.I.C.C.J.

Sub aspectul informațiilor care pot fi transmise organelor de urmărire penală și a folosirii lor în cauzele penale, Protocolul recunoaște posibilitatea ca organele de urmărire penală să fie sesizate de către D.I.P.I., însă acest fapt nu poate fi divulgat în cauză decât cu acordul scris al departamentului care va proceda la declasificarea informațiilor. Cu alte cuvinte, ca în cazul protocoalelor încheiate cu S.R.I., procurorul nu va putea menționa sursa informațiilor pentru o sesizare din oficiu a acestuia, trebuind să inventeze o minciună pentru a ascunde implicarea D.I.P.I. sau să omită precizarea sursei informației care a stat la baza sesizării sale. Totodată, conform art. 9 alin. (2) din Protocol, introducerea în dosarul cauzei a informațiilor primite de la D.I.P.I. se va face numai în măsura în care acele informații, documente sau materiale clasificate au utilitate probatorie determinantă. Cu alte cuvinte, Protocolul s-ar putea referi inclusiv la administrarea de probe de către D.I.P.I. și, ca urmare a declasificării lor, să fie folosite în procesul penal. În opinia noastră, o atare posibilitate nu poate considerată a fi legală, probele trebuind să fie obținute în cadrul procesului penal, și nu în afara sa.

Consecințele implementării tuturor acestor protocoale de colaborare între Ministerul Public și serviciile de informații a condus la conturarea unei practici care se întemeia pe norme stabilite în mod ilicit de instituții care nu aveau o atare competență (atributul legislativ fiind strict al Parlamentului sau al Guvernului ca legiuitor delegat) în domenii care erau deja reglementate prin lege (prin Codul de procedură penală). Durata existenței și aplicării unor astfel de protocoale a fost deosebit de mare și a creat incomensurabile violări ale dreptului la viață privată a unor persoane prin simplul prilej acordat serviciilor de informații de a deține informații de natură personală. Cuantumul ingerințelor și cel al informațiilor folosite de serviciile de informații în propriile scopuri nu pot fi estimate. Implementarea unor protocoale secrete reprezintă un bun exemplu al unui dezechilibru între puterile statului și între anumite instituții ale statului.

Niciuna dintre componentele sistemului judiciar sau politic nu poate fi considerată absolvită de vină: Ministerul Public a fost parte la protocoalele secrete și a delegat o atribuție a organelor judiciare către o altă instituție a statului; serviciile de informații (în special, S.R.I.) au început să se comporte ca organe de urmărire penală și să obțină, prin aceste protocoale, atribuții în domeniul judiciar, conducând la cea mai gravă încălcare a separației puterilor în stat; organele de urmărire penală sunt de blamat pentru că au tolerat și aplicat din comoditate aceste protocoale, deși era flagrantă încălcarea Constituției; Parlamentul este culpabil prin aceea că a cunoscut, aprobat și tolerat activitatea serviciilor de informații, deși comisiile de specialitate cunoșteau existența protocoalelor secrete; judecătorii, într-o mai mică măsură, pot fi socotiți culpabili în măsura în care au cunoscut informații despre existența și folosirea unor asemenea protocoale și nu au cenzurat folosirea lor prin mecanismele judiciare existente (constatarea nulității, excluderea probelor etc.).

Învățămintele pe care trebuie să le tragem din problematica reglementării punerii în executare a supravegherii tehnice prin protocoale secrete sunt următoarele: transparența este esențială într-o societate democratică, iar învinovățirea unuia sau mai multor organe nu reprezintă un demers constructiv. Dimpotrivă, trebuie să modificăm legislația într-un mod în care să nu mai existe posibilitatea implementării unor asemenea protocoale și activitatea desfășurată de serviciile de informații să fie controlată efectiv de Parlament, iar implicarea acestora în activitatea judiciară să se desfășoare numai potrivit unor norme clare și publice.

Capitolul V
Stadiul actual al reglementării punerii în executare a interceptării comunicațiilor

Cu urmare a situației inacceptabile privind punerea în executare a mandatelor de supraveghere tehnică de către ofițerii S.R.I., atât sub imperiul Codului de procedură penală anterior, atunci când nu aveau competență funcțională de a face acest lucru, cât și sub noul Cod, până la Decizia Curții Constituționale nr. 51/2016, atunci când operau sub auspiciile de „alt organ specializat al statului", s-a impus realizarea unui cadru de colaborare legal. Odată cu invalidarea, din punct de vedere constituțional, a respectivei expresii cuprinse în art. 142 alin. (1) C.pr.pen., dar și cu subsecventa reafirmare pe calea contenciosului constituțional a sancțiunii nulității absolute incidente în cazul nerespectării dispozițiilor legale privind competența organelor de urmărire penală, orientarea judiciară în privința interceptărilor telefonice s-a modificat radical.

În prezenta secțiune ne propunem să analizăm aspectele de actualitate strict referitoare la una dintre modalitățile concrete ale măsurii de supraveghere tehnică prevăzută de art. 138 alin. (1) lit. a) C.pr.pen., respectiv *interceptarea comunicațiilor* prin intermediul Centrului Național de Interceptare a Comunicațiilor din cadrul Serviciului Român de Informații.

Crearea C.N.I.C. nu poate fi situată în mod precis în timp, fiind pentru prima dată menționată ca structură a S.R.I. în Raportul de activitate al serviciului pe anul 2008, în care se menționa că: „***în calitate de autoritate națională în domeniul interceptării comunicațiilor**, Serviciul Român de Informații a asigurat – prin intermediul Centrului Național de Interceptare a Comunicațiilor (C.N.I.C.) – **punerea în aplicare, cu respectarea strictă a prevederilor legii**, a actelor de autorizare a interceptării comunicațiilor emise în condițiile art. 20-22 din Legea nr. 535/2004 privind prevenirea și combaterea terorismului sau în condițiile prevăzute de art. 91[1-5] din Codul de procedură penală, pentru toate structurile din Sistemul Național de Securitate și pentru **Ministerul Public***"[1] (s.n.). În mod evident, activitatea de interceptare a S.R.I. era una declarată public, nefiind necesare mențiuni suplimentare cu privire la caracterul flagrant nelegal al punerii în aplicare a mandatelor de interceptare și înregistrare.

În mod interesant, deși C.N.I.C. funcționează în cadrul S.R.I., a fost apreciat în doctrină ca fiind o structură administrativă distinctă, a cărei organizare și funcționare nu cunosc o bază legală și nu au o bază constituțională[2]. Sub acest aspect, autoarea citată apreciază că se impunea ca C.N.I.C. să fie considerată o autoritate administrativă autonomă, separată de S.R.I.[3], opinie cu care suntem de acord și care va trebui să fie avută în vedere de legiuitor.

Pentru a se asigura legalitatea desfășurării interceptării comunicațiilor, au fost instituite dispoziții legale în acest sens atât în Legea nr. 14/1992[4] privind organizarea și funcționarea Serviciului Român de Informații, cât și în Legea nr. 304/2004 privind organizarea judiciară[5].

---

[1] S.R.I., Raport privind activitatea desfășurată în anul 2008, p. 30, pe *www.sri.ro*

[2] *D. Tofan*, Câteva reflecții cu privire la Ordonanța de urgență a Guvernului nr. 6/2016 privind unele măsuri pentru punerea în executare a mandatelor de supraveghere tehnică dispuse în procesul penal, în Curierul Judiciar nr. 4/2016, p. 215.

[3] *Ibidem*, p. 214.

[4] Legea nr. 14 din 24 februarie 1992 privind organizarea și funcționarea Serviciului Român de Informații (M. Of. nr. 33 din 3 martie 1992).

[5] Legea nr. 304 din 28 iunie 2004 privind organizarea judiciară (republicată în M. Of. nr. 827 din 13 septembrie 2005).

Activitatea C.N.I.C. este amintită în art. 8 alin. (2) din Legea nr. 14/1992[1], în care se arată că acest centru asigură accesul nemijlocit și independent al organelor de urmărire penală la sistemele sale tehnice, în scopul executării măsurii interceptării comunicațiilor și a oricărui tip de comunicare la distanță.

C.N.I.C. va fi supus unor controale periodice pentru a se asigura că nu există abateri de la dispozițiile legale, cum s-a întâmplat anterior pronunțării Deciziei nr. 51/2016 a Curții Constituționale, controale realizate de către președintele Înaltei Curți de Casație și Justiție sau de către unul dintre judecătorii desemnați de acesta, în condițiile stabilite prin art. 30[1] din Legea nr. 304/2004. Aceste controale se vor desfășura semestrial sau ori de câte va fi nevoie și vor avea ca obiect respectarea dispozițiilor art. 8 alin. (2) din Legea nr. 14/1992 privind supravegherea tehnică realizată de organele de urmărire penală. În urma acestui control va fi întocmit un raport al președintelui Înaltei Curți de Casație și Justiție, care va fi pus la dispoziția publicului.

Modalitatea de colaborare a organelor judiciare cu C.N.I.C. este reglementată printr-un protocol încheiat între P.I.C.C.J. și S.R.I.[2], fiind un act cu caracter public. Acesta privește numai sprijinul tehnic acordat de C.N.I.C. pentru punerea în executare a interceptării comunicațiilor sub controlul direct și nemijlocit al organelor de urmărire penală. Între acestea vor fi incluse și direcțiile specializate din cadrul P.I.C.C.J.

Principala funcție a Protocolului este cea de a stabili limitele dintre activitatea organelor de urmărire penală și cea a S.R.I., în acest sens arătându-se că, potrivit art. 2 din Protocol, S.R.I. asigură „*accesul direct, nemijlocit și independent la sisteme tehnice deținute și administrate de acesta, prin Centrul Național de Interceptare a Comunicațiilor, pentru punerea în aplicare a actelor de autorizare emise în temeiul prevederilor Codului de procedură penală sau a legii speciale*". Prin dispozițiile menționate, organele de urmărire penală vor putea folosi sistemele informatice ale C.N.I.C. prin accesarea lor directă, fără nicio intermediere din partea S.R.I. și fără ca accesul acestora să fie condiționat sau supus vreunui control din partea serviciului. După cum se mai menționează în Protocol, măsurile vor permite existența unui sistem centralizat de punere în executare a mandatelor de supraveghere tehnică ce privesc interceptarea comunicațiilor.

Accesul independent și nemijlocit al organelor de urmărire penală se realizează prin: *i)* utilizarea aplicațiilor informatice de interceptare specifice, puse la dispoziție de S.R.I.; *ii)* managementul subiecților unui mandat și al mandatelor de supraveghere tehnică; *iii)* managementul utilizatorilor din cadrul structurii conectați la sistem; *iv)* direcționarea semnalului interceptat și/sau recepționarea acestuia către/de către structuri stabilite de Ministerul Public (colectarea înregistrărilor rezultate în urma interceptării); *v)* exportul produselor interceptate prin intermediul aplicațiilor informatice specifice.

---

[1] Potrivit art. 8 alin. (2) din Legea nr. 14/1992, „Pentru relația cu furnizorii de comunicații electronice destinate publicului, Centrul Național de Interceptare a Comunicațiilor din cadrul Serviciului Român de Informații este desemnat cu rolul de a obține, prelucra și stoca informații în domeniul securității naționale. La cererea organelor de urmărire penală, Centrul asigură accesul nemijlocit și independent al acestora la sistemele tehnice în scopul executării supravegherii tehnice prevăzute la art. 138 alin. (1) lit. a) din Codul de procedură penală. Verificarea modului de punere în aplicare în cadrul Centrului Național de Interceptare a Comunicațiilor a executării acestor supravegheri tehnice se realizează potrivit art. 30[1] din Legea nr. 304/2004 privind organizarea judiciară, republicată, cu modificările și completările ulterioare".

[2] Protocolul privind cooperarea între Serviciul Român de Informații și Ministerul Public pentru stabilirea condițiilor concrete de acces la sisteme tehnice ale Centrului Național de Interceptare a Comunicațiilor, înregistrat sub nr. 9331 din 07.12.2016 la Serviciul Român de Informații și sub nr. 2440/C din 08.12.2016 la Parchetul de pe lângă Înalta Curte de Casație și Justiție.

Rolul S.R.I. va fi numai unul tehnic și numai la solicitarea organelor de urmărire penală, acesta fiind limitat, potrivit art. 4 din Protocol, numai prin raportare la rețelele sau echipamentele tehnice conectate la sistemul C.N.I.C. Cu alte cuvinte, S.R.I. își va exercita doar funcția de administrator tehnic, asigurând buna funcționare a sistemului, fără să poată interveni în punerea în executare propriu-zisă. În esență, are următoarele sarcini: *i)* de a acorda sprijin tehnic, prin management și întreținerea aplicațiilor informatice și a echipamentelor, remedierea deranjamentelor software sau hardware; *ii)* de a acorda suport tehnic pentru instalarea și configurarea terminalelor de exploatare tehnică aflate în proprietatea sau administrarea Ministerului Public; *iii)* de a acorda suport tehnic și de a instrui personalul pentru realizarea interconectării cu C.N.I.C.; *iv)* de a stabili politici, strategii și proceduri de securitate.

Pentru ca accesarea C.N.I.C. să fie securizată, Ministerul Public trebuie să se asigure că terminalul folosit pentru acces este izolat de alte rețele și că va fi folosit numai în acest scop. Cu alte cuvinte, computerul destinat punerii în executare a interceptărilor nu poate fi folosit în alte scopuri decât interceptarea comunicațiilor, nu poate fi conectat la internet și nici la rețeaua internă a parchetului. În același timp, este interzisă modificarea sau instalarea de aplicații noi pe respectivele terminale.

Din punct de vedere legal, Protocolul pare a stabili suficiente reguli pentru eliminarea oricărui amestec al S.R.I. în activitatea organelor de urmărire penală în punerea în aplicare a mandatelor de supraveghere tehnică. Din punct de vedere tehnic, nu este complet edificator, fiind de preferat să se indice mai în detaliu criteriile tehnice importante. Apreciem că, deși regulile stabilite sunt puține ca număr, ele vor fi eficiente mai ales ca urmare a instituirii unei garanții prin controlul semestrial desfășurat de președintele Înaltei Curți de Casație și Justiție.

Cel mai recent control al președintelui Înaltei Curți de Casație și Justiție a avut loc în cursul lunii decembrie 2019, raportul fiind publicat pe site-ul instituției[1] și constituie un act care merită analizat în prezenta secțiune, întrucât explică atât elementele tehnice privind modalitatea concretă de punere în executare a mandatelor de supraveghere tehnică, cât și garanțiile tehnice instituite care previn accesul neautorizat al serviciilor secrete la rezultatele activităților de supraveghere tehnică.

Prima constatare a raportului vizează dotarea logistică a organelor de urmărire penală pentru realizarea interceptării comunicațiilor prin intermediul C.N.I.C., constituindu-se structuri specializate în cadrul acestora, separate fizic de C.N.I.C. Din punctul de vedere al sistemelor informatice, la acest moment, există terminalele necesare pentru punerea în executare a supravegherii tehnice, acestea fiind instalate și configurate independent de sistemul informatic al S.R.I. Niciun organ judiciar nu desfășoară activități la sediul C.N.I.C.

Se mai constată și că, la acest moment, a fost alocat personal tehnic specializat pentru desfășurarea operațiunilor specifice. Din acest punct de vedere, ne exprimăm anumite îngrijorări, deoarece personalul tehnic specializat va trebui să aibă calitatea prevăzută de art. 142 alin. (1) C.pr.pen.

Se subliniază că, din punctul de vedere al logisticii, există o separație între fluxurile de acces în sistemul informatic, fiind implementate patru asemenea fluxuri, fiecare funcționând independent – unul pentru S.R.I. în exercitarea atribuțiilor legale, unul pentru P.I.C.C.J. și câte unul pentru D.N.A. și D.I.I.C.O.T. Toate aceste autorități pot accesa simultan sistemul

[1] ICCJ, Raport privind verificarea efectuată de președintele Înaltei Curți de Casație și Justiție în temeiul art. 30[1] din Legea nr. 304/2004 privind organizarea judiciară, republicată, cu modificările și completările ulterioare, înregistrat sub nr. 11 din 7 ianuarie 2020, pe *www.scj.ro*

informatic, dar în mod autonom și independent, neputând să vizualizeze ori să acceseze operațiunile efectuate de celelalte autorități.

O altă constatare este că C.N.I.C. își respectă atribuțiile sale limitate privind administrarea sistemului tehnic de stocare a conținutului comunicațiilor transferate de operatorii de comunicații, în condițiile mandatelor de supraveghere tehnică introduse în sistem și acordă suportul tehnic necesar. Deosebit de importantă este constatarea folosirii unor mecanisme de criptare între conexiunile de date stabilite între utilizatori și servere, ceea ce împiedică interceptarea acestora în drumul către sediul parchetelor.

Din punct de vedere tehnic, în cuprinsul raportului se arată că procesele tehnice de interceptare a comunicațiilor se realizează în centrele operatorilor de telecomunicații, iar conținutul comunicațiilor interceptate este transferat în mod complet automatizat către sistemul de stocare administrat de C.N.I.C., fără intervenția umană a S.R.I. Această constatare este corectă tehnic, deoarece presupune ca S.R.I. să obțină de la furnizori conținutul comunicației prin intermediul sistemului informatic al acestora, acela reprezentând canalul de comunicație interceptat. Odată primite datele informatice, ele pot fi accesate numai de una dintre cele patru autorități menționate mai sus, fără a exista posibilitatea ca oricare dintre ele să acceseze datele unei alte autorități.

În ceea ce privește modalitatea de inițiere a interceptării comunicațiilor, aceasta se face prin terminalele din sediile organelor de urmărire penală, prin introducerea datelor solicitate în aplicația S.R.I., respectiv datele mandatului de supraveghere tehnică. În funcție de aceste date introduse, conținutul brut al comunicației este înregistrat, extras și transferat în mod automatizat de la operatorul de comunicații la sistemul de stocare administrat de C.N.I.C., fără a fi posibilă vreo intervenție umană pe fluxul de comunicație. Odată ajuns la Centru, ele sunt stocate pe serverul general într-o formă criptată pentru o perioadă limitată de timp, fiind expediate automatizat organului judiciar beneficiar, iar apoi distruse automat din server. Această ștergere este planificată și implementată astfel încât să aibă caracter permanent și ireversibil, interceptările fiind transmise în format criptat către terminalul organului de urmărire penală, care va deține unica lor copie.

Sub aspectul duratei mandatului, sistemul informatic nu permite realizarea unei interceptări a comunicațiilor peste durata mandatului, acesta închizându-se automat la expirarea mandatului. Corelativ, se stabilește și ora de la care va porni automat interceptarea.

Un element interesant este cel menționat în legătură cu imposibilitatea ștergerii sau modificării conținutului unei convorbiri efectuate sau a datelor aferente acesteia; în opinia noastră, soluția tehnică are similarități cu semnătura electronică extinsă, putând fi bazată pe o tehnologie identică. Cu toate acestea, fără mai multe date tehnice, trebuie doar să rămânem cu concluzia că operatorii nu vor putea modifica datele informatice.

În finalul raportului, președintele Înaltei Curți de Casație și Justiție, exercitând un control care are ca scop asigurarea garanțiilor privind protecția drepturilor fundamentale ale persoanelor, precum și respectarea dispozițiilor legale, concluzionează, în legătură cu personalul S.R.I. care lucrează în cadrul C.N.I.C., că: „*(i) nu interferează pe fondul activității autorităților judiciare de operare și gestionare a măsurilor de interceptare a comunicațiilor dispuse prin actele de autorizare emise în condițiile legii; (ii) nu are acces la conținutul comunicațiilor transferate automat de la operatorii de comunicații în sistemul de stocare administrat de Centrul Național de Interceptare a Comunicațiilor; (iii) nu are acces pe fluxul de interceptare în procesul tehnic de extragere și transferare către autoritatea judiciară beneficiară a traficului de voce și date interceptat*”[1].

[1] *Ibidem*, pp. 8-9.

În concluzie, ținând seama de toate cele expuse în prezenta secțiune, apreciem că, la acest moment, modalitatea tehnică de realizare a interceptării comunicațiilor se realizează cu o aparentă separație între organele de urmărire penală care pun în executare mandatele de supraveghere tehnică și personalul S.R.I. care oferă suport tehnic și logistic strict limitat la activități de administrare și mentenanță, fără posibilitatea de a interveni pe fluxul de interceptare sau de a obține rezultatele activităților de supraveghere tehnică. Concluziile raportului întocmit de președintele Înaltei Curți de Casație și Justiție arată o evoluție favorabilă în sensul respectării stricte a dreptului la viață privată al cetățeanului.

Cu toate acestea, cunoscând trecutul nefericit al S.R.I. și intervenția sa nelegală în activitatea de urmărire penală, trebuie să fim rezervați în a considera că mecanismul de control este unul real și eficient. Dispozițiile art. 30^1 din Legea nr. 304/2004 nu instituie un audit tehnic, ci un simplu control, astfel că rezervele noastre se îndreaptă către lipsa de specializare tehnică a președintelui Înaltei Curți de Casație și Justiție, dat fiind sistemul informatic deosebit de avansat, dar și folosirea, de către S.R.I., a unor aplicații create chiar de instituție. Concluziile raportului mai sus amintit se bazează, din punct de vedere tehnic, pe informații primite chiar de la S.R.I., care, deși până la acest moment nu au fost contrazise prin alte probe, trebuie să conducă la o modificare legislativă sub acest aspect pentru îndepărtarea oricărui control al serviciilor secrete asupra C.N.I.C. Întrucât, astfel cum se reține și în raport, există fluxuri distincte autonome și independente pentru interceptarea comunicațiilor, nu găsim niciun motiv pentru care, cu timpul, acest centru să capete o personalitate juridică proprie și să activeze în continuare independent față de S.R.I. sau chiar în subordinea Ministerului Justiției.

Capitolul VI
Concluzii

Interceptarea comunicațiilor și a altor comunicări la distanță reprezintă metoda specială de supraveghere cea mai des utilizată în practică, fiind cea care a suscitat cele mai multe discuții și probleme privind legalitatea probelor obținute în procesul penal, mai ales din cauza punerii în executare de către serviciile de informații, în locul organelor de urmărire penală. Această măsură poate avea un rol determinant în cauzele în care este întrebuințată, conducând la obținerea de probe directe privind existența unor infracțiuni.

Întrucât reprezintă o tehnică specială de investigație, având caracter secret și provocând o intruziune în viața privată a persoanei supravegheate, interceptarea comunicațiilor trebuie să fie prevăzută de lege, într-un mod clar și previzibil. Legiuitorul a reușit acest lucru, chiar și în considerarea faptului că nu sunt relevate aspectele tehnice care țin de punerea în executare a măsurii.

Autorizarea măsurii și punerea sa în executare va fi guvernată de aceleași reguli ca în cazul supravegherii tehnice, mijloacele de probă care vor rezulta vor fi procesele-verbale prevăzute de art. 143 C.pr.pen., dintre care cel mai important va fi procesul-verbal de redare integrală a convorbirilor, comunicărilor sau conversațiilor, prevăzut de art. 143 alin. (4) C.pr.pen., care va trebui certificat de procuror.

În trecut, măsura a fost folosită în mod excesiv, prin emiterea unui număr impresionant de mandate de supraveghere tehnică, toate fiind puse în executare de către S.R.I., până la pronunțarea Deciziei nr. 51/2016 a Curții Constituționale. Ulterior, numărul mandatelor emise a scăzut la o pătrime.

În prezent, modalitatea de realizare a interceptării comunicațiilor permite ca organele de urmărire penală să acceseze direct, prin terminale proprii, sistemul informatic dezvoltat de C.N.I.C. și prin acesta să implementeze în mod independent și nemijlocit orice mandat de supraveghere tehnică, fără a exista o imixtiune a S.R.I. De la situația unor protocoale secrete care au fost menite să ascundă adevărul și să permită încălcarea legii procesuale penale de către S.R.I. și procurori, s-a ajuns la un protocol public, transparent, care permite oricărei persoane să cunoască modul de desfășurare a activității de interceptare. S-a constituit și o garanție suplimentară, prin controlul semestrial al activității C.N.I.C. de către președintele Înaltei Curți de Casație și Justiție.

De lege ferenda, apreciem că activitatea de interceptare a comunicațiilor va trebui să fie desfășurată de un organ independent sau cel puțin aflat în subordinea Ministerului Justiției, pentru a se evita orice implicare viitoare a S.R.I. în desfășurarea oricăror acte de urmărire penală.

Titlul V
Accesul la un sistem informatic[1]

Capitolul I
Aspecte generale

Activitatea de urmărire penală trebuie întotdeauna să reacționeze la progresul infractorilor în a comite în moduri inovatoare infracțiuni, astfel că descoperirea și tragerea la răspundere a acestor persoane trebuie să țină pasul cu noile metode de săvârșire a infracțiunilor. Pentru a contribui la demersul organelor judiciare, este necesar ca statul să adopte noi proceduri prin care să sporească puterile de cercetare a acestora, punând, totodată, în balanță nevoile societății cu interesul privat al cetățeanului. În același sens, statul este dator să incrimineze și acele noi comportamente infracționale, care tind să perturbe orânduirea socială și care sunt cauzate de noile posibilități oferite de progresul tehnologic.

Pentru a preveni săvârșirea de infracțiuni, pentru a descoperi și trage la răspundere penală persoanele care comit astfel de fapte, s-au implementat noi procedee probatorii, care pot fi adaptate la schimbările tehnologice curente și care pot permite strângerea mai ușoară de probe. Aceste procedee probatorii sunt grupate de Codul de procedură penală, în principal, în Capitolul IV al Titlului IV al Părții generale a Codului și sunt denumite generic **„metode speciale de supraveghere sau cercetare"**.

Specificul acestor procedee probatorii constă în dependența lor de autoritatea statului, manifestată prin restrângerea drepturilor persoanei față de care se dispune folosirea metodelor speciale de supraveghere, dar și caracterul lor secret. Considerăm că aceste procedee probatorii sunt cele mai restrictive cu privire la viața privată a individului, motiv pentru care folosirea lor trebuie să fie văzută ca o *ultima ratio*, iar nu ca un mod comod de realizare a urmăririi penale. Din păcate, practica ne arată că folosirea metodelor speciale de supraveghere sau cercetare, în special a supravegherii tehnice, este discreționară și nejustificată. Nu de puține ori, ceea ce judecătorul de drepturi și libertăți este chemat să dispună nu reprezintă o anumită metodă de supraveghere tehnică, ci *o supraveghere tehnică completă*, în sensul art. 138 alin. (1) lit. a)-e) C.pr.pen., lăsând procurorului deplină libertate de a se folosi mai apoi de orice metodă de supraveghere tehnică pe care o va considera oportună. Considerăm greșită o atare abordare, având în vedere că fiecare dintre metodele de supraveghere tehnică presupune ingerințe aduse vieții private a persoanei, care trebuie analizate în mod distinct de judecătorul de drepturi și libertăți. Nu poate fi acceptată utilizarea unor procedee probatorii derogatorii și intruzive, precum accesul la un sistem informatic, doar pentru a permite organelor de urmărire penală să obțină probe într-un mod mai comod și mai rapid decât procedeele probatorii obișnuite[2].

[1] Materialul prezentului titlu a constituit primul referat științific din cadrul studiilor doctorale și a fost publicat în revista Caiete de Drept Penal nr. 3/2016 și 4/2016, sub denumirea „Considerații privind accesul la un sistem informatic ca metodă de supraveghere tehnică", fiind modificat și actualizat în prezenta lucrare.

[2] *O.S. Kerr*, op. cit., p. 317.

În cuprinsul acestei secțiuni, vom aborda metoda specială de supraveghere tehnică a *accesului la un sistem informatic*, detaliind specificul acestei metode, modalitatea în care se dispune folosirea ei, modul în care se efectuează, precum și distincțiile între aceasta și alte procedee probatorii. A fost introdusă în special în vederea combaterii criminalității informatice, care prezintă unele particularități față de alte forme de criminalitate, constând în globalizare, desfășurarea prin rețele de comunicații și crearea, în urma săvârșirii lor, a unor urme de date informatice[1]. Astfel, criminalitatea informatică nu se mulează pe regulile obișnuite ce țin de aspectele spațiale sau materiale ale săvârșirii unei infracțiuni, prezentând probleme specifice ce țin de teritorialitate (făptuitorul poate comite fapta într-o altă țară decât aceea în care se află victima) și de probațiune (nu vor exista urme materiale, ci numai urme digitale).

Accesul la un sistem informatic este o metodă specială puțin înțeleasă de către doctrina din țara noastră și, cu atât mai puțin, de practica judiciară, fiind confundată cu *percheziția informatică*. Cu toate că originea celor două procedee probatorii este aceeași, ele fiind preluate din Convenția de la Budapesta privind criminalitatea informatică[2], legiuitorul român a preferat să creeze două instituții distincte. Este eronat să se considere că accesul la un sistem informatic reprezintă fie același lucru cu percheziția informatică, fie doar o etapă premergătoare unei percheziții informatice. Așa cum vom arăta, realitatea este alta, cele două procedee probatorii derivând din art. 19 al Convenției de la Budapesta, scindat în două instituții care se întrepătrund, dar care au diferențe deosebit de importante[3]. Convenția de la Budapesta privind criminalitatea informatică din anul 2001 constituie sediul materiei pentru accesul la un sistem informatic, din punct de vedere legal și chiar tehnic, deoarece face legătura între terminologia juridică folosită de legiuitor și înțelesul exact al acestora în practică. În acest sens, sub aspect terminologic, trebuie arătat faptul că o parte dintre problemele care survin în domeniul de reglementare al Convenției de la Budapesta sunt soluționate de Comitetul Convenției de la Budapesta (T-CY)[4], prin notele interpretative emise de către acest comitet.

Accesul la un sistem informatic este prevăzut de art. 138 alin. (1) b) C.pr.pen. și este considerat o metodă specială de supraveghere tehnică, menționându-se în cuprinsul art. 138 alin. (13) C.pr.pen.

Accesul la un sistem informatic este definit în cuprinsul art. 138 alin. (3) C.pr.pen., în care se arată că: „*prin «acces la un sistem informatic» se înțelege pătrunderea într-un sistem informatic sau mijloc de stocare a datelor informatice fie direct, fie de la distanță, prin intermediul unor programe specializate ori prin intermediul unei rețele, în scopul de a identifica probe*". Considerăm că această definiție legală este cuprinzătoare, dar, în același timp, este suficient de generală pentru a cauza dificultăți de aplicare în practică, raportat la domeniul tehnic la care se referă. Fiind o metodă de supraveghere tehnică, va fi necesar ca accesul la un sistem informatic să fie autorizat de către judecătorul de drepturi și libertăți, conform art. 140 C.pr.pen.

---

[1] *A. Staniforth*, Blackstone's Handbook of Cyber Crime Investigation, Oxford University Press, Oxford, 2017, p. 8.

[2] Convenția de la Budapesta privind criminalitatea informatică (*Convention on cybercrime*) este o inițiativă a Consiliului Europei și a fost semnată la Budapesta la data de 23 noiembrie 2001. Aceasta a fost ratificată de un număr de 47 de state, printre care și România. Convenția a intrat în vigoare la data de 1 iulie 2004.

[3] *V. infra*, Titlul V, Capitolul IV.4.

[4] Conform art. 46 din Convenția de la Budapesta, statele semnatare se prezintă, prin reprezentanți, la consultații periodice privind Convenția de la Budapesta. În acest sens, Comitetul reprezintă forma instituționalizată, prin care statele semnatare își exprimă poziția și adoptă acte privind interpretarea Convenției. Notele interpretative sunt adoptate numai în cazul în care toți semnatarii le admit în mod unanim, ele exprimând modalitatea în care semnatarii înțeleg să aplice Convenția de la Budapesta.

Asemenea celorlalte metode de supraveghere tehnică, o trăsătură importantă a accesului la un sistem informatic este caracterul său secret față de persoana în privința căreia se dispune folosirea procedeului probatoriu[1]. Considerăm că este mai adecvat termenul de „secret" pentru a face distincție de termenul „nepublic". Astfel, urmărirea penală are caracter nepublic, însă subiecții procesuali pot fi încunoștințați de efectuarea unor acte de urmărire penală care îi privesc, excepția fiind **metodele speciale de supraveghere sau cercetare**, care au caracter secret până la terminarea acestora[2] ori până la terminarea urmăririi penale[3].

Deoarece domeniul informatic presupune cunoștințe tehnice medii spre avansate privind infrastructura sistemelor informatice și a mecanismelor în care acestea interacționează, se poate greși ușor în aplicarea procedeului probatoriu despre care facem vorbire. În acest sens, chiar și Codul de procedură penală conține definiții cu privire la anumiți termeni tehnici necesari în înțelegerea accesului la un sistem informatic. Considerăm că o abordare corectă și completă este de a pleca de la terminologia folosită de Codul de procedură penală și a Convenției de la Budapesta privind criminalitatea informatică. Principalii termeni care se impun a fi lămuriți sunt: „sistem informatic", „date informatice", „furnizor de servicii de comunicații electronice", „date referitoare la traficul informațional", „date referitoare la conținutul informațional".

În privința definiției „sistemului informatic", Codul de procedură penală preia în mod fidel prevederile art. 1 lit. a) din Convenția de la Budapesta, stabilind că: „*prin «sistem informatic» se înțelege orice dispozitiv sau ansamblu de dispozitive interconectate ori aflate în relație funcțională, dintre care unul sau mai multe asigură prelucrarea automată a datelor, cu ajutorul unui program informatic*" [art. 138 alin. (4) C.pr.pen.].

Prin „dispozitiv" se înțelege un ansamblu de componente electronice aflate într-o relație funcțională, care permit acestuia să ruleze programe informatice în vederea prelucrării automate a datelor. Dispozitivul poate o fi o sumă de componente autonome sau nu, în funcție de specificul acestuia. Un computer tip desktop va fi, prin excelență, un ansamblu de componente autonome (placă de bază, memorie, hard-disk/solid state drive, placă video, sursă de curent etc.), însă un laptop va fi un dispozitiv unitar (deoarece componentele, în mare parte, vor fi pe aceeași placă de circuite integrate și nu pot fi demontate de utilizator spre a fi înlocuite). În mod similar, un dispozitiv unitar și, implicit, un sistem informatic va fi și telefonul mobil, tableta, PDA-ul, MP3 player-ul și alte astfel de dispozitive[4]. Considerăm că ultima distincție este relevantă, raportat la obiectul care se va impune a fi ridicat de autorități spre a fi supus unui acces la sistem informatic ori unei percheziții informatice, deoarece, în cele mai multe situații, nu este necesar ca întreg sistemul informatic să fie ridicat și păstrat în custodie, fiind suficient să fie ridicate doar anumite părți. În schimb, nu va constitui sistem informatic un dispozitiv periferic – mouse, tastatură, imprimantă, unitate optică externă și chiar o unitate hard-disk externă, întrucât acestea sunt dispozitive care nu asigură prelucrarea datelor. Acesta este motivul pentru care, în cuprinsul definiției accesului la un sistem informatic, Codul de procedură penală face distincția între *sistem informatic* și *mijloc de stocare*.

Trebuie subliniat faptul că un telefon mobil modern, precum și o tabletă sau PDA (personal digital assistant – antecesorul smartphone-urilor) trebuie să fie considerate sisteme

[1] *M. Bulancea*, în M. Udroiu (coord.), Codul de procedură penală, 2015, p. 428.

[2] Conform art. 92 alin. (1) lit. a) C.pr.pen., avocatul suspectului sau inculpatului nu are dreptul de a participa la efectuarea actelor în care se utilizează metodele speciale de supraveghere sau cercetare.

[3] Art. 145 alin. (5) C.pr.pen.

[4] Conform interpretării date de Comitetul Convenției privind criminalitatea informatică (T-CY), prin Nota interpretativă nr. 1 din 5 Decembrie 2012 privind noțiunea de „sistem informatic".

informatice, deoarece prelucrează în mod automat date. Odată cu progresul tehnologic și miniaturizarea componentelor, distincția dintre un sistem informatic clasic – PC sau laptop – și un dispozitiv inteligent de ultimă generație – smartphone sau tabletă – devine una care nu schimbă caracterul de sistem informatic al dispozitivului.

O distincție care se impune a fi făcută este cea dintre un *sistem informatic* și un *suport de stocare a datelor informatice* (sau mijloc de stocare a datelor informatice). În ultima situație, suportul de stocare este un dispozitiv extern care nu procesează informațiile conținut, ci doar le înmagazinează. Din punct de vedere practic, se poate întrevedea o problemă: există mijloace de stocare a datelor care se conectează la un PC și unele care se conectează la o rețea, fizic ele putând fi identice[1]. Un hard-disk extern este un mijloc de stocare, însă un NAS – Network Attached Storage – este un *sistem informatic*, deoarece stocarea datelor se face pe baza unui program informatic care simulează în rețea faptul că dispozitivul NAS este un sistem informatic distinct. Deși pare o diferență neesențială, în practică, abordarea va fi diferită în accesarea sistemului informatic. În același timp, în ipoteza predării de obiecte, înscrisuri sau date informatice, se impune ca un NAS să nu fie ridicat, ci informațiile conținute în acesta să fie copiate, pentru a nu se perturba ceilalți utilizatori din rețea[2]. În schimb, un mijloc de stocare a datelor poate fi predat în mod direct organelor de urmărire penală, fiind un risc mai redus ca terțe persoane să fie afectate în urma predării sale.

Prin „sistem informatic" se poate înțelege și un ansamblu de dispozitive care sunt interconectate, mai multe dintre acestea putând prelucra date cu ajutorul unui program. Cel mai bun exemplu de un astfel de sistem informatic este o rețea locală de calculatoare care funcționează în cadrul unei instituții. În același timp, va fi considerat un sistem informatic și o serie de dispozitive interconectate prin internet, însă numai cu condiția ca între acestea să poată fi stabilită o legătură specifică[3]. De exemplu, nu va constitui un sistem informatic, în sens de ansamblu de dispozitive, telefonul angajatului unei societăți, proprietate proprie, care este utilizat și în scop de serviciu, primind și trimițând e-mailuri prin serverul de e-mail al societății. În schimb, vom fi în situația unui sistem informatic atunci când societatea achiziționează mai multe dispozitive tip smartphone pentru angajații săi, le configurează și le administrează în mod centralizat sau le oferă servicii interne diverse, precum acces la fișierele informatice ale societății, e-mail, schimb de contacte etc. Distincția are importanță practică, deoarece, în prima situație, se impune autorizarea individuală a fiecărui terminal smartphone, iar, în cea de-a doua situație, va fi suficient a se autoriza accesul la un sistem informatic cu privire la întreaga rețea de smartphone-uri ale societății. În toate cazurile, la momentul autorizării metodei speciale de supraveghere tehnică, trebuie să se prevadă în mod expres sistemele informatice care sunt vizate.

Noțiunea de „program informatic" constituie orice formă de instrucțiuni care pot fi furnizate unui sistem informatic în vederea procesării unor date, nefiind limitat la noțiunile de „sistem de operare" sau de „aplicație". Așa cum se arată și în Raportul Explicativ al Convenției de la Budapesta privind criminalitatea informatică, esențial este ca programul informatic să prelucreze în mod automat datele, fără intervenția omului. Acest lucru nu înseamnă că punerea în funcțiune a programului informatic nu poate fi determinată de către om. De exemplu,

[1] De exemplu, seria MyBook de la Western Digital este fizic identică cu seria MyCloud, primul fiind un hard-disk extern, iar cel de-al doilea fiind un NAS (Network Attached Storage).

[2] Și a se crea prejudicii nejustificate care, mai apoi, ar trebui să fie avansate de la bugetul de stat drept cheltuieli judiciare.

[3] În lipsa acestei legături specifice, precizarea interconectării printr-o rețea nu mai are nicio valoare, având în vedere că majoritatea sistemelor informatice sunt conectate la internet.

constituie un program informatic sistemul de operare Windows. Acesta poate în mod automat să copieze informații de pe un mijloc de stocare pe altul, fără intervenție umană, însă va face acest lucru numai la comanda unui utilizator.

Prin „date informatice" se înțelege, conform art. 138 alin. (5) C.pr.pen., orice reprezentare de fapte, informații sau concepte sub o formă adecvată prelucrării într-un sistem informatic, inclusiv un program capabil să determine executarea unei funcții de către un sistem informatic. Datele informatice, la rândul lor, se împart în *date conținut* și *date privind traficul informațional*.

„Datele conținut" nu sunt altceva decât datele informatice în sens restrâns, ele fiind informații sau concepte care sunt stocate într-un sistem informatic sau într-un mijloc de stocare a datelor și *pot constitui probe în procesul penal prin însuși conținutul lor*. În alte cuvinte, simpla identificare a acestor date într-un sistem informatic poate constitui o probă privind îndeplinirea laturii obiective a unor infracțiuni, precum *pornografia infantilă*, prevăzută de art. 374 C.pen. (în modalitatea *deținerii* ori *stocării*), chiar și dacă agentul a stocat respectivele materiale strict pentru uz personal[1]. În același timp, în cadrul datelor conținut, putem înțelege și orice alte date relevante din punct de vedere penal cu privire la săvârșirea unei infracțiuni: comunicațiile arhivate ale făptuitorului cu alți participanți, site-urile de internet vizualizate recent, conturile folosite ori orice alte date conservate în format electronic. Cu privire la e-mailurile și comunicațiile găsite pe sistemul informatic ori mijlocul de stocare al unei persoane, considerăm că vor fi aplicabile dispozițiile privind accesul la un sistem informatic, și nu cele privitoare la *interceptarea comunicațiilor ori a oricărui tip de comunicare*, atât timp cât se accesează comunicații anterioare și care nu sunt în desfășurare[2]. Pentru accesarea datelor conținut, este necesară autorizarea prealabilă a judecătorului de drepturi și libertăți, având în vedere natura acestor date și a restrângerii grave a dreptului la viață privată al persoanei căruia îi aparțin aceste date informatice. În schimb, nu același lucru poate fi spus despre predarea și conservarea unor astfel de date, care nu presupun și accesarea lor, aspect pe care îl vom sublinia într-o secțiune ulterioară[3].

„Datele privind traficul informațional" (sau *datele trafic/traffic data)* sunt date de altă natură decât datele conținut, ele referindu-se nu la conținutul comunicării ori al datelor transferate, ci la *modalitatea, ruta, destinația, data, locul, mărimea* și alte astfel de atribute ale datelor informatice trimise ori recepționate de către un sistem informatic. Codul de procedură penală nu prezintă o definiție a acestui tip de date, însă face referire la acestea în cuprinsul art. 154 alin. (1) C.pr.pen. privind *conservarea datelor informatice*. În schimb, acest tip de date sunt definite, de art. 35 alin. (1) lit. f) din Legea nr. 161/2003[4] și prin art. 1 lit. d) din Convenția de la Budapesta, ca fiind „*orice date informatice referitoare la o comunicare realizată printr-un sistem informatic, generate de un sistem informatic care a format o parte din lanțul de comunicare, indicând, originea comunicării, destinația, ruta folosită, data comunicării, mărimea informațiilor comunicate, durata transmiterii datelor și tipul de serviciului utilizat pentru comunicare*".

Specificul acestor date privind traficul informațional este acela că ele *nu presupun cunoașterea conținutului comunicării, ci numai a unor elemente accesorii acestuia*, așa cum am arătat mai sus. Totodată, datele privind traficul informațional sunt, prin natura lor, efemere,

[1] *S. Bogdan (coord.), D.A. Șerban, G. Zlati*, Noul Cod penal. Partea specială. Analize, explicații, comentarii. Perspectiva clujeană, Ed. Universul Juridic, București, 2014, p. 731.

[2] *V. infra*, Titlul V, Capitolul IV.2.

[3] *V. infra*, Titlul V, Capitolul IV.1.

[4] Legea nr. 161 din 19 aprilie 2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice și în mediul de afaceri, prevenirea și sancționarea corupției (M. Of. nr. 279 din 21 aprilie 2003).

fiind reținute de către furnizorii de servicii informatice numai pentru perioade scurte de timp, mai apoi fiind șterse. Ele sunt însă esențiale pentru descoperirea făptuitorilor și, astfel, se impune să fie puse la dispoziția organelor de urmărire penală cât mai repede cu putință. Colectarea datelor privind traficul informatic este necesară mai ales în primele momente ale urmăririi penale, iar divulgarea acestor date constituie o restrângere redusă adusă dreptului la viață privată al individului, deoarece nu se poate determina din aceste date care a fost conținutul comunicațiilor. Față de *datele conținut*, ele au un caracter accesoriu și fracționat, accesoriu în sensul în care spun ceva despre comunicarea datelor conținut, și nu despre ce reprezintă acestea, iar fracționat, deoarece ele se regăsesc în bucăți în fiecare sistem informatic prin care trec datele conținut. Însă importanța lor este că stabilesc persoanele între care a avut loc comunicarea, precum și *protocolul* folosit. Prin „protocol" vom înțelege tipul de serviciu: vizualizare pagini internet, e-mail, VOIP, FTP etc., date care pot sugera ce anume s-a transferat ori dacă vom fi în situația unei comunicații între două sau mai multe persoane. Trebuie menționat faptul că există metode de împiedicare a generării de date privind traficul informațional prin utilizarea de protocoale tip VPN (Virtual Private Network – implementare a funcției criptografice, care asigură transmiterea criptată a informației[1]) și TOR (The Onion Router), pentru a se evita descoperirea destinației comunicațiilor, precum și a tipului de informații comunicate, prin metode, precum criptarea in întregime a comunicațiilor[2].

Un alt termen deosebit de important atât în privința accesului la un sistem informatic, cât și în cazul *conservării datelor informatice*, prevăzut de art. 154 C.pr.pen., este cel de „furnizor de servicii". Denumirea de „furnizor de servicii" are o semnificație proprie, fundamentată pe sensul conferit de art. 1 lit. c) din Convenția de la Budapesta, preluat în legislația română, în cuprinsul art. 35 alin. (1) lit. e) din Legea nr. 161/2003.

Conform acestei definiții unitare, prin „furnizor de servicii" se poate înțelege:

- orice persoană fizică sau juridică ce oferă utilizatorilor posibilitatea de a comunica prin intermediul sistemelor informatice;
- orice altă persoană fizică sau juridică ce prelucrează sau stochează date informatice pentru persoanele prevăzute la punctul 1 și pentru utilizatorii serviciilor oferite de acestea.

În loc să adopte această terminologie, legiuitorul a preferat să utilizeze, în domeniul procedeului probatoriu al *conservării datelor informatice*, termenii de „furnizor de rețele publice de comunicații electronice" și „furnizor de servicii de comunicații electronice destinate publicului". Considerăm că terminologia folosită nu este conformă Convenției de la Budapesta, fiindcă restrânge în mod nejustificat aplicarea acesteia. Cu toate că definiția pare similară, exclude *furnizorii de servicii de comunicații electronice care nu sunt destinate publicului* (de exemplu, un furnizor care oferă servicii de comunicații private, într-un grup restrâns de utilizatori, sau un furnizor de servicii rețelistice private, restrânse la rețeaua internă a unei corporații). Era de preferat ca legiuitorul să fi rămas consecvent formei inițiale a Codului de procedură penală, anterioară modificărilor aduse prin Legea nr. 255/2013[3], în care se utiliza

[1] *M.E. Whitman, H.J. Mattord*, Principles of Information Security, Fifth Edition, Ed. Cengage Learning, Boston, 2016, p. 346.

[2] *M. Simon, J. Slay*, Investigating Modern Communication Technologies: The Effect of Internet-based Communication Technologies on the Investigation Process, în Journal of Digital Forensics, Security and Law, vol. 6, no. 4/2011, p. 39.

[3] Legea nr. 255 din 19 iulie 2013 pentru punerea în aplicare a Legii nr. 135/2010 privind Codul de procedură penală și pentru modificarea și completarea unor acte normative care cuprind dispoziții procesual penale (M. Of. nr. 515 din 14 august 2013).

termenul de „furnizor de servicii" în sensul Legii nr. 161/2003, și nu terminologia actuală, care creează o predispoziție la confuzie, mai ales în condițiile existenței unei legislații nepenale în domeniu.

Termenii folosiți mai sus nu sunt specifici Codului de procedură penală, fiind împrumutați din legislația aplicabilă în domeniul comunicațiilor electronice și definiți în cuprinsul art. 4 din O.U.G. nr. 111/2011 privind comunicațiile electronice[1].

Considerăm că sensul folosit de legiuitor în cazul dispozițiilor Codului de procedură penală trebuie să fie același ca în legislația nepenală, cu toate că dreptul penal cunoaște *principiul autonomiei conceptuale*[2], care considerăm că se va aplica și în cazul normelor procesuale penale. În același timp, doctrina arată că acest principiu nu trebuie înțeles în mod absolut, deoarece adeseori dreptul penal preia termeni specifici din alte ramuri de drept[3]. Opinăm că acesta este cazul și în privința acestor termeni specializați din domeniul legislației privind comunicațiile electronice, un domeniu de reglementare al dreptului public în care adeseori se regăsesc termeni tehnici precum cei expuși anterior.

Potrivit art. 4 alin. (1) pct. 8 din O.U.G. nr. 111/2011, prin „furnizor de rețele de comunicații electronice" se înțelege „*o persoană a cărei activitate constă, în tot sau în parte, în furnizarea unei rețele de comunicații electronice în condițiile regimului de autorizare generală*". Prin „rețea de comunicații electronice" se înțelege: „*sistemele de transmisie și, acolo unde este cazul, echipamentele de comutare sau rutare și alte resurse, inclusiv elementele de rețea care nu sunt active, care permit transportul semnalelor prin cablu, prin unde radio, prin mijloace optice ori alte mijloace electromagnetice, incluzând rețelele de comunicații electronice prin satelit, rețelele terestre fixe, cu comutare de circuite și cu comutare de pachete, inclusiv internet, și mobile, rețelele electrice, în măsura în care sunt utilizate pentru transmiterea de semnale, rețelele utilizate pentru transmisia serviciilor de programe audiovizuale și rețelele de televiziune prin cablu, indiferent de tipul de informație transmisă*" [art. 4 alin. (1) pct. 6 din O.U.G. nr. 111/2011].

În esență, furnizorul de rețele de comunicații electronice asigură infrastructura necesară pentru existența serviciului de comunicații și nu oferă în sine acest serviciu. Spre exemplu: o societate care realizează o rețea proprie de comunicații electronice prin amplasarea de antene radio pentru rețele radio mobile celulare publice va fi considerată doar *furnizor de rețea* în măsura în care realizează și întreține rețeaua, fără a oferi servicii de comunicații publice. Însă această societate va putea să-și cedeze folosința rețelei către un *furnizor de servicii de comunicații electronice*.

În cuprinsul aceluiași text normativ este prevăzută și definiția „serviciului de comunicații electronice", cu ajutorul căruia putem deduce în mod logic și semnificația termenului de „furnizor de servicii de comunicații electronice destinate publicului". Astfel, conform art. 4 alin. (1) pct. 9 din O.U.G. nr. 111/2011, prin „serviciu de comunicații electronice" se înțelege „*un serviciu, furnizat, de regulă, contra cost, care constă, în întregime sau în principal, în transmiterea semnalelor prin rețelele de comunicații electronice, incluzând serviciile de telecomunicații și pe cele prin rețelele utilizate pentru transmisia serviciilor de programe audiovizuale, dar fără a include serviciile prin care se furnizează conținutul informației transmise prin intermediul rețelelor ori serviciilor de comunicații electronice sau se exercită controlul editorial asupra acestui*

[1] O.U.G. nr. 111 din 14 decembrie 2011 privind comunicațiile electronice (M. Of. nr. 925 din 27 decembrie 2011), aprobată cu modificări prin Legea nr. 140/2012.

[2] *Fl. Streteanu*, op. cit., p. 14.

[3] *Ibidem*, p. 15.

conținut; de asemenea, nu se includ serviciile societății informaționale, definite la art. 1 pct. 1 din Legea nr. 365/2002 privind comerțul electronic, republicată, care nu constau, în întregime sau în principal, în transmiterea semnalelor prin rețelele de comunicații electronice". În consecință, prin noțiunea de „furnizor de servicii de comunicații electronice destinate publicului" vom înțelege *acea persoană autorizată conform legislației în vigoare și care furnizează servicii de comunicații publicului*.

În această categorie intră societățile, precum furnizorii de servicii de telefonie, internet, televiziune și radio, însă nu vor putea fi considerați furnizori de servicii de comunicații electronice acele persoane care *furnizează conținutul informației*. Prin „conținutul informației", în sensul O.U.G. nr. 111/2011, considerăm că putem înțelege „date conținut", astfel că furnizorul de date conținut nu va putea fi considerat furnizor de servicii de comunicații electronice. Prin urmare, considerăm că nu vor intra site-urile de internet, televiziunile, posturile de radio care furnizează conținut. Însă, prin interpretarea expresiei „*fără a include serviciile prin care se furnizează conținutul informației transmise prin intermediul rețelelor ori serviciilor de comunicații electronice*", apreciem că vor fi excluse și serviciile de comunicații prin internet, deoarece persoanele care furnizează astfel de servicii transmit conținutul informației prin intermediul rețelelor. Extrapolând, furnizorul de rețele publice de comunicații electronice furnizează echipamentele și infrastructura necesară pentru existența oricărui serviciu, mai apoi furnizorul de servicii de comunicații electronice va furniza și va asigura publicului însăși posibilitatea de a accesa infrastructura amintită, iar, în cele din urmă, *furnizorul de conținut* este cel care oferă un serviciu prin care este furnizat însuși conținutul informației transmise și care face legătura între utilizatori prin rețea. Acești furnizori de conținut pot oferi servicii, precum: e-mail, mesagerie instant sau servicii de voce prin internet.

Este de știut că în ultimii ani se preferă ca aceste tipuri de servicii să folosească sisteme de criptare care permit criptarea directă a informației între utilizatori, prin chei de criptare la care nu are acces serverul furnizorului. Exemple de astfel de servicii sunt cele de mesagerie/voce/video Whatsapp, Viber, Signal și iMessages. Conform declarațiilor acestor furnizori de servicii, datele stocate în server sunt criptate și nu pot fi decriptate decât de utilizatori pe baza unor chei de criptare specializate. În mod evident, algoritmii de criptare pot fi realizați în așa mod încât să permită o decriptare și de către furnizor, însă acest lucru nu se poate determina, deoarece majoritatea furnizorilor nu își divulgă algoritmul de criptare (din motive de securitate și pentru a nu divulga faptul că au o posibilitate reală de a decripta mesaje). Un exemplu bun este serviciul iMessages al societății comerciale Apple, care este considerat, în prezent, neinterceptabil[1] dacă este configurat în mod corect[2]. Totodată, modul în care funcționează serviciul este detaliat de către Apple într-un document public, menținut pe site-ul său și actualizat la fiecare versiune de iOS[3]. Conform acestui document[4], iMessages generează la activare două perechi de chei de securitate, fiecare formată dintr-o *cheie privată* și o *cheie publică*, cheile private fiind stocate în memoria terminalului Apple, și cele publice fiind trimise către serverele Apple, unde sunt asociate numărului de telefon sau adresei de e-mail a utilizatorului și numărului APN (Apple Push Notification Service). Una dintre chei se folosește

[1] *N. Weaver*, iPhones, the FBI, and Going Dark, pe *www.lawfareblog.com*

[2] În sensul în care utilizatorul se folosește pe deplin de opțiunile de securitate oferite în mod facil de terminalul Apple și serviciul iMessages.

[3] *www.apple.com/business/docs/iOS_Security_Guide.pdf*

[4] Versiunea iunie 2015.

pentru primirea ori trimiterea mesajelor, iar cealaltă pentru semnarea mesajelor. La momentul trimiterii unui mesaj, se realizează o criptare folosind cheile de criptare publice ale persoanei care primește mesajul și care semnează cu cheia sigură a terminalului folosit. Aceasta înseamnă că orice persoană care are o cheie publică a unui terminal poate trimite un mesaj, dar acest mesaj poate fi vizualizat numai de terminalul ce deține cheia de decriptare specifică. Totodată, la trimiterea mesajului, acesta se criptează cu cheia privată a terminalului pentru a asigura autenticitate (numai cu o cheie privată putându-se cripta/semna), iar, la primire, partea care constituie semnătura persoanei care trimite este decriptată folosindu-se de cheia publică a terminalului care a expediat mesajul. În așa fel se realizează o criptare *end-to-end*.

Este de remarcat faptul că, de multe ori, furnizorul de rețele publice de comunicații este și furnizor de servicii de comunicații. În esență, distincția dintre un **furnizor de rețele publice de comunicații electronice** și un **furnizor de servicii de comunicații electronice destinate publicului** stă în existența sau nu a unei infrastructuri rețelistice și a tipului de serviciu pe care acesta îl oferă. În cazul unui furnizor de rețele publice de comunicații, legea se referă la o persoană care deține o infrastructură electronică interconectată (o rețea) și care oferă acces la această rețea, fără a pune la dispoziție serviciile specifice. O astfel de persoană este cea care deține și operează o rețea și distribuie serviciile unei astfel de rețele.

În schimb, noțiunea de „furnizor de servicii de comunicații destinate publicului" se referă la orice persoană care oferă servicii de comunicații publice fără a avea o rețea, precum servicii de telefonie, internet, televiziune, radio etc.

Un neajuns al terminologiei folosite de Codul de procedură penală este necesitatea ca acești furnizori să fie autorizați prin lege pentru *rețele publice*. În măsura în care un furnizor de servicii de comunicații nu furnizează servicii de comunicații publice, ci private, el nu va intra sub incidența prevederilor Codului de procedură penală.

Un alt neajuns este faptul că, în opinia noastră, este respectat numai primul sens al noțiunii de „furnizor de servicii", astfel cum acesta este prevăzut de Convenția de la Budapesta. Al doilea sens, care, așa cum am arătat, consideră drept furnizor de servicii „*orice altă persoană fizică sau juridică ce prelucrează sau stochează date personale pentru persoanele prevăzute la punctul 1 și pentru utilizatorii serviciilor oferite de acestea*" nu este prevăzut de legea procesuală penală. Apreciem că această persoană, care este distinctă de cele prevăzute de O.U.G. nr. 111/2011 și de Codul de procedură penală, nu cade sub incidența legii.

Din punctul de vedere al metodei de supraveghere tehnică a accesului la un sistem informatic, considerăm că se impune aplicarea sensului de „furnizor de servicii", prevăzut de Legea nr. 161/2003, având în vedere caracterul restrictiv al termenilor folosiți de art. 154 C.pr. pen. Totodată, opinăm că poate fi interpretată ca voință a legiuitorului crearea unei restrângeri a aplicabilității termenului de „furnizor de servicii" numai la acei furnizori de servicii publice de comunicații.

Capitolul II
Autorizarea accesului la un sistem informatic

Secțiunea 1. Condițiile legale pentru autorizarea accesului la un sistem informatic

Accesul la un sistem informatic, asemenea celorlalte metode de supraveghere tehnică, presupune restrângerea drepturilor și libertăților persoanei vizate de acest procedeu probatoriu, motiv pentru care se impune folosirea sa numai în situații prevăzute expres de lege și cu garantarea respectării proporționalității între interesul public și interesul persoanei.

Necesitatea încuviințării procedeului probatoriu servește un dublu scop, cel de a conferi organelor de urmărire penală puteri sporite în activitatea de administrare a probelor și cel de a garanta legalitatea administrării probei. Deoarece accesul la un sistem informatic constituie o măsură de supraveghere tehnică care îngrădește drepturile persoanei care fac obiectul procedeului probatoriu, pot fi incidente dispozițiile art. 360 C.pen. privind infracțiunea de *acces ilegal la un sistem informatic*, autorizarea judecătorului de drepturi și libertăți servind drept *cauză justificativă*, în sensul prevederilor art. 21 C.pen. Mandatul judecătorului va constitui o *autorizare oficială*[1] pentru exercitarea dreptului de a proceda la accesul la un sistem informatic.

Trebuie menționat că accesul la un sistem informatic nu va întruni, în toate cazurile, elementele de tipicitate ale infracțiunii arătate mai sus, existând situații în care sistemul informatic accesat va fi public, însă, raportat la dispozițiile art. 138 alin. (3) C.pr.pen. care nu disting între sisteme informatice publice și private, considerăm că este necesară această măsură de supraveghere tehnică și în situația în care sistemul informatic este public. Într-o atare situație, va fi incident numai cel de-al doilea scop al autorizării supravegherii tehnice: garantarea legalității administrării probei. Un exemplu de sistem informatic public este „rețeaua de socializare" Facebook, în care utilizatorii pot publica pe internet poze, păreri și alte elemente personale, cu scopul ca acestea să fie vizualizate de către alți utilizatori. Prin intermediul acestui sistem informatic, pot fi săvârșite o multitudine de infracțiuni, astfel că se impune supravegherea tehnică a acestuia prin accesarea informațiilor relevante din punct de vedere penal sau care pot duce la prevenirea săvârșirii de infracțiuni sau la tragerea la răspundere penală a făptuitorilor[2]. Deoarece se realizează o monitorizare a acțiunilor pe care le desfășoară în mod public acea persoană, precum și analizarea acțiunilor trecute ale acelei persoane pe rețeaua Facebook, această situație este asemănătoare cu celelalte mijloace de supraveghere tehnică prevăzute de Codul de procedură penală. În același timp, dată fiind natura măsurii și a datelor informatice, este insuficient pentru asigurarea legalității probei o simplă tipărire a unor capturi de ecran cu cele constatate pe această rețea de socializare, deoarece nu este garantată integritatea datelor informatice obținute, ele fiind redate sub formă de suport tipărit, pierzându-și orice valoare de date informatice.

[1] *Fl. Streteanu*, op. cit., p. 543.

[2] *E.M. Egawhary*, The Surveillance Dimensions of the Use of Social Media by UK Police Forces, în Surveillance & Society, vol. 17, no. 1/2019, pp. 92-93.

De lege ferenda, considerăm că se impune a se face distincția între un sistem informatic accesibil publicului și unul neaccesibil publicului. Într-o asemenea situație, nu putem vorbi despre restrângerea dreptului la viață al persoanei atât timp cât datele informatice sunt publice. În acest sens, chiar și un acces la un sistem informatic transfrontalier este permis, conform art. 32 lit. a) din Convenția de la Budapesta privind criminalitatea informatică. Cu toate acestea, procedeul probatoriu va rămâne o tehnică specială de investigare, întrucât va avea un caracter secret.

Organul competent să dispună asupra folosirii măsurilor de supraveghere tehnică și, în consecință, și asupra accesului la un sistem informatic, este *judecătorul de drepturi și libertăți*, ca regulă. În mod excepțional, *procurorul,* potrivit art. 141 C.pr.pen., va putea dispune limitat, pentru o durată de maximum 48 de ore și cu controlul ulterior al judecătorului de drepturi și libertăți, efectuarea supravegherii tehnice în oricare dintre modalitățile prevăzute de lege.

Măsurile de supraveghere tehnică pot fi dispuse numai atunci când sunt îndeplinite mai multe condiții cumulative, unele prevăzute în cuprinsul art. 139 alin. (1) C.pr.pen. Mai înainte de orice condiție prevăzută expres de lege, este necesar să fi fost începută urmărirea penală pentru o faptă prevăzută de legea penală. Această condiție reiese din faptul că începerea urmăririi penale este actul procesual care creează întreg cadrul pentru desfășurarea activităților de urmărire penală, inclusiv administrarea probelor, supravegherea tehnică fiind un procedeu probatoriu. Cu toate acestea, prima condiție a art. 139 alin. (1) este cea a existenței unei *suspiciuni rezonabile cu privire la pregătirea sau săvârșirea unei infracțiuni* dintre cele prevăzute de art. 139 alin. (2) C.pr.pen., astfel că este posibilă folosirea supravegherii tehnice și într-o anchetă *proactivă*, având ca scop prevenirea săvârșirii unor infracțiuni grave. Nu în ultimul rând, accesul la un sistem informatic, ca orice altă măsură de supraveghere tehnică, poate fi dispus numai în cursul urmăririi penale, nu și în celelalte faze ale procesului penal.

Referitor la infracțiunile care pot atrage utilizarea supravegherii tehnice, legiuitorul a prevăzut o listă exhaustivă de asemenea infracțiuni, nominalizându-le în cuprinsul art. 139 alin. (2) C.pr.pen., la care am făcut referire într-o secțiune anterioară[1]. Remarcăm faptul că legiuitorul a inclus în cuprinsul acestei liste și „infracțiunile care se săvârșesc prin sisteme informatice sau mijloace de comunicații electronice", astfel că gravitatea infracțiunii care poate atrage folosirea supravegherii tehnice nu este corelată în mod necesar cu limitele de pedeapsă și cu valoarea socială ocrotită, ci și cu *mijlocul de săvârșire*. Însă nu vom interpreta aceste dispoziții în sensul elementului laturii obiective *mijlocului* (instrumentului) de săvârșire a infracțiunii, deoarece textul art. 139 alin. (2) C.pr.pen. se referă la *infracțiuni care se săvârșesc*, și nu la infracțiuni săvârșite. Distincția este importantă, deoarece sensul presupune o condiție *a priori* față de săvârșirea unei infracțiuni, sugerând că mijlocul constituie un element constitutiv al respectivei infracțiuni, limitându-se sfera de aplicare a supravegherii tehnice numai la anumite infracțiuni. Astfel, nu este suficient ca infracțiunea să fie *in concreto* săvârșită prin sisteme informatice sau mijloace de comunicații electronice, ci este necesar ca această împrejurare să fie un element de tipicitate al infracțiunii. În mod corect a arătat și literatura de specialitate în același sens, cu privire la Codul de procedură penală anterior[2], că prevederea se referea la infracțiuni care au ca specific comiterea acestora prin mijloace de comunicare electronică.

În contextul supravegherii tehnice prin acces la un sistem informatic, considerăm că această prevedere este una necesară, deoarece, în cazul săvârșirii unei infracțiuni prin intermediul

[1] *V. supra*, Titlul III, Capitolul I.2.

[2] *Gh. Mateuț*, Tratat, vol. II, 2012, pp. 225-226.

unui sistem informatic, probele care pot fi administrate sunt deseori limitate la cele în legătură cu accesarea unui sistem informatic ori obținerea unor date informatice. *De lege ferenda*, se impune completarea situațiilor în care se poate dispune accesul la un sistem informatic cu situația în care *mijlocul săvârșirii infracțiunii este in concreto un sistem informatic*, însă această condiție ar trebui să fie prevăzută ca o condiție specifică doar acestei măsuri de supraveghere tehnice. După cum am mai spus în cuprinsul lucrării, credem că se impune restructurarea metodelor speciale de supraveghere sau cercetare, fiecare trebuind să aibă condiții speciale de autorizare, însă procedura de autorizare să fie unitară.

Legiuitorul a reglementat și un criteriu subsidiar și general privitor la pedeapsă pentru a include orice infracțiune care ar fi de o anumită gravitate în sfera celor care pot justifica, sub aspectul criteriului de gravitate, dispunerea supravegherii tehnice. Prin teza ultimă a art. 139 alin. (2) C.pr.pen., supravegherea tehnică se poate dispune și *în cazul altor infracțiuni pentru care legea prevede pedeapsa închisorii de 5 ani sau mai mare*. Această prevedere a fost criticată deja în prezenta lucrare ca fiind mult prea largă pentru a proteja împotriva unei ingerințe excesive în viața privată a unei persoane.

O a doua condiție care se impune a fi îndeplinită este cea privitoare la *proporționalitatea măsurii cu restrângerea drepturilor și libertăților fundamentale*. Această condiție este prevăzută de art. 139 alin. (1) lit. b) C.pr.pen. și se impune a fi analizată de judecătorul de drepturi și libertăți prin prisma criteriilor prevăzute de textul de lege: *particularitățile cauzei*, *importanța informațiilor ori a probelor ce urmează a fi obținute sau gravitatea infracțiunii*.

Proporționalitatea trebuie analizată atât raportat la supravegherea tehnică în întregime, cât și cu privire la măsurile concrete de supraveghere tehnică ce sunt solicitate prin cerere de către procuror. Accesul la un sistem informatic nu va fi proporțional în situația în care o persoană este urmărită penal pentru reproducerea de programe informatice fără drept, în condițiile în care un alt procedeu probatoriu, percheziția informatică, ar fi suficient și proporțional pentru stabilirea stării de fapt. Întrucât problema proporționalității a fost deja analizată în detaliu, facem trimitere la secțiunea dedicată acestei probleme[1].

A treia condiție impusă de Codul de procedură penală pentru dispunerea supravegherii tehnice este *necesitatea procedeului probatoriu* pentru obținerea probei. Cu alte cuvinte, condiția se referă la *subsidiaritatea*[2] măsurilor de supraveghere tehnică față de orice alt procedeu probatoriu. Această condiție este prevăzută în cuprinsul art. 139 alin. (1) lit. c) C.pr.pen. și limitează folosirea mijloacelor de supraveghere tehnică, cu excepția cazurilor în care *probele nu ar putea fi obținute în alt mod sau obținerea lor ar presupune dificultăți deosebite ce ar prejudicia ancheta ori există un pericol pentru siguranța persoanelor sau a unor bunuri de valoare*. Întrucât această condiție a fost deja analizată în prezenta lucrare, facem trimitere la secțiunea dedicată acesteia[3].

[1] *V. supra*, Titlul III, Capitolul I.3.

[2] *Gh. Mateuț*, Observații critice privind noua reglementare a supravegherii tehnice într-o prezentare comparativă, în Caiete de Drept Penal nr. 3/2015, p. 24.

[3] *V. supra,* Titlul III, Capitolul I.4.

Secțiunea a 2-a. Autorizarea accesului la un sistem informatic de către judecătorul de drepturi și libertăți

Precum în cazul tuturor măsurilor de supraveghere tehnică, pentru a se dispune accesul la un sistem informatic, este necesar ca procurorul să întocmească o propunere, în care să fie cuprinse toate elementele legale prevăzute de art. 140 alin. (2) C.pr.pen., pe care să o transmită judecătorului de drepturi și libertăți. Pentru autorizarea măsurii, competența revine judecătorului de drepturi și libertăți din cadrul instanței competente să judece cauza în primă instanță sau din cadrul instanței corespunzătoare în grad acesteia în a cărei circumscripție se află sediul parchetului din care face parte procurorul care a formulat cererea.

În privința dispunerii supravegherii tehnice de către *judecătorul de drepturi și libertăți*, procedura este prevăzută de art. 140 C.pr.pen. și impune, mai întâi, verificarea de către judecătorul de drepturi și libertăți a respectării condițiilor prevăzute de art. 139 C.pr.pen.

Această verificare se face pe baza cererii depuse de către procuror și în urma verificării dosarului cauzei, care va fi înaintat de către procuror împreună cu propunerea prin care solicită să se dispună supravegherea tehnică. În cuprinsul acesteia, procurorul trebuie să includă toate elementele prevăzute de art. 140 alin. (2) C.pr.pen.[1]. Întrucât prin accesul la un sistem informatic pot fi aflate deosebit de multe elemente din viața privată a unei persoane, chiar mai multe decât în cazul altor măsuri de supraveghere tehnică, se impune un control strict de proporționalitate din partea judecătorului de drepturi și libertăți. Viața omului modern se desfășoară nu numai în spațiul real, ci și în cel virtual, unde, pe baza dispozitivelor deținute, se va putea manifesta liber, crezând că nu este urmărit sau că activitățile sale nu pot fi depistate. Realitatea este departe de aceasta, probele care pot fi obținute prin accesul la un sistem informatic putând fi mai fidele decât oricare altele cu privire la obiceiurile persoanei, prietenii acesteia, conversațiile purtate, locațiile frecventate, preferințele sale în domeniul vestimentar, tehnologic, politic, sexual etc. Mai ales activitățile sale trecute vor fi relevate, inclusiv cele pe care le face din curiozitate, fiind integrate, în contextul urmăririi penale, ca probe (de pildă, căutări de amuzament referitoare la diferite tipuri de droguri pot releva un interes aparte al persoanei față de consumul de droguri, element util urmăririi penale în unele situații).

Procurorul va trebui să demonstreze temeiurile care impun accesul la un sistem informatic, respectiv probele ce s-ar putea obține prin această măsură, precum și motivul pentru care un procedeu probatoriu clasic sau o altă măsură de supraveghere tehnică mai puțin invazivă nu ar fi adecvate.

Judecarea cererii formulate de procuror are loc în aceeași zi cu formularea ei, în camera de consiliu, fără citarea părților și cu prezența obligatorie a procurorului. Soluțiile pe care le poate pronunța judecătorul de drepturi și libertăți sunt fie respingerea cererii, fie admiterea ei.

După admiterea propunerii procurorului de utilizare a metodelor de supraveghere tehnică, judecătorul de drepturi și libertăți emite, conform art. 140 alin. (5) C.pr.pen., *mandatul de*

[1] Conform acestui articol, cererea trebuie să cuprindă: „indicarea măsurilor de supraveghere tehnică care se solicită a fi dispuse, numele sau alte date de identificare a persoanei împotriva căreia se dispune măsura, dacă sunt cunoscute, indicarea probelor ori a datelor din care rezultă suspiciunea rezonabilă cu privire la săvârșirea unei infracțiuni pentru care se poate dispune măsura, indicarea faptei și a încadrării juridice, iar, în cazul măsurii supravegherii video, audio sau prin fotografiere, dacă se solicită și încuviințarea ca organele de urmărire penală să pătrundă în spații private indicate pentru a activa sau a dezactiva mijloacele tehnice ce urmează a fi folosite pentru executarea măsurii supravegherii tehnice, motivarea caracterului proporțional și subsidiar al măsurii".

supraveghere tehnică, acesta trebuind să cuprindă mai multe elemente prevăzute expres de Cod. Aceste elemente sunt cele care trebuie cuprinse și în încheierea de admitere a cererii, motiv pentru care le vom aborda unitar. Deoarece *accesul la un sistem informatic* este o metodă de supraveghere tehnică, și în cazul autorizării folosirii acestei metode, mandatul va trebui să conțină aceleași elemente comune, precum și un element specific – *punctul de acces la sistemul informatic*.

Elementele comune care nu pun probleme deosebite sunt cele privind *denumirea instanței*, *data, ora și locul emiterii*, *numele, prenumele* și *calitatea persoanei care a dat încheierea și a emis mandatul*, *semnătura judecătorului și ștampila instanței*. Considerăm că nu era necesar ca mențiunea privind locul emiterii mandatului de supraveghere tehnică să mai fie prevăzută expres de către legiuitor, deoarece, fiind vorba despre un judecător de drepturi și libertăți, se subînțelege faptul că acesta își va desfășura activitatea numai la sediul instanței, iar judecarea cererii se va face în *cameră de consiliu*, cu prezența procurorului, nefiind permisă emiterea mandatului de supraveghere tehnică, decât odată cu soluționarea cererii procurorului. În schimb, ora emiterii mandatului de supraveghere tehnică, alături de dată, prezintă semnificație deosebită, deoarece de la acel moment curge obligativitatea procurorului de a pune în executare mandatul de supraveghere tehnică. Un alt element comun care nu ridică probleme este perioada pentru care se dispun măsurile de supraveghere tehnică, aceasta putând fi de maxim 30 de zile.

Alături de acestea, în cuprinsul art. 140 alin. (5) lit. e) teza a II-a C.pr.pen., legiuitorul a prevăzut că este obligatorie menționarea *scopului* pentru care s-a încuviințat măsura. În opinia noastră, aceste element este inutil în cuprinsul unui mandat de supraveghere tehnică, deoarece, fiind vorba de un procedeu probatoriu, scopul măsurilor de supraveghere tehnică este subînțeles, la fel ca în cazul oricărui procedeu probatoriu. Acest zel al legiuitorului de a prevedea elementul scop în cuprinsul mandatului de supraveghere tehnică este neînțeles atât timp cât nici procurorului nu îi este cerut să prevadă în cuprinsul cererii formulate, conform art. 140 alin. (2) C.pr.pen., scopul pentru care solicită încuviințarea utilizării supravegherii tehnice.

Metoda de supraveghere tehnică a accesului la un sistem informatic cunoaște anumite particularități în privința conținutului mandatului de supraveghere tehnică, care provin din aspectele tehnice specifice ale măsurii.

Conform art. 140 alin. (5) lit. d) C.pr.pen., încuviințarea măsurii concret încuviințate trebuie să indice nu numai faptul că se încuviințează accesul la un sistem informatic, dar trebuie indicate și operațiunile specifice care pot fi executate – pătrunderea pe un suport de stocare anterior predat, pătrunderea într-un sistem informatic aflat la distanță[1], instalarea de programe informatice pentru monitorizarea acțiunilor utilizatorului[2], copierea la distanță a unor date informatice[3], precum și ștergerea unor date informatice[4] etc. Apreciem că vor trebui

[1] În această situație va trebui determinat precis sistemul informatic la distanță fie prin anumite trăsături constructive (adresă MAC, configurație), fie prin trăsături atribuite (precum adresa IP) sau să se permită ca sistemul să fie determinabil în concret de către organul de urmărire penală pe bază de adresă de domeniu. În cazul în care sistemul informatic este doar determinabil, este important ca judecătorul de drepturi și libertăți să introducă criterii care să identifice suficient de precis sistemul informatic, fără a se permite procurorului să acceseze orice sistem informatic.

[2] Keyloggere, programe care transmit în timp real capturi de ecran etc.

[3] *S. McBrearty, N. McKelvey, K. Curran*, Legal, Ethical and Social Issues in the case of an Intrusive Remote Monitoring Software, în International Journal of Information and Network Security (IJINS), vol. 1, no. 4/2012, p. 331.

[4] Credem că această operațiune poate fi admisă numai în măsura în care datele informatice, prin însăși existența lor, pun în pericol o valoare socială ocrotită de legea penală. Un exemplu în acest sens îl reprezintă

menționate și datele informatice care sunt căutate, astfel încât mandatul să limiteze ingerința adusă dreptului la viață privată a persoanei[1]. Nu vor putea fi folosite ca probe acele date informatice care excedează mandatul de supraveghere tehnică, decât dacă deținerea acestora ar constitui infracțiune, și aceasta s-ar încadra între cele menționate în cuprinsul art. 139 alin. (2) C.pr.pen.

Un alt element care trebuie să se regăsească în cuprinsul mandatului de supraveghere tehnică este numele persoanei supuse măsurii, dacă acesta este cunoscut. În situația accesului la un sistem informatic, considerăm că persoana supusă accesului va fi proprietarul atât al sistemului informatic ori al suportului de stocare, cât și proprietarul datelor informatice. Dacă se urmărește accesul la un sistem informatic asupra unui sistem informatic al unei persoane, însă datele informatice aparțin altei persoane, considerăm că ambele persoane vor trebui menționate în cuprinsul mandatului de supraveghere tehnică, precizându-se în mod clar care este calitatea acestora față de datele informatice. De exemplu, dacă se realizează o copie a datelor informatice care se predau procurorului, în temeiul art. 170 alin. (2) lit. a) C.pr.pen., de către o terță persoană, suportul de stocare va aparține statului, însă datele informatice vor fi ale unei alte persoane, impunându-se menționarea numelui acesteia, dacă este cunoscut, în cuprinsul mandatului de supraveghere tehnică.

Un aspect specific al accesului la un sistem informatic este elementul indicării *punctului de acces la sistemul informatic* în cuprinsul mandatului de supraveghere tehnică, potrivit art. 140 alin. (5) lit. g) C.pr.pen. Deși nu există o definiție legală pentru termenul de „punct de acces la un sistem informatic", considerăm că o astfel de definiție se poate deduce prin paralela cu echipamentele de rețea denumite „routere", care sunt puncte de acces la o rețea și care permit trecerea dintr-un sistem informatic într-un alt sistem informatic (de exemplu, din rețeaua locală în internet și invers). Astfel, vom vorbi de *puncte de acces* numai în situațiile în care se va efectua un acces la un sistem informatic *de la distanță*, și nu un *acces direct*, prin utilizarea, ca punct de acces la sistemul țintă, a unui alt sistem informatic. De exemplu, punct de acces va fi și sistemul informatic utilizat de procuror pentru a accesa un site, dar și un computer PC dintr-o rețea locală prin care se va accesa sistemul informatic țintă[2]. Definiția „punctului de acces", în accepțiunea noastră, este *orice sistem informatic prin mijlocirea căruia se poate realiza accesul la un alt sistem informatic la distanță*.

Un argument în sprijinul acestei definiții sunt prevederile art. 143 alin. (4) C.pr.pen.[3], care fac distincție între datele de identificare ale unui sistem informatic și ale unui punct de acces. Astfel, în accepțiunea legiuitorului, **sistemul informatic** este sistemul-țintă, iar **punctul de acces** este doar un sistem-mijloc prin intermediul căruia se ajunge la sistemul-țintă.

---

materialele pornografice cu minori, care se impun a fi copiate în condiții în care se poate asigura autenticitatea și integritatea datelor copiate, iar mai apoi datele informatice să fie șterse, în situația în care acestea sunt accesibile publicului.

[1] *O.S. Kerr*, op. cit., p. 299.

[2] Există situații în care unele computere din rețea nu au acces la internet, ci numai la rețeaua internă, însă este posibilă folosirea unui sistem informatic, care are legătură la internet, drept punct de acces pentru sistemul țintă, deoarece acestea vor fi în aceeași rețea locală și vor putea comunica liber între ele.

[3] Conform art. 143 alin. (4) C.pr.pen.: „Convorbirile, comunicările sau conversațiile interceptate și înregistrate, care privesc fapta ce formează obiectul cercetării ori contribuie la identificarea ori localizarea persoanelor, sunt redate de către procuror sau organul de cercetare penală într-un proces-verbal în care se menționează mandatul emis pentru efectuarea acestora, numerele posturilor telefonice, datele de identificare ale sistemelor informatice ori ale punctelor de acces, numele persoanelor ce au efectuat comunicările, dacă sunt cunoscute, data și ora fiecărei convorbiri sau comunicări. Procesul-verbal este certificat pentru autenticitate de către procuror".

Considerăm că identificarea punctului de acces este obligatorie, deoarece este necesară pătrunderea și în acest sistem informatic, chiar și pentru a obține acces la sistemul țintă, astfel că judecătorul de drepturi și libertăți va trebui să se pronunțe asupra autorizării accesului la punctul de acces în vederea protejării dreptului la viață privată al persoanei care deține punctul de acces. Nu va fi necesar ca punctul de acces să fie menționat în cuprinsul mandatului de supraveghere tehnică dacă acesta este un sistem informatic aparținând organelor care pun în executare măsura accesului la un sistem informatic.

Una dintre prevederile art. 140 alin. (5) C.pr.pen. care s-ar fi impus să fie aplicabilă în cazul accesului la un sistem informatic este cea privind *supravegherea video, audio sau prin fotografiere în spații private*, prin care se permite organelor de urmărire penală să pătrundă în spații private pentru a activa sau dezactiva mijloacele tehnice ce urmează a fi folosite pentru executarea măsurii de supraveghere tehnică. În concret, accesul la un sistem informatic poate avea caracter continuu, prin monitorizarea operațiunilor efectuate de persoana față de care s-a dispus accesul la un sistem informatic, altele decât comunicațiile acesteia[1], putând fi necesar accesul nemijlocit la sistemul informatic care se dorește accesat în mod continuu în vederea instalării unor programe informatice care să transmită la distanță date informatice[2]. *De lege ferenda*, considerăm că se impune a se prevedea această posibilitate și în cazul accesului la un sistem informatic pentru a putea permite eludarea sistemelor de securitate de bază ale sistemului informatic care face obiectul măsurii[3].

Secțiunea a 3-a. Autorizarea provizorie a accesului la un sistem informatic de către procuror

În mod excepțional și cu controlul ulterior al judecătorului de drepturi și libertăți, Codul de procedură penală permite procurorului să autorizeze temporar, pentru o perioadă care nu poate depăși 48 de ore, folosirea oricăror mijloace de supraveghere tehnică, inclusiv accesul la un sistem informatic. Întrucât am tratat pe larg problema autorizării provizorii de către procuror într-o secțiune anterioară[4], facem trimitere la aceasta, urmând ca în prezenta parte a lucrării să detaliem unele particularități în cazul supravegherii tehnice prin acces la un sistem informatic.

Deși credem că autorizarea măsurii de către procuror ar trebui eliminată, în cazul infracțiunilor comise prin sisteme informatice, poate fi utilă o reacție rapidă prin acces la un sistem informatic, putând fi aplicabil cazul pierderii, alterării sau distrugerii probelor ca o condiție particulară de autorizare. De pildă, există date din care rezultă că făptuitorul va încerca

[1] De exemplu, documentele sau fișierele pe care le accesează, fișierele pe care le creează, parolele pe care le folosește să acceseze unele site-uri etc.

[2] În cazul unor sisteme moderne, poate fi deosebit de greu să se obțină accesul la sistemul informatic fără a fi dezactivate mijloacele de securitate interne ale sistemului de operare. De multe ori, cea mai simplă metodă de a le depăși este de a instala programe direct pe sistemul informatic, prin inserarea în memorie a unor programe, atunci când sistemul de operare nu este pornit. Un exemplu în acest sens este crearea unui utilizator adițional cu care să se realizeze mai apoi accesul la distanță.

[3] Acestea pot fi eludate cel mai bine prin programe care se vor rula în momentul pornirii sistemului informatic, fiind instalate pe un suport extern (stick USB/suport optic), și vor modifica parolele de acces ale sistemului în măsura în care nu este criptat.

[4] *V. supra*, Titlul III, Capitolul II.3.

să își ascundă urmele prin ștergerea datelor informatice din anumite sisteme informatice, precum site-urile de pornografie infantilă[1]. Pentru a preîntâmpina acest lucru, este necesar a se realiza un acces la sistemul informatic și a se copia toate datele necesare soluționării cauzei mai înainte de a fi șterse. Neajunsul acestei situații stă în rapiditatea deosebită prin care ar putea avea loc acțiunea infractorului, făcând puțin fezabil ca și printr-o ordonanță de autorizare provizorie să se poată obține probe.

Pentru autorizarea de către procuror a accesului la un sistem informatic pentru o perioadă de 48 de ore, Codul de procedură penală cuprinde o serie de prevederi exprese, care nu se regăsesc în cazul *accesului la un sistem informatic* dispus prin procedura obișnuită. Conform art. 141 alin. (5) C.pr.pen., se arată că procurorul *poate* dispune prin ordonanță *realizarea și conservarea unei copii a acestor date informatice* și *suprimarea accesării sau îndepărtarea acestor date informatice din sistemul informatic*. În același timp, se arată că toate copiile se vor realiza cu mijloace tehnice și proceduri adecvate de natură să asigure integritatea informațiilor conținute de acestea. Considerăm că intercalarea acestui text de lege între dispozițiile privind infirmarea și confirmarea supravegherii tehnice poate conduce la confuzii cu privire la momentul în care procurorul poate să exercite acțiunile arătate.

Realizarea și conservarea unei copii a datelor informatice accesate se poate face numai în momentul în care se efectuează accesul la un sistem informatic, nu și la un moment ulterior, indiferent de soluția pe care o va da judecătorul de drepturi și libertăți asupra confirmării autorizării măsurii. În opinia noastră, procurorul este obligat să dispună conservarea datelor informatice în toate cazurile în care acestea constituie probe pertinente concludente și utile cauzei, deoarece accesul la un sistem informatic presupune fixarea datelor informatice obținute pe suporți de stocare în cazul în care au legătură cu cauza. În măsura în care, la momentul accesului, nu se face acest lucru, datele informatice pot fi pierdute definitiv chiar și dacă s-ar mai încerca încă o dată accesarea lor. Este importantă mențiunea privind asigurarea integrității datelor obținute în urma accesului, deoarece indică o trăsătură importantă a accesului la un sistem informatic: nevoia de a menține integritatea datelor obținute din sistemul informatic, și nu a celor conținute în continuare de acest sistem. Aceasta este o deosebire față de percheziția informatică, unde datele obținute sunt copii exacte ale datelor de pe sistemul informatic accesate fără modificarea datelor din sistemul țintă. În schimb, în cazul accesului la un sistem informatic, nu se pretinde ca integritatea datelor din sistemul informatic să fie menținută (datele putând fi și distruse, așa cum vom arăta mai jos), ci este necesar doar ca datele copiate să își mențină integritatea. Cu toate acestea, se impune a fi folosite metode care să mențină cât mai bine integritatea datelor și în momentul copierii. De exemplu, există metode de copiere cu sistemul de operare pornit care permit transferarea fără modificare a atributelor fișierelor – data creării, data ultimei modificări, data ultimei accesări etc. În sensul păstrării integrității datelor informatice rezultate din supravegherea tehnică prin acces la un sistem informatic, legiuitorul a prevăzut în cuprinsul art. 142[1] C.pr.pen. posibilitatea utilizării unei semnături digitale extinse.

Suprimarea accesării sau îndepărtarea datelor informatice sunt două operațiuni distincte la care poate apela procurorul pentru a nu mai permite accesarea (*largo sensu*) datelor de către public ori de către persoana față de care s-a dispus măsura. Prin „suprimarea accesării" se înțelege orice operațiune care blochează accesul la datele informatice, fără a le distruge.

[1] Uneori, acestea își schimbă locația, pagina de internet sau doar serverul (inclusiv adresa IP) o dată pe oră sau de mai multe ori pe zi.

Metodele concrete sunt variate, dar un bun mijloc de a suprima accesarea este deconectarea sistemului informatic de la rețea ori criptarea datelor cu un algoritm și o parolă cunoscută numai de procuror. Prin „îndepărtarea datelor" vom înțelege operațiunea prin care datele sunt distruse, șterse de pe suportul de stocare pe care se află sau de pe sistemul informatic. Operațiunea este de bază pentru orice utilizator de sistem informatic, însă, nu de puține ori, ștergerea unor date informatice nu este definitivă. Considerăm că trebuie folosite procedee care să asigure ștergerea definitivă a datelor informatice (distrugerea fizică a mediului de stocare, suprascrierea unui hard-disk de mai multe ori cu informație aleatorie etc.), însă, uneori, însuși dispozitivul de stocare permite ștergerea definitivă a datelor ca operațiune comună[1]. Atât suprimarea accesării, cât și îndepărtarea datelor sunt operațiuni care trebuie întrebuințate atunci când însăși existența datelor informatice reprezintă un pericol social, însă se va impune copierea acestora mai înainte. De exemplu, se va impune luarea acestor măsuri în cazul în care se accesează un *server* care distribuie public materiale pornografice cu minori, astfel că oprirea „serviciului" impune fie suprimarea accesării (prin blocarea rețelei, întreruperea conexiunii cu DNS-ul etc.), fie îndepărtarea datelor prin ștergere, astfel încât acest server și datele informatice să nu mai poată fi accesate de către nicio persoană din acel moment. Aceste operațiuni constituie o aplicare a dispozițiilor Convenției de la Budapesta privind criminalitatea informatică, în care se prevede, în cuprinsul art. 19 alin. (3) lit. d), că statele semnatare se obligă să adopte instrumente legale care să permită suprimarea accesării datelor informatice sau îndepărtarea acestora din sistemul informatic.

[1] Solid-state drive-urile utilizează memorie flash NAND care nu presupune stocarea magnetică a datelor, astfel că operațiunea de ștergere comun utilizată de orice sistem de operare va duce la îndepărtarea definitivă a datelor, ca urmare a specificului tehnologiei de stocare.

Capitolul III
Punerea în executare a accesului la un sistem informatic

Secțiunea 1. Organele competente să pună în executare accesul la un sistem informatic

Ulterior emiterii mandatului de supraveghere tehnică la care am făcut referire în secțiunea precedentă, este admisă folosirea mijlocului de supraveghere tehnică al accesului la un sistem informatic de către organele de urmărire penală. Alături de competența de încuviințare a mijlocului de supraveghere tehnică, considerăm că se impune a se determina persoanele care vor efectua în mod concret activitatea specific-concretă pe care o implică accesul la un sistem informatic.

Regulile privind efectuarea accesului la un sistem informatic sunt identice ca în cazul celorlalte metode de supraveghere tehnică, fiind prevăzute de art. 142 C.pr.pen., sens în care facem trimitere la explicațiile scrise într-o secțiune anterioară[1], urmând ca în prezenta secțiune să detaliem anumite particularități ale punerii în executare a accesului la un sistem informatic.

Dacă, în cazul unor anumite metode de supraveghere tehnică, procurorul are un rol mai puțin pronunțat, considerăm că accesul la un sistem informatic se va putea realiza în practică direct de către procuror, în funcție de dificultatea operațiunilor ce necesită a fi efectuate. Astfel, procurorul va putea el însuși, fără nicio dificultate, să realizeze, de exemplu, un acces la un sistem informatic asupra unor mijloace de stocare optice, fără a fi necesar ajutorul vreunui lucrător specializat. Desigur, acest exemplu este cel mai simplu, deoarece nu se pune problema pierderii integrității datelor[2], însă dovedește faptul că, în cazul accesului la un sistem informatic, însuși procurorul sau organul de cercetare penală pot realiza anumite operațiuni, în limitele cunoștințelor informatice pe care le dețin. În toate cazurile, atunci când procurorul va delega punerea în executare a mandatului de supraveghere tehnică privind accesul la un sistem informatic către un lucrător specializat din cadrul poliției, considerăm că este necesar ca realizarea accesului la un sistem informatic să se realizeze în prezența procurorului ori a organului de cercetare penală, deoarece art. 143 alin. (1) C.pr.pen. prevede doar competența unui organ de urmărire penală în consemnarea activităților de supraveghere tehnică.

Alături de organele arătate mai jos, trebuie să amintim, în cadrul problemei competenței, și dispozițiile art. 142 alin. (2) C.pr.pen., prin care se prevede obligația furnizorilor de rețele publice de comunicații și a furnizorilor de servicii de comunicații electronice sau de orice tip de comunicare ori de servicii financiare de a *colabora cu organele de urmărire penală sau cu autoritățile prevăzute la art. 142 alin. (1) C.pr.pen. în limitele competențelor acestora, pentru punerea în executare a mandatului de supraveghere tehnică*.

---

[1] *V. supra*, Titlul III, Capitolul III.1.

[2] Suporții optici tip CD, DVD, Blu-Ray Disc sunt, prin natura lor, suporți care, odată scriși, nu mai pot fi modificați prin interacțiunea utilizatorului. Ca atare, nu se impune folosirea de dispozitive speciale pentru menținerea integrității datelor, decât minime măsuri de prevenire a deteriorării fizice a suportului optic prin zgâriere sau murdărire.

Persoanele chemate să dea concurs supravegherii tehnice pot fi furnizorii de rețele publice de comunicații electronice, furnizorii de servicii de comunicații electronice destinate publicului, în sensul celor arătate într-o secțiune anterioară[1], un furnizor de servicii financiare ori un furnizor de servicii de comunicare de orice alt tip. În privința ultimului tip de furnizor, acesta ar presupune furnizori de alte servicii de comunicare decât cele electronice.

Raportat la definițiile furnizorilor de rețele publice de comunicații ori furnizorilor de servicii de comunicații electronice destinate publicului, considerăm că vor trebui să colaboreze numai acele persoane care sunt autorizate prin lege să desfășoare activitățile și serviciile respective, iar în cadrul acestora nu vor intra furnizorii de servicii conținut, la care am făcut referire. Deoarece acești furnizori de conținut nu sunt prevăzuți, considerăm că aceștia nu vor avea obligația legală de a colabora cu organele de urmărire penală în privința punerii în executare a unui mandat de supraveghere tehnică. Întrucât accesul la un sistem informatic este un procedeu invaziv pentru furnizorul de conținut și poate perturba furnizarea serviciilor oferite de acesta, se impune ca o eventuală solicitare din partea procurorului de a se face un acces pe înseși sistemele furnizorului să fie refuzată, în vederea protejării drepturilor clienților săi împotriva perturbării serviciilor și pentru a garanta că informațiile conținut ale unor alte persoane decât cea vizată de mandatul de supraveghere tehnică nu sunt divulgate. O atare măsură ar trebui să poată fi contestată ca fiind disproporționată față de scopul urmărit.

Așa cum vom arăta într-o secțiune ulterioară[2], procedeul probatoriu al *predării obiectelor, înscrisurilor sau datelor informatice*, prevăzut de art. 170 C.pr.pen., nu permite organului de urmărire penală să procedeze la accesarea datelor informatice aflate pe mediile de stocare furnizate, pentru aceasta fiind nevoie de încuviințarea judecătorului de drepturi și libertăți de a se proceda la accesul la un sistem informatic sau la realizarea unei percheziții informatice. Însă, în cazul furnizorilor de conținut, considerăm că aceștia vor putea fi obligați să predea datele informatice privind persoana vizată de mandatul de supraveghere tehnică, în măsura în care procurorul va dispune predarea datelor informatice, conform art. 170 C.pr.pen. Într-o asemenea situație, s-ar fi impus aplicarea dispozițiilor art. 170 alin. (5) C.pr.pen.[3] privind predarea unei copii a datelor informatice de către furnizorul de conținut, deoarece remiterea originalului datelor informatice ar obliga și la remiterea suportului de stocare ori a sistemului informatic pe care se află aceste date, iar acest lucru ar aduce prejudicii nejustificate furnizorului de conținut. Așa cum arată și art. 19 pct. 4 din Convenția de la Budapesta[4] privind criminalitatea informatică, statul este ținut să ia măsuri legislative care să permită obligarea persoanelor care dețin date informatice să le predea, în măsura în care acestea sunt necesare și proporționale. Considerăm că va fi o lipsă gravă de proporționalitate atunci când se dispune predarea de către un furnizor de conținut important a unui sistem informatic atât timp cât copia datelor informatice poate fi suficientă, deoarece în acest mod se pot produce daune furnizorului care ar trebui să fie avansate de stat și recuperate mai apoi, fiind cheltuieli judiciare privind administrarea probelor, în sensul art. 272 alin. (1) C.pr.pen.

[1] *V. supra*, Titlul V, Capitolul I.

[2] *V. infra*, Titlul V, Capitolul IV.1.

[3] Acest alineat a fost abrogat prin intrarea în vigoare a O.U.G. nr. 18/2016 (M. Of. nr. 389 din 23 mai 2016).

[4] Conform art. 19 pct. 4 din Convenția de la Budapesta: „Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, **as is reasonable**, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2" (s.n.).

În același timp, oferirea în întregime a sistemului informatic sau a tuturor datelor stocate pe un sistem informatic poate afecta grav drepturile celorlalți utilizatori ai serviciului, ale căror date ar putea fi accesate de către organele de urmărire penală. O situație similară este cea a oferirii parolelor de acces în sistemul informatic. Aceste date și parole de acces nu reprezintă date informatice necesare, în sensul art. 19 pct. 4 din Convenția de la Budapesta, și nu pot face obiectul accesului la un sistem informatic. În situația în care se cer date informatice unui furnizor de conținut, este necesar ca procurorul să determine exact datele informatice, prin indicarea utilizatorului ori a numelui persoanei pentru care se solicită datele informatice. În sprijinul acestui mod de lucru, sunt și dispozițiile art. 170 alin. (6) C.pr.pen., care, deși nu vor fi aplicabile pentru că alineatul antemenționat a fost abrogat, subliniază faptul că predarea unor date informatice secrete sau confidențiale se impune a fi făcută într-un mod în care să se asigure păstrarea secretului ori a confidențialității.

În privința acțiunilor concrete care trebuie să fie realizate de către persoanele arătate în cuprinsul art. 142 alin. (2) C.pr.pen., suntem de părere că acestea, prin administratorii de sisteme informatice, trebuie să acorde tot sprijinul tehnic posibil pentru a se pune în executare mandatul de supraveghere tehnică, realizând o *colaborare efectivă și dinamică*. Prin „colaborare dinamică" ne referim la faptul că persoanele despre care facem vorbire trebuie să colaboreze în mod continuu, și nu doar punctual, fiind insuficient să acorde doar datele de acces la sistem, aceștia trebuind să se asigure că organul de urmărire penală nu va întâmpina dificultăți, având în vedere specificul fiecărui sistem informatic în parte[1]. Sensul dispoziției „în limita competențelor acestora" trebuie interpretat ca referindu-se la furnizorii arătați mai sus, și nu la organele de urmărire penală sau la celelalte organe cărora le poate fi delegată punerea în executare a mandatului de supraveghere tehnică. O interpretare contrară ar duce la ideea că furnizorii de rețele publice de comunicații electronice și furnizorii de servicii de comunicații electronice destinate publicului sau de orice tip de comunicare ori de servicii financiare vor putea ajuta organele desemnate de procuror (ori însuși procurorul) numai în măsura competenței acestor organe de urmărire penală, ceea ce ar implica o formă de control a competenței din partea furnizorilor. În opinia noastră, sensul legal este cel arătat mai devreme, prin „competență" înțelegându-se *posibilitatea concretă a furnizorului de a sprijini organele însărcinate cu punerea în executare a mandatului de supraveghere tehnică, în limita posibilităților și a domeniului de activitate*.

Codul de procedură penală impune tuturor persoanelor care dau concurs tehnic, inclusiv persoanelor prevăzute de art. 142 alin. (2) C.pr.pen., să păstreze secretul operațiunii efectuate, sub sancțiunea legii penale. Această obligație se va extinde și asupra *furnizorilor de conținut*, deoarece și aceștia își vor da concursul spre realizarea unui acces la un sistem informatic, chiar și prin predarea datelor informatice. Prevederea aceasta este una necesară atât pentru a se asigura secretul operațiunilor autorizate, cât și pentru a proteja persoana față de care s-a dispus încuviințarea metodelor de supraveghere tehnică. În măsura în care persoanele în cauză divulgă informații privind realizarea supravegherii tehnice, vor fi întrunite elementele constitutive ale celei de-a doua forme tip a infracțiunii de divulgarea informațiilor secrete de

[1] Administratorii de sistem sunt persoanele care cunosc cel mai bine sistemul informatic, fiind de multe ori și arhitecții acestuia. Ei trebuie să furnizeze toate informațiile necesare organului de urmărire penală și să îl asiste în realizarea accesului la sistemul informatic. În consecință, este preferabilă prezența fizică a administratorului de rețea, alături de procuror ori de către lucrătorul specializat desemnat cu realizarea accesului la sistemul informatic, în momentul accesării sistemului, fără ca administratorul să aibă posibilitatea de a interveni direct.

serviciu sau nepublice, prevăzută de art. 304 alin. (2) C.pen.[1], în cazul în care subiectul activ nu va avea calitatea de funcționar, însă, dacă are această calitate, i se va putea reține infracțiunea de divulgarea secretului profesional, prevăzută de art. 227 alin. (1) C.pen.[2].

Secțiunea a 2-a. Competența teritorială de realizare a accesului la un sistem informatic

Alături de competența în dispunerea folosirii metodei speciale de supraveghere constând în *accesul la un sistem informatic*, se impune a se observa particularitățile competenței teritoriale a realizării accesului. Principala problemă, în cazul accesului la un sistem informatic, este locul în care se află dispozitivul sau dispozitivele vizate de mandatul de supraveghere tehnică.

Așa cum am arătat într-o secțiune precedentă[3], se impune ca judecătorul de drepturi și libertăți să arate, în cuprinsul încheierii prin care dispune accesul la un sistem informatic, conform art. 140 alin. (5) lit. g) C.pr.pen., *punctul de acces la un sistem informatic*.

Considerăm că această mențiune impune o analiză asupra a ceea ce se înțelege prin „punct de acces la un sistem informatic", precum și asupra implicațiilor acestui termen asupra competenței teritoriale de utilizare a mijlocului de supraveghere tehnică.

În opinia noastră, prin „punct de acces la un sistem informatic" înțelegem locul din care se accesează sistemul informatic, fie în sensul în care se accesează în mod direct dispozitivul/grupul de dispozitive care alcătuiesc sistemul informatic. Deoarece accesul la un sistem informatic implică, după caz, accesul direct la dispozitiv ori accesul la distanță asupra unui dispozitiv, *punct de acces la un sistem* va fi fie locația fizică a sistemului informatic, fie locul din care se accesează sistemul de la distanță. În ultimul caz, punctul de acces la un sistem informatic va fi sistemul informatic, folosit pentru a pătrunde în sistemul informatic țintă, putând fi un calculator (*lato sensu*, orice sistem informatic poate fi folosit) care aparține fie unei persoane particulare, fie chiar organului de urmărire ori unui *lucrător specializat*, în conformitate cu art. 142 alin. (1) C.pr.pen.

În toate cazurile, din punct de vedere teritorial, *punctul de acces la un sistem informatic* va fi un dispozitiv aflat pe teritoriul statului român, însă acest lucru nu este valabil și pentru sistemul informatic în care se dispune pătrunderea. Ca atare, survine următoarea problemă de procedură: *este competent organul care execută mandatul de supraveghere să realizeze un acces la un sistem informatic care nu se află pe teritoriul României?*

Răspunsul este unul dificil de găsit și implică nuanțări cu privire atât la tipul de sistem informatic care se accesează, cât și la caracterul public sau nepublic al datelor care sunt stocate pe acesta. În principiu, considerăm că, raportat la punctul de acces la sistemul informatic, organele naționale vor fi competente teritorial, având în vedere că actul de procedură, din punct de vedere fizic, se realizează pe teritoriul României. În mod evident, nu se pune problema unui

[1] Conform art. 304 alin. (2) C.pen., constituie infracțiune: „divulgarea, fără drept, a unor informații secrete de serviciu sau care nu sunt destinate publicității, de către cel care ia cunoștință de acestea, se pedepsește cu închisoare de la o lună la un an sau cu amendă".

[2] Conform art. 227 alin. (1) C.pen., constituie infracțiune: „divulgarea, fără drept, a unor date sau informații privind viața privată a unei persoane, de natură să aducă un prejudiciu unei persoane, de către acela care a luat cunoștință despre acestea în virtutea profesiei ori funcției și care are obligația păstrării confidențialității cu privire la aceste date, se pedepsește cu închisoare de la 3 luni la 3 ani sau cu amendă".

[3] *V. supra*, Titlul V, Capitolul II.2.

acces la sistemul informatic prin pătrunderea directă asupra dispozitivului – caz care implică accesul direct, nemijlocit asupra dispozitivului, însă aceasta este incidentă în cazul unui acces la distanță.

Totuși, acest argument este unul simplist și poate fi considerat formal, raportat la problema că datele informatice obținute sunt stocate pe dispozitive care nu se află pe teritoriul țării. Problema de față are conotații actuale, iar reglementările internaționale nu sunt actualizate la noile realități ale mijloacelor folosite de făptuitori în realizarea infracțiunilor, folosindu-se de mediul informatic, aspect care aduce probleme de jurisdicție care servesc numai la ajutarea făptuitorilor să eludeze răspunderea penală. Așa cum am arătat în cuprinsul acestei lucrări, legislația internațională aplicabilă și care a stat la baza dispozițiilor din Codul de procedură penală privind *accesul la un sistem informatic* este Convenția de la Budapesta privind criminalitatea informatică din anul 2001. Conform acesteia, se trasează unele directive privind cooperarea internațională, care, la acest moment, considerăm că sunt ineficiente în descoperirea unor anumite infracțiuni, în principal, cele care se desfășoară în mediul informatic (pornografie infantilă, comercializarea de stupefiante, arme etc.). Mai recent, mediul online dă prilejul comiterii și a unor noi forme de infracțiuni, precum diverse tipuri de hărțuire (cyberstalking[1], cyberharrassement[2], cyberbullying[3]), șantaj sexual (sextortion[4]) și acțiuni de exploatare sexuală desfășurate împotriva minorilor (online child sexual predation[5]).

Obstacolul principal la cercetarea unor astfel de fapte, în opinia noastră, este dat de problema suveranității naționale, care se impune a fi respectată, în situația desfășurării accesului la sisteme informatice. Raportat la evoluția tehnologică, considerăm că o atare abordare este depășită, impunându-se a se găsi noi criterii pentru fundamentarea competenței teritoriale în domeniul acesta.

Soluția care poate fi găsită în cazul acesta este a considera că internetul, sistemul informatic mondial, nu aparține niciunui stat, ci constituie un „spațiu virtual" de sine stătător și care nu este la acest moment reglementat de către nicio autoritate la nivel internațional (cu excepția *ICANN*, care nu are atribuții decât în domeniul de infrastructură, mai precis al numelor de domeniu) și nu se supune vreunei jurisdicții singulare. Ceea ce caracterizează internetul este posibilitatea ca acesta să fie accesat din orice colț al lumii, permițând, teoretic, ca orice faptă să fie comisă în mai multe jurisdicții, în situația în care ea se comite prin internet (conform principiului *ubicuității*). Această trăsătură duce, în mod necesar, la concluzia că o multitudine de state pot deveni competente în anumite situații concrete.

---

[1] *M.-H. Maras*, Cybercriminology, Oxford University Press, New York, 2017, p. 232. Aceasta este forma cea mai des întâlnită de hărțuire online și presupune urmărirea persoanei prin sisteme informatice, accesul ilegal la conturile sale de e-mail, la rețelele de socializare etc., precum și transmiterea unor mesaje din partea victimei către prieteni sau rude, în scopul de a amenința, hărțui sau induce frică victimei.

[2] *Ibidem*, p. 234. „Cyberharrassment" semnifică folosirea unui sistem informatic pentru a alarma, enerva, ataca sau jigni o persoană. O formă o constituie *revenge porn,* respectiv folosirea unor imagini intime ale victimei, fără consimțământul acesteia, pentru a o umili sau a-i produce un rău.

[3] *Ibidem*, p. 238. „Cyberbullying" constituie o formă de agresiune verbală sau hărțuire, realizată de minori împotriva altor minori, prin intermediul sistemelor informatice.

[4] *Ibidem*, p. 240. „Șantajul sexual" sau „sextortion" constituie amenințarea cu diseminarea unor fotografii sau înregistrări video cu caracter explicit privind victima, dacă aceasta nu urmează indicațiile făptuitorului. Ea va constitui o formă concretă de șantaj, din perspectiva legii române.

[5] *Ibidem*, p. 241. În general, se referă la activități de pornografie infantilă, dar include și interacțiunile directe dintre un pedofil și un minor, prin care se încearcă obținerea încrederii acestuia, pentru a realiza anumite acte solicitate de pedofil.

De pildă, un cetățean român înregistrează, pe un site de socializare american, un anunț mincinos, prin care face cunoscut faptul că vinde un produs, acesta fiind mai apoi contactat de un cetățean german care îi transferă o sumă de bani cu titlu de preț dintr-o bancă elvețiană, pentru ca, în final, cetățeanul german să nu primească niciodată marfa cumpărată. Această simplă infracțiune de înșelăciune pune probleme serioase asupra competenței teritoriale ale organelor de urmărire penală. Statul român se poate considera competent, deoarece cetățeanul român a înregistrat anunțul de vânzare în România; S.U.A. se poate considera competentă în virtutea faptului că acțiunea de inducere în eroare s-a desfășurat prin intermediul serverelor de pe teritoriul american; statul german se poate considera competent, deoarece victima se afla pe teritoriul Germaniei în momentul în care a fost indusă în eroare; iar statul elvețian se poate considera competent, deoarece suma plătită – paguba – a fost transferată dintr-un cont elvețian. Acest exemplu este unul simplu, însă este posibil ca acțiunea de inducere în eroare să fie mai complexă din punctul de vedere al mijloacelor folosite: cetățeanul român se folosește de o conexiune la distanță cu un calculator dintr-o altă țară să înregistreze mesajul, considerând că nu va putea fi depistat așa ușor – astfel s-ar mai putea adăuga încă o jurisdicție competentă. Exemplul poate fi complicat și mai mult, deoarece însăși infrastructura internetului implică mai multe sisteme informatice interconectate, fiecare preluând și retransmițând datele informatice, de multe ori modificându-le forma.

Soluția la această dilemă este o competență fundamentată pe ideea posibilității dobândirii accesului la datele informatice căutate din teritoriul unui anumit stat. În concret, în privința accesului la un sistem informatic la distanță, considerăm, *de lege ferenda*, că este competent orice stat care *poate să aducă datele informatice în punctul de acces la sistemul informatic*, atât timp cât operațiunea se limitează la citirea unor date informatice existente. În cazul în care, prin accesul la un sistem informatic, s-ar dori modificarea unor date informatice – inclusiv instalarea de programe informatice care să înregistreze și să trimită mai departe acțiunile utilizatorului –, va trebui să constatăm lipsa competenței teritoriale a organelor de urmărire penală române, prin raportare la acțiunile invazive și ofensive. Excepția de la această regulă o reprezintă suprimarea accesului sau îndepărtarea datelor informatice care sunt interzise prin instrumente internaționale.

Această distincție se explică prin faptul că datele obținute prin accesul la un sistem informatic nu sunt altceva decât copii ale informațiilor transmise de către sistemul informatic țintă, ca atare, dispozitivul asupra căruia se exercită accesul rămâne nemodificat cu privire la datele informatice (datele informatice transmise rămân identice cu ele însele). În schimb, în cazul instalării unor programe informatice în vederea obținerii de date ulterior pătrunderii în sistem ori în cazul modificării datelor informatice (de pildă, distrugere), vom fi în situația depășirii competenței teritoriale a organului de urmărire penală.

De lege lata, nu se poate susține ceea ce am arătat mai sus, deoarece nu există niciun temei legal care să permită acest lucru, din contră, Convenția de la Budapesta privind criminalitatea informatică interzice accesul la un sistem informatic desfășurat de către un agent al unui stat atunci când sistemul informatic se află pe teritoriul altui stat. Conform art. 19 par. 1 din Convenția de la Budapesta, statele sunt obligate să adopte în legislația națională proceduri care să permită organelor competente efectuarea de perchiziții informatice și dobândirea accesului la un sistem informatic atunci când fie sistemul informatic, fie mediul de stocare al datelor informatice se află pe teritoriul său.

În situația în care sistemul informatic care trebuie accesat, indiferent dacă se impune un acces direct ori un acces la distanță, este într-un stat străin, organul desemnat cu efectuarea

măsurii de supraveghere este obligat să procedeze conform dispozițiilor art. 25-35 din Convenția de la Budapesta, privind cooperarea internațională în materia infracțiunilor de criminalitate informatică. Relevant la cele arătate mai sus, se impune a se sublinia că există, la acest moment, cadrul legal la nivel internațional pentru a asigura cooperarea între organele judiciare ale statelor semnatare ale Convenției. În urma cooperării internaționale, organele judiciare ale statului în care se află sistemul informatic vor efectua un acces la sistemul informatic, în măsura în care acceptă cererea de acordare a ajutorului în privința acestei metode de supraveghere. Desigur, fiind vorba de concursul unei autorități străine, se impune a se recurge la un procedeu probatoriu care să fie compatibil cu reglementările privind cooperarea internațională în materie penală. Din păcate, în cuprinsul legii române privind cooperarea internațională în materie penală – Legea nr. 302/2004, republicată[1] –, nu există nicio prevedere privind accesul la un sistem informatic. În măsura în care se va dori efectuarea operațiunilor specifice accesului la un sistem informatic, va fi necesar a se solicita realizarea unei *percheziții informatice*, fiind aplicabile dispozițiile art. 176 din Legea nr. 302/2004, republicată (ori art. 200 raportat la art. 176 din Legea nr. 302/2004, republicată, în cazul statelor Schengen).

Trebuie observat faptul că nu există niciun mijloc legal de a proceda direct la efectuarea unui acces la un sistem informatic atunci când acesta se află în afara țării, în ipoteza refuzului statului străin de a proceda la efectuarea acestui act de procedură. Acesta va putea în mod discreționar să refuze să realizeze acest act, având ca motive temeiurile de *ordine publică*[2].

Acesta este un neajuns major al reglementării internaționale și, *de lege ferenda*, se impune, ca o soluție drastică, introducerea permisiunii ca statul solicitant să procedeze în mod unilateral la realizarea accesului la sistemul informatic aflat pe teritoriul statului străin, în situația unui refuz.

O situație aparte este cea în care o infracțiune informatică este comisă de către agențiile unui alt stat, operațiuni în sinea lor ilegale și al căror caracter secret se impune a fi menținut. Astfel de acte pot fi uneori considerate drept acte de agresiune, și astfel investigarea lor de către statul victimă va fi în mod evident blocată de către agențiile statului care a declanșat aceste atacuri, de pildă, pe motiv de *ordine publică*. Astfel de cazuri sunt numeroase, de la pătrunderea în sistemul informatic NASA, până la infiltrarea unor centrale nucleare iraniene (prin virusul Stuxnet și o vulnerabilitate 0-day).

O altă situație care implică dificultăți deosebite este situația în care un site prin care se desfășoară activități ilicite (de pildă, The Pirate Bay – distribuire de materiale informatice piratate) ori care constituie mijlocul de săvârșire a unei infracțiuni (de exemplu, infracțiunile de pornografie infantilă) beneficiază de o infrastructură (în sensul de multiple sisteme informatice) aflată în mai multe țări. În această situație, dificultatea va fi una deosebită, raportat la posibilitatea identificării competenței teritoriale, în vederea cooperării internaționale în materie penală. În privința site-ului The Pirate Bay, proprietarii acestuia chiar se mândresc cu acest lucru, asemănându-și site-ul cu hidra mitologică.

În același sens, în cazul unor site-uri cu specific pornografic, în vederea nedescoperirii proprietarilor acestora, sunt folosite diverse metode, precum modificarea, uneori și orară, a serverului de pe care funcționează site-ul, a adresei IP, chiar și fără schimbarea numelui de domeniu ori folosirea unui domeniu în cadrul rețelei TOR. Acest aspect poate induce în eroare

[1] Legea nr. 302 din 28 iunie 2004 privind cooperarea judiciară internațională în materie penală (republicată în M. Of. nr. 377 din 31 mai 2011).

[2] Termenul în original este *ordre public* și nu trebuie confundat cu sensul folosit de legiuitorul român în cuprinsul Codului de procedură penală.

un organ de urmărire penală, deoarece datele informatice își modifică locația (de multe ori și țara) foarte repede, fiind imposibil de realizat operațiuni de acces în condițiile legislative actuale. Fără a intra în detalii tehnice, arătăm că operațiunea de mai sus este posibilă, deoarece modificarea se va opera prin schimbări în configurația domain name serverului: în primul rând, domeniul are conexat întotdeauna emitentul său, care are obligația de a transmite orice cerere pe acel domeniu către un server, denumit *domain name server* – acest sistem informatic este cel care atribuie adresa IP pe care o are sistemul informatic care conține datele. Astfel, în exemplul dat, se operează numai modificări în domain name server, comutându-se pe un alt server cu o nouă adresă IP.

O altă problemă practică apare în determinarea competenței teritoriale a organului de urmărire penală atunci când se folosește rețeaua TOR (The Onion Router) pentru realizarea comunicațiilor sau pentru accesarea unor pagini de internet. Această rețea asigură anonimizarea informațiilor trimise sau accesate de către un utilizator către un sistem informatic. Mai mult, în cadrul acestei rețele, se pot stabili site-uri care să ruleze numai printr-o adresă anonimizată. Problema de natură practică este descoperirea a însăși locației sistemului informatic, însă, deoarece toate comunicațiile se realizează criptat, trecând prin nenumărate alte sisteme informatice (denumite nod-uri, ele sunt multiple pentru anonimizarea informației și situate în multiple locații), nu se poate stabili locația sistemului informatic și nici măcar adresa sa IP.

Încă de la începutul rețelei, pe care o cunoaștem acum ca „internet", cunoscută inițial ca ARPANET, existau subrețele secrete denumite *darknet*. Termenul este folosit încă de la existența ARPANET pentru a denumi o serie de adrese de internet care sunt secrete și care nu pot fi accesate în mod obișnuit din ARPANET. În lume există mai multe astfel de rețele, cele mai cunoscute sunt realizate în cadrul calculatoarelor din rețeaua TOR, descrisă mai sus. Prin intermediul unui darknet, se pot vinde sau cumpăra bunuri interzise (droguri, arme etc.), precum și se pot propaga servicii ilegale (pornografie infantilă, escorte, asasinate etc.), de regulă, tranzacțiile realizându-se cu moneda bitcoin. Aceste site-uri nu sunt publice, ele neputând fi accesate de către un utilizator obișnuit, ci implică cunoașterea modului de acces și a unor adrese specifice care pot fi accesate din cadrul rețelei TOR. Cu toate acestea, nu este dificil de obținut accesul pe un asemenea darknet, fiind suficient ca un utilizator să caute pe internet modalitatea și, cu siguranță, va afla în scurt timp cum poate accesa darknet-ul. Acesta aduce cea mai mare dificultate în privința procedurilor de combatere a criminalității informatice, deoarece persoanele și chiar sistemele informatice sunt foarte greu de identificat, iar folosirea metodei de supraveghere a accesului la sistem informatic, chiar și în situația în care sistemul informatic ar fi în România, nu poate duce la obținerea de probe care să respecte prevederile art. 100 C.pr.pen.

Spre deosebire de darknet, Deep Web este acea situație în care conținutul unui anumit site ori sistem informatic nu este indexat de către un motor de căutare (Google, Yahoo, Bing), însă este public și disponibil online. O astfel de pagină sau sistem informatic este accesibil oricui, în măsura în care cunoaște adresa IP a serverului.

Una dintre situațiile în care suntem de părere că organele de urmărire penală pot realiza acte de acces în sisteme informatice aflate pe teritoriul unui stat străin este aceea în care informațiile sunt publice. Această posibilitate este prevăzută și în cuprinsul art. 32 lit. a) din Convenția de la Budapesta și nu implică autorizarea prealabilă a statului pe teritoriul căruia se află sistemul informatic.

Cel mai bun exemplu pentru accesul la un sistem informatic public este o rețea de socializare, unde o persoană bănuită că ar fi săvârșit o infracțiune prezintă public opinii, imagini sau alte mesaje din care rezultă că ar fi comis fapta. Considerăm că intră în caracterul de informație publică datele informatice care pot fi obținute de către orice utilizator obișnuit fără a se folosi programe specializate în vederea eludării sau dezactivării măsurilor de securitate ale sistemului informatic. În această categorie intră site-urile sau sistemele informatice (deoarece nu este necesar ca sistemul informatic să aibă o interfață HTTP specifică unui site), care fie beneficiază de un domeniu (adică o denumire generică aleasă având extensii precum .ro, .com, .info ori orice astfel de extensie recunoscută), fie care nu beneficiază de un domeniu (caz în care accesul se va realiza prin adresa sa de internet IPV4 sau IPV6). De pildă, este publică o informație distribuită pe Facebook, chiar dacă, pentru a fi vizionată, organul de urmărire penală trebuie să-și creeze un cont pe acea rețea de socializare. În același timp, nu va fi publică informația disponibilă pe un tracker de torrente privat în care înregistrarea se face pe bază de invitație.

O altă situație în care este posibil accesul la sistemul informatic, pentru a obține date informatice specifice, este atunci când deținătorul sistemului informatic pe care sunt stocate datele își dă acordul și permite accesul în sistemul informatic, în condițiile în care acesta are dreptul legal de a permite accesul. În alte cuvinte, această posibilitate, prevăzută de art. 32 lit. b) din Convenția de la Budapesta, este aplicabilă numai atunci când deținătorul sistemului informatic (de cele mai multe ori, un particular), în mod voluntar, acceptă ca organele de urmărire penală dintr-un alt stat să pătrundă în sistemul său informatic pentru a identifica probe, în măsura în care are posibilitatea legală să permită acest acces. Totodată, acesta poate să culeagă datele informatice cerute și să le transmită organelor de urmărire penală solicitante.

Limita acestui acces voluntar este dată de *facultatea legală a deținătorului informatic să divulge datele stocate*. De exemplu, un furnizor de servicii de internet dintr-o țară vecină are posibilitatea legală să divulge din propriul sistem informatic log-urile de acces privind un anumit IP, precum și persoana abonatului care a folosit acel IP la un anumit moment. În același timp, în funcție de clauzele contractuale (Terms of service) ale unui site, este posibil a fi divulgate o multitudine de date informatice în măsura în care, la încheierea contractului, persoana a consimțit să permită furnizorului acest lucru. Acest drept se poate conferi odată cu înregistrarea pe un anumit site ori ca urmare a modificării clauzelor contractuale care guvernează serviciile oferite de site-ul respectiv. În schimb, vom fi în situația în care o persoană deținătoare de sistem informatic nu va putea divulga datele informatice sau nu va putea permite accesul în sistemul informatic, deoarece clauzele sale contractuale o obligă la confidențialitate, de exemplu, în cazul unor servicii de tip e-mail. În măsura în care acesta permite accesul la sistemul informatic și nu are dreptul să facă acest lucru în mod voluntar, considerăm că probele obținute se impun a fi excluse, fiind obținute în mod nelegal.

Cea de-a doua condiție impusă este ca deținătorul sistemului informatic să permită accesul sau să remită el însuși datele informatice în mod voluntar. Conform dispozițiilor Convenției de la Budapesta, nu sunt prevăzute căi prin care deținătorul ar putea fi constrâns, el fiind liber să refuze solicitarea emisă de organele de urmărire penală, chiar în mod arbitrar, fără a fi incidente sancțiuni.

Din punct de vedere procedural, considerăm că, în baza mandatului emis de judecătorul de drepturi și libertăți, organul de urmărire penală are dreptul să procedeze la adresarea unei solicitări către deținătorul sistemului informatic în care să îi solicite aprobarea privind accesul la un sistem informatic, în condițiile în care sistemul informatic se află pe teritoriul unui

stat străin. Într-o atare situație, nu vom fi în cazul unei cooperări internaționale în materie penală, deoarece va exista acordul unui particular pentru a se proceda la accesul la sistemul său informatic, nefiind exercitate prerogative de ordine publică pe teritoriul unui alt stat, ceea ce ar contraveni suveranității acelui stat. Cu toate acestea, este imperios necesar să se obțină acordul autorităților străine competente pentru a face acest lucru, chiar dacă acest acord nu este unul dus la nivelul unui act juridic. S.U.A. (semnatară a Convenției de la Budapesta) manifestă o atitudine mai permisivă privind modalitatea în care acționează în asemenea situații, recomandând, în cazul contactării directe a unui furnizor de servicii de comunicații electronice, ca organele de urmărire penală să: a) aibă acordul prealabil al autorităților autohtone să facă acest lucru; b) să aibă aprobarea Oficiului de Afaceri Externe al Departamentului de Justiție al S.U.A. – organ care este la curent cu practicile acceptate în cazul diferitelor state; c) să aibă date clare că nu ar fi privite în mod defavorabil asemenea practici de către autoritățile autohtone[1]. Nu putem fi de acord cu o asemenea abordare, o opinie similară fiind susținută recent și de Comitetul pentru aplicarea Convenției de la Budapesta prin Nota interpretativă nr. 3 a T-CY din 3 decembrie 2014, unde se arată că unele semnatare consideră că o atare acțiune ar constitui o infracțiune.

În afara celor două situații, considerăm că, *de lege lata*, organul de urmărire penală nu poate trece direct la efectuarea accesului la sistemului informatic în condițiile în care sistemul informatic nu se află pe teritoriul țării. În aceste condiții, considerăm că singura modalitate de a se realiza un acces la un sistem informatic atunci când acesta se află în străinătate este atunci când sistemul informatic este public, în sensul în care *datele informatice conținut* care vor face obiectul măsurii sunt publice.

Secțiunea a 3-a. Modalități de realizare a accesului la un sistem informatic

Pentru a se stabili operațiunile care pot fi desfășurate de organele de urmărire penală, se impune a se interpreta sensul dispozițiilor art. 138 alin. (3) C.pr.pen., prin prisma modalităților practice în care acestea se desfășoară. În concret, în această secțiune a lucrării, vom aborda *(a)* problema accesului prin pătrundere directă într-un sistem informatic și *(b)* a accesului prin pătrundere la distanță.

Potrivit art. 138 alin. (3) C.pr.pen., în care se definește metoda specială a accesului la un sistem informatic, se înțelege pătrunderea într-un sistem informatic sau mijloc de stocare a datelor informatice fie direct, fie de la distanță, prin intermediul unor programe specializate ori prin intermediul unei rețele, în scopul de a identifica probe. Fiindcă Codul de procedură penală împarte în două modalitățile de acces la un sistem informatic, le vom trata distinct în cele ce urmează.

§1. Accesul direct la un sistem informatic

Prima modalitate prevăzută de Codul de procedură penală în cazul accesului la un sistem informatic este *accesul direct*, prin aceasta înțelegându-se acea pătrundere într-un sistem informatic realizată prin operațiuni desfășurate în locul în care se află sistemul informatic. În

[1] Departamentul de Justiție al Statelor Unite ale Americii, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations (manual oficial), 2002, p. 25.

cazul mijloacelor de stocare a datelor informatice, singura modalitate de acces la un sistem informatic va fi prin acces direct, deoarece un mijloc de stocare nu poate fi conectat într-o rețea, iar, dacă va fi legat (sau introdus) într-un sistem informatic, atunci va fi o parte a sistemului informatic și va trebui tratat ca atare.

Accesul direct la un sistem informatic are multe similarități cu percheziția informatică, însă considerăm că diferențele vor fi unele semnificative. Deoarece nu se impune menținerea integrității datelor informatice conținute de sistemul informatic țintă, se va putea proceda la accesarea sistemului informatic în orice mod și în funcție de timpul pe care îl au organele de urmărire penală. Pentru a se menține secretul supravegherii tehnice, este preferabil a nu se lăsa semne externe care să trădeze intervenția unei persoane, de exemplu, lipsa sistemului informatic[1]. Există două metode de lucru posibile: acces direct în sistem offline și copierea datelor informatice sau în sistem online și selectarea mai bună a datelor informatice prin analizarea lor din punct de vedere funcțional[2]. Prima variantă este specifică percheziției informatice, dar este cu mult mai laborioasă. Prin „online" și „offline" nu vom înțelege numai simplul fapt că sistemul informatic este pornit sau oprit, ci vom înțelege *funcționarea sistemului de operare* instalat pe acesta.

În opinia noastră, deoarece accesul la un sistem informatic nu presupune menținerea integrității datelor în sistemul informatic accesat, se poate proceda la un acces online pentru obținerea cât mai rapidă a probelor. Totodată, în cazul unui sistem online, se pot instala programe care se pot folosi ulterior pentru realizarea altor măsuri de supraveghere tehnică (interceptarea comunicațiilor și supravegherea video, audio sau prin fotografiere).

În cazul accesului direct la un sistem informatic online, se poate proceda mai eficient la accesarea datelor informatice decât într-un sistem aflat la distanță, deoarece accesul fizic la sistemul de stocare poate învinge de multe ori sistemul de siguranță[3]. Un exemplu în acest sens este accesarea offline a sistemului informatic și modificarea registrului SAM[4] al Windows pentru schimbarea parolei unui utilizator, continuând cu logarea ca acel utilizator, folosindu-se noua parolă creată.

În practică, sistemele informatice care se pot dovedi extrem de utile sunt telefoanele mobile tip smartphone, care sunt într-o evoluție continuă, perfecționându-se chiar zilnic prin actualizarea programelor pe care le au. Față de orice altă măsură de supraveghere tehnică, accesul la un sistem informatic aplicat asupra unui telefon mobil poate furniza date importante cu privire la: comunicațiile anterioare ale persoanei, a locațiilor în care aceasta a fost, poate furniza parolele de acces către alte sisteme informatice, imagini, înregistrări video și audio (inclusiv cu informația privind locația în care au fost înregistrate[5]), conexiuni cu dispozitive wireless, bluetooth, registre privind activitatea senzorilor telefonului etc.

[1] Un laptop sau PC nu va putea fi luat temporar, însă un telefon mobil poate fi luat datorită dimensiunii sale reduse, precum și a faptului că astfel de dispozitive se fură adeseori, iar persoana vizată nu va bănui că este vizată de un mandat de supraveghere tehnică.

[2] Este mai rapid să se pătrundă într-un sistem prin evitarea mijloacelor de securitate, deoarece se pot observa elemente greu de obținut în cazul unui sistem online: sesiuni active de e-mail, de site-uri de socializare, precum și accesul prin intermediul parolelor stocate de browsere.

[3] Mai puțin în cazul criptării sistemului informatic, când se impune capturarea directă a cheii de criptare aflată în sistemul RAM, altfel decriptarea unui sistem offline durând deosebit de mult timp.

[4] Security Accounts Manager – un registru criptat cu utilizatorii și parolele în cazul sistemului Windows.

[5] Funcția se numește „geo-tagging" și este activată implicit în cazul pozelor la telefoanele care rulează sistemul Android.

S-a arătat în literatura de specialitate că numărul de smartphone-uri în uz într-o anumită zonă poate determina evenimentele care au loc în acea locație, având în vedere că aceste sisteme informatice sunt proiectate să simtă cât mai bine mediul în care se află și să se adapteze la el, un aspect deosebit de important fiind faptul că ele încearcă să determine tot timpul un lucru fundamental: locația lor[1]. Prin accesul la un sistem informatic asupra mai multor telefoane mobile aparținând unor anumite persoane se poate determina dacă au fost în același loc împreună (dovedindu-se că două persoane s-au întâlnit). Totodată, datele informatice stocate pot constitui un așa numit „alibi al interacțiunii sociale" atunci când, pe baza datelor informatice din telefonul mobil, se poate determina că o persoană nu a fost la data pretinsei săvârșiri a infracțiunii în locul stabilit[2]. Un astfel de program este Facebook Messenger, care, în cuprinsul mesajelor transmise între utilizatori, poate trimite și locația pe care o are persoana care trimite mesajul, alături de ora la care aceasta trimite mesajul.

Trebuie menționat faptul că toate sistemele informatice conțin fișiere tip *log* în care sunt stocate evenimente importante pentru sistemul de operare, precum momentul în care a fost pornit, erorile care apar, perifericele conectate și deconectate, conexiunile internet stabilite, practic, o vastă bază de date de informații care se stochează de la momentul instalării sistemului de operare până în momentul ștergerii sale. Problema principală cu acest tip de fișier este faptul că se află într-o continuă modificare și accesare, astfel că abordarea copierii acestuia se va face în mod similar celei specifice unei percheziții informatice – cu sistemul de operare închis, pentru a nu se crea noi evenimente în cuprinsul acestor registre[3]. Ulterior, acestea pot fi deschise cu programe specializate și interpretate pentru a se găsi informații relevante. De exemplu, în cazul unui sistem tip server, acesta va stoca adresele IP ale sistemelor informatice care l-au accesat, precum și datele furnizate. Aceste informații pot fi esențiale în cazul pornografiei infantile, deoarece constituie o probă directă în dovedirea infracțiunii săvârșite de persoana care a accesat materialele de pe serverul care va fi supus accesului la un sistem informatic.

Însă, deși aceste date sunt de maximă importanță, trebuie avut grijă în privința elementului „timp", deoarece aceste loguri folosesc ora și data locală a calculatorului pe care lucrează[4]. Astfel, în determinarea momentului accesării unor informații, se vor avea în vedere (chiar și în situația în care vorbim despre fișiere obișnuite, nu doar de log-uri de acces într-un server) următoarele chestiuni: *posibilitatea unei date și ore setate incorect*, *probleme legate de fusul orar*, *problema aplicării orei de vară*, *sincronizarea între timp și eveniment*. Ultima problemă este similară cu problema alibiului, deoarece este necesar a se dovedi că o anumită persoană se afla în timpul operării calculatorului la momentul comiterii faptei, și nu o altă persoană[5]. Dovedirea faptului că o anumită persoană s-a aflat în fața sistemului informatic și l-a utilizat se poate face prin mai multe metode, însă una dintre cele mai utile este pe baza istoricului de site-uri vizitate. Atunci când un utilizator folosește sistemul informatic, adeseori accesează

[1] *H. Pieterse, M. Olivier*, în G. Peterson, S. Shenoi (coord.), Advances in Digital Forensics X. 10th IFIP WG 11.9 International Conference, Vienna, Austria, January 8-10, 2014, Revised Selected Papers, Ed. Springer, New York, 2014, pp. 237-238.

[2] *S. Beyer, M. Mulazzani, S. Schrittwieser, M. Huber, E. Weippl*, în G. Peterson, S. Shenoi (coord.), op. cit., p. 298.

[3] *Q. Do, B. Martini, J. Looi, Y. Wang, K.K. Choo*, în G. Peterson, S. Shenoi (coord.), op. cit., p. 92.

[4] *O.V. Manzhai*, Procedure Analysis of the Special Investigative Actions through Cyberspace in Countries of Common and Continental Law, în Internal Security, vol. 4, no. 1/2012, p. 145.

[5] *D.-Y. Kao, Y.-H. Chiu*, în Y.-Q. Shi, H.J. Kim, F. Pérez-González, C.-N. Yang (coord.), Digital Forensics and Watermarking. 13th International Workshop, IWDW 2014, Taipei, Taiwan, October 1-4, 2014, Revised Selected Papers, Ed. Springer, New York, 2015, pp. 510-511.

site-uri de socializare sau site-uri de-email în care acesta își introduce datele personale, o parte dintre acestea fiind reținute în istoricul de site-uri vizitate (de exemplu, titlul paginii, element reținut în istoric, poate fi utizator@gmail.com, Inbox) și permițând, pe baza orei accesării, stabilirea persoanei care a folosit în acel moment sistemul informatic[1].

O problemă deosebit de importantă în cazul accesului la sistemul informatic este problema *integrității datelor informatice*. Prin „integritatea datelor informatice" putem înțelege atât integritatea datelor informatice de pe sistemul informatic, cât și integritatea datelor informatice care sunt rezultatul unui acces la un sistem informatic. Codul de procedură penală nu prevede dispoziții exprese privind asigurarea integrității datelor informatice și nici nu impune organelor judiciare o obligație în acest sens, decât în cazul accesului la un sistem informatic dispus prin autorizarea procurorului, și chiar și atunci acesta se referă la integritatea datelor obținute prin copiere, iar nu a datelor originale. O atare obligație se va regăsi în cazul unui alt procedeu probatoriu, *percheziția informatică*, care, în opinia noastră, ar trebui să constituie procedeul probatoriu care garantează cel mai bine drepturile și libertățile persoanei. Cu toate acestea, nu trebuie să confundăm problema cu necesitatea menținerii integrității datelor informatice rezultate din supravegherea tehnică, ceea ce va constitui întotdeauna o obligație pentru organele de urmărire penală. Păstrarea integrității datelor informatice obținute poate fi garantată prin semnarea cu ajutorul unei semnături digitale extinse a datelor informatice, în conformitate cu art. 142[1] C.pr.pen.

§2. Accesul la distanță

Cea de-a doua modalitate de efectuare a accesului la un sistem informatic este accesul la distanță, realizat prin intermediul unui alt sistem informatic și a unei rețele care va lega sistemul informatic mijloc și sistemul informatic țintă.

Deoarece securitatea rețelelor este de importanță fundamentală în mediul informatic modern, va fi mai greu să se realizeze un acces la distanță decât un acces direct, deoarece măsurile de siguranță pot bloca mai bine încercările organelor de urmărire penală de a pătrunde în sistemul informatic țintă. Un alt element esențial este faptul că accesul la distanță se poate realiza numai în cazul unui sistem online, întrucât în cazul unuia oprit nu va funcționa rețeaua acestuia și nu se va permite pornirea sa[2]. Odată neutralizate sistemele de securitate ale sistemului informatic, accesul la distanță se poate realiza la același nivel de eficacitate ca accesul direct.

Situații particulare ale accesului la distanță sunt site-urile, rețelele de socializare și trackerele de torrente. Aceste tipuri de sisteme sunt publice, astfel vor putea fi accesate la distanță chiar dacă sistemul informatic este în afara României. De remarcat este faptul că, dacă site-ul străin desfășoară activități licite, nu se vor putea lua măsuri ofensive împotriva acestuia (suprimarea accesului sau îndepărtarea datelor informatice), ci numai copierea de date, în măsura în care ele sunt accesibile publicului.

În privința oricărui site ori a unei rețele de socializare, credem că va fi necesară încuviințarea măsurii supravegherii tehnice a accesului la un sistem informatic raportat la prevederile

[1] *B. Shavers*, Placing the Suspect Behind the Keyboard. Using Digital Forensics and Investigative Techniques to Identify Cybercrime Suspects, Ed. Elsevier, Waltham, Massachusetts, 2013, p. 105.

[2] Cu excepția unor sisteme specializate, nu este posibilă pornirea de la distanță, prin internet, a unui computer, o atare posibilitate putând exista în cazul unui sistem informatic din aceeași rețea LAN, dar numai dacă sistemul informatic este anume configurat să permită acest lucru (Wake-On-LAN).

fără echivoc ale art. 138 alin. (3) C.pr.pen. Accesul se va realiza prin programe care permit înregistrarea site-ului într-o formă care poate fi arhivată și accesată ulterior (site downloadere). Totodată, se poate folosi o metodă mixtă în care se accesează datele și se realizează o captură de ecran[1] a întregii proceduri desfășurate. Astfel, prin captura de ecran se va înregistra video fiecare operațiune desfășurată de organul de urmărire penală, fără a influența în vreun mod datele informatice obținute.

O altă problemă specifică o reprezintă trackerele de bittorrent despre care am mai făcut vorbire în prezenta lucrare. În cazul acestora, metodele vor fi specifice și vor avea ca scop identificarea tuturor utilizatorilor rețelei prin intermediul adreselor IP. Trackerele de torrent pot fi private sau publice, primele necesitând înregistrarea cu un cont special (fie plătit, fie obținut în urma unei invitații din partea altui utilizator).

Dacă trackerul de torrent este unul public, organul de urmărire penală poate efectua un acces la sistemul informatic, prin accesarea trackerului care strânge toate adresele IP ale utilizatorilor care folosesc serviciul. În acest fel, printr-o acțiune de *infiltrare*, se pot obține în mod public adresele IP ale persoanelor care descarcă sau încarcă materiale pirat. Acest lucru este posibil ca urmare a specificului bitorrent care implică un server de distribuție, denumit *tracker*, și utilizatori conectați la acesta, denumiți *peers* și *seeds*. Trackerul nu conține niciodată materialul pirat, însă va face legătura între persoanele care descarcă (*peers*) și persoanele care încarcă (*seeds*). Sistemul este considerat *peer-to-peer*, de la individ la individ, tracker-ul realizând contactul dintre persoanele care descarcă și cele care încarcă. Însă, din fericire, trackerul stochează și face publice toate adresele IP ale persoanelor care accesează un torrent și le furnizează tuturor celorlalți, publicarea acestor adrese fiind de natura protocolului.

[1] Există programe informatice specializate care preiau semnalul dat de placa video și îl transformă în timp real în fișiere video. Plăcile video nVidia vin cu software-ul, numit *Shadowplay*, care permite acest lucru fără instalarea de programe specializate.

Capitolul IV
Distincțiile dintre accesul la un sistem informatic, procedeele probatorii comune și alte metode speciale de supraveghere sau cercetare

Accesul la un sistem informatic are ca specific faptul că se urmărește accesarea datelor informatice cuprinse într-un sistem informatic sau într-un mijloc de stocare a datelor informatice, însă între acest procedeu probatoriu și altele există aspecte comune care pot crea confuzie în privința procedeului probatoriu folosit. Semnificația practică este deosebit de importantă, deoarece nu toate procedeele probatorii se efectuează în urma aceleiași proceduri de încuviințare, unele fiind de competența procurorului, iar altele fiind de competența judecătorului de drepturi și libertăți. În măsura în care se va realiza un acces la un sistem informatic, însă nu a fost respectată procedura de dispunere a măsurilor de supraveghere tehnică, actul prin care s-a dispus efectuarea accesului la un sistem informatic va fi lovit de nulitate, iar rezultatul accesului la un sistem informatic va fi exclus din procesul penal ca fiind obținut în mod nelegal.

În cele ce urmează vom aborda principalele procedee probatorii care se aseamănă și se întrepătrund uneori cu accesul la un sistem informatic.

Secțiunea 1. Predarea obiectelor, înscrisurilor sau a datelor informatice și accesul la un sistem informatic

Considerăm că un procedeu probatoriu utilizat deseori în practică, *predarea obiectelor, înscrisurilor sau a datelor informatice*, prevăzut de art. 170 C.pr.pen., poate crea confuzie atunci când se impune predarea unor date informatice. Această confuzie poate apărea, de aceea trebuie determinat cu precizie scopul procedeului probatoriu.

În cazul unor înscrisuri sau alte obiecte, procedeul probatoriu prevăzut de art. 170 C.pr.pen. nu ridică probleme deosebite, deoarece acestea pot fi studiate în mod liber de către organul de urmărire penală. În schimb, în cazul datelor informatice, acestea nu au o formă fizică, ele prezentându-se sub aspectul unui obiect care constituie **un mijloc de stocare sau un sistem informatic**. Conform art. 170 alin. (2) lit a) C.pr.pen., procurorul poate dispune ca „*orice persoană fizică sau juridică de pe teritoriul României să comunice anumite date informatice aflate în posesia sa sau sub controlul său, care sunt stocate într-un sistem informatic ori pe un suport de stocare a datelor informatice*".

Deoarece accesul la un sistem informatic se poate face și direct, în locația în care se află sistemul informatic sau mijlocul de stocare, se pune problema de a ști dacă accesarea datelor informatice predate în temeiul art. 170 C.pr.pen. se poate face în absența autorizării metodei speciale de supraveghere a accesului la un sistem informatic. Cu alte cuvinte, problema ridicată este dacă, în temeiul art. 170 C.pr.pen., datele informatice obținute pot fi folosite direct sau va fi necesară obținerea unui mandat pentru accesarea lor sau pentru realizarea unei percheziții informatice, atât timp cât ele au caracterul de date conținut și accesarea lor (citirea, tipărirea, copierea lor etc.) va constitui o restrângere a dreptului la viață privată al persoanei care a generat sau căreia îi aparțin aceste date informatice.

Remarcăm o diferență esențială între predarea de obiecte și înscrisuri și predarea datelor informatice în aceea că nu este suficient ca datele să fie predate, ele trebuind să fie și accesate pentru a constitui probe în procesul penal. Spre deosebire de datele la care se referă art. 170 alin. (2) lit. b) C.pr.pen., datele informatice prevăzute la art. 170 alin. (2) lit. a) C.pr.pen. sunt *date conținut*, astfel că predarea lor nu va permite justificarea organelor de urmărire penală de a le accesa de pe sistemul informatic sau suportul de stocare pe care se află. Admiterea acestui lucru ar permite efectuarea de acțiuni specifice fie accesului la un sistem informatic, fie și unei percheziții informatice în lipsa controlului judecătorului de drepturi și libertăți, ceea ce ar prezenta o gravă încălcare a dreptului la viață privată al persoanei. Pentru garantarea acestui drept, legiuitorul a impus procedura autorizării metodelor de supraveghere tehnică, prevăzută de art. 140 C.pr.pen., și procedura dispunerii percheziției informatice, prevăzută de art. 168 C.pr.pen. Din punctul de vedere al respectării drepturilor persoanei vizate de aceste două procedee probatorii, este evident faptul că o percheziție informatică aduce garanții în plus față de accesul la un sistem informatic, care se realizează fără știința persoanei față de care se ia măsura.

În opinia noastră, în toate cazurile în care se dorește obținerea unor date informatice de la o persoană conform art. 170 alin. (2) lit. a) C.pr.pen., procurorul va trebui să emită o ordonanță prin care să solicite transmiterea datelor informatice fie prin punerea la dispoziție a sistemului informatic ori suportului de stocare pe care se află, fie prin remiterea unei copii a acestor date, respectându-se integritatea datelor copiate. Odată ce datele informatice au fost predate, procurorul nu va fi îndreptățit să le acceseze în nicio situație, deoarece aceasta ar reprezenta un *acces la un sistem informatic*, pentru care este necesar să aibă autorizarea judecătorului de drepturi și libertăți, iar în mandatul de supraveghere tehnică să se prevadă în mod explicit suportul de stocare ori sistemul informatic predat. Admitem posibilitatea ca procurorul să solicite emiterea unui mandat de supraveghere și mai înainte de a emite ordonanța de predare a datelor informatice, însă va trebui să aducă la cunoștința judecătorului de drepturi și libertăți intenția de a solicita predarea datelor informatice respective. Necesitatea unei autorizări din partea judecătorului de drepturi și libertăți reiese din formularea definiției „accesului la un sistem informatic", conform art. 138 alin. (3) C.pr.pen., aceasta fiind „*pătrunderea într-un sistem informatic sau mijloc de stocare a datelor informatice fie direct, fie de la distanță, prin intermediul unor programe specializate ori prin intermediul unei rețele, în scopul de a identifica probe*". În toate situațiile în care datele informatice predate sunt citite într-un sistem informatic, vom avea o acțiune care se circumscrie definiției unui acces la un sistem informatic, prin aceea că procurorul pătrunde într-un sistem informatic sau într-un suport de stocare a datelor informatice în vederea identificării de probe. Deoarece dispozițiile legale sunt neechivoce, este necesar ca procurorul să fi fost autorizat să întreprindă un acces la sistemul informatic respectiv, în lipsa căruia probele obținute vor trebui excluse ca fiind obținute în mod nelegal. Opinia noastră este una împărtășită și de doctrina străină, care afirmă că, pentru a putea obține date informatice de la un terț, se impune o autorizare din partea unui judecător, iar datele informatice obținute vor putea fi folosite numai în cauza în care au fost obținute[1].

Un alt procedeu probatoriu care este propice de a fi utilizat ulterior predării datelor informatice este percheziția informatică, aceasta fiind, în opinia noastră, procedeul probatoriu care se impune a fi o regulă într-o astfel de situație, asigurând toate garanțiile necesare pentru

[1] *O.S. Kerr*, op. cit., p. 309.

respectarea vieții private a persoanei a căror date informatice se vor accesa, precum și integritatea acestora. Despre acest procedeu probatoriu vom vorbi mai mult într-o secțiune ulterioară[1].

Secțiunea a 2-a. Interceptarea comunicațiilor ori a oricărui tip de comunicare la distanță și accesul la un sistem informatic

Ca urmare a progresului tehnologic în domeniul telecomunicațiilor, este din ce în ce mai greu să se facă distincția între accesul la un sistem informatic și interceptarea comunicațiilor ori a oricărui tip de comunicare la distanță. La acest moment, toate convorbirile telefonice purtate între persoane vor trece prin sisteme informatice, în măsura în care este vorba de o rețea publică de telefonie. Această stare este de natură să creeze confuzie în privința aplicării metodei de supraveghere tehnică a accesului la un sistem informatic. În același timp, se dezvoltă servicii mixte, de telefonie prin internet – VoIP –, care transformă telefonia clasică, bazată pe receptoare clasice și fire de cupru într-un sistem informatic în care transmisiunea se face pe baza unor cabluri coaxiale de televiziune sau chiar prin fibră optică și folosirea unor dispozitive care transformă în semnal digital vocea umană încă de la sursă. În același timp, se dezvoltă servicii de telecomunicații care nu mai sunt legate de numere de telefon, fiind în schimb atașate unui cont direct la furnizorul de servicii prin internet.

Considerăm că aceste metode de supraveghere tehnică se întrepătrund atunci când comunicațiile se realizează prin intermediul unui sistem informatic, inclusiv atunci când acesta este un telefon mobil modern. Așa cum am arătat, accesul la un sistem informatic poate avea și caracter continuu, însă atât timp cât prin accesul continuu sunt vizate comunicațiile pe care le face persoana față de care s-a dispus supravegherea tehnică, vom fi în situația unei *interceptări a comunicațiilor*, și nu în situația unui acces la un sistem informatic. În concret, procedeul de interceptare s-ar realiza mai întâi prin accesul la un sistem informatic și prin instalarea unor programe care să transmită o copie a tuturor acțiunilor utilizatorului, inclusiv copii ale comunicațiilor sale, indiferent de natura lor, e-mail, Skype, VoIP[2]. În concret, distincția nu constă în caracterul continuu al supravegherii tehnice, ci în *natura datelor informatice monitorizate*. Dacă datele informatice constituie *date conținut* care nu se referă la comunicațiile prin sistem informatic, atunci vom fi în cazul unui acces la un sistem informatic, și nu în cazul unei interceptări. Aceasta este situația în care se vor accesa date informatice privind convorbirile anterioare ale persoanei față de care s-a dispus măsura, deoarece nu reprezintă comunicații, acestea fiind lipsite de caracterul lor spontan, nefiind interceptate, ci accesate.

În cazul în care se va utiliza sistemul informatic pentru interceptarea comunicațiilor desfășurate prin acel sistem, considerăm că se va impune autorizarea de către judecătorul de drepturi și libertăți a ambelor măsuri de supraveghere tehnică, interceptarea comunicațiilor ori a oricărui tip de comunicare la distanță și accesul la un sistem informatic. Cu toate acestea, nu vom fi în situația unui procedeu probatoriu mixt, acesta fiind în continuare cel al interceptării comunicațiilor, însă, deoarece se va accesa un sistem informatic pentru realizarea acestuia, considerăm că se impune autorizarea din partea judecătorului de drepturi și libertăți pentru o mai bună protejare a vieții private a persoanei. Această soluție decurge din regimul

[1] *V. infra*, Titlul V, Capitolul IV.4.

[2] A se vedea, în acest sens, *C.S.D. Brown*, Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice, în International Journal of Cyber Criminology (IJCC), vol. 9, no. 1/2015, p. 70.

prevăzut de Codul de procedură penală pentru accesarea datelor informatice, fie prin măsuri de supraveghere tehnică, fie prin percheziție informatică. În acest din urmă caz, Codul de procedură penală impune un regim similar celui al percheziției domiciliare, relevând riscurile deosebite pe care le implică pentru viața privată a persoanei accesarea datelor sale informatice.

Secțiunea a 3-a. Supravegherea video, audio sau prin fotografiere și accesul la un sistem informatic

În mod asemănător cu interceptarea comunicațiilor ori a oricărui tip de comunicare la distanță, în cazul unei supravegheri audio, video sau prin fotografiere, se poate întrebuința un sistem informatic aparținând persoanei față de care s-a dispus supravegherea tehnică.

Având în vedere definițiile celor două măsuri de supraveghere tehnică, precum și specificul acestora, considerăm că, în cazul folosirii sistemului informatic al persoanei față de care s-a luat măsura, prin utilizarea perifericelor sale – cameră și microfon –, se va realiza o supraveghere video, audio sau prin fotografiere, și nu un acces la un sistem informatic. Această concluzie decurge din aceea că definiția celei din urmă măsuri de supraveghere tehnică nu limitează supravegherea video, audio sau prin fotografiere la utilizarea unor dispozitive specifice – tehnică operativă –, decât în situațiile în care aceasta va fi instalată de către organele însărcinate cu efectuarea supravegherii tehnice. Ca atare, nu excludem posibilitatea de a se folosi însuși sistemul informatic al persoanei față de care s-a luat măsura, prin instalarea unor programe specifice care să activeze microfonul și camera încorporată a sistemului informatic. Însă subliniem faptul că, pentru activitatea de instalare a programelor informatice necesare realizării unei supravegheri video, audio sau prin fotografiere prin intermediul unui sistem informatic, va fi necesară pătrunderea în sistemul informatic și modificarea unor date informatice, fiind obligatorie încuviințarea separată și a măsurii accesului la un sistem informatic.

O împrejurare demnă de menționat este faptul că, în cazul supravegherii video, audio sau prin fotografiere, este necesară pătrunderea în sistemul informatic de la distanță sau atunci când acesta se află într-un spațiu public (de pildă, un laptop lăsat într-o cafenea timp de câteva minute). Acest lucru se deduce din interpretarea dispozițiilor art. 140 alin. (5) lit. h) C.pr.pen., în care se impune ca judecătorul de drepturi și libertăți să încuviințeze organele de urmărire penală să pătrundă în spații private pentru a activa sau dezactiva tehnica operativă în cazul unei supravegheri video, audio sau prin fotografiere, însă textul de lege nu face referire decât la dispozitivele proprii ale acestora, nu și la utilizarea sistemului informatic al persoanei vizate.

În același timp, distincția fundamentală dintre supravegherea video, audio sau prin fotografiere și accesul la un sistem informatic este reprezentată de natura probelor care urmează a fi obținute: în primul caz, este vorba de înregistrări video sau audio, iar, în al doilea caz, este vorba de *date informatice conținut*. Considerăm că organul de urmărire penală nu va fi îndreptățit să pătrundă într-un sistem informatic, să instaleze programe specifice pentru supravegherea video, audio sau prin fotografiere folosindu-se de sistemul informatic, fără să i se fi încuviințat accesul la un sistem informatic. Această nevoie decurge din faptul că nu va fi îndreptățit să acceseze și datele informatice conținut, precum și să realizeze copii după acestea, decât în situația în care s-a încuviințat și accesul la un sistem informatic ca măsură de supraveghere tehnică. Or, prin instalarea unui program care să permită supravegherea video și audio, se fac modificări *datelor informatice conținut* din sistemul informatic.

De exemplu, se va accesa la distanță un sistem informatic constând în laptopul persoanei care va face obiectul mandatului de supraveghere tehnică și se va instala un program care va permite controlarea de la distanță atât a microfonului, cât și a camerei video încorporate a laptopului, permițând declanșarea acestora de la distanță. Odată efectuată comanda, acestea vor înregistra audio și video în mod continuu și vor încărca fișierele obținute într-un sistem informatic aparținând organelor de urmărire penală, fără ca utilizatorul laptopului să remarce acest lucru. Același exemplu poate fi modificat pentru a fi incident în cazul unui telefon mobil modern – smartphone –, care, așa cum am arătat deja, constituie un sistem informatic în sensul legii.

De lege ferenda, considerăm că toate operațiunile care presupun pătrunderea într-un sistem informatic pentru interceptarea comunicațiilor ori pentru realizarea de supravegheri video, audio sau prin fotografiere, prin mijlocirea sistemului informatic, ar trebui să fie incluse în măsura de supraveghere a accesului la un sistem informatic.

Secțiunea a 4-a. Percheziția informatică și accesul la un sistem informatic

Procedeul probatoriu care are cele mai multe elemente comune cu accesul la un sistem informatic este percheziția informatică, reglementată de art. 168 C.pr.pen., atât prin natura operațiunilor care se efectuează, cât și din punctul de vedere al obiectului asupra căruia se realizează procedeul.

Considerăm că percheziția informatică va fi procedeul probatoriu care se va impune ca regulă în cursul urmăririi penale, în locul accesului la un sistem informatic, deoarece prezintă mai multe garanții atât pentru respectarea vieții private a persoanei, cât și pentru eficacitatea procedeului probatoriu și a reducerii posibilității de a obține date informatice care să nu îndeplinească condițiile probei într-un proces penal sub aspectul legalității și loialității obținerii lor.

Un prim element de distincție este cel privitor la natura procedeului probatoriu: accesul la un sistem informatic este o metodă specială de supraveghere, iar percheziția informatică este un procedeu probatoriu obișnuit. Una dintre consecințele acestei naturi este posibilitatea persoanei față de care s-a dispus accesul la un sistem informatic ori percheziția informatică de a participa la efectuarea actului, acesta neavând un caracter secret. În cazul accesului la un sistem informatic, operațiunea se va desfășura în secret, trebuind să se evite lăsarea de indicii care să permită persoanei vizate să sesizeze că s-a realizat un acces la un sistem informatic, în schimb, în cazul percheziției informatice, va fi obligatoriu, conform art. 168 alin. (11) C.pr.pen., ca procedura să se efectueze în prezența suspectului sau a inculpatului, în măsura în care aceste persoane sunt cunoscute. Așa cum s-a arătat în doctrină[1], prevederile Codului de procedură penală sunt lacunare raportat la prezența persoanelor care dețin sistemele informatice ori au alte calități în procesul penal (persoane vătămate, părți civile, terțe persoane), însă care vor avea un interes legitim în a participa la această operațiune. De exemplu, în cazul percheziției informatice asupra unui server aparținând unei societăți comerciale, reprezentantul acesteia nu va putea să se asigure care date informatice sunt extrase din sistem, în cazul în care numai o parte dintre acestea aparțin făptuitorului din cauză. Sub acest aspect, din perspectiva altor

[1] *G. Zlati*, Percheziția sistemelor informatice și a mijloacelor de stocare a datelor informatice (II), în Caiete de Drept Penal nr. 4/2014, p. 87.

persoane decât suspectul și inculpatul, percheziția informatică nu asigură mai multe garanții, în afara accesului la un sistem informatic. În același timp, această lacună creează impedimente în realizarea percheziției informatice[1], prin aceea că pot exista obstacole de securitate – parole, chei de securitate – care să împiedice accesarea datelor, însă ar putea fi uneori furnizate de persoana vătămată.

Faza procesuală în care se va dispune efectuarea accesului la sistemul informatic va fi întotdeauna cea a urmăririi penale, în schimb, legea procesuală penală admite ca percheziția informatică să se realizeze și în cursul judecății, din dispoziția instanței. În toate cazurile, procedura de efectuare a percheziției informatice va fi aceeași. Cu toate acestea, nu putem fi de acord cu o percheziție informatică efectuată în cursul judecății raportat la specificul unui asemenea procedeu probatoriu, care implică nu numai descoperirea unor obiecte și ridicarea lor dintr-un spațiu privat (cum este cazul percheziției domiciliare), ci și interpretarea datelor informatice conținute de sistemul informatic. Această din urmă operațiune ar trebui, *de lege ferenda*, să se desfășoare sub controlul direct al instanței, și nu sub controlul procurorului, care, prin acest procedeu probatoriu, poate efectua o continuare a administrării probelor asemenea unei urmăriri penale. În baza principiului nemijlocirii în cursul judecății, considerăm că percheziția informatică propriu-zisă (care este efectuată după obținerea copiilor) ar trebui să aibă loc în fața instanței, și nu în fața unui organ de urmărire penală, iar instanța să efectueze ea însăși aceste acte cu ajutorul propriilor specialiști[2]. Ca atare, considerăm că se impune modificarea textului de lege ca, în privința administrării probei în cursul judecății, rolul procurorului să fie limitat la cel de a asigura obținerea datelor informatice prin copierea lor, nu și realizarea propriu-zisă a percheziției informatice.

În cursul urmăririi penale, judecătorul de drepturi și libertăți dispune efectuarea unei percheziții informatice, la cererea motivată a procurorului, atunci când, pentru descoperirea și strângerea probelor, este necesară cercetarea unui sistem informatic sau a unui suport de stocare a datelor informatice. Cererea care va învesti judecătorul de drepturi și libertăți trebuie să fie însoțită de dosarul cauzei.

Pentru a se dispune efectuarea unei percheziții informatice, este necesară doar începerea urmăririi penale *in rem*, nu și efectuarea în continuare a urmăririi penale față de suspect. Cu toate acestea, considerăm că dispozițiile art. 305 alin. (3) C.pr.pen. impun o obligație a procurorului în a dispune efectuarea în continuare a urmăririi penale față de suspect, și nu posibilitatea de a face acest lucru. În situația în care, deși există date sau probe din care rezultă că o anumită persoană a săvârșit fapta pentru care s-a început urmărirea penală, iar procurorul nu a dispus începerea urmăririi penale *in personam*, considerăm că această nelegalitate nu va putea antrena respingerea cererii de efectuare a percheziției domiciliare. Această concluzie rezultă din aceea că judecătorul de drepturi și libertăți nu este chemat să cenzureze omisiunea procurorului, ci să încuviințeze procedeul probatoriu în baza condițiilor prevăzute de art. 168 alin. (2) C.pr.pen. Cu toate acestea, în procedura camerei preliminare se va putea constata nulitatea relativă a încheierii prin care s-a dispus percheziția informatică și se va putea dispune excluderea probelor obținute, în cazul în care se va putea justifica o vătămare ca urmare a încălcării dreptului la apărare.

[1] *Ibidem*.

[2] Pe care, de altfel, sistemul judiciar îi are, raportat la informatizarea instanțelor, care este din ce în ce mai extinsă. Acești specialiști ai instanței, informaticienii, sunt folosiți deseori în realizarea audierii unor martori protejați sau a audierii prin videoconferință a persoanei aflate în detenție, astfel că aceștia contribuie în mod necesar la realizarea unor acte în timpul judecății, chiar dacă nu sunt nominalizați de Codul de procedură penală.

Spre deosebire de accesul la un sistem informatic, judecătorul de drepturi și libertăți nu va cuprinde în încheierea prin care va dispune perchiziția informatică și punctul de acces la sistemul informatic. Acest lucru decurge din faptul că sistemul informatic nu va putea fi percheziționat la distanță, astfel că nu se va recurge la folosirea vreunui punct de acces.

Spre deosebire de accesul la un sistem informatic, percheziția informatică va avea caracter *static*, deoarece va surprinde numai datele informatice existente la un moment dat, or, accesul la un sistem informatic permite monitorizarea tehnică a activităților pe care le desfășoară făptuitorul pe o perioadă mai întinsă de timp. Este permis și accesul multiplu la același sistem informatic, spre deosebire de percheziția informatică care nu presupune întreruperi[1].

Un mare avantaj al folosirii percheziției informatice este posibilitatea extinderii acesteia către alte sisteme ori alți suporți de stocare decât cei față de care s-a dispus inițial procedeul probatoriu. Conform art. 168 alin. (8) C.pr.pen., procurorul poate dispune de îndată conservarea, copierea datelor informatice de pe alte sisteme informatice ori suporți de stocare, solicitând completarea de îndată a mandatului de percheziție informatică. Această prevedere nu se regăsește în cazul accesului la un sistem informatic, deși, în opinia noastră, era important ca legiuitorul să o prevadă, mai ales în această situație. Cu toate acestea, procurorul se va putea folosi de procedura autorizării supravegherii tehnice prevăzută de art. 141 C.pr.pen. în situația dată, cu respectarea dispozițiilor legale.

În cazul în care judecătorul de drepturi și libertăți va respinge completarea mandatului de percheziție informatică, vom fi în cazul unei lacune legislative, deoarece nu se prevede ce se va întâmpla cu datele și probele obținute, având în vedere că operațiunile de copiere și conservare s-au realizat mai înainte de formularea cererii de completare a mandatului. În opinia noastră, considerăm că procurorul nu va putea îndeplini toate operațiunile specifice unei percheziții informatice, ci numai a conservării și copierii datelor, fără a se realiza accesarea lor, fiind obligat să aștepte soluția judecătorului de drepturi și libertăți. În cazul în care judecătorul de drepturi și libertăți va respinge completarea mandatului, considerăm că se va impune distrugerea copiilor efectuate de procuror, chiar și în lipsa unei prevederi legale, în mod identic cu situația în care se infirmă măsurile de supraveghere tehnică autorizate de procuror în cursul urmăririi penale.

O diferență deosebit de importantă o constituie starea în care se află sistemul informatic în cazul accesului la un sistem informatic și în cazul percheziției informatice. Raportat la necesitatea asigurării integrității datelor informatice stocate pe obiectele ridicate, procurorul va dispune, conform art. 168 alin. (9) C.pr.pen., realizarea de copii. Aceste copii vor trebui să fie copii fizice, și nu copii logice[2], astfel că nu va fi suficientă copierea doar a datelor logice, în sensul de fișiere, ci va trebui să se realizeze o clonă identică la nivel fizic cu suportul de stocare al sistemului informatic, inclusiv a blocurilor de date șterse prin copiere bit-cu-bit. Vom avea în vedere două integrități: a sistemului informatic țintă, care trebuie menținută, și a copiilor obținute din copierea datelor sistemului informatic. În cazul unei percheziții informatice, ambele integrități trebuie conservate, pe când, în cazul accesului la sistemul informatic, nu se va impune menținerea integrității datelor de pe sistemul țintă, acestea putând fi modificate prin accesare. Totuși, trebuie exercitată o maximă prudență în această situație, pentru a se conserva cât mai bine atributele fișierelor (în special ultima accesare a sa).

[1] *G. Zlati*, Percheziția sistemelor informatice și a mijloacelor de stocare a datelor informatice (I), în Caiete de Drept Penal nr. 3/2014, p. 24.

[2] *Ibidem*, p. 31.

Capitolul V
Concluzii

Cu toate că reglementarea măsurii de supraveghere tehnică a accesului la un sistem informatic este deficitară, fiind lipsită de claritate și de un suport legal expres, care să înlăture confuzia în aplicarea acesteia, considerăm că poate avea un rol important în viitor, mai ales în situațiile în care apelarea la procedeul probatoriu al percheziției informatice îngreunează sau face imposibilă descoperirea făptuitorilor și strângerea de probe în vederea tragerii lor la răspundere penală.

Accesul la un sistem informatic este, în prezent, singurul mijloc legal de a obține probe aflate pe un sistem informatic la distanță, mai ales atunci când acesta este un server de e-mail sau un serviciu de rețea de socializare. Având în vedere că acestea din urmă sunt adeseori publice, *de lege ferenda*, se impune accesul la un sistem informatic care să constituie o măsură de supraveghere tehnică numai în situația în care datele accesate nu sunt publice ori se va dori pătrunderea ofensivă într-un sistem informatic pentru a suprima accesul la date informatice ori pentru a le îndepărta.

Existența acestei măsuri de supraveghere tehnică este impusă de necesitatea prevenirii și pedepsirii infracțiunilor care se comit prin intermediul unui sistem informatic. Un prim pas este lărgirea posibilității folosirii acestei măsuri de supraveghere tehnică în cazul în care infracțiunea urmărită (sau a cărei săvârșire se pregătește) se realizează prin intermediul unui sistem informatic.

În concluzie, accesul la un sistem informatic, în modalitatea în care este reglementat la acest moment, creează confuzii în aplicarea acestuia, care se impun a fi remediate de către legiuitor, în condițiile în care utilitatea sa și avantajele față de alte procedee probatorii sunt de netăgăduit. Cu toate acestea, având în vedere tendințele de evoluție a societății, se impune cunoașterea cât mai bună a acesteia, în vederea înțelegerii riscurilor pe care folosirea măsurii antemenționate le prezintă în privința respectării drepturilor și libertăților persoanei.

Titlul VI
Supravegherea video, audio sau prin fotografiere

Capitolul I
Aspecte generale

Secțiunea 1. Utilitatea metodei speciale de supraveghere

Supravegherea unei persoane constituie o tehnică specială de investigare folosită de mult timp în activitatea de informații, fiind cunoscută și sub denumirea de „spionaj", constând într-o metodă de culegere de informații, prin supravegherea acțiunilor altora (de obicei, inamici), în vederea lărgirii cunoașterii despre persoana care este spionată[1]. În contextul culegerii de informații, supravegherea este cunoscută încă din vremuri antice și folosită în prezent ca o metodă esențială de a afla mișcările sau acțiunile unei persoane sau organizații vizate. În sens larg, supravegherea nu înseamnă numai o metodă folosită de un stat, dar constă și într-o metodă de culegere de informații pentru organizații criminale care vor pândi o locație pentru a determina dacă se pot comite fapte penale[2] (de pildă, furturi din locuințe) sau chiar în vederea organizării unor atentate teroriste[3]. Alături de toate aceste scopuri, supravegherea poate fi folosită și pentru prevenirea sau sancționarea unor infracțiuni, fiind prevăzută de legiuitor ca o formă de supraveghere tehnică prin care se pot strânge probe în procesul penal.

Supravegherea video, audio sau prin fotografiere constituie o tehnică specială de supraveghere complexă[4] prin care organele de urmărire penală sunt abilitate să realizeze înregistrări ale unei persoane, constând atât în înregistrări de imagine (video și fotografii), cât și de sunet (înregistrări audio), în vederea obținerii de probe în procesul penal.

În general, termenul de „supraveghere" este folosit pentru tehnici care urmăresc scopuri variate, între care: obținerea de probe pentru dovedirea săvârșirii unei infracțiuni sau a unei fapte ilicite; obținerea de informații detaliate despre activitățile țintă (descoperirea persoanelor implicate, a rutinelor sau obiceiurilor acestora); verificarea informațiilor furnizate de informatori sau pentru a strânge informații asupra unor versiuni de urmărire penală; cunoașterea în permanență a mișcărilor și localizării unei persoane, pentru a strânge probe în vederea obținerii unei mărturisiri cu ocazia audierii persoanei acuzate (prezentarea unor înregistrări video sau audio în cursul audierii poate contribui la obținerea unei declarații de recunoaștere); localizarea unor persoane prin intermediul supravegherii locurilor des frecventate sau a persoanelor cu care se asociază; obținerea de informații necesare pentru a solicita un mandat de percheziție

[1] *R. Kirchner, Jr.*, Surveillance and Threat Detection: Prevention versus Mitigation, Ed. Elsevier, Woburn, 2014, p. 19.

[2] *Ibidem*, p. 89.

[3] *Ibidem*, p. 97.

[4] *Gh. Mateuț*, Procedură penală, 2019, p. 675.

domiciliară; obținerea de probe într-o cauză civilă; identificarea unor persoane[1]. În mod evident, aceste scopuri se vor restrânge în aplicare numai la cele care sunt relevante față de metoda specială de supraveghere tehnică a supravegherii video, audio sau prin fotografiere pe care noi o analizăm în prezenta lucrare.

Ca orice măsură de supraveghere tehnică, aceasta va avea un caracter tehnic, ceea ce semnifică utilizarea unor dispozitive apte și necesare pentru realizarea scopului măsurii. S-a susținut că supravegherea ar include monitorizarea, observarea, ascultarea persoanelor, a mișcărilor acestora, a conversațiilor acestora și a oricăror alte activități sau comunicații și poate privi înregistrarea acestor activități sau folosirea unui dispozitiv de supraveghere pentru realizarea, în tot sau în parte, a activității de supraveghere[2].

Relevanța acestei metode speciale de supraveghere ca procedeu probatoriu este una deosebită, întrucât permite obținerea de probe directe în procesul penal, putând contribui determinant la tragerea la răspundere penală a infractorilor. Lesne poate fi înțeles că o supraveghere video, audio sau audiovideo poate surprinde momentul săvârșirii infracțiunii, fiind probă suficientă pentru a se dovedi existența infracțiunii (directă și determinantă), constituind și o probă foarte greu de combătut pentru apărare. Metoda de supraveghere tehnică va putea fi utilizată și pentru obținerea de probe indirecte în procesul penal, în special când este folosită pentru a observa și înregistra mișcările și activitățile unei persoane.

Dintre metodele speciale de supraveghere, credem că supravegherea video, audio sau prin fotografiere este aptă să producă cea mai gravă ingerință drepturilor fundamentale ale persoanei față de care se ia măsura, restrângându-i dreptul la viață privată, dreptul la domiciliu și libertatea de conștiință. Dacă în cazul altor metode speciale, ele vor conduce la obținerea de probe numai în situația în care persoana realizează anumite activități, precum folosirea unui sistem informatic sau realizarea de apeluri telefonice, această metodă de supraveghere va putea surprinde întreaga viață a persoanei, până la cele mai mici detalii. Vor putea fi cunoscute toate interacțiunile sale, până la cele mai intime posibile, afectând grav viața sa privată. Dreptul său la domiciliu va fi afectat atunci când prin supraveghere se urmărește captarea și înregistrarea activităților sale domestice, sens în care, după cum vom vedea, legiuitorul a stabilit limite mai restrânse pentru realizarea supravegherii. Chiar și libertatea de conștiință va fi afectată, întrucât vor putea fi observate și înregistrate toate nemulțumirile, credințele și opiniile unei persoane, mai ales cele pe care nu și le-ar exprima public, dar le poate expune atunci când este singur în locuința sa.

Din punct de vedere legal, necesitatea reglementării unei astfel de măsuri de supraveghere tehnică era necesară pentru a justifica ingerința care poate fi adusă dreptului la viață privată al persoanei supuse măsurii. Lipsa unei atare prevederi, dată fiind utilitatea supravegherii în unele cauze, ar fi constituit o ingerință nelegală în viața privată a unei persoane prin raportare la art. 8 par. 2 Conv.EDO. Asemenea lipsuri au fost constatate în repetate rânduri de către Curtea Europeană a Drepturilor Omului, atunci când autoritățile din domeniul judiciar au procedat la folosirea supravegherii video, audio sau prin fotografiere (ori măsuri echivalente) fără ca măsura să fie prevăzută expres de lege. În cauza *Govell c. Marea Britanie*, Curtea[3] a constatat că supravegherea s-a desfășurat prin încălcarea dreptului la viață privată, întrucât legislația nu prevedea dispoziții privind autorizarea unei astfel de măsuri, existând numai ghiduri

[1] *P. Jenkins*, op. cit., pp. 4-5.

[2] *S. McKay*, Covert Policing, 2015, p. 157.

[3] CEDO, cauza *Govell c. Marea Britanie*, Hotărârea din 14 ianuarie 1998, §62, pe *hudoc.echr.coe.int*

polițienești ale Home Office care nu erau obligatorii și nici opozabile *erga omnes*. Ulterior, în cauza *Khan c. Marea Britanie*[1], Curtea a constatat că în cauza *Govell c. Marea Britanie* nu numai că nu exista un cadru legal pentru supraveghere, dar acest cadru legal trebuia să fie în concordanță cu statul de drept, pentru a-i oferi o protecție contra arbitrariului prin caracterul previzibil și clar al legii, astfel ca, pentru acuzat, ingerința în viața sa privată să fie una previzibilă dacă s-ar deda la activități infracționale. Această lipsă a unei prevederi legale privind realizarea supravegherii tehnice a fost constatată de către Curte și în cauza *Allan c. Marea Britanie*[2] în care s-a demonstrat că supravegherea a avut loc în locul de detenție al persoanei acuzate de săvârșirea infracțiunii de omor, în timp ce acesta discuta cu o un vizitator, precum și în timp ce discuta cu o altă persoană arestată.

Secțiunea a 2-a. Supravegherea video, audio sau prin fotografiere înainte de intrarea în vigoare a Codului de procedură penală

Metoda specială de supraveghere tehnică a supravegherii video, audio sau prin fotografiere nu constituie o noutate pentru procesul penal român, posibilitatea folosirii acesteia existând și în cuprinsul Codului de procedură penală anterior, în care era prevăzută alături de localizarea prin GPS. De altfel, era o metodă de supraveghere folosită regulat în cercetarea cazurilor de corupție sau în orice alte cazuri în care se impunea realizarea unui flagrant.

Potrivit art. 91^4 C.pr.pen. anterior, „*dispozițiile art. 91^1-91^3 se aplică în mod corespunzător și în cazul înregistrărilor în mediul ambiental, localizării sau urmăririi prin GPS ori prin alte mijloace electronice de supraveghere*". Ca atare, se prevedea ca, în cazul înregistrărilor ambientale, să se autorizeze măsura în condițiile în care se puteau autoriza și interceptările și înregistrările telefonice sau prin orice alt mijloc electronic de comunicare, sens în care facem trimitere la explicațiile date într-o secțiune anterioară[3].

Expresia folosită de legiuitor era „înregistrări în mediu ambiental", desemnând faptul că nu era posibil ca supravegherea tehnică să se realizeze doar prin observarea unei persoane, impunându-se, în toate cazurile, înregistrarea. Nu se făcea nicio trimitere cu privire la felul înregistrărilor care puteau fi făcute. Sub acest aspect, Codul de procedură penală actual este superior, întrucât presupune posibilitatea de a realiza atât înregistrări video, cât și înregistrări audiovideo, doar audio sau realizarea de fotografii. Modificarea nu deschide noi posibilități în privința felului înregistrărilor, cu excepția fotografiilor, dar permite judecătorului de drepturi și libertăți să limiteze ingerința adusă vieții private a unei persoane prin indicarea în mandatul de supraveghere tehnică a tipului de înregistrare permis. În mod neîndoielnic, o înregistrare audio va fi mai puțin vătămătoare ca una audiovideo, mai ales dacă se realizează în spații private, întrucât nu vor putea fi înregistrate activitățile și mișcările unei persoane, ci vor putea fi surprinse numai conversațiile purtate. Sub aspectul proporționalității, judecătorul de drepturi și libertăți va trebui să cântărească dacă, față de particularitățile cauzei, se impune un tip de supraveghere mai intruziv, precum supravegherea audiovideo, sau este suficientă și numai o înregistrare audio sau chiar fotografierea.

[1] CEDO, cauza *Khan c. Marea Britanie*, Hotărârea din 4 octombrie 2000, §26, pe *hudoc.echr.coe.int*
[2] CEDO, cauza *Allan c. Marea Britanie*, Hotărârea din 5 februarie 2003, §35, *hudoc.echr.coe.int*
[3] *V. supra*, Titlul IV, Capitolul I.2.

Față de legislația actuală, legislația procesuală penală anterioară nu includea nicio mențiune cu privire la posibilitatea autorizării înregistrărilor în mediu ambiental în spații private, existând lipsuri grave ale legislației în această privință, întrucât absența unei mențiuni exprese nu ar fi permis, în mod legal, pătrunderea în spații private, precum locuința unei persoane, pentru a fi instalate și dezinstalate dispozitive de supraveghere. Afirmăm acest lucru privind retrospectiv aspectul menționat, nelegalitatea fiind văzută prin prisma existenței unei ingerințe suplimentare față de măsura de supraveghere, ceea ce ar fi impus o autorizare suplimentară. În plus, lipsa mențiunii din Codul de procedură penală anterior afecta previzibilitatea legii, sub acest aspect legislația fiind în dezacord cu art. 8 Conv.EDO, ingerința adusă prin pătrunderea în spații private și instalarea de dispozitive tehnice de supraveghere nefiind prevăzută de lege[1].

Secțiunea a 3-a. Forma actuală a supravegherii video, audio sau prin fotografiere

În prezent, supravegherea video, audio sau prin fotografiere constituie o metodă de supraveghere tehnică, amintită expres în cuprinsul art. 138 alin. (13) C.pr.pen. Fiind o astfel de metodă, va prelua toate caracteristicile supravegherii tehnice cu privire la condițiile legale de autorizare, procedura autorizării și punerea în executare a măsurii. Întrucât face parte din supravegherea tehnică, folosirea acestei metode speciale va conduce la obținerea de probe în procesul penal.

Dincolo de definiția legală, este de necontestat caracterul de metodă de supraveghere tehnică al acestei măsuri, întrucât reprezintă un procedeu probatoriu prin care sunt restrânse drepturile fundamentale ale persoanei supuse măsurii, se desfășoară în secret, are un caracter numai pentru viitor, se poate dispune numai în cursul urmăririi penale și autorizarea ei se va face de judecătorul de drepturi și libertăți în condițiile legii.

Față de reglementarea actuală, a fost introdusă posibilitatea fotografierii activităților desfășurate de persoana supusă măsurii, o atare posibilitate nefiind prevăzută expres în legislația procesuală penală anterioară.

Conform art. 138 alin. (6) C.pr.pen., „*prin «supraveghere video, audio sau prin fotografiere» se înțelege fotografierea persoanelor, observarea sau înregistrarea conversațiilor, mișcărilor ori a altor activități ale acestora*".

Fotografierea constituie o modalitate nouă de realizare a supravegherii tehnice, fiind introdusă expres pentru prima dată în actualul Cod de procedură penală. În ceea ce ne privește, apreciem că fotografierea va fi incidentă atunci când se va desfășura un filaj al unei persoanei, consemnându-se mișcările acesteia și surprinzându-se fotografic momentele în care realizează acțiuni relevante pentru cauză. Deși înregistrările video par a fi mai utile unei cauze, legiuitorul a prevăzut fotografierea și din considerente tehnice, întrucât nu se va putea proceda la realizarea de înregistrări video decât dacă persoana se află la o distanță considerabilă de organele de cercetare penală care pun în executare măsura. Oricum, la distanță, sunetul nu se va propaga suficient de mult încât să poată fi captat eficient, mai ales într-un mediu zgomotos, acțiunile persoanei putând fi surprinse suficient de bine cu un aparat foto.

Echipamentele video care pot fi folosite în înregistrări ambientale vor avea dimensiuni reduse pentru a nu fi detectate, ceea ce le limitează performanțele optice și nu permit mărirea

[1] CEDO, cauza *Khan c. Marea Britanie*, Hotărârea din 4 octombrie 2000, §27.

imaginii. Acest neajuns este unul fizic, neputând fi depășit decât prin întrebuințarea unor obiective de dimensiuni ridicate[1], care ar putea fi detectate de o persoană aflată în apropriere, mai ales în situația în care sunt îndreptate față de acestea de la mică distanță. Însă, folosite dintr-o mașină cu geamuri întunecate și de la distanțe mari, fotografierea constituie o alternativă bună la înregistrările video. Fotografierea are și avantajul că va produce rezultate de o calitate superioară, ca urmare a faptului că un senzor de cameră foto nu este ținut de formatele clasice video (HD, FullHD, 4k etc.). Consecința este că o fotografie va putea fi mărită și își va păstra calitatea, surprinzând mai multe detalii, iar o filmare nu (sau cel puțin nu într-o asemenea măsură). Din punct de vedere tehnic, o fotografie făcută cu un aparat foto bun, de generație recentă, va avea o rezoluție de 4000×6000 de pixeli, adică 24 de megapixeli, iar o cameră video care înregistrează în format 4k va avea o rezoluție de numai 4096×2160 de pixeli, adică aproximativ 10 megapixeli. Este lesne de înțeles că rezoluția crescută a unei fotografii va permite mărirea acesteia.

Chiar și de la distanță redusă, o persoană cu un aparat foto (mai modest, în astfel de situații) nu va atrage atâtea suspiciuni, putând să fie deghizată ca un turist care realizează fotografii partenerei, pentru ca în fundal să surprindă persoana vizată.

Fotografierea unei persoane va reprezenta o alternativă de succes pentru dovedirea împrejurării că o persoană se afla într-un anumit loc la un anumit moment, putând constitui o probă indirectă în procesul penal. Chiar dacă există mijloace de localizare precisă, acestea fie nu sunt apte pentru a fi folosite în interiorul unei clădiri (de exemplu, un complex comercial), fie presupun instalarea de dispozitive dinainte (ceea ce nu este fezabil tot timpul), putând fi suficientă o fotografie cu persoana în respectivul loc.

Observarea constituie o modalitate de realizare a supravegherii video, audio sau prin fotografiere, care prezintă o problematică specifică privind caracterul tehnic al metodei speciale. În sinea ei, expresia „observarea conversațiilor, mișcărilor sau activităților unei persoane" nu ar presupune nevoia unor mijloace tehnice care să permită desfășurarea supravegherii tehnice, ceea ce ar însemna că în această categorie ar intra și filajul, dacă este desfășurat fără înregistrarea video, audio sau prin fotografiere. Într-o opinie se arată că reprezintă o condiție esențială a metodei speciale de supraveghere folosirea unui dispozitiv tehnic în scopul realizării supravegherii[2]. Într-o altă opinie, cu care nu suntem de acord, se susține că „*supravegherea care nu se materializează într-o înregistrare audiovideo nu presupune o procedură specială de autorizare, legiuitorul considerând că ingerința adusă vieții private într-un asemenea caz are un caracter minim și nu justifică reglementarea unor garanții speciale*"[3]. Autorul din urmă citat nu are în vedere că legiuitorul a cuprins și modalitatea observării ca alternativă la înregistrare în cuprinsul dispozițiilor art. 138 alin. (6) C.pr.pen. Textul folosit de legiuitor va trebui să fie interpretat într-un alt sens, cel în care, deși nu se realizează o înregistrare, va exista **o acțiune de observare a persoanei desfășurată prin mijloace tehnice**, și nu prin propriile simțuri, astfel că observarea – chiar și sistematică – realizată prin filaj nu va intra în cuprinsul metodei speciale de supraveghere tehnică, întrucât nu se va realiza prin mijloace tehnice decât în cazul în care se și înregistrează. Observarea va putea fi utilizată în situații precum monitorizarea

[1] Un obiectiv apt pentru a fi folosit în fotografiere la distanțe mari, utilizat în fotografierea animalelor sălbatice, este Canon EF 100-400 mm f/4.5-5.6 L IS II USM, dezavantajul fiind dimensiunea sa de 28 cm lungime. La aceasta se va adăuga și aparatul foto, astfel că e lesne de înțeles că o persoană cu un asemenea aparat va ridica suspiciuni.

[2] *Gh. Mateuț*, Procedură penală, 2019, p. 675.

[3] *M. Bulancea, R. Slăvoiu*, în M. Udroiu (coord.), Codul de procedură penală, 2017, pp. 651-652.

spațiilor private, în care există riscul desfășurării unor activități ale persoanei care nu au legătură cu obiectul cauzei. Este lesne de înțeles că în asemenea circumstanțe este preferabil ca persoana supravegheată să nu fie și înregistrată dacă activitățile nu au legătură cu obiectul cauzei și ar constitui o ingerință maximă adusă vieții private. De pildă, în cazul în care se dispune supravegherea în spații private, precum dormitorul sau cabina de duș a unei persoane, nu va putea exista niciun interes legitim al organelor de urmărire penală de a înregistra toate activitățile care se desfășoară, fiind preferabil ca unele activități să fie doar observate și, dacă sunt surprinse fapte care ar avea legătură cu cauza, numai atunci să se procedeze la înregistrarea lor. Trebuie ținut cont de faptul că legislația procesuală penală nu prevede nicio posibilitate concretă ca o persoană ce a fost supusă măsurii să obțină distrugerea datelor rezultate din măsurile de supraveghere tehnică ce nu au legătură cu cauza, acestea fiind distruse doar la un an de la soluționarea definitivă a cauzei[1]. În tot acest timp, va exista riscul ca aceste înregistrări să poată fi puse la dispoziția subiecților principali, a părților, a organelor de urmărire penală, a instanței etc., simpla lor existență constituind o ingerință la viața privată a unei persoane. Observarea se va putea folosi și pentru surprinderea unor momente tactice, în vederea luării unor măsuri specifice, precum organizarea flagrantului. O atare situație poate fi incidentă atunci când se vor amplasa camere la intrarea unui depozit unde se așteaptă un transport de droguri (supus livrării supravegheate), putându-se realiza flagrantul atunci când ajung la locație toți presupușii membrii ai grupării organizate.

Înregistrarea constituie modalitatea cea mai reprezentativă pentru supravegherea tehnică prin mijloace video, audio sau prin fotografiere, deoarece va putea releva, după caz, situația de la momentul supravegherii din punct de vedere vizual și/sau auditiv, putând plasa organul judiciar la momentul realizării acțiunii[2]. Practic, toate sunetele sau imaginile vor fi captate și memorate pe un suport digital (suporții analogici, magnetici fiind deja căzuți în desuetudine), putând fi oricând revăzute de organul de urmărire penală sau de instanță.

Astfel cum vom vedea, înregistrările se împart în mai multe tipuri: video – în care va fi prezentă numai componenta vizuală; audiovideo – în care vom avea atât componentă video, cât și componentă audio; audio – în care se va înregistra numai componenta audio. În funcție de specificul infracțiunii cercetate, se vor implementa cele trei tipuri de înregistrări posibile. De pildă, în cazul unei infracțiuni de luare de mită realizată prin participarea autorizată la anumite activități, va fi utilă autorizarea supravegherii video pentru surprinderea momentului remiterii sumei de bani.

În situația unei înregistrări audiovideo, este necesar ca persoana vizată să fie în relativă apropiere pentru a putea fi surprinsă de mijloacele tehnice specifice, sunetul neputând fi captat decât la o distanță redusă, întrucât va trebui ca dispozitivul care realizează înregistrarea să realizeze simultan și înregistrarea audio.

Înregistrarea audio va putea fi realizată prin microfoane amplasate în mod conspirativ, prin utilizarea unui simplu reportofon în cazul unor conversații desfășurate în public sau cu ajutorul unor microfoane specializate pentru captarea conversațiilor la mare distanță sau care se desfășoară în interiorul unor clădiri.

Alături de modalitățile sub care se poate materializa forma de supraveghere tehnică în discuție, legiuitorul a menționat și ce activități ale persoanei supuse măsurii pot fi înregistrate,

[1] *V. supra*, Titlul III, Capitolul III.4.

[2] *J.R. Spencer*, Hearsay Evidence in Criminal Proceedings, Ed. Hart Publishing, Portland, Oregon, 2008, p. 203.

conform art. 138 alin. (6) C.pr.pen., supravegherea putând viza *conversațiile, mișcările* și *activitățile* persoanelor.

Conversațiile care pot fi supuse măsurii de supraveghere tehnică a supravegherii video, audio sau prin fotografiere sunt cele care vor fi purtate în mod nemijlocit[1], în cazul în care acestea se realizează printr-un mijloc de comunicare la distanță, putând fi incidentă metoda interceptării comunicațiilor.

Mișcările persoanelor pot face obiectul metodei speciale de supraveghere, prin aceasta, persoana care face obiectul măsurii fiind urmărită pentru a se stabili locațiile în care se deplasează și persoanele cu care se întâlnește. Această modalitate a supravegherii se aseamănă cu localizarea sau urmărirea prin mijloace tehnice, întrucât va putea conduce la aflarea localizării persoanei la un anumit moment. În concret, persoana care face obiectul măsurii va fi urmărită de organele de cercetare penală sau de lucrători de poliție, fiindu-i înregistrate mișcările și deplasările ori doar observate prin mijloace tehnice. O atare supraveghere se poate realiza în mod facil în acele comunități care au instalate camere de supraveghere publice. În cazul unui oraș precum Cluj-Napoca, se va putea supraveghea deplasarea unei persoane prin intermediul camerelor folosite de primărie pentru supravegherea în timp real, fără ca organele de cercetare penală să trebuiască să se afle în locația învecinată persoanei supravegheate. În funcție de evoluțiile tehnologice și de implementarea de noi sisteme de supraveghere, mișcările unei persoane vor putea fi urmărite prin camere cu detecție și recunoaștere facială, astfel de sisteme fiind în dezvoltare și implementate experimental în Londra și Moscova.

Credem că, prin „activitățile" persoanelor, legiuitorul a instituit un termen general care să acopere orice activitate a omului, alta decât mișcările și conversațiile purtate de acesta, lăsând posibilitatea ca organele de urmărire penală să supravegheze orice aspect al vieții considerat a fi relevant pentru cauza penală, în condițiile legii.

Secțiunea a 4-a. Noțiunea de „spațiu privat" în contextul metodei speciale de supraveghere

Supravegherea video, audio sau prin fotografiere poate îmbrăca forma supravegherii în spații private, legiuitorul reglementând distinct această ipoteză prin includerea unor limitări în privința procedurii de autorizare. Totodată, în cazul mandatului de supraveghere care are ca obiect această metodă de supraveghere va putea fi încuviințată și activitatea de pătrundere în spațiul privat în vederea activării sau dezactivării mijloacelor tehnice folosite.

În mod justificat s-a arătat că activitatea de supraveghere în spații private reprezintă un atentat grav la respectarea vieții private, ce trebuie exercitat în conformitate cu dispozițiile legale în vederea înlăturării oricăror abuzuri[2]. Jurisprudența Curții Europene a Drepturilor Omului a stabilit că o ascultare a conversațiilor prin intermediul microfoanelor din apartamentul persoanei sau prin sonorizarea apartamentului unui terț frecventat de subiectul mandatului de supraveghere constituie o ingerință gravă la viața privată a unei persoane, mai amplu[3] decât în cazul în care se vor monitoriza numai mișcările persoanei în spații publice prin metode mai puțin invazive, precum localizarea GPS[4].

[1] *Gh. Mateuț*, Procedură penală, 2019, p. 675.

[2] *S. Grădinaru*, Supravegherea tehnică, 2014, p. 247.

[3] CEDO, cauza *Vetter c. Franța*, Hotărârea din 31 august 2005, §26, pe *hudoc.echr.coe.int*

[4] CEDO, cauza *Uzun c. Germania*, Hotărârea din 2 decembrie 2010, §80, pe *hudoc.echr.coe.int*

Deși ingerința ce poate fi adusă vieții private va fi una majoră, legiuitorul nu a definit noțiunea de „spațiu privat" nici în cuprinsul art. 140 alin. (5) lit. h) C.pr.pen., în care se precizează că: „*în cazul măsurii supravegherii video, audio sau prin fotografiere în spații private, mențiunea privind încuviințarea solicitării ca organele de urmărire penală să pătrundă în spații private pentru a activa sau dezactiva mijloacele tehnice ce urmează a fi folosite pentru executarea măsurii supravegherii tehnice*".

Ținând seama de similaritățile cu percheziția domiciliară, concluzionăm că va fi necesară autorizarea expresă a judecătorului de drepturi și libertăți atunci când se va pătrunde în spații care pot fi asimilate noțiunii de „domiciliu", în sensul art. 157 alin. (2) C.pr.pen. Conform acestei dispoziții legale, „*prin «domiciliu» se înțelege o locuință sau orice spațiu delimitat în orice mod ce aparține ori este folosit de o persoană fizică sau juridică*". Definiția pare foarte generală și credem că expune suficient de clar locurile unde își desfășoară o persoană viața privată, reprezentând criteriul real după care trebuie să ne ghidăm în evidențierea unui spațiu privat. De pildă, locul de muncă poate fi considerat un spațiu privat al angajatului în relația cu angajatorul său, întrucât viața privată a unei persoane va include și activitățile sale profesionale[1]. În atare context, delimitarea nu va fi una fizică între angajat și angajator; din perspectiva noastră, aceeași rațiune va trebui să fie avută în vedere și în stabilirea întinderii noțiunii de „spațiu privat" prin raportare la dispozițiile incidente în cazul supravegherii.

Legiuitorul a ales să preia expresia de „spațiu privat" în cadrul supravegherii video, audio sau prin fotografiere în locul termenului de „domiciliu". Considerăm că acest termen este preluat din recomandările Comisiei europene pentru democrație prin drept – Comisia de la Veneția privind supravegherea video. În anul 2007, Comisia de la Veneția a emis două recomandări privind supravegherea video: privind supravegherea video în spații publice realizată de autorități publice și protecția drepturilor omului[2]; privind supravegherea video realizată de operatori privați în spațiul public și privat și de autorități publice în spații private și protecția drepturilor omului[3]. Prin cele două opinii, Comisia de la Veneția a subliniat că supravegherea video constituie o ingerință în viața privată chiar și atunci când se desfășoară în spații publice, fiind necesar să se determine sfera privată a vieții unei persoane. În acest demers, s-a considerat că prin expresia de „sferă privată" sunt avute în vedere spațiile private, precum locuințele, birourile, magazinele, discotecile, cafenelele, restaurantele, unde proprietarul, clientul sau cel care deține licența de funcționare este răspunzător pentru ce se întâmplă[4]. Ca atare, considerăm că expresia „spațiul privat" este mai greu de definit decât termenul de „locuință" folosit de legiuitor, presupunând ca element caracteristic exercitarea unui element din viața privată a unei persoane.

Pentru reglementarea supravegherii în spații private, Comisia de la Veneția a formulat mai multe recomandări, între care: existența unor prevederi legale care să guverneze atât supravegherea în spații private, cât și publice; legiferarea condițiilor legale pentru supraveghere să fie realizată de autorități publice, dar și de entități private în aceste spații; respectarea condițiilor prevăzute de art. 8 Conv.EDO; procesarea, în condițiile legii, a datelor cu caracter personal obținute în urma supravegherii; încunoștințarea persoanelor despre existența unei

[1] CEDO, cauza *Antović și Mirković c. Muntenegru*, Hotărârea din 28 februarie 2017, §59, pe *hudoc.echr.coe.int*

[2] Adoptată în a 70-a Sesiune Plenară a Comisiei de la Veneția, 16-17 martie 2007.

[3] Adoptată în a 71-a Sesiune Plenară a Comisiei de la Veneția, 1-2 iunie 2007.

[4] Comisia de la Veneția, Opinie asupra supravegherii video realizată de operatori privați în spații publice și în sfera privată și de către autorități publice în sfera privată și protejarea drepturilor omului, adoptată în a 71-a Sesiune Plenară a Comisiei de la Veneția, 1-2 iunie 2007, §16, pe *www.venice.coe.int*

supravegheri publice (în afara cazului în care aceasta este evidentă prin montarea vizibilă de camere); încunoștințarea persoanelor care au fost supravegheate despre modul în care datele obținute au fost folosite, cui i-au fost transferate și posibilitatea de a cere să aibă acces la ele și să obțină distrugerea lor, precum și desemnarea unei autorități independente care să verifice respectarea acestor reglementări.

Secțiunea a 5-a. Clasificarea supravegherii video, audio sau prin fotografiere

După locul în care se va desfășura activitatea desfășurată de persoana care face obiectul măsurii, supravegherea va putea fi *publică* sau *în spații private*. Supravegherea publică a unei persoane va viza conversațiile, mișcările și activitățile desfășurate într-un spațiu public, acestea trebuind să fie observate sau înregistrate cu ajutorul mijloacelor tehnice. Cel mai adesea, supravegherea în spații publice se va realiza de lucrători de poliție, care vor urmări persoana supusă măsurii și vor filma sau fotografia mișcările și activitățile sale. *Supravegherea în spații private* va însemna că vor trebui supravegheate conversațiile și activitățile unei persoane în domiciliul acesteia, la locul de muncă, într-o cameră de hotel etc. În aceste situații, nu se poate concepe ca persoana desemnată să pună în executare măsura să fie în aceeași cameră cu persoana vizată, fiind necesară folosirea unor mijloace tehnice, precum microfoane sau camere video ascunse ori disimulate în alte obiecte, dispozitive prin care se pot înregistra sunete prin pereți, camere de termoviziune etc.

În funcție de gradul de continuare a supravegherii, aceasta poate fi clasificată în: *supraveghere secvențială* și *supraveghere continuă*. O *supraveghere secvențială* se va desfășura doar în momentele în care organele care pun în executare măsura aleg să activeze mijloacele tehnice amplasate în locuința persoanei supuse măsurii ori realizează filajul acesteia sau accesează camerele de supraveghere publice pentru a urmări mișcările acesteia. Acest tip de supraveghere permite momente de întrerupere decise de organele de urmărire penală. În schimb, *supravegherea continuă* va presupune că dispozitivele tehnice pentru înregistrarea video și audio vor funcționa fără întrerupere și vor înregistra ambiental tot ce se petrece în locația în care au fost amplasate. Sub acest aspect, nu va avea importanță asupra continuității dacă dispozitivele opresc înregistrarea atunci când nu detectează sunet sau mișcare, aceasta fiind o ipoteză des întâlnită la astfel de dispozitive în vederea economisirii de spațiu de stocare sau a bateriei. Întreruperea se va realiza de dispozitiv, nu de organul de urmărire penală, reluându-se înregistrarea în momentul în care se percepe un sunet peste o anumită intensitate sau dispozitivul observă mișcare.

După natura mijlocului de probă care va rezulta din activitatea de supraveghere tehnică, vom avea: *supraveghere video*, *supraveghere audio* și *supraveghere audiovideo*.

În funcție de procedeul probatoriu care va conduce la obținerea probei, supravegherea tehnică se clasifică în: *supraveghere primară* și *supraveghere derivată*. În cazul unei *supravegheri primare*, aceasta va constitui obiectul mandatului de supraveghere tehnică, realizându-se singură sau în paralel cu alte mijloace de supraveghere tehnică, punerea în executare fiind efectuată de procuror, organe de cercetare penală sau lucrători de poliție, conform art. 142 alin. (1) C.pr.pen. Cu alte cuvinte, măsura va avea un caracter independent față de alte metode speciale de supraveghere sau cercetare.

Supravegherea derivată va fi incidentă atunci când prin aceasta se vor obține mijloace de probă derivate dintr-o altă metodă de investigație. Într-o atare situație, supravegherea va fi o parte integrantă a unei investigații complexe, realizată prin utilizarea investigatorilor sub acoperire, furnizând probe derivate din această metodă specială de cercetare. Altfel spus, măsura va avea un caracter secundar față de metoda specială de cercetare, servind numai pentru obținerea probei în procesul penal. Astfel cum vom vedea în secțiunile ulterioare, prin utilizarea investigatorilor sub acoperire, participarea autorizată la anumite activități și livrarea supravegheată se vor putea obține numai informații, nu și probe în procesul penal, pentru aceasta trebuind să se apeleze la procedee probatorii derivate (supraveghere tehnică, audierea investigatorilor sub acoperire etc.). Punerea în executare se va face de către investigatorii sub acoperire sau colaboratorii autorizați prin ordonanța procurorului, în conformitate cu dispozițiile art. 148 alin. (3) C.pr.pen. care derogă de la art. 142 alin. (1) C.pr.pen.

Capitolul II
Autorizarea supravegherii video, audio sau prin fotografiere

Secțiunea 1. Condiții legale pentru autorizarea supravegherii video, audio sau prin fotografiere

Supravegherea video, audio sau prin fotografiere presupune severa restrângere a drepturilor și libertăților persoanei vizate de acest procedeu probatoriu, motiv pentru care legea condiționează folosirea acestuia numai când sunt îndeplinite anumite condiții și cu garantarea respectării proporționalității între interesul public și interesul persoanei.

Organul competent să dispună asupra folosirii metodei speciale de supraveghere este *judecătorul de drepturi și libertăți*, ca regulă. În mod excepțional, *procurorul*, potrivit art. 141 C.pr.pen., va putea dispune limitat, pentru o durată de maximum 48 de ore și cu controlul ulterior al judecătorului de drepturi și libertăți, supravegherea video, audio sau prin fotografiere.

Metoda specială de supraveghere tehnică se va putea încuviința numai dacă sunt îndeplinite condițiile cumulative prevăzute de art. 139 C.pr.pen. O condiție implicită constă în necesitatea începerii urmăririi penale pentru o faptă prevăzută de legea penală. Această condiție reiese din faptul că începerea urmăririi penale este actul procesual care creează întreg cadrul pentru desfășurarea activităților de urmărire penală, inclusiv administrarea probelor, întrucât Codul de procedură penală actual nu mai recunoaște faza actelor premergătoare din Codul de procedură penală anterior.

Prima condiție de autorizare a acestui procedeu probatoriu este existența unei *suspiciuni rezonabile cu privire la pregătirea sau săvârșirea unei infracțiuni* de o anumită gravitate dintre cele indicate la art. 139 alin. (2) C.pr.pen. Față de cele analizate anterior cu privire la această condiție comună tuturor metodelor speciale de supraveghere, precizăm că nu considerăm că legiuitorul a conferit suficientă atenție caracterului invaziv al supravegherii video, audio sau prin fotografiere, apreciind că se impunea ca această măsură de supraveghere tehnică să poată fi întrebuințată numai în cazul unor infracțiuni grave. Nu credem că era justificată posibilitatea autorizării folosirii măsurii de supraveghere tehnică pentru infracțiuni contra patrimoniului. Totodată, nu credem că se impunea menținerea, în cazul acestei măsuri de supraveghere tehnică, a criteriului subsidiar al aplicării măsurii și unor *infracțiuni pentru care legea prevede pedeapsa închisorii de 5 ani sau mai mare*, aceasta putând include și majoritatea infracțiunilor împotriva siguranței pe drumurile publice, fapte des întâlnite în practică și care nu pot fi considerate de o gravitate deosebită. *De lege ferenda*, se impune ca legiuitorul să prevadă un criteriu subsidiar al pedepsei închisorii de cel puțin 7 ani, alături de eliminarea infracțiunilor contra patrimoniului din categoria infracțiunilor care pot justifica autorizarea măsurii de supraveghere tehnică.

Măsura de supraveghere poate fi întrebuințată numai în cursul urmăririi penale, împrejurare comună cu toate metodele speciale de supraveghere sau cercetare. În cazul în care se realizează o înregistrare privată, respectiv una care să se încadreze în dispozițiile art. 139 alin. (3) C.pr.pen., aceasta se va putea administra, la propunerea participantului care are calitate să facă acest lucru, chiar și în cursul judecății (de pildă, o înregistrare realizată de inculpat privitor la discuțiile sale cu victima prin care se dovedește caracterul mincinos al plângerii penale formulate în cauză).

A doua condiție care se impune a fi îndeplinită pentru autorizarea măsurii de supraveghere este cea privitoare la *proporționalitatea măsurii cu restrângerea drepturilor și libertăților fundamentale*. Această condiție este prevăzută de art. 139 alin. (1) lit. b) C.pr.pen. și se impune a fi analizată de către judecătorul de drepturi și libertăți prin prisma criteriilor prevăzute de textul de lege: *particularitățile cauzei*, *importanța informațiilor ori a probelor ce urmează a fi obținute* sau *gravitatea infracțiunii*. Acest criteriu este cel mai important pentru autorizarea oricărei metode speciale de supraveghere și este cel care trebuie analizat cu cea mai mare seriozitate de către judecătorul de drepturi și libertăți.

Proporționalitatea trebuie analizată prin raportare la gravitatea ingerinței aduse dreptului la viață privată al persoanei, judecătorul de drepturi și libertăți trebuind să constate că nu va exista o disproporție între acțiunile statului și necesitatea apărării dreptului individului. Proporționalitatea este un criteriu complex în care toate subcriteriile sale se află într-o legătură directă, influențându-se reciproc. De pildă, în analiza judecătorului se poate stabili că, prin particularitățile cauzei, o supraveghere video continuă a infractorului va conduce la descoperirea unei infracțiuni de furt și la prevenirea de noi fapte, importanța informațiilor obișnuite va fi deosebită, putând consta în probe directe privind vinovăția, dar gravitatea concretă a faptei nu va justifica folosirea unor metode speciale de supraveghere. În același fel, dacă gravitatea va fi una deosebită, particularitățile cauzei și importanța informațiilor care pot fi obținute ar putea să nu justifice recurgerea la o atare măsură atunci când se supraveghează locuința făptuitorului, în cazul în care acesta nu desfășoară activitățile infracționale la acea locație și nici nu intră în contact cu complicii săi în acea locație.

Prin „particularitățile cauzei" vom înțelege acele împrejurări specifice unei anumite cauze penale care vor impune utilizarea metodelor speciale de supraveghere sau cercetare pentru soluționarea cauzei, deoarece un altfel de procedeu probatoriu nu ar fi propice pentru a stabili starea de fapt. Sub acest aspect, trebuie să fie evaluat modul în care supravegherea poate să furnizeze probe în procesul penal prin prisma modalităților concrete în care se pregătește fapta sau în care a fost săvârșită fapta[1]. Ceea ce se impune a se analiza aici este și natura infracțiunii prin raportare la mijloacele de comitere. Unele infracțiuni pot fi dovedite numai prin anumite metode speciale de supraveghere sau cercetare, iar altele pot fi dovedite prin procedee probatorii obișnuite. În cazul infracțiunilor de corupție, modul în care se realizează luarea de mită poate să determine ca supravegherea video, audio sau prin fotografiere să fie necesară prin raportare la natura infracțiunii și la modul în care se comite, respectiv prin primirea directă a unei sume de bani.

Prin „importanța informațiilor ori a probelor ce urmează a fi obținute" înțelegem contribuția pe care o pot avea informațiile sau probele obținute pentru stabilirea împrejurărilor esențiale ale cauzei. Întrucât supravegherea video, audio sau prin fotografiere poate conduce la obținerea de probe directe în procesul penal, importanța informațiilor obținute va putea fi deosebit de mare. Judecătorul trebuie să găsească un just echilibru, întrucât cu cât este mai invazivă metoda de supraveghere, cu atât este mai capabilă să furnizeze o probă determinantă în procesul penal.

„Gravitatea infracțiunii" presupune o analiză a pericolului social concret pe care îl presupune săvârșirea infracțiunii care face obiectul urmăririi penale. Îndeplinirea acestui criteriu se va stabili de către organele judiciare, printr-un just echilibru între interesul public de

[1] *Gh. Mateuț*, Procedură penală, 2019, p. 681.

a urmări o faptă și restrângerea dreptului la viață privată[1]. Criteriul este unul judiciar și ține de intima convingere a judecătorului dacă se impune încuviințarea supravegherii tehnice, chiar dacă vor fi îndeplinite condițiile prevăzute de art. 139 alin. (2) C.pr.pen., care sunt criterii legale privind gravitatea faptei. În opinia noastră, supravegherea va trebui să fie încuviințată numai dacă faptele sunt de o gravitate mare și, chiar și atunci, judecătorul de drepturi și libertăți va trebui să indice concret metodele de supraveghere pe care le consideră a fi proporționale, unele având un caracter vădit mai invaziv în viața privată a unei persoane. În acest sens, este necesar să se indice dacă se vor realiza înregistrări sau se va proceda numai la observarea persoanei, dacă supravegherea va fi continuă sau secvențială, dacă se vor realiza înregistrări audio, video, audiovideo sau fotografii, dacă se va folosi tactica filajului etc.

A treia condiție impusă de Codul de procedură penală pentru încuviințarea măsurii de cercetare este *necesitatea procedeului probatoriu* pentru obținerea probei. Cu alte cuvinte, condiția se referă la *subsidiaritatea* măsurilor speciale de supraveghere sau cercetare față de orice alt procedeu probatoriu. Această condiție este prevăzută în cuprinsul art. 139 alin. (1) lit. c) C.pr.pen. și restrânge folosirea supravegherii tehnice doar în situația în care „*probele nu ar putea fi obținute în alt mod sau obținerea lor ar presupune dificultăți deosebite ce ar prejudicia ancheta ori există un pericol pentru siguranța persoanelor sau a unor bunuri de valoare*". Această condiție este comună cu celelalte măsuri de supraveghere tehnică și măsura specială de cercetare nu prezintă caracteristici particulare în plus, astfel că facem trimitere la cele expuse mai devreme în prezenta lucrare[2].

Secțiunea a 2-a. Autorizarea supravegherii video, audio sau prin fotografiere în spații publice

Întrucât măsura face parte din supravegherea tehnică, pentru autorizarea măsurii vor fi incidente dispozițiile art. 140 C.pr.pen., sens în care în prezenta secțiune vom face scurte considerații privind particularitățile autorizării supravegherii video, audio sau prin fotografiere în spații publice, urmând ca autorizarea supravegherii în spații private să fie analizată într-o secțiune ulterioară[3].

Pentru a se putea autoriza metoda specială de supraveghere tehnică, este necesar ca procurorul să întocmească o *propunere* în acest sens, în care să fie cuprinse toate elementele legale prevăzute de art. 140 alin. (2) C.pr.pen., pe care să o transmită judecătorului de drepturi și libertăți.

Competența de judecare a propunerii revine judecătorului de drepturi și libertăți din cadrul instanței competente să judece cauza în primă instanță sau din cadrul instanței corespunzătoare în grad acesteia în a cărei circumscripție se află sediul parchetului din care face parte procurorul care a formulat cererea.

Pentru autorizarea supravegherii video, audio sau prin fotografiere de către *judecătorul de drepturi și libertăți* se impune, mai întâi, verificarea de către acest organ judiciar a respectării condițiilor prevăzute de art. 139 C.pr.pen., la care am făcut referire în secțiunea anterioară.

[1] A se vedea, în acest sens, CEDO, cauza *Ibrahim ș.a. c. Marea Britanie*, Hotărârea din 13 septembrie 2016, §274.

[2] *V. supra*, Titlul III, Capitolul I.4.

[3] *V. infra*, Titlul VI, Capitolul II.3.

Această verificare se face pe baza propunerii depuse de către procuror și în urma studierii dosarului cauzei, care va fi înaintat de către procuror împreună cu propunerea de autorizare a măsurii speciale de cercetare. În cuprinsul propunerii, procurorul are obligația de a include toate elementele prevăzute de art. 140 alin. (2) C.pr.pen.[1], trebuind să fie detaliată și sub aspectul modalității concrete de punere în executare a supravegherii video, audio sau prin fotografiere, întrucât indicarea concretă a modului în care va fi pus în executare mandatul va avea implicații asupra proporționalității măsurii[2]. Credem că dacă procurorul va propune măsura de supraveghere tehnică a supravegherii video, audio sau prin fotografiere și nu va indica modalitatea concretă, judecătorul de drepturi și libertăți trebuie să respingă cererea ca fiind nefondată, întrucât o autorizare a acestei măsuri fără nicio limitare va constitui o ingerință disproporționată asupra vieții private a persoanei. Numai în cazuri excepționale vor putea fi admise toate formele de supraveghere video, audio sau prin fotografiere, dar și atunci va trebui motivată necesitatea fiecăreia.

Judecarea propunerii procurorului are loc în aceeași zi cu formularea ei, în camera de consiliu, fără citarea părților și cu prezența obligatorie a procurorului. Soluțiile pe care le poate pronunța judecătorul de drepturi și libertăți sunt fie respingerea cererii, fie admiterea ei.

Respingerea cererii se va dispune conform art. 140 alin. (6) C.pr.pen., atunci când judecătorul de drepturi și libertăți va respinge în totalitate cererea procurorului, fie ca inadmisibilă, fie ca nefondată.

În cazul oricăreia dintre soluțiile adoptate de către judecătorul de drepturi și libertăți, aceasta nu va putea fi supusă niciunei căi de atac, însă procurorul va fi îndreptățit să formuleze o nouă cerere de încuviințare în cazul respingerii, dacă vor fi îndeplinite cerințele prevăzute de art. 140 alin. (8) C.pr.pen.[3].

Admiterea cererii se face prin încheierea judecătorului de drepturi și libertăți, care va proceda la emiterea imediată a mandatului de supraveghere tehnică, întocmind în mod obligatoriu o minută.

După admiterea cererii procurorului, judecătorul de drepturi și libertăți emite, conform art. 140 alin. (5) C.pr.pen., un mandat care trebuie să cuprindă mai multe elemente regăsite și în încheierea de admitere a cererii. Mandatul emis va fi un mandat de supraveghere tehnică.

Elementele comune care nu pun probleme deosebite sunt cele privind *denumirea instanței*, *data, ora și locul emiterii*, *numele, prenumele* și *calitatea persoanei care a dat încheierea și a emis mandatul*, *semnătura judecătorului și ștampila instanței*. Față de obiectul măsurii de supraveghere tehnică, nu va fi necesară indicarea numărului de cont, nici elementele de identificare a numărului de telefon sau a punctului de acces la un sistem informatic, nici datele de identificare a căii de comunicare. Un alt element comun care nu ridică probleme este perioada maximă pentru care se dispune supravegherea tehnică, aceasta putând fi de maximum 30 de zile.

Alături de acestea, în cuprinsul art. 140 alin. (5) lit. e) teza a II-a C.pr.pen., legiuitorul a prevăzut că este obligatorie menționarea *scopului* pentru care s-a încuviințat măsura. Întrucât, în cazul supravegherii tehnice, vom fi în situația autorizării unui procedeu probatoriu, scopul

[1] Conform acestui articol, cererea trebuie să cuprindă: „(...) numele sau alte date de identificare a persoanei împotriva căreia se dispune măsura, dacă sunt cunoscute, indicarea probelor ori a datelor din care rezultă suspiciunea rezonabilă cu privire la săvârșirea unei infracțiuni, indicarea faptei și a încadrării juridice, (...) motivarea caracterului proporțional și subsidiar al măsurii (...)".

[2] *I. Bălan*, Dreptul la respectarea vieții private și supravegherea video, audio sau prin fotografiere. Partea a II-a, în Pandectele Române nr. 8/2015, pp. 75-76.

[3] Cu privire la formularea unei noi cereri de autorizare, *v. supra*, Titlul III, Capitolul II.2.

va fi obținerea de probe cu privire la săvârșirea unei infracțiuni, pregătirea săvârșirii unei infracțiuni sau descoperirii și identificării persoanelor care au participat sau participă la săvârșirea respectivelor infracțiuni.

În privința *indicării concrete a măsurii încuviințate*, judecătorul de drepturi și libertăți va trebui să detalieze care sunt modalitățile concrete de realizare a supravegherii, numai cele menționate expres putând fi puse în executare de către procuror. Sub acest aspect, facem trimitere la secțiunea dedicată modalităților de realizare a supravegherii video, audio sau prin fotografiere, care vor fi tratate într-o secțiune ulterioară[1].

Numele persoanei supuse măsurii nu va trebui indicat decât dacă vor fi cunoscute datele de identificare ale acestei persoane, în caz contrar trebuind să se arate că nu se cunoaște persoana. Apreciem că o atare situație va putea apărea numai dacă se va proceda la încuviințarea unei supravegheri în spații publice; în cazul unei supravegheri a spațiilor private, se va putea determina persoana care ar putea fi supusă măsurii, aceasta fiind cel puțin proprietarul spațiului privat.

În ceea ce privește prelungirea măsurii de supraveghere tehnică și a duratei maxime de autorizare a supravegherii video, audio sau prin fotografiere în spații publice, facem trimitere la explicațiile generale privind autorizarea supravegherii tehnice. Durata maximă va fi restrânsă în cazul supravegherii în spații private, după cum vom arăta în secțiunea următoare.

Secțiunea a 3-a. Autorizarea supravegherii video, audio sau prin fotografiere în spații private

În cazul supravegherii video, audio sau prin fotografiere în spații private, legiuitorul a inclus câteva elemente noi prin care să se urmărească restrângerea ingerinței aduse drepturilor fundamentale ale persoanei față de care se va încuviința măsura. În această privință, autorizarea supravegherii în spații private presupune două particularități: *necesitatea unei dispoziții privind pătrunderea în spații private pentru activarea sau dezactivarea mijloacelor tehnice ce urmează a fi folosite* și *durata totală a supravegherii în spații private*.

În mod corect s-a constatat în doctrină că, în cazul supravegherii în spații private, legea română este deficitară, întrucât nu se prevede cu claritate întinderea și modalitățile de exercitare a pătrunderii în spații private pentru activarea și dezactivarea mijloacelor tehnice, în special sub aspectul faptului că nu există nicio limitare temporală a instalării și dezinstalării mijloacelor tehnice[2]. Omisiunea legiuitorului este îngrijorătoare, întrucât nu constituie o garanție suficientă împotriva posibilelor ingerințe abuzive ale organelor de urmărire penală în viața privată a unei persoane. Este drept că textul legal vorbește despre activarea și dezactivarea mijloacelor tehnice, dar nu se specifică de câte ori se poate pătrunde pentru a face acest lucru pe durata de valabilitate a mandatului de supraveghere tehnică. Nu se poate admite ca organele de urmărire penală să pătrundă în mod regulat în spațiul privat al unei persoane pentru a activa, reactiva, dezactiva sau înlocui dispozitivele utilizate pentru supravegherea video sau audio, o atare ipoteză constituind o ingerință disproporțională în viața privată. *De lege ferenda*, se impune ca mandatul să precizeze și că acesta se acordă numai pentru câte două pătrunderi în fiecare spațiu privat – pentru instalarea și apoi dezinstalarea mijloacelor tehnice.

[1] *V. infra*, Titlul VI, Capitolul III.2.

[2] *S. Grădinaru*, Supravegherea tehnică, 2014, p. 248.

O altă critică este existența riscului de efectuare a unor percheziții ilegale de către organele de urmărire penală cu ocazia activării și dezactivării mijloacelor tehnice[1], nefiind exclusă posibilitatea unei sesizări din oficiu, ca urmare a celor care pot fi găsite în casa persoanei supuse supravegherii tehnice. Sub acest aspect, va trebui să avem în vedere dacă organele de urmărire penală s-au limitat la a constata existența unor bunuri la vedere sau au procedat la realizarea unor căutări prin deschiderea mobilierului sau altor obiecte ce ar putea conține bunuri. Apreciem că numai în cazul în cazul în care se descoperă bunuri a căror deținere este interzisă de lege și acestea au fost lăsate la vedere în încăperea unde se vor monta mijloace tehnice de supraveghere, organele de urmărire penală se vor putea sesiza legal pentru săvârșirea unei infracțiuni, putând, ulterior, solicita încuviințarea unei percheziții domiciliare.

S-a susținut că legiuitorul a omis să precizeze că pătrunderea în spațiile private se va putea face pentru instalarea și dezinstalarea mijloacelor tehnice, referindu-se doar la activarea și dezactivarea acestora, ceea ce ar presupune că ar trebui să fie folosite dispozitive tehnice deja aflate în spațiul privat, neputându-se adăuga la lege[2]. Nu putem fi de acord cu această poziție, întrucât interpretarea dispozițiilor art. 140 alin. (5) lit. h) C.pr.pen. trebuie să se facă în sensul ca textul să poată produce efecte în contextul legislativ în care se poate autoriza supravegherea tehnică în spații private. Nu considerăm incidente referirile autoarei la jurisprudența Curții Europene a Drepturilor Omului privind Marea Britanie în cauzele în care s-a constatat lipsa unor dispoziții legale privind posibilitatea de autorizare a unor înregistrări în spații private, întrucât în respectivele cauze s-a constatat lipsa unui cadru legal de autorizare[3] a unor astfel de măsuri de supraveghere tehnică, și nu doar aspecte privind legiferarea instalării și dezinstalării tehnicii folosite. Cu toate acestea, problema reală a legii este o lipsă de claritate cu privire la numărul, natura și timpul cât poate fi autorizată pătrunderea în spații private, întrucât legiuitorul nu a obligat judecătorul de drepturi și libertăți să detalieze acțiunile specifice ce au fost autorizate. Soluția la o astfel de problemă a fost găsită în dreptul englez, unde, pentru supravegherea video și audio în spații private (*intrusive surveillance*), este necesară o autorizare separată (*interference with property and entry onto land or equipment*) și este necesar ca în actul de autorizare să se prevadă fiecare acțiune pe care o pot face organele de poliție: pătrunderea în vederea identificării locurilor unde se pot instala dispozitive, pătrunderea pentru instalarea dispozitivelor și pătrunderea pentru recuperarea dispozitivelor, acestea putând fi autorizate prin acte diferite, esențial fiind ca persoana care le autorizează să descrie fiecare acțiune[4], nu doar să emită o autorizare generală, așa cum s-ar deduce din Codul de procedură penală român.

Organul care va putea fi împuternicit prin încheierea judecătorului de drepturi și libertăți să pătrundă în spațiile private pentru a activa sau dezactiva mijloacele tehnice ce urmează a fi folosite trebuie să aibă calitatea prevăzută expres de art. 140 alin. (5) lit. h) C.pr.pen., de *organ de urmărire penală*, neputându-se accepta ca acesta să aibă o altă calitate, precum cea de lucrător de poliție, investigator sub acoperire ori colaborator. O atare dispoziție limitează posibilitatea concretă a instalării unor mijloace tehnice, sancțiunea nerespectării unei atare limitări fiind nulitatea absolută. Credem că era preferabil ca legiuitorul să fi inclus și posibilitatea ca instalarea și dezinstalarea mijloacelor de supraveghere tehnică să fi putut fi realizată

[1] *Ibidem*.

[2] *Ibidem*.

[3] CEDO, cauza *Khan c. Marea Britanie*, Hotărârea din 4 octombrie 2000, §27; cauza *Allan c. Marea Britanie*, Hotărârea din 5 februarie 2003, §35-36, pe *hudoc.echr.coe.int*

[4] *C. Harfield, K. Harfield*, Covert Investigation, 2018, pp. 136-137.

de lucrători specializați din cadrul poliției, întrucât și aceștia pot să fie delegați să pună în executare supravegherea tehnică, potrivit art. 142 alin. (1) C.pr.pen. Situația este cu atât mai inexplicabilă cât timp un investigator sub acoperire sau un colaborator pot fi autorizați să realizeze supravegherea video, audio sau prin fotografiere, conform art. 148 alin. (3) C.pr.pen., însă vor putea să o realizeze numai prin tehnica operativă asupra propriei persoane. În anumite cauze complexe în care s-ar impune supravegherea continuă în spații private, omisiunea legii va crea piedici reale în a se putea instala și dezinstala mijloacele tehnice ori va da prilej la eludarea legii.

În privința necesității unei dispoziții referitoare la pătrunderea în spații private, apreciem că, din punct de vedere tehnic, ar exista posibilitatea unei supravegheri video, audio sau prin fotografiere, fără a fi necesară pătrunderea în spații private a persoanelor care pun în executare metoda de supraveghere tehnică, atunci când va fi autorizat accesul la un sistem informatic, și supravegherea se va realiza prin intermediul camerelor video și microfoanelor dispozitivului persoanei. Întrucât accesul la un sistem informatic poate fi realizat și la distanță, în funcție de particularitățile concrete ale cauzei și ale dispozitivelor care vor fi supuse măsurii, se poate obține accesul la distanță într-un laptop (sau alt dispozitiv, inclusiv televizor inteligent) și supravegherea să se realizeze prin acest dispozitiv.

O altă ipoteză în care nu va fi necesară pătrunderea în spații private va fi atunci când mijlocul tehnic de înregistrare se va atașa asupra persoanei vizate sau asupra unui investigator sub acoperire sau colaborator, caz în care nu va exista o pătrundere pentru a activa sau dezactiva mijloacele tehnice.

În consecință, astfel cum am arătat deja mai sus, va fi deosebit de important ca procurorul să expliciteze în propunere modalitatea în care se va realiza supravegherea video, audio sau prin fotografiere a persoanei, revenind judecătorului de drepturi și libertăți să analizeze fiecare dintre aceste modalități și să o aleagă pe cea care este cel mai puțin invazivă și, după caz, cea care nu ar presupune o restrângere a dreptului la un domiciliu al persoanei vizate și al dreptului la viață privată.

Odată cu emiterea mandatului de supraveghere tehnică, judecătorul de drepturi și libertăți va trebui să indice și perioada pentru care s-a autorizat măsura, aceasta fiind de cel mult 30 de zile. În cazul în care există motive temeinic justificate, măsura poate fi prelungită la propunerea motivată a procurorului, fiecare prelungire neputând depăși 30 de zile. Apreciem că, pentru fiecare prelungire, judecătorul de drepturi și libertăți trebuie să reevalueze ingerința adusă vieții private a persoanei prin raportare la durata supravegherii, putând reevalua autorizarea inițială de a prelungi doar metode mai puțin invazive. De pildă, dacă probele obținute prin supravegherea audiovideo nu sunt suficiente pentru a justifica (alături de celelalte condiții legale) prelungirea unei astfel de măsuri, judecătorul de drepturi și libertăți va putea prelungi măsura supravegherii tehnice numai în ceea ce privește supravegherea audio, pe care o considerăm o ingerință mai redusă în viața privată a persoanei față de supravegherea audiovideo.

Chiar dacă sub aspectul duratei inițiale și a celei pentru care se poate prelungi măsura nu există nicio diferență față de celelalte măsuri de supraveghere tehnică, în privința duratei maxime pentru care poate fi prelungită măsura, legiuitorul a prevăzut o durată totală mai scurtă față de celelalte măsuri, respectiv de 120 de zile[1]. Deși este o măsură de limitare a ingerinței

[1] Conform art. 144 alin. (3) C.pr.pen., „durata totală a măsurilor de supraveghere tehnică, cu privire la aceeași persoană și aceeași faptă, nu poate depăși, în aceeași cauză, 6 luni, cu excepția măsurii de supraveghere video, audio sau prin fotografiere în spații private, care nu poate depăși 120 de zile".

în viața privată a unei persoane, nu există nicio noutate față de legislația procesuală penală anterioară, pentru care durata totală a măsurii nu putea fi mai mare de 120 de zile. Practic, legiuitorul a menținut posibilitatea realizării supravegherii video, audio sau prin fotografiere pentru o durată de 120 de zile, mărind durata totală a celorlalte măsuri de supraveghere tehnică la 6 luni.

Capitolul III
Punerea în executare a supravegherii video, audio sau prin fotografiere

Secțiunea 1. Particularități privind punerea în executare a supravegherii video, audio sau prin fotografiere

Alături de aspectele generale privind punerea în executare a mandatului de supraveghere tehnică, pe care le-am tratat în context general, se impun a fi formulate câteva mențiuni particulare privind punerea în executare a supravegherii video, audio sau prin fotografiere, însoțite de considerații privind modalitățile concrete ale acestei metode speciale de supraveghere.

În ceea ce privește supravegherea video, audio sau prin fotografiere în spații private, această variantă a metodei speciale de supraveghere va putea presupune pătrunderea în spații private. Pătrunderea va trebui să se realizeze prin mijloace care să provoace cât mai puține distrugeri pentru proprietate și, în mod evident, să păstreze caracterul secret al supravegherii tehnice. Pentru a fi evitată periclitarea secretului operațiunii, considerăm că se impune urmărirea persoanei supravegheate prin filaj în vederea stabilirii momentului tactic oportun de instalare sau dezinstalare a dispozitivelor tehnice de înregistrat[1].

Va fi socotită pătrundere într-un spațiu privat și dacă se obține consimțământul unei persoane pentru a se intra în respectivul spațiu, de pildă, atunci când într-o instituție publică se va instala un dispozitiv de supraveghere, vor putea fi obținute cheile respectivului birou de la portar ori altă asemenea persoană. Din păcate, dacă această persoană sprijină organele de urmărire penală, nu va putea fi considerată ca dând un concurs tehnic în sensul art. 142 alin. (3) C.pr.pen. și nu va putea fi obligată să păstreze secretul operațiunii. Cu toate acestea, dacă persoana va avea calitatea de funcționar public, vor fi incidente dispozițiile art. 277 alin. (1) C.pen. privind infracțiunea de compromiterea intereselor justiției.

Pătrunderea în spațiile private, fiind o parte din punerea în executare a mandatului de supraveghere tehnică, va putea fi realizată de către procuror sau de către organele de cercetare penală. Față de prevederile exprese ale art. 140 alin. (5) lit. h) C.pr.pen., nu va putea fi permisă pătrunderea altor persoane – lucrători specializați ai poliției, investigatori, colaboratori – în spații private pentru instalarea și dezinstalarea mijloacelor tehnice de supraveghere.

Sub aspectul valorificării probelor obținute din supravegherea video, audio sau prin fotografiere, mijlocul de probă principal care va rezulta din punerea în executare a măsurii va fi un proces-verbal. Alături de acesta, vor rezulta și suporții de stocare pe care se vor regăsi înregistrările audio, audiovideo sau video, precum și fotografiile care au fost capturate.

Rezultatele supravegherii tehnice vor fi cuprinse, în conformitate cu art. 143 C.pr.pen., într-un proces-verbal de consemnare a activităților de supraveghere tehnică. Deși există similarități cu alte măsuri de supraveghere tehnică, în cazul supravegherii video, audio sau prin fotografiere, vor fi necesare unele mențiuni suplimentare, în funcție de modalitatea concretă de punere în executare.

[1] *D.E. Hall*, Criminal Law and Procedure, Fifth Edition, Ed. Delmar Cengage, New York, 2009, p. 113.

Dacă sunt surprinse conversațiile anumitor persoane, acestea vor trebui să fie redate întocmai ca în cazul metodei speciale a interceptărilor comunicațiilor, în conformitate cu dispozițiile art. 143 alin. (4) C.pr.pen. În cazul în care se vor realiza și înregistrări video sau audiovideo, procesul-verbal va trebui să conțină și o descriere a activităților surprinse, întrucât acestea sunt tot rezultate ale activităților care au fost realizate. Sensul gândit de legiuitor nu a fost să instituie doar obținerea respectivelor înregistrări, ci ca procesul-verbal prin care se consemnează activitățile să conțină și o descriere a celor surprinse. Acest aspect este mai evident în cazul supravegherii prin fotografiere, unde se va întocmi și anexa procesului-verbal și o planșă fotografică, făcându-se mențiuni pe aceasta asupra activităților constatate.

În situația realizării unui filaj sau a unei urmăriri prin intermediul unei rețele de camere de supraveghere publice, va trebui indicat traseul persoanei urmărite și locațiile în care s-a oprit, precum și activitățile efectuate sau persoanele cu care aceasta a intrat în contact.

În cazul în care se va proceda la supravegherea în spații private și va fi necesară pătrunderea în aceste spații, procesul-verbal de consemnare a activităților va trebui să conțină și indicarea și descrierea operațiunilor de instalare și dezinstalare a dispozitivelor tehnice. Va trebui să se indice data și ora la care a început activitatea de pătrundere, unde au fost instalate mijloacele de supraveghere, cum au fost instalate, dacă s-au cauzat anumite distrugeri și care au fost persoanele care au realizat activitatea. Este necesară întocmirea unui proces-verbal pentru fiecare activitate de acest fel.

Secțiunea a 2-a. Modalități de realizare a supravegherii video, audio sau prin fotografiere

§1. Supravegherea ambientală a unui spațiu privat

Cea mai intruzivă formă de supraveghere va fi cea audiovideo în spații private, denumită și „supravegherea ambientală a unui spațiu privat". După cum am mai menționat în prezenta lucrare, conform dispozițiilor Codului de procedură penală, nu va fi obligatorie realizarea unei înregistrări pentru a se realiza supravegherea, fiind suficientă observarea persoanei vizate sau a locului vizat prin intermediul unor dispozitive tehnice. Vor putea fi folosite echipamente audio, precum: microfonul dinamic, microfonul cristal, microfonul condensator, microfoanele cu electret, microfoane de contact (care preiau vibrațiile unor ziduri subțiri, uși, geamuri), microfoane parabolice (pentru captare la distanță)[1]. Tot o înregistrare în spații private a fost considerată și folosirea unei camere de termoviziune asupra casei unei persoane bănuite, descoperindu-se că aceasta cultiva marijuana prin emisiile particulare ale lămpilor folosite[2]. În privința înregistrărilor audiovideo, vor fi folosite camere de mici dimensiuni, care vor filma la distanță scurtă între ele și persoanele vizate, putând fi disimulate în obiecte casnice, prize, mobilier etc.

[1] *M.V. Tudoran*, Teoria și practica interceptărilor, 2012, p. 171.

[2] *R.V. del Carmen*, Criminal Procedure. Law and Practice, 8th Edition, Ed. Wadsworth Cengage Learning, Belmont, 2010, pp. 494-495. Ca o notă suplimentară, cultivarea de plante în interiorul unei locuințe presupune furnizarea de lumină artificială pentru a susține creșterea și dezvoltarea plantei; astfel de surse, până recent, presupuneau lămpi cu halogen care consumă cantități mari de energie (câteva sute de watti pe lampă) și degajă deosebit de multă căldură.

În vederea realizării supravegherii, poate fi necesar ca organele însărcinate cu punerea în executare să pătrundă în spații private pentru a activa sau dezactiva mijloacele tehnice prin care se realizează supravegherea. Aceste dispozitive vor trebui să fie ascunse în așa mod încât să nu atragă atenția asupra lor. Locațiile propice pentru astfel de dispozitive vor fi instalațiile electrice – prizele, echipamentele IT, instalațiile de lumini, tavanele false sau zonele ascunse în care nu există acces facil (în spatele unui dulap, după un birou etc.). După specificul dispozitivului tehnic folosit, poate fi necesar ca acesta să fie legat la o sursă de curent, fiind preferabil să aibă și o baterie, pentru a nu se întrerupe înregistrarea în cazul în care se oprește brusc alimentarea cu energie electrică.

Uneori, dispozitivele pot fi inserate prin găurirea zidului despărțitor dintre spațiul privat și o încăpere învecinată, putându-se introduce doar un microfon prin orificiu. Dacă este posibil, se poate profita de realizarea unor lucrări de renovare pentru îngroparea dispozitivelor în stratul de glet sau în tencuiala zidului ori amplasarea lor în spatele unei mobile de mari dimensiuni (de exemplu, dulapurile metalice din unitățile de parchet sau din secțiile de poliție).

În cazurile prezentate mai sus, o problemă aparte o va constitui transmiterea înregistrărilor, aceasta putându-se face prin intermediul unei rețele de telefonie mobilă sau prin altfel de unde radio. În unele situații poate fi nevoie ca organele de urmărire penală să folosească dispozitive tehnice în apropierea zonei supuse supravegherii ambientale pentru a capta semnalele dispozitivelor de supraveghere. Aceasta se va putea realiza, după caz, de echipamente aflate într-o autoutilitară parcată în apropiere, care poate fi deghizată ca o mașină aparținând unei companii de utilități, de transport etc., pentru a nu atrage atenția persoanei supravegheate.

Vom fi tot în cazul unei supravegheri ambientale în spații private dacă mijlocul tehnic folosit este amplasat în afara locuinței persoanei supravegheate, dar, prin capacitățile tehnice, dispozitivul folosit este apt să producă aceleași rezultate ca un dispozitiv amplasat în locuință, putând permite surprinderea evenimentelor și conversațiilor purtate[1].

§2. Înregistrări ambientale realizate de un investigator sub acoperire sau un colaborator

Înregistrările ambientale pot fi realizate și în cadrul măsurii speciale de cercetare a utilizării investigatorilor sub acoperire și a colaboratorilor. Această modalitate de realizare a supravegherii tehnice presupune, în prealabil, autorizarea de către procuror a metodei speciale de cercetare a utilizării investigatorilor sub acoperire sau cu identitate reală și a colaboratorilor, prevăzută de art. 148 C.pr.pen. După cum am arătat în secțiunea dedicată clasificării tipurilor de supraveghere video, audio sau prin fotografiere, într-o asemenea situație, vom avea o supraveghere derivată și secvențială, realizată prin intermediul mijloacelor tehnice atașate investigatorului sub acoperire și a colaboratorului. În cursul unei investigații prin metoda specială de cercetare arătată, nu vor putea să se obțină probe, ci numai informații, pentru obținerea de probe fiind necesare procedee probatorii derivate din activitatea investigatorului sau a colaboratorului.

Conform art. 148 alin. (3) C.pr.pen., „*în cazul în care procurorul apreciază că este necesar ca investigatorul sub acoperire să poată folosi dispozitive tehnice pentru a obține fotografii sau înregistrări audio și video, sesizează judecătorul de drepturi și libertăți în vederea emiterii mandatului de supraveghere tehnică*". Semnificația acestui text de lege presupune că va fi

[1] *C. Harfield, K. Harfield*, Covert Investigation, 2018, p. 96.

necesară o autorizare suplimentară față de aceea dată de procuror pentru ca investigatorul sau colaboratorul să poată folosi dispozitive audiovideo de înregistrare, măsura fiind autorizată pentru acesta. Ca atare, numai investigatorul sau colaboratorul vor putea pune în aplicare supravegherea derivată. În opinia noastră, acest lucru determină doar posibilitatea ca aceştia să poarte asupra lor tehnica de înregistrare, fără a putea ca ei să o instaleze într-un spațiu privat, deoarece autorizarea privește *folosirea de către investigator sau colaborator* a dispozitivelor tehnice, astfel că aceştia trebuie să fie în contact permanent cu dispozitivul sau ca acesta să se afle la dispoziția lor. Va fi incidentă o atare situație atunci când investigatorul își va folosi telefonul mobil pentru a înregistra conversațiile desfășurate în camera în care se află, inclusiv dacă părăsește temporar încăperea. Nu va fi exclusă posibilitatea ca organele de urmărire penală să fie în legătură electronică permanentă cu mijloacele tehnice de înregistrare aflate asupra investigatorului sau colaboratorului sau chiar acestea să realizeze înregistrarea prin captarea undelor radio transmise de dispozitivul tehnic.

§3. Supravegherea prin intermediul accesului la un sistem informatic

O modalitate nouă prin care se poate realiza supravegherea unei persoane constă în utilizarea concomitentă și a măsurii de supraveghere tehnică a accesului la un sistem informatic, precum și folosirea componentelor audio și video ale sistemului informatic, pentru a se realiza observarea sau înregistrarea persoanei vizate.

În desfășurarea activității concrete se va proceda la accesarea la distanță (sau directă) a dispozitivului (laptop, computer desktop, telefon mobil, tabletă, televizor inteligent, boxă inteligentă[1] etc.) și se va instala un program care să permită controlul la distanță și care să înregistreze toate conversațiile persoanei ori mișcările și activitățile sale din vecinătatea dispozitivului. Astfel de programe există deja la nivel comercial și permit părinților să își monitorizeze copiii prin intermediul telefoanelor mobile, inclusiv prin posibilitatea ascultării în mediu ambiental a activităților acestora.

§4. Înregistrări ambientale realizate de o parte sau de o altă persoană

În conformitate cu dispozițiile art. 139 alin. (3) C.pr.pen., înregistrările efectuate de părți sau de alte persoane constituie mijloace de probă când privesc propriile convorbiri sau comunicări pe care le-au purtat cu terții. Astfel cum am arătat pe larg într-o secțiune precedentă[2], aceste înregistrări sunt cunoscute ca înregistrări private, fiind supuse unui regim distinct de cel al măsurilor de supraveghere tehnică autorizate de organele judiciare. Consecința este că supravegherea video, audio sau prin fotografiere va putea fi realizată de un privat, parte în procesul penal sau nu, pentru înregistrările purtate de acesta cu terții. De cele mai multe ori, aceste înregistrări vor fi făcute intenționat de respectivele părți, însă numai sub forma unor înregistrări în mediu ambiental, nefiind de conceput ca o persoană să realizeze interceptări de comunicații, întrucât aceasta ar constitui infracțiune.

[1] Recent, au existat incidente în care boxele inteligent fabricate de Google și Amazon pentru integrarea în casele oamenilor a asistenților digitali au captat, înregistrat și transmis către serverele societăților conversațiile purtate de persoane în vecinătatea acestor dispozitive, fără ca utilizatorul să fie încunoștințat. A se vedea: *A. Cuthbertson*, Google defends listening to private concversations on Google Home – but what intimate moments are recorded?, pe *www.independent.co.uk*; *TJ McCue*, Amazon Alexa Accused Again of Spying: Here is Another Solution, pe *www.forbes.com*

[2] *V. supra*, Titlul II, Capitolul III.

În cuprinsul celei de-a doua teze a art. 139 alin. (3) C.pr.pen. sunt incluse și *alte înregistrări care pot constitui mijloace de probă dacă nu sunt interzise de lege*. O atare situație o vom întâlni în cazurile legitime de realizare a unor înregistrări private sau publice de către alte persoane decât părțile. De pildă, va intra în această categorie înregistrarea realizată de camerele de supraveghere ale unei primării cu privire la activitățile desfășurate în zone publice sau înregistrările realizate de un magazin de haine cu privire la activitățile clienților care intră în respectivul magazin.

Ceea ce este în comun pentru aceste tipuri de înregistrări este caracterul lor incidental sau întâmplător, neputând fi concepută o supraveghere video, audio sau prin fotografiere în mod continuu ca fiind una legală, dacă va privi activitatea unei persoane determinate. Dimpotrivă, activitatea va fi una infracțională, fapta putând fi încadrată ca infracțiunea de hărțuire, prevăzută de art. 208 alin. (1) C.pen. Chiar dacă nu ar exista un element intențional, și supravegherea curții interioare a casei poate fi considerată nelegală (deși scopul poate fi unul legitim – prevenirea furtului din locuință) dacă o parte a înregistrării va surprinde și curtea vecinului, în lipsa consimțământului său expres de a se realiza astfel de înregistrări.

În toate situațiile, organele de urmărire penală nu vor putea proceda la eludarea dispozițiilor legale și să strângă probe în temeiul art. 139 alin. (3) C.pr.pen., întrucât aceasta ar constitui o fraudă la lege. Ca atare, dispozițiile legale menționate vor fi aplicabile numai în situația în care un organ sau o autoritate a statului realizează o înregistrare în afara oricărui proces penal și fără a avea intenția de a obține probe într-un proces penal. De pildă, va fi legală proba care rezultă din înregistrarea ambientală efectuată prin camerele de supraveghere ale unei unități de parchet din care rezultă sustragerea unui bun din incinta parchetului, întrucât, prin înregistrare, autoritățile publice nu au încercat să surprindă săvârșirea unei anumite infracțiuni. Nu va fi legală situația în care un investigator sub acoperire sau un colaborator va proceda la realizarea unor înregistrări ambientale, chiar dacă ar acționa la fel ca o persoană care poate avea calitatea de parte în cauză și chiar dacă participă la conversație, întrucât legea obligă ca pentru această situație să existe un mandat de autorizare al judecătorului de drepturi și libertăți, conform art. 148 alin. (3) C.pr.pen.[1].

§5. Înregistrări ale spațiilor publice

Odată cu dezvoltarea tehnologiei și a prețului din ce în ce mai scăzut al camerelor video, unele comunități au ales să procedeze la supravegherea video a spațiilor publice pentru motivul legitim al creșterii siguranței publice. Camerele video se instalează pentru supravegherea generală a persoanelor, în scopul combaterii criminalității sau în scopul monitorizării traficului și a oricăror evenimente din trafic, crescând siguranța pe drumurile publice și instituind o mai bună disciplină a șoferilor. O astfel de supraveghere va constitui o ingerință adusă dreptului la viață privată al persoanei, însă nu una suficient de gravă încât să contrabalanseze interesul legitim al societății, în afara situațiilor în care scopul urmărit este urmărirea penală într-o anumită cauză. În concret, conform recomandărilor Comisiei de la Veneția în privința supravegherii video în spații publice, este necesar ca persoanele care ar putea fi supuse supravegherii să fie încunoștințate de aceasta într-un mod vizibil sau ca mijloacele tehnice de supraveghere să fie evidente, pentru a se considera că se desfășoară în concret o supraveghere și orice persoană

[1] Apreciem că vom fi într-o situație similară cu cea constatată de CEDO în cauzele *Van Vondel c. Olanda*, Hotărârea din 25 ianuarie 2008, §49; *M.M. c. Olanda,* Hotărârea din 24 septembrie 2003, §41, pe *hudoc.echr.coe.int*

care ar putea fi vizată își dă, prin prezența sa, consimțământul de a fi supravegheată[1]. Oricât de deschisă ar putea fi o persoană, ea tot va avea secrete pe care le va dori păstrate, inclusiv activitățile sale desfășurate în public, precum persoanele cu care se întâlnește în public, și nu se așteaptă ca, la momentul ieșirii din domiciliu, să fie urmărită și monitorizată de sisteme de supraveghere performante care să extragă, în mod automat, informații despre aceasta[2].

Diferența dintre supravegherea generală în spații publice și cea prevăzută de art. 138 alin. (1) lit. c) C.pr.pen. constă în caracterul țintit al acesteia din urmă, întrucât nu se va monitoriza situația dintr-un loc, ci se va proceda la urmărirea unei persoane precis determinate. Acest mod de realizare a supravegherii este denumit, în dreptul englez, ca *directed surveillance*[3]. În țara noastră, realizarea unei astfel de supravegheri, chiar dacă vor fi folosite sisteme de supraveghere publice, va presupune autorizarea prealabilă a judecătorului de drepturi și libertăți, precum și desfășurarea supravegherii de către organele de urmărire penală sau lucrătorii specializați din poliție. În concret, se va permite accesul la sistemele de supraveghere ale unei comunități (de regulă, operate de poliția locală) și, prin vizionarea în timp real a persoanei supravegheate, se vor putea realiza înregistrări ale acesteia într-un mod care nu presupune prezența organelor de urmărire penală în aceeași locație.

Un posibil dezavantaj al acestei abordări este caracterul lipsit de flexibilitate al sistemelor de supraveghere video, bună parte dintre camere având un câmp vizual fix, modelele de camere cu baleiaj (Pan-Tilt-Zoom) fiind considerabil mai scumpe. Totodată, limitele tehnologice actuale conduc la un preț ridicat al camerelor cu optică suficient de avansată pentru a captura de la distanță detalii privind trăsăturile faciale ale unei persoane. În plus, camerele de supraveghere publice nu au capacitatea captării sunetului, fiind strict limitate la componenta video. Chiar și în situația în care există fonduri disponibile pentru achiziționarea de camere de supraveghere care să înregistreze audio, să aibă baleiaj și cu optică sofisticată care să permită mărirea imaginii, se impune ca pentru scopul urmărit să fie dezactivate funcțiile care nu sunt strict necesare[4], în unele situații, aceste limitări fiind impuse de regulamentele europene[5].

În România, cel puțin în localitățile cu o populație mai mare, amplasarea unor camere pentru supravegherea traficului poate constitui o măsură care să permită monitorizarea deplasărilor unei persoane, dacă aceasta va folosi o mașină. Nu trebuie omis faptul că o supraveghere de acest fel poate fi completată prin filaj, în vederea asigurării succesului activității.

Viitorul tehnologiei de supraveghere în spații publice îl reprezintă supravegherea video cu recunoaștere facială, care ar permite monitorizarea generalizată a persoanelor cu identificarea instant a acestora și stocarea datelor nu numai vizuale, ci și de identificare[6]. Un astfel de sistem se dorește a fi implementat în Londra și Moscova, însă tendința la nivel european este de a se

[1] Comisia de la Veneția, Opinie asupra supravegherii video realizată în spații publice de autorități publice și protejarea drepturilor omului, adoptată în a 70-a Sesiune Plenară a Comisiei de la Veneția, 16-17 iunie 2007, §83.

[2] *E.D. Cohen*, op. cit., p. 132.

[3] *C. Harfield, K. Harfield*, Covert Investigation, 2018, p. 95.

[4] European Data Protection Board, Guidelines 3/2019 on processing of personal data through video devices, adoptată la 10 iulie 2019, §126, pe *edpb.europa.eu*

[5] De pildă, art. 5 lit. c) din Regulamentul nr. 679 din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) prevede conceptul de „minimizare a datelor colectate".

[6] *W.Q. Yan*, Introduction to Intelligent Surveillance. Surveillance Data Capture, Transmission, and Analytics, Third Edition, Ed. Springer, Cham, 2019, p. 96.

opri dezvoltarea unui asemenea sistem până la analizarea mai bună a implicațiilor privind viața privată a unei persoane. Nu trebuie omis faptul că, pentru ca sistemul să funcționeze corect, el va trebui în mod automat să analizeze fețele tuturor oamenilor dintr-o anumită zonă și să determine persoana căutată, ceea ce poate conduce la înregistrarea de informații și despre celelalte persoane. În opinia noastră, chiar dacă un astfel de sistem ar face sarcinile organelor de urmărire penală mai ușoare, chiar și în existența unui mandat de supraveghere tehnică emis de un judecător de drepturi și libertăți, ingerința față de viața privată ar fi una prea mare pentru a fi proporțională cu scopul urmărit, dacă vom avea în vedere majoritatea infracțiunilor prevăzute de art. 139 alin. (2) C.pr.pen. Nu suntem de acord cu activarea permanentă a unui asemenea sistem, el permițând identificarea și monitorizarea tuturor persoanelor și stabilirea detaliată a traseului lor zilnic și al activităților acestora. Ceea ce credem că se poate implementa este o supraveghere prin recunoaștere facială dispusă de judecătorul de drepturi și libertăți, în cazuri limitate și numai pentru situații precum prevenirea infracțiunilor de terorism, fără alte excepții.

§6. Filajul

O metodă de investigație recunoscută ca fiind parte a supravegherii video, audio sau prin fotografiere, filajul[1], constă în urmărirea conspirativă de către organele de urmărire penală sau lucrătorii de poliție a persoanei care face obiectul mandatului de supraveghere tehnică pentru a obține înregistrări sau fotografii cu privire la activitățile acesteia. Spre deosebire de alte metode de punere în executare a supravegherii, filajul presupune o activitate de teren cu menținerea contactului vizual al organelor de urmărire penală față de persoana supravegheată, implicând un efort deosebit din punct de vedere logistic din partea acestora[2]. Urmărirea unei persoane nu se va putea realiza numai de către o singură persoană, deseori fiind necesare mai multe persoane să contribuie, pentru a nu ridica suspiciuni asupra operațiunii. În cazul în care se supraveghează mișcările unei persoane care se deplasează cu un autovehicul, va fi obligatoriu ca aceasta să se realizeze de mai multe echipe, inclusiv prin segmentarea teritorială a posibilului traseu, astfel încât echipele de filaj să preia una de la cealaltă sarcina de supraveghere. În mod evident, urmărirea pe o distanță mai mare a unei mașini va trezi suspiciuni din partea conducătorului mașinii supravegheate, dacă se va realiza de același echipaj.

Prin filaj se pot observa atât interacțiunea în timp real și în spații publice a persoanei vizate, cât și localizarea acesteia prin supravegherea directă a locațiilor în care se va deplasa. Simpla urmărire a persoanei, în lipsa unor mijloace tehnice de supraveghere (de observare, înregistrare sau fotografiere), va constitui filaj, dar nu va trebui autorizată de judecătorul de drepturi și libertăți. Considerăm că o atare situație este nefericită, permițând organelor de urmărire penală să urmărească o persoană doar în scopul obținerii de informații în cursul procesului penal, pentru o durată nelimitată de timp, o astfel de măsură constituind o ingerință adusă vieții private, care, potrivit opiniei noastre, nu este în acord cu art. 8 par. 2 Conv.EDO.

[1] *M. Udroiu*, Procedură penală, vol. I, 2019, p. 562.
[2] *D.E. Hall*, op. cit., p. 113.

Capitolul IV
Distincțiile dintre supravegherea video, audio sau prin fotografiere și alte metode speciale

Supravegherea video, audio sau prin fotografiere are ca specific faptul că urmărește surprinderea conversațiilor, mișcărilor și activităților unei persoane prin captarea sunetelor și imaginilor în mod nemijlocit. Cu alte cuvinte, supravegherea va avea în vedere ceea ce se desfășoară în mediul ambiental al dispozitivului prin care se realizează observarea sau înregistrarea, și nu prin interceptarea unui semnal digital. Prin acest procedeu probatoriu pot fi obținute probe similare cu cele care se pot obține prin alte metode de supraveghere, existând numeroase interferențe între supravegherea video, audio sau prin fotografiere și alte metode speciale de supraveghere sau cercetare. Semnificația practică este importantă, întrucât va fi necesară autorizarea metodei de supraveghere corecte sau, după caz, autorizarea concomitentă a mai multor metode speciale de supraveghere, atunci când se impune obținerea de probe prin metode complexe.

În cele ce urmează vom aborda principalele procedee probatorii care se aseamănă și se întrepătrund uneori cu supravegherea video, audio sau prin fotografiere.

Secțiunea 1. Interceptarea comunicațiilor ori a oricărui tip de comunicare la distanță

Înregistrările la care se face referire în art. 138 alin. (1) lit. c) C.pr.pen. trebuie să se distingă de interceptarea comunicațiilor ori a oricărui tip de comunicare la distanță, pentru a nu exista o confuzie între măsurile care trebuie autorizate, în special atunci când sunt implicate dispozitive de comunicare la distanță uzuale, precum telefoanele mobile.

Principala diferență constă în existența sau nu a unei interceptări a comunicațiilor, fără de care măsura va trebui să fie supraveghere video, audio sau prin fotografiere. În doctrină s-a prezentat o aparentă situație problematică în care două persoane aflate în același loc care discută în limbi diferite, dar folosesc o aplicație instalată pe un telefon mobil pentru a furniza o traducere instant, caz în care ar putea exista o problemă ca urmare a suprapunerii existente între o comunicare nemijlocită a unei persoane într-o limbă pe care cealaltă parte nu o înțelege și cea realizată printr-un dispozitiv tehnic[1]. Situația nu este problematică dacă vom folosi criteriul existenței unei interceptări, întrucât nu prezintă importanța caracterului tehnic al traducerii, supravegherea realizându-se ambiental și captând toate sunetele din încăperea în care se află ambele persoane, neexistând nicio interceptare a unui semnal al telefonului mobil. În mod evident se va înregistra și traducerea făcută prin telefon, dar traducerea nu va avea natura unei comunicări, nefiind transmisă la distanță celuilalt interlocutor, întrucât acesta este prezent.

O altă situație în care nu va fi incidentă interceptarea comunicațiilor ori a oricărui tip de comunicare la distanță este atunci când se înregistrează convorbirile dintr-o cameră și, întâmplător, persoana supravegheată vorbește la telefon folosind difuzorul încorporat, putând

[1] *M. Bulancea, R. Slăvoiu*, în M. Udroiu (coord.), Codul de procedură penală, 2017, p. 652.

fi captat pe înregistrare și interlocutorul. Nici în situația descrisă nu va exista o interceptare, întrucât captarea semnalului sonor nu se va realiza prin canalul de comunicație (rețeaua furnizorului de servicii de comunicații), ci la unul dintre interlocutori.

O altă problemă ipotetică este folosirea unui program telefonic de înregistrare a apelurilor telefonice, situație în care vor fi captate și înregistrate toate conversațiile purtate de o persoană cu acel telefon mobil. Nici o atare situație nu va constitui interceptare, întrucât înregistrarea se va realiza de către un terminal de telefonie pe baza semnalului primit și trimis de către acesta.

O diferență între cele două metode speciale de supraveghere este că, în cazul interceptării comunicațiilor, nu va fi posibilă numai observarea conținutului acestora, precum poate fi în cazul supravegherii video, audio sau prin fotografiere, realizându-se în toate cazurile înregistrarea convorbirilor sau comunicațiilor.

Secțiunea a 2-a. Accesul la un sistem informatic

Ca urmare a faptului că am tratat deja în prezenta lucrare distincțiile dintre accesul la un sistem informatic și supravegherea video, audio sau prin fotografiere, facem trimitere la secțiunea dedicată distincțiilor dintre cele două măsuri[1]. Apreciem că nu pot exista confuzii între cele două măsuri, însă atunci când supravegherea video, audio sau prin fotografiere se va face prin intermediul unui sistem informatic deținut de către persoana supravegheată, se va impune autorizarea de către judecătorul de drepturi și libertăți și a accesului la un sistem informatic. Dacă punerea în executare va implica un sistem informatic al unui terț – de regulă, autoritate publică – și va exista acordul acestuia, punerea la dispoziție a sistemului informatic (de pildă, sistemul de control al rețelei de camere de supraveghere a unui oraș) va reprezenta doar concursul tehnic al acelei persoane, aceasta fiind ținută să păstreze secretul operațiunii.

Secțiunea a 3-a. Localizarea sau urmărirea prin mijloace tehnice

Întrucât atât supravegherea video, audio sau prin fotografiere, cât și localizarea sau urmărirea prin mijloace tehnice pot fi întrebuințate pentru urmărirea unei persoane, se impun a fi făcute câteva distincții între cele două măsuri de supraveghere tehnică.

Deși ambele măsuri se pot referi la persoane, numai localizarea va putea fi întrebuințată dacă se va dori urmărirea unui bun, datorită specificului acestei măsuri. Practic, dispozitivul de urmărire se va atașa pe bun, neavând importanță persoana care îl va manipula. Dimpotrivă, în cazul supravegherii, va fi urmărită persoana, inclusiv persoana care va intra în contact cu un bun, fiind fotografiată sau înregistrată video sau audio. Astfel, chiar dacă s-ar dori supravegherea unui bun, în realitate vor fi urmărite și înregistrate toate persoanele care vor intra în contact cu acesta.

Localizarea sau urmărirea prin mijloace tehnice va avea un caracter mai puțin intruziv în viața privată a unei persoane și va fi măsura preferată dacă se dorește cunoașterea cu caracter continuu a locației unei persoane. Nu se vor putea obține informații cu privire la acțiunile și conversațiile persoanei, ci numai date privind mișcările ei, celelalte aspecte putând fi, cel mult, intuite.

[1] *V. supra*, Titlul V, Capitolul IV.3.

Prin supravegherea video, audio sau prin fotografiere pot fi obținute și probe directe cu privire la săvârșirea unei infracțiuni, însă, în cazul localizării, vor putea fi obținute numai date de localizare care vor avea caracterul de probe indirecte.

Din punctul de vedere al continuității măsurii, supravegherea video, audio sau prin fotografiere va putea fi numai secvențială atunci când este folosită în scop de localizare și urmărire, ca urmare a necesităților logistice și a costurilor deosebite. Dimpotrivă, localizarea sau urmărirea prin mijloace tehnice va avea caracter continuu, întrucât se realizează în mod automat printr-un dispozitiv de localizare.

Deși ambele metode speciale de supraveghere vor presupune folosirea unor mijloace tehnice, acestea vor fi diferite nu neapărat sub aspectul capacității și specificațiilor tehnice (de pildă, în ambele cazuri se poate utiliza un telefon mobil), ci mai ales sub aspectul naturii informațiilor transmise de către aceste dispozitive către organele de urmărire penală, unele transmițând înregistrări video, audio sau fotografii, altele transmițând doar date geografice referitoare la persoana sau obiectul pe care sunt atașate. Considerăm că, din punct de vedere tehnic, este posibil ca un dispozitiv să fie folosit atât pentru realizarea de înregistrări video și audio, cât și pentru localizarea unei persoane. De exemplu, astfel de dispozitive sunt camerele video de bord pe care le pot întrebuința persoanele în scopuri legitime, dar pot fi folosite și pentru a înregistra conversații și video în interiorul unui autovehicul, multe dintre acestea având și modul GPS instalat care va înregistra locația exactă ca informație pe fundalul fișierului video. Dacă se va folosi un asemenea dispozitiv, apreciem că se va impune autorizarea atât a localizării sau urmăririi prin mijloace tehnice, cât și a supravegherii video, audio sau prin fotografiere.

Capitolul V
Concluzii

Supravegherea video, audio sau prin fotografiere constituie o metodă specială de supraveghere deosebit de intruzivă în viața privată a unei persoane, motiv pentru care folosirea ei se impune a fi limitată doar la cauzele care prezintă o gravitate și complexitate deosebită. Ea este susceptibilă de foarte multe abuzuri, necesitând a fi strict controlată de organele care o autorizează și o pun în executare, întrucât poate rezulta în aflarea celor mai intime detalii ale unei persoane.

Metoda specială presupune supravegherea video, audio, audiovideo sau prin fotografiere, fiind posibilă înregistrarea sau numai observarea mișcărilor sau activităților persoanelor. Ținând seama de posibilitatea de a înregistra în timp real activități, măsura de supraveghere tehnică este aptă să conducă la obținerea de probe directe în procesul penal.

Supravegherea video, audio sau prin fotografiere se poate realiza în spații publice sau în spații private, în cel din urmă caz fiind restrânsă numai la o durată maximă de 4 luni de zile, mai scurtă decât în cazul altor măsuri de supraveghere tehnică. În mod nefericit, legiuitorul nu a inclus condiții suplimentare pentru autorizarea unei supravegheri în spații private.

În considerarea modalităților de realizare a supravegherii video, audio sau prin fotografiere, procurorul va avea un rol important în a stabili, mai înainte de autorizare, modalitatea concretă în care se va desfășura măsura, fiind obligat să o precizeze în propunerea pe care o va formula în fața judecătorului de drepturi și libertăți. Acesta din urmă va trebui să analizeze propunerea în special prin prisma proporționalității ei și să determine care modalitate concretă de desfășurare a supravegherii va îndeplini condițiile legale, ținând seama de diferențele de ingerință ce pot fi aduse inclusiv între aceste modalități concrete de punere în executare.

Dacă se va impune o supraveghere în spații private, judecătorul de drepturi și libertăți va putea să autorizeze pătrunderea în spații private pentru activarea sau dezactivarea mijloacelor tehnice folosite pentru supraveghere. Această activitate se va putea realiza numai de organele de urmărire penală, făcând parte din punerea în executare a măsurii. Un neajuns al legii este că nu prevede reguli clare privind pătrunderea în spații private, neexistând dispoziții pentru a o limita. În acest sens se impune ca, în virtutea respectării art. 8 Conv.EDO, judecătorul de drepturi și libertăți să indice de câte ori au voie organele de urmărire penală să pătrundă, cum se va realiza aceasta, ce activități pot desfășura pentru instalarea sau dezinstalarea tehnicii, cât timp pot sta în locația privată etc.

Prin dezvoltarea tehnologică, supravegherea în spații private nu va fi condiționată de pătrunderea în respectivul spațiu, putând fi utilizate microfoane puternice și specializate care pot recepționa sunetul prin pereți sau, mai ales, prin geamurile unei locuințe. Totodată, dacă se va autoriza și accesul la un sistem informatic, se va putea proceda la înregistrarea persoanei prin intermediul propriului său dispozitiv. Despre metodele astfel folosite va trebui să fie informat judecătorul de drepturi și libertăți prin propunerea formulată de procuror, mandatul de supraveghere tehnică trebuind să fie expres și cât mai limitat doar la măsurile necesare într-o societate democratică.

Titlul VII
Localizarea sau urmărirea prin mijloace tehnice

Capitolul I
Aspecte generale

Secțiunea 1. Utilitatea metodei speciale de supraveghere

Ultima metodă specială de supraveghere tehnică prevăzută de Codul de procedură penală este *localizarea sau urmărirea prin mijloace tehnice*, prin care legiuitorul a dorit să confere organelor de urmărire penală posibilitatea de a afla, în timp real, locația unei persoane urmărite în vederea tragerii la răspundere penală, executării mandatului de arestare preventivă sau în vederea executării pedepsei. Ca în cazul oricărei metode speciale de supraveghere, măsura va putea fi autorizată numai pentru viitor, în situația în care s-ar dori obținerea datelor de localizare trecute ale persoanei, aceasta ar putea fi realizată numai prin metoda specială de cercetare a obținerii datelor de trafic și de localizare prevăzută de art. 152 C.pr.pen.

Sub aspectul gravității ingerinței aduse drepturilor și libertăților fundamentale ale unei persoane, în mod corect s-a considerat că localizarea unei persoane reprezintă o ingerință forte în viața privată a unei persoane[1], însă, prin natura sa, va avea un caracter mai puțin invaziv decât alte metode speciale de supraveghere, de exemplu, interceptarea comunicațiilor unei persoane[2] sau supravegherea video, audio sau prin fotografiere.

Utilitatea metodei speciale de supraveghere constă în posibilitatea determinării cu mare precizie a locului în care se află o persoană sau un obiect, fără a presupune monitorizarea ei continuă și directă de către organele de urmărire penală, prin filaj[3]. Din acest punct de vedere, metoda este mai facil de aplicat, întrucât presupune un efort minim și este aptă să mențină secretă desfășurarea operațiunii față de persoana vizată.

Dincolo de efortul minim care trebuie depus în punerea în executare a măsurii, amintim că realizarea supravegherii tehnice se va realiza prin mijloace tehnice care sunt mai greu de eludat de către persoanele urmărite, în special dacă se bazează pe dispozitive folosite curent (telefoane mobile, tablete). Comparativ, o persoană are posibilitatea de a alege să nu vorbească la telefon dacă se simte supravegheată, putând folosi metode de comunicații criptate, deosebit de greu de interceptat, dar tot va avea asupra sa un telefon mobil sau se va deplasa cu un mijloc de transport pe care poate fi atașat un dispozitiv de localizare.

Gradul de fidelitate al măsurii va fi unul ridicat, rezultatele privind localizarea putând fi supuse unei verificări tehnice pentru autenticitate, nefiind susceptibile de a fi influențate de percepția subiectivă a unei persoane sau eroarea umană. Localizarea cea mai precisă se

[1] *Gh. Mateuț*, Procedură penală, 2019, p. 675.
[2] CEDO, cauza *Uzun c. Germania*, Hotărârea din 2 decembrie 2010, §72, pe *hudoc.echr.coe.int*
[3] *D.E. Hall*, op. cit., p. 113.

poate realiza prin dispozitive de tip GPS, care vor putea indica o poziție absolută pe glob cu coordonate exacte de latitudine și longitudine[1]. Având caracterul de date informatice, ele vor putea fi supuse procedurii de semnare și certificare prin utilizarea unei semnături electronice extinse, conform art. 142[1] C.pr.pen.

Caracterul tehnic și continuu conduce la rezultate care pot fi ușor folosite de organele judiciare dacă se vor suprapune pozițiile geografice obținute prin măsură pe o hartă, prin raportare la alte obiective cunoscute putându-se stabili corelații între deplasările persoanei și alte acțiuni (de pildă, se va determina unde este angajată). În același timp, realizându-se o hartă a deplasărilor pentru o perioadă mai lungă de timp, se vor putea determina obiceiurile persoanei urmărite, prin raportare la rutele folosite, punctele unde se oprește, durata opririi etc.

Cunoașterea locației în timp real a unei persoane poate fi utilă și pentru realizarea altor măsuri de supraveghere tehnică, permițând, în cazul supravegherii video, audio sau prin fotografiere în spații private, instalarea și dezinstalarea, în condiții de siguranță și de confidențialitate, a mijloacelor tehnice de supraveghere.

Prin coroborarea mai multor localizări prin mijloace tehnice, dispuse față de persoane diferite, se va putea proba că două sau mai multe persoane au fost în aceeași locație în același moment, putând fi prezumată concluzia că aceste persoane s-au întâlnit, întrucât gradul de precizie în localizare va fi unul mare.

Scopul principal al folosirii unei asemenea metode speciale de supraveghere constă în *descoperirea locației unei persoane căutate*, dar și în *monitorizarea mișcărilor persoanei*, pentru a obține probe indirecte în procesul penal. Nu va conta unde se va amplasa dispozitivul de localizare – asupra unei persoane sau asupra unui obiect – pentru a se considera ca scopul supravegherii tehnice să îl constituie activitățile persoanei, din perspectiva locației desfășurării acestora.

Scopul secundar al metodei speciale este monitorizarea mișcărilor unui bun, de pildă, al unui transport de bunuri ilicite[2], în cadrul metodei speciale de cercetare a livrării supravegheate. În atare situație, va conta mai puțin cine va mișca din loc respectivul obiect, ci va conta faptul că acesta se va deplasa dintr-o locație în alta. Și în această privință, vor putea fi obținute probe indirecte în procesul penal.

Scopul terțiar al metodei speciale de supraveghere constă în sprijinirea punerii în executare a mandatului de arestare preventivă și a mandatului de executare al pedepsei, atunci când persoana nu este găsită sau se sustrage. Într-o asemenea situație, supravegherea tehnică se va dispune în cadrul procedurii speciale a *dării în urmărire*, posibilitatea aceasta fiind prevăzută de art. 523 alin. (1) lit. a) C.pr.pen.

Secțiunea a 2-a. Localizarea sau urmărirea prin mijloace tehnice înainte de intrarea în vigoare a Codului de procedură penală

Metoda specială de supraveghere tehnică nu constituie o noutate pentru procesul penal, posibilitatea folosirii acesteia fiind reglementată și în cuprinsul Codului de procedură penală

[1] *J.K. Petersen*, Handbook of Surveillance Technologies, Third Edition, Ed. CRC Press, Boca Raton, Florida, 2012, p. 70.

[2] *G. Suleiman, A.O. Umar, S.E. Adekunle*, Development and Implementation of Vehicle Movement Notification and Location using GSM, GPS and Web based Information System, în International Journal Computer Network and Information Security no. 8/2018, pp. 38-39.

anterior sub două forme: *i)* împreună cu interceptarea și înregistrarea convorbirilor sau comunicărilor efectuate prin telefon ori prin orice mijloc electronic de comunicare [art. 91[1] alin. (1) C.pr.pen. anterior] și *ii)* în mod distinct (art. 91[4] C.pr.pen. anterior). Diferența dintre cele două metode consta în tehnologia folosită – prima se realiza pe baza informațiilor obținute de la furnizorul de servicii de comunicații electronice, a doua se realiza pe baza localizării prin alte mijloace tehnice (de exemplu, dispozitive GPS).

Prima modalitate a localizării, potrivit Codului de procedură penală anterior, era reglementată de art. 91[1] alin. (1) C.pr.pen., astfel: „*interceptarea și înregistrarea convorbirilor sau comunicărilor efectuate prin telefon ori prin orice mijloc electronic de comunicare se realizează cu autorizarea motivată a judecătorului, la cererea procurorului care efectuează sau supraveghează urmărirea penală, în condițiile prevăzute de lege, dacă sunt date ori indicii temeinice privind pregătirea sau săvârșirea unei infracțiuni pentru care urmărirea penală se efectuează din oficiu, iar interceptarea și înregistrarea se impun pentru stabilirea situației de fapt ori pentru că identificarea* ***sau localizarea participanților*** *nu poate fi făcută prin alte mijloace ori cercetarea ar fi mult întârziată*" (s.n.). În cazul acesta, metoda specială de supraveghere era interceptarea și înregistrarea convorbirilor telefonice care, cel puțin în ultimul deceniu înainte de abrogarea Codului de procedură anterior, se realiza în exclusivitate de S.R.I. ca unică entitate abilitată. Întrucât, din punct de vedere tehnic, exista o interconectare cu fiecare furnizor de servicii de comunicații publice, orice convorbire sau comunicare telefonică putea fi interceptată, cu această ocazie preluându-se și alte date decât cele de conținut ale convorbirii – date trafic, date despre echipament, dar și datele de localizare. Astfel, deși se urmărea interceptarea convorbirilor, între informațiile obținute ca metadate se afla și locația, existând întotdeauna o posibilitate ca organele de urmărire penală să le folosească[1].

Un neajuns al acestei metode era localizarea insuficient de precisă, ținând seama de limitările rețelelor de telefonie mobilă în localizare, în special în mediul rural, unde precizia poate fi și de 1 km[2]. În mediul urban, precizia putea fi foarte mare, însă acest lucru se datora faptului că celulele de comunicații erau mai restrânse, ca urmare a densității mai mari de turnuri de recepție. În plus, trebuie să avem în vedere că o localizare urma să se realizeze doar atunci când se efectua un apel telefonic, informațiile de localizare fiind cele mai relevante în atare situație[2].

Metoda de localizare prin interceptarea comunicațiilor nu se mai regăsește în cuprinsul Codului de procedură penală, fiind inoperabilă la acest moment, întrucât lipsește un cadru legislativ și logistic necesar pentru a permite procurorului și organelor de cercetare penală să pună în executare o astfel de localizare prin mijloace tehnice. Mai exact, în legislația actuală, simpla autorizare a interceptării comunicațiilor nu va permite și obținerea datelor de localizare, trebuind să fie autorizată și localizarea sau urmărirea prin mijloace tehnice. Nici dacă s-ar obține o asemenea autorizare, nu ar fi posibilă localizarea, deoarece, conform Protocolului încheiat între P.I.C.C.J. și S.R.I. la data de 08.12.2016, va fi posibilă folosirea echipamentelor C.N.I.C. din cadrul S.R.I. numai pentru punerea în executare a supravegherii tehnice, constând în

[1] *M. Furini, V. Tamanini*, Location privacy and public metadata in social media platforms: attitudes, behaviors and opinions, în Multimedia Tools and Applications, vol. 74, no. 21/november 2015, p. 9811.

[2] *J. Yang, A. Varshavsky, H. Liu, Y. Chen*, Accuracy Characterization of Cell Tower Localization, Conferința UbiComp 2010: Ubiquitous Computing, 12th International Conference, Copenhaga, Danemarca, 26-29 september 2010, pe *www.researchgate.net*

interceptarea comunicațiilor ori a oricărui tip de comunicare la distanță[1]. În lipsa unei mențiuni exprese privind posibilitatea folosirii echipamentelor pentru a procesa datele de localizare, nu va putea fi pusă în executare măsura de supraveghere tehnică prevăzută de art. 138 alin. (1) lit. d) C.pr.pen. prin C.N.I.C.

A doua metodă specială de localizare prevăzută de Codul de procedură penală anterior este cea care își găsește corespondentul în legislația actuală, anterior fiind prevăzută de art. 91[4] C.pr.pen. anterior. Potrivit acestui articol, „*dispozițiile art. 91[1]-91[3] se aplică în mod corespunzător și în cazul înregistrărilor în mediul ambiental, localizării sau urmăririi prin GPS ori prin alte mijloace electronice de supraveghere*". Prevederea într-un articol distinct a localizării sau urmăririi prin GPS ori prin alte mijloace tehnice semnifică împrejurarea că legiuitorul și-a dorit existența și a unei metode separate de localizare, care să nu se fundamenteze pe rețelele de telefonie mobilă. Deși era reglementată alături de înregistrările în mediu ambiental, cu care nu are legătură metoda despre care face vorbire, legiuitorul a prevăzut aceleași condiții de autorizare și punere în executare.

La momentul la care au fost introduse respectivele dispoziții legale[2], localizarea prin GPS nu se putea realiza prin telefoanele mobile de la acea vreme, întrucât erau dispozitive relativ simple față de cele actuale, fiind obligatorie, la acel moment, întrebuințarea unui dispozitiv separat de localizare amplasat asupra unei persoane sau unui obiect. Deoarece se impunea cunoașterea persoanei sau a obiectului, precum și locația sa inițială, conform dispozițiilor Codului de procedură penală anterior, darea în urmărire nu se putea realiza cu această a doua metodă dacă viza persoana urmărită, dat fiind faptul că nu se putea amplasa un dispozitiv GPS asupra unei persoane a cărei locație nu este cunoscută.

Secțiunea a 3-a. Forma actuală a localizării sau urmăririi prin mijloace tehnice

În prezent, localizarea sau urmărirea prin mijloace tehnice constituie o metodă de supraveghere tehnică, amintită expres în cuprinsul art. 138 alin. (13) C.pr.pen. Fiind o astfel de metodă, va prelua toate caracteristicile supravegherii tehnice cu privire la condițiile legale de autorizare, procedura autorizării și punerea în executare a măsurii, astfel că facem trimitere la părțile din lucrare în care am detaliat fiecare dintre aceste aspecte, urmând ca în secțiunile care vor urma să tratăm numai particularitățile acestei măsuri în cadrul mai larg al supravegherii tehnice.

Nu poate fi contestat caracterul de măsură de supraveghere tehnică al localizării sau urmăririi prin mijloace tehnice, întrucât reprezintă un procedeu probatoriu prin care sunt restrânse drepturile fundamentale ale persoanei supuse măsurii, se desfășoară în mod secret,

[1] Conform art. 1 din Protocolul nr. 2440/C din 08.12.2016 (P.I.C.C.J.) și 9331 din 07.12.2016 (S.R.I.), „părțile cooperează potrivit competențelor și atribuțiilor prevăzute de lege pentru: a) stabilirea condițiilor concrete de acces nemijlocit și independent al Ministerului Public la sisteme tehnice ale Centrului Național de Interceptare a Comunicațiilor din cadrul Serviciului Român de Informații, în scopul exercitării supravegherii tehnice prevăzute de art. 138 alin. (1) lit. a) din Codul de procedură penală; b) promovarea și asigurarea cooperării permanente, prompte și eficiente între Serviciul Român de Informații, prin structurile sale și Ministerul Public, respectiv structurile acestuia, pentru realizarea activităților prevăzute la litera a)".

[2] Metoda specială de supraveghere a localizării sau urmăririi prin GPS ori prin alte mijloace electronice de supraveghere a fost introdusă prin pct. 49 al art. I din Legea nr. 356 din 21 iulie 2006 (M. Of. nr. 677 din 7 august 2006).

fără cunoștința persoanei supravegheate, are un caracter numai pentru viitor, se poate dispune numai în cursul urmăririi penale și încuviințarea ei se va face de judecătorul de drepturi și libertăți, în condițiile legii.

În ceea ce privește definiția actuală a metodei speciale de supraveghere, legiuitorul a prevăzut-o la art. 138 alin. (7) C.pr.pen., în care se arată că: „*prin «localizare sau urmărire prin mijloace tehnice» se înțelege folosirea unor dispozitive care determină locul unde se află persoana sau obiectul la care sunt atașate*". După cum se poate observa, nu există modificări majore în privința metodei speciale de supraveghere din punctul de vedere al definiției și al obiectului acesteia față de legislația procesuală penală anterioară. Pentru înțelegerea metodei speciale, o să facem câteva precizări privind termenii folosiți de legiuitor.

Deși par a fi doi termeni distincți, legiuitorul a ales să se refere la „localizare" și la „urmărire" pentru a nu crea confuzie pentru persoanele care vor trebui să autorizeze sau să pună în executare măsura. *Localizarea* va însemna, în mod evident, determinarea coordonatelor geografice a locației persoanelor sau obiectului vizat de măsură, termenul nefiind susceptibil de alte interpretări. În schimb, *urmărirea* persoanei putea cauza o anumită confuzie ca termen de sine stătător, întrucât urmărirea unei persoane nu este obligatoriu a fi făcută prin localizarea acesteia. De pildă, va constitui o urmărire a persoanei și acțiunea de filaj, care se va realiza potrivit art. 138 alin. (1) lit. c) C.pr.pen., însă scopul măsurii nu va fi cel de poziționare geografică precisă a persoanei, ci urmărirea acțiunilor pe care le întreprinde. Sub acest aspect, rezultă că localizarea sau urmărirea persoanei se va face exclusiv pentru a se cunoaște poziția sa geografică actuală sau pentru a monitoriza toate mișcările sale pe durata prevăzută de mandatul de supraveghere tehnică. Trebuie să ținem seama că nevoia de claritate și previzibilitate a măsurilor de supraveghere tehnică este subliniată de Curtea Europeană a Drepturilor Omului inclusiv prin raportare la tehnologiile folosite[1] și la întinderea pe care trebuie să o aibă fiecare măsură prevăzută distinct de lege[2].

Expresia de „mijloace tehnice" este folosită pentru a se sublinia că în localizare se vor folosi tehnologii de diverse tipuri pentru determinarea locației. Cel mai lesne de înțeles mijloc este rețeaua de sateliți de geolocație, denumită de Codul de procedură penală anterior ca „GPS". Termenul anterior folosit nu era precis, întrucât există mai multe sisteme de geolocație satelitară la nivel mondial, fiecare având particularitățile sale, printre care diferențe de precizie, zonă vizată etc[3]. Sistemele de poziționare GPS au devenit o soluție viabilă de localizare în aplicații comerciale începând cu anii 1990, fiind ulterior dezvoltate într-atât de mult încât sunt accesibile publicului larg la prețuri mici ce pot justifica includerea tehnologiei în telefoane mobile[4].

În privința tehnologiilor concrete care vor putea fi folosite, această problemă va face obiectul unei secțiuni separate[5]. În ceea ce privește *dispozitivele* prin care se determină locația obiectului sau persoanei la care sunt atașate, acestea pot fi un telefon mobil sau un dispozitiv anume destinat transmiterii locației, dotat cu capacitate de localizare, dar și de transmitere de informații și atașat în mod secret pe un obiect sau o persoană.

---

[1] CEDO, cauza *Roman Zakharov c. Rusia*, Hotărârea din 4 decembrie 2015, §229.

[2] CEDO, cauza *Kruslin c. Franța*, Hotărârea din 24 aprilie 1990, §34.

[3] Primul sistem implementat a fost cel american, GPS – Global Positioning System, operat de Forțele Spațiale ale S.U.A., ulterior fiind dezvoltat cel rusesc GLONASS – Global Navigation Satellite System, operat de Roscosmos, mai apoi european GALILEO, indian NAVIK etc.

[4] *J.K. Petersen*, op. cit., p. 56.

[5] *V. infra*, Titlul VII, Capitolul III.5.

Capitolul II
Particularitățile autorizării localizării și urmăririi prin mijloace tehnice

Deoarece metoda specială de supraveghere tehnică a localizării sau urmăririi prin mijloace tehnice presupune o ingerință adusă dreptului la viață privată al unei persoane, se impune ca atât procurorul – la momentul formulării propunerii de încuviințare a supravegherii tehnice, cât și judecătorul de drepturi și libertăți – la momentul soluționării propunerii, să precizeze cât mai exact în ce va consta localizarea și urmărirea, cum se vor desfășura și ce mijloace vor fi folosite. Întrucât procedura de autorizare a măsurilor de supraveghere tehnică am tratat-o deja într-o secțiune distinctă, în cele ce urmează vom detalia aceste particularități.

Conform art. 140 alin. (2) C.pr.pen., cererea procurorului de încuviințare a supravegherii tehnice trebuie să includă „*indicarea măsurilor de supraveghere tehnică care se solicită a fi dispuse*". Regula instituită de legiuitor nu presupune numai indicarea textului de lege care reglementează măsura solicitată, ci impune detalierea modului în care se va realiza supravegherea tehnică, pentru ca judecătorul de drepturi și libertăți să poată aprecia asupra îndeplinirii condițiilor legale, în special caracterul proporțional și subsidiar al măsurii. În cadrul acestei analize, judecătorul de drepturi și libertăți ar putea încuviința o asemenea măsură în locul unei alte măsuri de supraveghere tehnică mai intruzive, precum realizarea supravegherii video, audio sau prin fotografiere.

Sub acest aspect, trebuind să fie menținut un just echilibru între interesul public și cel privat, pentru stabilirea caracterului proporțional al măsurii, procurorul va trebui mai întâi să detalieze ce va fi supus localizării sau urmăririi prin mijloace tehnice: *o persoană* sau un *obiect*. Este evident că, în cazul localizării unei persoane, ingerința adusă vieții private va fi mai mare, în această categorie intrând localizarea sau urmărirea persoanei prin atașarea unui dispozitiv în haine, în bagajul de mână, în poșetă, în interiorul mașinii folosite[1] etc. În schimb, va exista o ingerință mult mai redusă în cazul în care se va realiza localizarea unui obiect, de pildă, un container de transport maritim în care se află droguri (de regulă, în cadrul livrării supravegheate). În această din urmă situație, va fi afectată numai viața privată a persoanelor care iau contact cu transportul și, chiar și într-o asemenea situație, ingerința va fi redusă, întrucât vor desfășura activități în jurul obiectului pe care s-a atașat dispozitivul de localizare. Nu va constitui o ingerință deosebit de mare în viața privată a unui șofer de autocamion dacă va fi monitorizat prin măsura de supraveghere tehnică transportul său, relevându-se un număr mic de informații despre viața sa privată: numărul de opriri, localuri preferate de-a lungul drumului, dacă respectă dispozițiile legale privind orele de conducere și orele de repaus etc. Oricum, ținând seama de costurile asociate cu transportul de marfă, multe societăți realizează urmărirea în timp real a flotei de camioane prin sistem GPS, aceasta constituind o formă de supraveghere privată, consimțită de angajat.

În lipsa mențiunilor arătate mai sus, apreciem că nu se poate încuviința metoda specială de supraveghere tehnică, întrucât judecătorul de drepturi și libertăți nu va putea realiza un control complet al condițiilor de fond prevăzute de art. 139 alin. (1) C.pr.pen.

[1] CEDO, cauza *Uzun c. Germania*, Hotărârea din 2 decembrie 2010, §11-13, pe *hudoc.echr.coe.int*

Prin încheierea judecătorului de drepturi și libertăți prin care se admite propunerea procurorului, urmează a se încuviința localizarea sau urmărirea prin mijloace tehnice, fiind necesar ca acesta să indice toate mențiunile cuprinse la art. 140 alin. (5) C.pr.pen., între care vor prezenta aspecte particulare, în cazul acestei metode speciale, următoarele elemente: *indicarea măsurii concrete încuviințate*, *numele persoanei supuse măsurii de supraveghere tehnică ori datele de identificare ale acesteia, dacă sunt cunoscute*, și *elementele de identificare a fiecărui telefon*.

Referitor la *indicarea măsurii concrete încuviințate*, judecătorul de drepturi și libertăți va trebui să arate expres că localizarea se va face față de o persoană sau față de un obiect și să determine dacă măsura se va pune în executare printr-un dispozitiv atașat sau prin accesarea telefonului persoanei supravegheate ori prin alte mijloace de localizare. Această din urmă mențiune va fi importantă, întrucât, dacă se dorește localizarea persoanei prin telefonul său mobil, va trebui autorizată deodată și măsura accesului la un sistem informatic față de acea persoană, pentru a se încuviința pătrunderea în telefon în vederea instalării unui program de localizare.

Numele persoanei supuse măsurii de supraveghere tehnică ori datele de identificare ale acesteia, dacă sunt cunoscute, vor trebui precizate în cazul în care măsura se dispune față de o persoană. În cazul în care se va dori localizarea sau urmărirea prin mijloace tehnice a unui obiect, chiar dacă Codul de procedură penală nu conține vreo dispoziție expresă, prin analogie va trebui identificat bunul care va fi supus urmăririi – transportul supravegheat, containerul naval etc. În contextul în care măsura specială de cercetare a livrării supravegheate presupune o supraveghere permanentă a unui transport ilegal sau suspect, localizarea sau urmărirea prin mijloace tehnice va reprezenta o obligație practică. Din această situație reiese unul dintre neajunsurile Codului de procedură penală prin neunificarea procedurii de autorizare[1], deoarece ar presupune ca, mai întâi, procurorul să autorizeze livrarea supravegheată, apoi să obțină distinct un mandat de supraveghere tehnică, conducând la întârzierea punerii în executare a măsurii.

Elementele de identificare a fiecărui telefon vor trebui să fie menționate numai dacă se va proceda la localizarea sau urmărirea prin mijloace tehnice cu ajutorul dispozitivului GPS încorporat în telefonul mobil urmărit sau folosit de persoana vizată de măsura de supraveghere tehnică.

[1] *Gh. Mateuț*, Observații critice privind noua reglementare a supravegherii tehnice într-o prezentare comparativă, în Caiete de Drept Penal nr. 3/2015, p. 13.

Capitolul III
Particularitățile punerii în executare a localizării și urmăririi prin mijloace tehnice

Secțiunea 1. Organul care va pune în executare măsura

În conformitate cu dispozițiile art. 142 alin. (1) C.pr.pen., punerea în executare a metodei speciale de supraveghere a localizării și urmăririi prin mijloace tehnice se va face de către procuror. Prin dispoziția expresă a procurorului, punerea în executare poate fi delegată organelor de cercetare penală sau lucrătorilor specializați din cadrul poliției.

Particularitatea punerii în executare a metodei speciale de supraveghere constă în identificarea semnificației acestei activități, prin raportare la toate operațiunile materiale care se vor realiza. Ținând seama de definiția măsurii, credem că vor avea semnificația de punere în executare numai acțiunile de localizare sau urmărire prin mijloace tehnice, nu și alte acțiuni. Astfel, punerea în executare va însemna că organul competent va proceda la întrebuințarea mijloacelor tehnice pentru monitorizarea, înregistrarea locației persoanei sau obiectului urmărit cu caracter de continuitate. Cu alte cuvinte, se va asigura că dispozitivul care transmite locația este funcțional și se recepționează locația transmisă de acesta, în caz contrar luând toate măsurile necesare. În funcție de specificul infracțiunii care face obiectul urmăririi penale, se vor putea utiliza și mijloace care nu transmit la distanță locația, acestea trebuind să fie recuperate pentru a putea fi valorificate rezultatele supravegherii tehnice.

După ce se va încheia punerea în executare a metodei speciale de supraveghere, rezultatul supravegherii tehnice va îmbrăca forma unui proces-verbal încheiat în conformitate cu dispozițiile art. 143 alin. (1) C.pr.pen.

Apreciem că în cadrul punerii în executare a măsurii nu va intra însăși operațiunea de amplasare asupra unui obiect sau asupra unei persoane a dispozitivului prin care se determină locația, întrucât aceasta constituie o operațiune tehnică anterioară localizării efective și nu este conținută de definiția măsurii. Spre deosebire de interceptarea comunicațiilor, persoana care va atașa dispozitivul de localizare nu va avea acces la datele rezultate din supravegherea tehnică, nu va avea niciun control asupra procedurii și nu va realiza ea însăși localizarea sau urmărirea dispozitivului. De cele mai multe ori, activitatea respectivă va presupune atașarea magnetică a unei cutii de mici dimensiuni de șasiul mașinii persoanei supravegheate (sub mașină), operațiunea putând fi realizată în trafic în decurs de câteva secunde. În schimb, în cazul metodei speciale prevăzute de art. 138 alin. (1) lit. a) C.pr.pen., punerea în executare se va suprapune cu însăși conectarea terminalului folosit la serverele C.N.I.C. din cadrul S.R.I., implementarea în sistemul informatic al mandatului și setarea sistemului pentru realizarea operațiunii permițând un control deplin pentru persoana care pune în executare măsura.

Ca atare, față de conținutul concret al măsurii, apreciem că atașarea dispozitivului de localizare va putea fi realizată și de un investigator sub acoperire ori un colaborator, acesta din urmă neavând calitatea de lucrător specializat al poliției, deoarece această operațiune nu va intra în sfera punerii în executare a supravegherii tehnice.

Secțiunea a 2-a. Consemnarea activităților rezultate din localizarea sau urmărirea prin mijloace tehnice

În conformitate cu dispozițiile art. 143 alin. (1) C.pr.pen., activitățile de supraveghere tehnică desfășurate prin localizarea sau urmărirea prin mijloace tehnice se vor consemna într-un proces-verbal. Acesta se va încheia de procuror sau de organul de cercetare penală, consemnându-se fiecare activitate realizată. Întrucât acest act procedural prezintă numai câteva aspecte particulare, facem trimitere la secțiunea în care am analizat în mod unitar consemnarea activităților de supraveghere tehnică[1].

Deși textul are o aplicabilitate generală, din analizarea dispozițiilor art. 143 alin. (1) C.pr.pen.[2], observăm că se face o trimitere cu relevanță pentru metoda specială de supraveghere a localizării și urmăririi prin mijloace tehnice, ca urmare a mențiunii privind „*consemnarea rezultatelor activităților efectuate (…) care contribuie la identificarea ori localizarea persoanelor*". Aceste informații vor trebui să fie consemnate într-un format absolut – prin date geografice precise, indicându-se latitudinea și longitudinea la care se afla persoana sau obiectul cercetat, dar și într-un format relativ – indicarea adresei prin numele străzii, numărul, localitatea, județul sau, după caz, drumul național/județean sau comunal, tronsonul și kilometrul. Frecvența cu care se va reda locația va depinde de împrejurările cauzei și de dispozitivul folosit, acestea putând fi optimizate de organele de urmărire penală în funcție de nevoi. Întrucât dispozitivele care se vor atașa în mod ascuns la o persoană sau un obiect vor avea o baterie, frecvența localizării va influența durata de viață a bateriei dispozitivului. În concret, dacă se vor realiza doar poziționări la fiecare minut, bateria va rezista câteva zile, dacă însă numărul va fi mai redus, va putea rezista câteva săptămâni. Deși pare un element tehnic, considerăm că este important a se menționa în procesul-verbal și dacă se modifică frecvența comunicării locației dispozitivului.

Alături de datele de localizare, vor fi esențiale mențiunile privind *data și ora*, fără de care nu se poate stabili relevanța probatorie a datelor de localizare. Numai prin coroborarea elementului spațial – localizarea – cu cel temporal – data și ora – se va putea realiza urmărirea unei persoane sau a unui obiect. Nu va fi suficient să se precizeze doar data și ora începutului și încheierii activității de supraveghere tehnică, ci va fi necesar să se precizeze pentru fiecare locație geografică data și ora la care persoana sau obiectul se afla la acea locație.

Întrucât elementele amintite mai sus sunt exprimate prin simple mențiuni generate de un sistem informatic de forma „dispozitiv – oră – locație", este preferabil ca organele de urmărire penală să includă în cuprinsul procesului-verbal și procesarea geografică a datelor prin suprapunerea lor peste hărți. Acest lucru se realizează în mod facil cu un sistem informatic, chiar și dispozitivele de urmărire GPS comerciale având această facilitate. Ar fi de neconceput ca la dosarul cauzei să existe numai un set de coordonate geografice care, scoase din context, nu furnizează în mod facil probe. Organele judiciare nu sunt sisteme informatice, procurorul trebuind să exercite o diligență deosebită în modul în care prezintă probele obținute, în scopul

[1] *V. supra*, Titlul III, Capitolul III.

[2] Conform art. 143 alin. (1) C.pr.pen., „procurorul sau organul de cercetare penală întocmește un proces-verbal pentru fiecare activitate de supraveghere tehnică, în care sunt consemnate rezultatele activităților efectuate care privesc fapta ce formează obiectul cercetării sau contribuie la identificarea ori localizarea persoanelor, datele de identificare ale suportului care conține rezultatul activităților de supraveghere tehnică, numele persoanelor la care se referă, dacă sunt cunoscute, sau alte date de identificare, precum și, după caz, data și ora la care a început activitatea de supraveghere și data și ora la care s-a încheiat".

de a face mai facilă administrarea justiției de către instanță. Cu ajutorul unui sistem informatic, se va putea determina și viteza cu care se deplasa persoana sau obiectul urmărit.

Cu ocazia întocmirii procesului-verbal de consemnare a activităților de supraveghere tehnică, va trebui să se descrie mișcările persoanei urmărite prin metoda specială de supraveghere, indicându-se locul relativ unde se află, direcția în care pornește la un anumit moment și persoanele cu care se întâlnește (în cazul în care și acestea sunt supuse măsurii localizării și datele se pot corobora).

O mențiune care nu prezintă mari dificultăți o reprezintă *numele persoanelor* la care se referă activitățile efectuate, dacă acestea sunt cunoscute, ele trebuind să fie prevăzute în procesul-verbal alături de identificarea echipamentului folosit pentru acestea. Dacă se va întrebuința măsura pentru localizarea unui obiect, atunci credem că acesta va trebui să fie identificat prin *datele sale de identificare*, de pildă, numărul de înmatriculare al autovehiculului, marca, modelul etc., precum și identificarea echipamentului folosit și care a fost atașat.

O mențiune cu privire la metoda specială de supraveghere care nu este prevăzută de legiuitor este *modul în care s-a realizat atașarea dispozitivului și persoana care a realizat această activitate*. Credem că această mențiune este importantă pentru a cunoaște și aspectele anterioare localizării, în vederea verificării legalității unui atare procedeu. Întrucât se impune ca un dispozitiv să fie atașat în mod ascuns asupra unei persoane sau a unui bun, trebuie verificat dacă prin această activitate nu se aduce vreo ingerință suplimentară vieții private a unei persoane, precum pătrunderea în spații private de către persoana care va atașa dispozitivul.

Și în cazul localizării sau urmăririi cu mijloace tehnice, rezultatul activităților se va copia din punct de vedere digital și copia se va atașa într-un plic sigilat la procesul-verbal, în conformitate cu dispozițiile art. 143 alin. (2) C.pr.pen. Ca urmare a caracterului tehnic al localizării, rezultatul activităților va avea forma unor date informatice, generate de dispozitivul atașat persoanei sau obiectului urmărit și care vor fi transmise către un sistem informatic aflat în posesia organelor de urmărire penală. Transmisia și recepția se vor realiza în timp real, dispozitivul sau sistemul informatic de recepție va avea rolul de a capta informațiile transmise de dispozitivul de urmărire și de a le prezenta persoanei care pune în executare metoda specială de supraveghere. Alternativ, pot fi folosite dispozitive care nu realizează transmisii, ci doar stochează locațiile persoanei supravegheate, acestea trebuind să fie recuperate la momentul încetării măsurii.

Secțiunea a 3-a. Localizarea prin intermediul telefonului mobil

O variantă de a realiza localizarea sau urmărirea unei persoane prin mijloace tehnice constă în instalarea de programe specializate pe telefonul său mobil prin care să se transmită organelor de urmărire penală locația persoanei urmărite sau accesarea, prin alte căi, a modului GPS de pe acesta și transmiterea informațiilor către organul de urmărire penală. O atare posibilitate trebuie avută în vedere, în condițiile în care majoritatea telefoanelor mobile sunt dotate cu module GPS de mare precizie și au o conexiune constantă la internet[1]. În plus, la o simplă căutare pe internet se pot găsi numeroase aplicații comerciale pentru localizarea unui alt terminal, majoritatea fiind comercializate pentru părinții care vor să își monitorizeze copiii,

[1] *J.K. Petersen*, op. cit., p. 10; *M. Black, R.G. Smith*, Electronic Monitoring in the Criminal Justice System, în Trends and Issues in Crime and Criminal Justice no. 5/2003, p. 2.

dar pot fi folosite și pentru alte scopuri[1]. Din perspectiva obținerii informațiilor în această modalitate, dar în scopul securității naționale, încă din anul 2010, autoritățile S.U.A. (U.S. Department of Justice) au avut inițiativa de a cere dreptul de a realiza astfel de operațiuni de monitorizare a persoanelor, fără emiterea unui mandat[2]. În mod fericit, această solicitare legislativă a fost respinsă, întrucât o supraveghere în masă, fără mandat, ar fi încălcat în mod grav drepturile fundamentale ale persoanelor. În doctrina americană s-a subliniat că este mai puțin intruzivă o astfel de metodă de localizare decât interceptarea comunicațiilor[3], însă unele instanțe au conchis că, pentru a fi autorizată, localizarea prin intermediul telefonului mobil trebuie prevăzută distinct de lege[4].

În niciun caz, organele de urmărire penală nu trebuie să recurgă la tehnici și programe comerciale care au riscul inerent de a dezvălui că telefonul este urmărit, ci vor trebui să folosească programe specializate care să mențină secretul operațiunii. Din acest punct de vedere, securitatea din ce în ce mai bună a telefoanelor mobile împiedică instalarea unor astfel de programe fără ca ele să fie vizibile utilizatorului. Ultima versiune a sistemului de operare Android împiedică obținerea de informații privind localizarea dispozitivului de către aplicații care rulează în fundal și nu sunt vizibile utilizatorului[5].

Mai mult, chiar dacă nu este vizibilă o aplicație de localizare, folosirea modulului GPS poate fi trădată de meniurile care vor indica activarea sa, chiar dacă utilizatorul îl dezactivează (este necesar ca un program dedicat să poată porni modulul GPS pentru precizie maximă). Un alt aspect care poate trăda existența unui program instalat în vederea supravegherii constituie scăderea duratei de viață a bateriei, simptom care poate fi evident pentru unii utilizatori.

Cu toate acestea, trebuie remarcat faptul că doar prin încuviințarea metodei speciale de supraveghere a localizării sau urmăririi prin mijloace tehnice nu va exista autorizarea necesară pentru a o realiza prin intermediul telefonului mobil, fiind necesară emiterea unui mandat care să prevadă și accesul la un sistem informatic. Deoarece telefoanele mobile conțin date cu caracter personal deosebit de intime și pentru că instalarea unui program într-un telefon mobil presupune, prin ea însăși, pătrunderea în sistemul informatic, se va impune și autorizarea metodei speciale de supraveghere prevăzută la art. 138 alin. (1) lit. b) C.pr.pen.

Secțiunea a 4-a. Localizarea prin dispozitive atașate asupra persoanei sau obiectului

Metoda obișnuită de realizare a localizării sau urmăririi prin mijloace tehnice este atașarea asupra persoanei urmărite sau asupra obiectului urmărit a unui dispozitiv care va comunica foarte precis locația, la intervale regulate de timp, prin intermediul localizării GPS sau a unui dispozitiv echivalent de localizare.

Ca urmare a evoluției tehnologiei, dispozitivele electronice care permit localizarea au devenit din ce în ce mai compacte, putând fi ușor atașate asupra unei persoane sau asupra unui

[1] *A.-M. Oostveen, A. Vasalou, P. van den Besselaar, I. Brown*, Child Location Tracking in the US and the UK: Same Technology, Different Social Implications, în Surveillance & Society, vol. 12, no. 4/2014, pp. 582-583.

[2] *E.D. Cohen*, op. cit., p. 137.

[3] *D.E. Hall*, op. cit., p. 410.

[4] U.S. District Court, Southern District, Texas, Magistrate No. H-05-557M, 14 octombrie 2005, pe *www.courtlistener.com*

[5] *developer.android.com*

obiect. Utilizarea lor nu a fost gândită inițial în scopul prevenirii și combaterii infracțiunilor, ci în scop militar, odată cu dezvoltarea tehnologiei fiind accesibilă și publicului. Sistemul GPS (alături de alte sisteme internaționale compatibile) folosește sateliți din orbita pământului pentru a comunica ora exactă către receptorii GPS aflați în dispozitive care, prin calcule matematice și semnalul de la mai mulți sateliți, vor determina poziția exactă pe glob.

În privința dispozitivelor GPS, acestea pot fi de dimensiuni reduse, până la dimensiunea unei monede, fiind folosite inclusiv de cercetători pentru a studia migrația păsărilor, unde dimensiunea redusă este esențială pentru a putea fi susținută de zborul unei păsări[1]. Modele pur comerciale destinate supravegherii copiilor pot avea dimensiunea unui breloc și încorporează și un telefon mobil. Ținând seama de aceste dimensiuni reduse, precum și de specificul supravegherii tehnice – în special durata acesteia –, pot fi atașate asupra unei persoane astfel de dispozitive, pentru a se realiza localizarea și urmărirea deplasărilor sale. În cazul dispozitivelor GPS pentru obiecte, chiar și cele ce pot fi achiziționate de particulari, destinate pentru a fi montate pe șasiul unor mașini, pot avea dimensiunile unui telefon mobil, dar cu o durată de viață a bateriei de câteva săptămâni[2].

Este posibil ca dispozitivul GPS să fie unul pasiv (fără transmitere de date), fără să aibă capacitatea de a transmite în timp real poziția sa către organele de urmărire penală, necesitând ca acesta să fie recuperat pentru obținerea datelor[3]. Această situație era incidentă mai mult atunci când tehnologia era mai puțin avansată, necesitând dispozitive cu un consum energetic mai mare pentru transmisie, însă nu este de omis că există aplicații curente pentru o astfel de metodă. De pildă, în cazul unui transport aerian sau maritim, poziționarea GPS va fi posibilă, dar comunicațiile vor fi limitate, întrucât transportul urmărit nu va fi în raza de recepție a furnizorilor de servicii de comunicații[4] tip GSM.

O altă tehnologie care poate fi utilizată este cea a radiolocației în timp real, care poate fi folosită în interiorul unor clădiri, precum depozitele, fabricile etc., pentru supravegherea unei persoane sau a unui obiect, însă presupune instalarea de tehnică operativă locală pentru a capta semnalul, dar are avantajul că funcționează în interiorul unei clădiri, unde un dispozitiv GPS devine inutilizabil[5].

În viitor, este posibil ca dispozitive de geolocație să fie introduse în corpul uman, sub formă de implanturi (folosite deja asupra animalelor)[6], tatuaje electronice[7] sau chiar injectarea unor naniți (roboți microscopici) în vederea localizării unor persoane[8].

---

[1] De exemplu, un dispozitiv GPS gândit pentru păsări, precum pinguinul african sau gâsca de mare (cu greutăți între 2,5-3,5kg), poate avea dimensiunea de 38x17x12mm și greutatea de 8g cu tot cu baterie și transmițător GSM, pe *www.pathtrack.co.uk*

[2] *T. Claypoole, R. Balough*, Location Tracking and US Law: How Technology alters Expectations, în Journal of Internet Law no. 11/2012, p. 25.

[3] CEDO, cauza *Uzun c. Germania*, Hotărârea din 2 decembrie 2010, §11-13, pe *hudoc.echr.coe.int*

[4] Cu excepția comunicațiilor prin satelit, care vor fi excluse, pentru că presupun dispozitive mai mari, cu consum mai mare de energie.

[5] *B. Shah*, Wireless Location for Blueforce Tracking, în Law & Order no. 2/2014, p. 39.

[6] *M. Perras, S. Nebel*, Satellite Telemetry and its Impact on the Study of Animal Migration, în Nature Education Knowledge no. 3(12):4, 2012, pe *www.nature.com*

[7] *Y. Wang, Y. Qiu, S.K. Ameri et al.*, Low-cost, μm-thick, tape-free electronic tattoo sensors with minimized motion and sweat artifacts, în Revista Nature (Nature Partner Journals – Flexible Electronics 2) no. 6/2018, pe *doi.org*

[8] *J.K. Petersen*, op. cit., p. 347.

Toate dispozitivele care se vor atașa de o persoană sau de un obiect vor suferi de problema inerentă a necesității atașării, în prealabil, a dispozitivului. Această operațiune poate implica riscuri mari asupra persoanei care o realizează sau poate periclita caracterul secret al metodei de supraveghere, fiind preferabil a se încerca atașarea unui dispozitiv de localizare de mijloace de transport folosite regulat de persoana vizată.

Capitolul IV
Concluzii

Metoda specială de supraveghere a localizării sau urmăririi prin mijloace tehnice reprezintă un procedeu probatoriu prin care organele de urmărire penală pot afla deplasările sau locația unei persoane în cursul urmăririi penale, putând obține prin aceasta probe indirecte. Acestea vor avea o mare fidelitate, întrucât folosesc tehnologie de localizare care produce rezultate verificabile științific și pot fi mai greu de combătut. Localizarea poate fi întrebuințată asupra unei persoane sau asupra unui bun.

Nivelul ingerinței aduse vieții private a persoanei supuse măsurii va fi unul mai restrâns decât în cazul altor metode speciale de supraveghere sau cercetare, neputând fi cunoscute activitățile concrete desfășurate de persoana supravegheată, ci numai unde au loc acestea.

Punerea în executare va presupune doar localizarea sau urmărirea prin mijloace tehnice a persoanei, nefiind incluse operațiunile de instalare și dezinstalare a mijloacelor tehnice de localizare, întrucât aceste activități nu sunt menționate de lege.

În funcție de particularitățile metodei folosite, rezultatele activităților de supraveghere tehnică prin această metodă pot fi obținute în timp real sau odată cu dezinstalarea dispozitivului de urmărire de pe persoana sau obiectul țintă.

Din punctul de vedere al metodelor concrete folosite, contextul legislativ și logistic nu mai permite monitorizarea în timp real prin folosirea datelor obținute de la furnizorii de servicii de comunicații electronice sau furnizorii de rețele publice de comunicații electronice.

Ținând cont de caracterul tehnic al metodei, se va putea folosi concomitent cu accesul la un sistem informatic, pentru a se realiza localizarea sau urmărirea persoanei pe baza dispozitivului mobil pe care îl are asupra sa.

Titlul VIII
Obținerea datelor privind tranzacțiile financiare ale unei persoane

Capitolul I
Aspecte generale

Secțiunea 1. Utilitatea reglementării metodei speciale de cercetare a obținerii datelor privind tranzacțiile financiare ale unei persoane

În vederea cercetării unor infracțiuni, este necesar ca organele de urmărire să cunoască destinația și traseul unor sume de bani ori efectuarea unor operațiuni de către persoanele față de care se efectuează urmărirea penală sau aflate în legătură cu acestea. Desfășurarea unor tranzacții financiare poate servi mai multe scopuri infracționale, de la săvârșirea unei infracțiuni, obținerea folosului în urma săvârșirii infracțiunii, la ascunderea proveniență bunurilor rezultate din săvârșirea infracțiunii, dar și asigurarea lichidității necesare pentru a-și pregăti sustragerea de la răspunderea penală.

Pot fi imaginate multe situații în care obținerea datelor privind tranzacțiile financiare ale unei persoane poate furniza *probe directe* privind săvârșirea unei infracțiuni: de pildă, se va putea dovedi săvârșirea infracțiunilor de luare, respectiv dare de mită, atunci când mituitorul transferă o sumă de bani în contul funcționarului public mituit (disimulând, de regulă, operațiunea) sau realizează tranzacții succesive prin intermediul mai multor instituții de credit în cadrul unei infracțiuni de spălarea banilor[1], caz în care folosirea metodei speciale de cercetare va fi esențială[2]. Metodele de cercetare în astfel de situații constituie o adaptare la tehnicile din ce în ce mai complexe folosite de infractori în domeniul infracțiunilor economico-financiare[3]. În același sens, retragerea unor sume de bani considerabile din conturile unui inculpat poate constitui o probă că acesta se pregătește să fugă sau să se ascundă pentru a se sustrage de la urmărirea penală[4].

Aparent, metoda specială de cercetare ar privi doar aspecte de ordin patrimonial ce țin de o anumită persoană, dar, în realitate, constituie o restrângere deosebită a vieții private a

[1] Potrivit art. 49 alin. (1) lit. a) din Legea nr. 129 din 11 iulie 2019 pentru prevenirea și combaterea spălării banilor și finanțării terorismului, precum și pentru modificarea și completarea unor acte normative constituie infracțiunea de spălarea banilor: „schimbarea sau transferul de bunuri, cunoscând că provin din săvârșirea de infracțiuni, în scopul ascunderii sau al disimulării originii ilicite a acestor bunuri ori în scopul de a ajuta persoana care a săvârșit infracțiunea din care provin bunurile să se sustragă de la urmărire, judecată sau executarea pedepsei".

[2] *L.C. Kovesi*, Punerea sub supraveghere a conturilor bancare și a conturilor asimilate conturilor bancare, în Dreptul nr. 8/2003, p. 152.

[3] *C. Olaru*, op. cit., p.121.

[4] Retragerea unor sume de bani considerabile de la instituțiile de credit unde o persoană are conturi poate fi încadrată în sensul realizării de pregătiri pentru a fugi sau a se ascunde, în sensul art. 223 alin. (1) lit. a) teza a II-a C.pr.pen., însă va trebui coroborată cu alte elemente de fapt din care să rezulte incidența acestui caz de arestare.

unei persoane prin aflarea unor informații particulare privind obiceiurile acesteia, preferințele, viciile, starea de sănătate, dar și altele.

Deoarece are ca scop *dezvăluirea conținutului tranzacțiilor financiare*, organele de urmărire penală vor afla informații ce țin de sfera privată și care ar fi putut fi cunoscute acestora prin alte procedee probatorii, împrejurare care restrânge dreptul la viață privată[1].

Alături de obținerea de probe privind pregătirea sau săvârșirea unei infracțiuni, se vor obține, în mod necesar și inevitabil, informații care nu vor avea legătură cu cauza. În condițiile în care societatea modernă încurajează folosirea sistemelor bancare, cardurilor și modalităților electronice de plată (inclusiv prin intermediul smartphone-ului), în detrimentul folosirii monedei fizice, se poate lesne imagina cum întregile cumpărături ale unei persoane pot fi monitorizate de organele de urmărire penală. Prin procedeul probatoriu la care facem referire se vor putea cunoaște magazinele preferate ale persoanei, tipul acestora – supermarket, magazine de haine (de bărbați sau de femei), magazine de bijuterii, de telefoane, de băuturi etc.; se vor cunoaște dacă plătește utilități și la ce furnizori are abonament; dacă are probleme de sănătate – vizitarea unor clinici private, medici privați, achiziția regulată de produse din farmacii de un preț similar (existența unui tratament pentru o boală); deplasările persoanei – cumpărarea de benzină de la diverse benzinării din țară sau străinătate, plata pentru cazarea într-un hotel sau orice achiziție realizată cu cardul la un furnizor al cărei locație e cunoscută sau prin retragerea de bani de la un ATM (ale căror locații sunt indicate în orice astfel de operațiune). Dincolo de ce se poate cumpăra, se va putea cunoaște cât se cumpără, putându-se trage concluzii importante, mai ales în cazul unor achiziții exorbitante într-o perioadă scurtă. Nu vor fi uitate nici tranzacțiile financiare cu persoane particulare – împrumuturi, diverse plăți, care vor fi supuse atenției organelor de urmărire penală în vederea verificării caracterului lor real.

Datoriile către instituțiile de credit sau instituțiile financiare nebancare nu vor fi omise, organele de urmărire penală putând constata plata unor rate către o anumită instituție financiară. Chiar și micile operațiuni financiare realizate prin telefoane mobile prin intermediul emitenților de monedă electronică (de pildă, Vodafone M-pesa sau Orange Money) vor putea fi aflate, chiar dacă acestea sunt mai puțin populare în România (fiind larg folosite în țări în curs de dezvoltare din Africa sau Asia).

Alături de operațiunile obișnuite realizate prin intermediul unei instituții de credit, vor trebui avute în vedere și alte tranzacții financiare relevante, precum investițiile unei persoane sau instrumente financiare derivate, fonduri de investiții, în acțiuni etc. Depistarea unor astfel de tranzacții va fi ușoară, întrucât toate se realizează, pornesc sau se întorc la contul bancar al unei anumite persoane care va alimenta conturi la fonduri de investiții sau brokeri în domeniul pieței de capital. Mai mult decât atât, astfel cum vom vedea, în cadrul entităților financiare vor intra toate acele persoane juridice care derulează operațiuni financiare de orice natură și care sunt supuse supravegherii de către o autoritate publică – Banca Națională a României ori Autoritatea de Supraveghere Financiară.

În conținutul tranzacțiilor financiare va fi inclus, în mod obligatoriu, partenerul de tranzacționare – indiferent care ar fi acesta –, organele de urmărire penală putând descoperi participarea mai multor persoane la săvârșirea unei infracțiuni și dovedi legătura dintre acestea. De pildă, în cazul cercetării unei infracțiuni de spălarea banilor, ascunderea caracterului ilicit

[1] *B. Micu*, Aspecte practice specifice obținerii datelor privind tranzacțiile financiare ale unei persoane, în Dreptul nr. 1/2018, p. 145.

al dobândirii bunurilor se va realiza în etapa de stratificare[1], în care făptuitorul va proceda la trecerea banilor prin mai multe conturi pentru a le ascunde proveniența, uneori disimulându-le în vânzări sau cumpărări de bunuri sau servicii, sau va proceda la cumpărarea ori răscumpărarea de instrumente financiare. În consecință, va fi deosebit de important, pentru dovedirea existenței infracțiunii de spălarea banilor, identificarea fiecărei verigi din lanțul infracțional, inclusiv prin identificarea persoanelor interpuse în comiterea infracțiunii pentru tragerea lor la răspundere penală și, după caz, audierea lor în vederea probării vinovăției autorului.

Corelativ cu restrângerea vieții private, măsura va afecta și persoana care trebuie să furnizeze datele privind tranzacțiile financiare ale unei persoane, fiind incident un caz de derogare de la secretul bancar prevăzut de art. 111 din O.U.G. nr. 99/2006[2]. Întrucât punerea în executare a măsurii de cercetare se face întotdeauna prin transmiterea mandatului (ori ordonanței procurorului de autorizare provizorie) către un terț, este important de avut în vedere că obținerea de date privind tranzacțiile financiare ale unei persoane reprezintă și o restrângere a drepturilor entității financiare solicitate, întrucât o obligă la furnizarea unor informații ce țin și de viața privată a acesteia. Protejarea secretului bancar nu este importantă doar pentru beneficiarul unor servicii financiare, ci și pentru instituția solicitată, care va fi ținută să verifice dacă procedeul probatoriu este aplicat în mod corespunzător prin: asigurarea primirii mandatului judecătorului de drepturi și libertăți; verificarea corespondenței dintre conținutul mandatului și solicitările suplimentare ale organelor de urmărire penală[3]; analizarea interferenței unor alte procedee probatorii care trebuie dispuse separat[4]; transmiterea limitativă a datelor solicitate[5]. În caz contrar, chiar și dacă entitatea financiară ținută la secretul bancar ar răspunde unei solicitări din partea organelor de urmărire penală, ea va putea fi trasă la răspundere de către clientul său pentru eventuale prejudicii create acestuia[6].

Secțiunea a 2-a. Obținerea datelor privind tranzacțiile financiare ale unei persoane înainte de intrarea în vigoare a Codului de procedură penală

Pentru a sprijini demersurile organelor de urmărire penală, legiuitorul a prevăzut o metodă specială de cercetare pentru obținerea datelor privind tranzacțiile financiare ale unei persoane prin Codul de procedură penală adoptat în anul 2010. Anterior, în Codul de procedură penală

[1] *G. Lombardo (coord.), M. Nardo, V. Roversi, N. Craiu, C. Moldoveanu, L. Banu, P. Ricca*, Manual de instruire privind combaterea spălării banilor și a finanțării terorismului, Imprimeria Națională, București, 2009, p. 10; *D.A. Leslie*, Legal Principles for Combatting Cyberlaundering, Ed. Springer, Cham, 2014, p. 73.

[2] O.U.G. nr. 99 din 6 decembrie 2006 privind instituțiile de credit și adecvarea capitalului (M. Of. nr. 1027 din 27 decembrie 2006).

[3] De exemplu, organele de urmărire penală transmit mandatul, dar solicită date privind tranzacțiile ori înscrisuri la care nu s-a făcut referire în mandat.

[4] În măsura în care mandatul judecătorului de drepturi și libertăți se referă la probe care nu intră sub incidența art. 138 alin. (9) C.pr.pen., acestea vor fi transmise numai dacă se va dispune de către procuror procedeul probatoriu cerut de lege, de pildă, cel prevăzut de art. 170 C.pr.pen.

[5] Dacă mandatul se va emite în conformitate cu art. 140 alin. (5) lit. g) C.pr.pen., prin indicarea limitativă a conturilor, entitatea financiară nu va fi îndreptățită să transmită date privind tranzacțiile unei persoane de pe celelalte conturi și nu va fi îndreptățită nici să transmită informații, anume că persoana față de care s-a dispus măsura ar deține alte conturi, în absența unei ordonanțe a procurorului, în acest sens art. 153 C.pr.pen. fiind aplicabil.

[6] În acest sens, a se vedea *A.-R. Trandafir, G. Marin*, Obținerea de informații ori înscrisuri de la instituțiile de credit în cursul urmăririi penale, publicat pe *www.juridice.ro*

din 1968, nu exista un procedeu probatoriu similar, care să permită aplicarea sa unei categorii largi de infracțiuni. În schimb, legislația specială includea procedee probatorii care puteau fi întrebuințate în mod similar cu metoda specială de cercetare în discuție. Meritul Codului de procedură penală din 2010 constă în unificarea acestora sub o singură reglementare și introducerea autorizării măsurii de către judecătorul de drepturi și libertăți[1].

Sub imperiul legislației anterioare, s-a susținut că scopul tehnicilor speciale echivalente, denumite de doctrină „supravegherea conturilor bancare", consta în verificarea sumelor de bani care circulă prin conturile persoanelor fizice sau juridice care fac obiectul cercetărilor în cazurile de crimă organizată, spălare de bani sau finanțare a terorismului, în vederea strângerii de probe sau identificării făptuitorului[2].

În vederea prevenirii și cercetării infracțiunilor de corupție, Legea nr. 78/2000 prevedea în cuprinsul art. 27 alin. (1) lit. a)[3] posibilitatea autorizării de către procuror, pentru o perioadă de 30 de zile, a *punerii sub supraveghere a conturilor bancare și a conturilor asimilate acestora*. Lipsa de claritate a legiuitorului este evidentă atunci când se are în vedere că, la lit. d) a aceluiași alineat, legea îi conferă procurorului posibilitatea de a autoriza *comunicarea de înscrisuri, documente bancare, financiare ori contabile*, acestea conținând, de regulă, informații privind tranzacțiile realizate de persoana față de care se ia măsura. Totodată, conform art. 27 alin. (2) din Legea nr. 78/2000, procurorul putea dispune prelungirea măsurii menționate la art. 27 alin. (1) lit. a) din Legea nr. 78/2000 pentru o perioadă de maximum 4 luni, prin prelungiri care nu puteau depăși 30 de zile.

În domeniul legislației privind combaterea criminalității organizate, Legea nr. 39/2003 privind prevenirea și combaterea criminalității organizate[4] prevedea la art. 15 alin. (1) lit. a) aceeași măsură de supraveghere, reglementată în mod identic cu cea prevăzută în Legea nr. 78/2000.

Legislația specială în domeniul prevenirii și combaterii spălării banilor prevedea, până la intrarea în vigoare a Codului de procedură penală, o măsură similară celei din Legea nr. 78/2000. Potrivit art. 35 alin. (1) lit. a) din Legea nr. 656/2002 pentru prevenirea și sancționarea spălării banilor, precum și pentru instituirea unor măsuri de prevenire și combatere a finanțării terorismului (abrogată în prezent), procurorul putea dispune *punerea sub supraveghere a conturilor bancare și a conturilor asimilate acestora*, prin ordonanță motivată, pentru o perioadă de cel mult 30 de zile. Tot ca în cazul legislației pentru prevenirea și combaterii infracțiunilor de corupție, măsura putea fi prelungită de procuror pentru o durată maximă de 4 luni, prin prelungiri care nu puteau depăși 30 de zile.

Corelativ cu legislația specială anterioară pentru prevenirea și combaterea unor anumite categorii de infracțiuni, legiuitorul a extins posibilitatea întrebuințării unei metode similare cu obținerea datelor privind tranzacțiile financiare ale unei persoane și pe criterii de organizare judiciară (competență), permițând ca procurorii din cadrul D.N.A. și D.I.I.C.O.T. să folosească procedeul probatoriu în cauzele cercetate de aceștia.

[1] *Gh. Mateuț*, Procedură penală, 2019, p. 707.
[2] *C. Olaru*, op. cit., p. 116.
[3] Acest articol a fost abrogat la 1 februarie 2014, prin art. 41 pct. 3 din Titlul II din Legea nr. 255/2013.
[4] Publicată în M. Of. nr. 50 din 29 ianuarie 2003.

Prin dispozițiile art. 16 alin. (1) lit. a) din Legea nr. 508/2004[1] se prevedea posibilitatea procurorilor din cadrul D.I.I.C.O.T. de a dispune, pentru o perioadă de 30 de zile, *punerea sub supraveghere a conturilor bancare și a conturilor asimilate acestora* în vederea strângerii de probe sau identificării făptuitorului. Măsura putea fi prelungită pentru o durată maximă de 120 de zile, fiecare prelungire trebuind să fie motivată și dispusă pentru o durată de cel mult 30 de zile. În mod similar, chiar și în cadrul D.N.A., a fost prevăzută această măsură în cuprinsul art. 16 din O.U.G. nr. 43/2002[2].

Dacă puteam fi de acord cu întrebuințarea măsurii de punere sub supraveghere a conturilor bancare și a conturilor asimilate acestora în cazul unor infracțiuni de gravitate deosebită, apreciem că legiuitorul a greșit în trecut când a permis folosirea măsurii dacă urmărirea penală se efectua de un procuror D.N.A. sau D.I.I.C.O.T. Chiar dacă în cuprinsul prevederilor legale arătate era necesară efectuarea urmăririi penale față de infracțiuni care intrau în competența acestor organe de urmărire penală, este lesne de înțeles că această condiție nu trebuia să se aplice tuturor infracțiunilor cercetate în cauză, ci cel puțin uneia, cea care atrăgea competența organului de urmărire penală, putând fi administrate probe prin acest procedeu probatoriu și față de alte infracțiuni.

Abrogarea tuturor măsurilor speciale de cercetare din legislația penală specială era necesară pentru crearea unui cadru unitar privind cercetarea infracțiunilor, astfel că legiuitorul a ales în mod inspirat ca diferitele dispoziții – chiar dacă aveau în vedere aceeași măsură – să fie abrogate. În același timp, s-a avut în vedere și necesitatea reformării modalității de autorizare a măsurii care era deficitară, permițând procurorului să dispună asupra unei metode de cercetare deosebit de intruzive în viața privată, fără autorizarea judecătorului. Cu toate acestea, perspectiva istorică asupra reglementării măsurii ne arată că aceasta a fost gândită pentru prevenirea și combaterea unor infracțiuni grave, precum spălarea de bani, infracțiunile de corupție, infracțiunile de criminalitate organizată și cele date în urmărirea procurorilor din cadrul D.I.I.C.O.T. și D.N.A. Dincolo de gravitatea faptelor, complexitatea acestora este una deosebită, uneori impunând organelor de urmărire penală să folosească măsuri de cercetare intruzive în vederea probării faptelor și descoperii infractorilor. Credem că actuala legislație nu este suficient de restrictivă în condiționarea autorizării unor astfel de măsuri, permițând, astfel cum se va vedea mai jos, posibilitatea autorizării măsurii pentru orice infracțiune pedepsită cu mai mult de 6 ani închisoare.

Secțiunea a 3-a. Obținerea datelor privind tranzacțiile financiare ale unei persoane, prevăzută de Codul de procedură penală de la forma adoptată de Parlament până la forma în vigoare

Prin Legea nr. 135/2010 privind Codul de procedură penală s-a realizat unificarea măsurilor prevăzute fragmentat în legislația specială, prin introducerea unei măsuri de supraveghere tehnică unitară.

[1] Legea nr. 508 din 17 noiembrie 2004 privind înființarea, organizarea și funcționarea în cadrul Ministerului Public a Direcției de Investigare a Infracțiunilor de Criminalitate Organizată și Terorism (M. Of. nr. 1089 din 23 noiembrie 2004). Legea a fost abrogată odată cu intrarea în vigoare a O.U.G. nr. 78 din 16 noiembrie 2016 pentru organizarea și funcționarea Direcției de Investigare a Infracțiunilor de Criminalitate Organizată și Terorism, precum și pentru modificarea și completarea unor acte normative (M. Of. nr. 938 din 22 noiembrie 2016).

[2] O.U.G. nr. 43 din 4 aprilie 2002 privind Direcția Națională Anticorupție (republicată în M. Of. nr. 899 din 7 octombrie 2005).

În forma sa inițială, anterioară modificării prin legea de punere în aplicare, legiuitorul a inclus această măsură în art. 138 alin. (1) lit. g) C.pr.pen. ca măsură de supraveghere tehnică denumită „solicitarea și obținerea, potrivit legii, a datelor referitoare la tranzacțiile financiare, precum și a datelor financiare ale unei persoane". În definiția măsurii din cuprinsul art. 138 alin. (9) C.pr.pen. anterior se prevedea că: „*prin «solicitarea și obținerea, potrivit legii, a datelor referitoare la tranzacțiile financiare, precum și a datelor financiare ale unei persoane» se înțelege operațiunile prin care se asigură cunoașterea conținutului tranzacțiilor financiare efectuate prin intermediul unei bănci sau al altei instituții competente ori obținerea de la o bancă sau de la altă instituție financiară de înscrisuri ori informații aflate în posesia acesteia referitoare la conturile sau tranzacțiile unei persoane*".

Din simpla lecturare a textului măsurii de supraveghere tehnică se desprinde concluzia că, față de reglementarea actuală, nu exista nicio diferență între obținerea conținutului tranzacțiilor unei persoane și obținerea de informații privind situația financiară a unei persoane. Anterior intrării în vigoare a Codului de procedură penală, măsura de cercetare a obținerii de date privind situația financiară a unei persoane nu era prevăzută, denumirea marginală a art. 153 C.pr.pen. fiind „obținerea listei convorbirilor telefonice", astfel că textul de lege a fost substituit de legiuitor.

Totodată, măsura era imprecisă prin folosirea termenilor, precum „date financiare", „bancă", „instituții competente", dar și redundantă sub aspectul menționării că măsura trebuie dispusă **potrivit legii**.

Această formă criticată nu a intrat în vigoare niciodată, fiind modificată semnificativ prin Legea de punere în aplicare a Codului de procedură penală, prin care s-a renumerotat art. 138, obținerea datelor privind tranzacțiile financiare ale unei persoane fiind cuprinsă în art. 138 alin. (1) lit. e) C.pr.pen., redenumită sub numele purtat azi. Odată cu intrarea în vigoare a Codului de procedură penală, a fost introdusă și forma actuală a definiției metodei speciale de cercetare în discuție, cu mențiunea că măsura făcea parte din supravegherea tehnică și era supusă acelorași reguli și proceduri de autorizare. Totodată, a fost introdusă și măsura specială de cercetare a obținerii situației financiare a unei persoane în cuprinsul art. 153 C.pr.pen., măsură care era supusă încuviințării prealabile a judecătorului de drepturi și libertăți.

Întrucât în practică au existat mai multe situații în care scopul măsurii de supraveghere tehnică prevăzute de art. 138 alin. (1) lit. e) C.pr.pen. și cel al măsurii speciale de cercetare prevăzute de art. 153 C.pr.pen. era similar, s-a ajuns la confuzii între cele două procedee probatorii[1]. În plus, lipsa de reglementare a procedurii în fața judecătorului de drepturi și libertăți în cazul încuviințării măsurii de cercetare a condus la aplicarea procedurii încuviințării metodelor de supraveghere tehnică. Consecința a fost reevaluarea impactului pe care măsura prevăzută de art. 153 C.pr.pen. îl are asupra vieții private a persoanei, apreciindu-se că aflarea situației financiare a unei persoane nu justifică gradul de protecție conferit de lege prin încuviințarea prealabilă a judecătorului de drepturi și libertăți.

Prin O.U.G. nr. 18/2016[2] s-a realizat o reformare a dispozițiilor legale menționate, obținerea datelor privind tranzacțiile financiare ale unei persoane fiind eliminată din sfera supravegherii tehnice și inclusă în cea a metodelor speciale de cercetare prin excluderea măsurii din cuprinsul art. 138 alin. (13) C.pr.pen., în care sunt enumerate măsurile care constituie

[1] *A.-R. Trandafir, G. Marin*, Obținerea de informații ori înscrisuri de la instituțiile de credit în cursul urmăririi penale, publicat pe *www.juridice.ro*

[2] Publicată în M. Of. nr. 389 din 23 mai 2016.

supraveghere tehnică. Totodată, a fost creată o procedură de autorizare paralelă cu cea a supravegherii tehnice, cu mici diferențe pe care le vom analiza distinct și care, în opinia noastră, nu justificau încărcarea Codului de procedură penală cu dispozițiile art. 146[1] C.pr.pen., care aduc prea puțină noutate. Ceea ce a fost imperios necesar a fost delimitarea măsurii de cercetare a obținerii datelor privind tranzacțiile financiare ale unei persoane de măsura de cercetare similară, respectiv obținerea de date privind situația financiară a unei persoane, prin relaxarea procedurii de autorizare în cazul acesteia din urmă.

În forma prezentă a Codului de procedură penală, obținerea de date privind tranzacțiile financiare ale unei persoane este prevăzută de art. 138 alin. (1) lit. e) C.pr.pen., definită de art. 138 alin. (9) C.pr.pen., iar procedura autorizării întrebuințării ei este cuprinsă în art. 146[1] C.pr.pen.

Conform art. 138 alin. (9) C.pr.pen., „*prin «obținerea datelor privind tranzacțiile financiare ale unei persoane» se înțelege operațiunile prin care se asigură cunoașterea conținutului tranzacțiilor financiare și al altor operațiuni efectuate sau care urmează să fie efectuate prin intermediul unei instituții de credit ori al altei entități financiare, precum și obținerea de la o instituție de credit sau de la altă entitate financiară de înscrisuri ori informații aflate în posesia acesteia referitoare la tranzacțiile sau operațiunile unei persoane*".

Din definiția expusă mai sus rezultă că obiectul măsurii îl reprezintă conținutul concret al tranzacțiilor financiare și al altor operațiuni prin intermediul unei instituții financiare, urmărindu-se ca, în timp real și pentru viitor, cu limitare în timp, sau ca, retroactiv și fără limitare în timp, să se cunoască ce tranzacții financiare se pregătesc, se realizează ori s-au realizat față de o persoană, în ce cuantum, ce monedă (ori instrument financiar sau de investiții) sau prin ce metodă. În cel mai elementar exemplu, organele de urmărire penală pot monitoriza ce cumpără sau vinde o persoană, cui transmite sume de bani sau de la cine primește, ce depozite constituie, ce investiții face, fără ca acea persoană să afle că este monitorizată.

Deși definiția dată de Codul de procedură penală include noțiunea de „date privind tranzacțiile financiare", prin întrebuințarea procedeului probatoriu vor fi obținute *probe privind desfășurarea unei tranzacții sau operațiuni financiare* de către persoana împotriva căreia se dispune măsura. Această concluzie rezultă în mod neîndoielnic din dispozițiile art. 146[1] alin. (1) lit. c) C.pr.pen., în care legiuitorul include condiția subsidiarității, potrivit căreia: *probele* nu ar putea fi obținute în alt mod sau obținerea lor ar fi în detrimentul urmăririi penale, siguranței persoanelor sau unor bunuri de valoare.

Capitolul II
Natura juridică a metodei speciale de cercetare

O metodă a cărei naturi juridice poate fi supusă unei dezbateri este obținerea datelor privind tranzacțiile financiare ale unei persoane, prevăzută de art. 138 alin. (1) lit. e) C.pr.pen., definită de alin. (9) al aceluiași articol și normată de art. 146[1] C.pr.pen. Afirmația noastră este susținută de modificările aduse de legiuitor prin O.U.G. nr. 18/2016, atunci când dintre metodele de supraveghere tehnică a fost înlăturată măsura, concomitent cu introducerea art. 146[1] C.pr.pen., prin care se instituie procedura autorizării folosirii ei. În doctrină se reține în mod unanim că obținerea datelor privind tranzacțiile financiare ale unei persoane reprezintă *o metodă specială de cercetare* ca urmare a modificărilor aduse de lege[1]. Cu toate acestea, metodei nu i se neagă caracterul asemănător supravegherii tehnice, aceiași autori amintiți determinând trecerea măsurii în categoria metodelor speciale de cercetare ca urmare a înlăturării lor din categoria supravegherii tehnice prin O.U.G. nr. 18/2016. Din punctul nostru de vedere, aceste opinii au puncte valide, dar și puncte slabe, deoarece o metodă specială de supraveghere prezintă anumite caracteristici intrinseci care sunt mai importante decât simpla omisiune a Codului de procedură penală de a le mai prevedea ca atare. Specifice oricărei metode speciale de supraveghere sunt următoarele caracteristici esențiale: *gradul ridicat de intruziune în viața privată a persoanei*, *existența unei proceduri de autorizare prin care se analizează proporționalitatea măsurii cu drepturile cetățenești restrânse de către judecătorul de drepturi și libertăți*, *subsidiaritatea măsurii față de alte procedee probatorii*, dar și *condiționarea autorizării de începerea urmăririi penale față de o categorie restrânsă de infracțiuni considerată de legiuitor ca fiind de o gravitate deosebită*.

În mod corect se susține că nu există nicio diferență de reglementare între acest procedeu probatoriu și supravegherea tehnică, condițiile care se cer a fi îndeplinite fiind similare[2]. Mai mult, același autor identifică în mod just gradul deosebit de intruziv al măsurii obținerii datelor privind tranzacțiile financiare ale unei persoane, recunoscând rolul din ce în ce mai mare al sistemului bancar în desfășurarea de tranzacții concomitent cu abandonarea sistemului de plată prin monedă fizică[3]. Argumentele prezentate, precum și existența caracteristicilor esențiale ale unei măsuri de supraveghere tehnică i-ar putea conferi acesteia natura de metodă specială de supraveghere, însă legiuitorul a introdus o diferență semnificativă, ceea ce ne determină să conchidem că măsura poate fi numai una de cercetare: curgerea distinctă față de supravegherea tehnică a unui termen maxim de autorizare pentru această măsură[4]. Mai precis, prin introducerea clară a unui termen maxim de autorizare de 6 luni pentru obținerea datelor privind tranzacțiile financiare ale unei persoane, care este distinct prevăzut de cel cuprins în art. 144 alin. (3) C.pr.pen., rezultă că voința legiuitorului a fost de a nu limita această măsură la durata totală a măsurilor de supraveghere tehnică de 6 luni. În plus, astfel cum vom

[1] *Gh. Mateuț*, Procedură penală, 2019, p. 707; *M Bulancea, R. Slăvoiu*, în M. Udroiu (coord.), Codul de procedură penală, 2017, p. 714; *A.-R. Trandafir, G. Marin*, Obținerea de informații ori înscrisuri de la instituțiile de credit în cursul urmăririi penale, publicat pe *www.juridice.ro*

[2] *Gh. Mateuț*, Procedură penală, 2019, p. 708.

[3] *Ibidem*.

[4] *A.-R. Trandafir, G. Marin*, Obținerea de informații ori înscrisuri de la instituțiile de credit în cursul urmăririi penale, publicat pe *www.juridice.ro*

vedea într-o secțiune viitoare, termenul de 6 luni prevăzut în cazul obținerii datelor privind tranzacțiile financiare ale unei persoane se referă la aceeași cauză și aceeași persoană, fiind posibilă folosirea măsurii pentru o perioadă maximă similară, în urma disjungerii cauzei[1].

Un alt argument în susținerea caracterului de măsură specială de cercetare este posibilitatea întrebuințării procedeului probatoriu în cazul în care există o suspiciune rezonabilă privind pregătirea sau săvârșirea *oricărei* infracțiuni, condiție care nu este suficient de restrictivă față de restrângerea dreptului persoanei la viață privată. Legiuitorul a greșit atunci când nu a menținut același nivel de gravitate al faptei cercetate ca la măsurile de supraveghere tehnică, permițând aplicarea acesteia pentru orice faptă cercetată. Bunăoară, sunt lesne de imaginat situații în care nu se va putea obține un mandat de supraveghere tehnică pentru localizarea unei persoane, dar activitățile sale curente – manifestate în tranzacții financiare cu carduri – vor putea ajuta la localizarea sa, mai mult, chiar la stabilirea traseului acesteia, a repetabilității sale etc. Cu alte cuvinte, menținerea unor dispoziții critice permite o fraudă la lege din partea organelor de urmărire penală prin utilizarea măsurii de cercetare în locul unei măsuri de supraveghere tehnică, în vederea obținerii aceluiași scop.

Ținând seama de toate aceste argumente, caracterul de metodă specială de cercetare este unul determinat legal și, cel puțin în actuala reglementare, măsura va trebui considerată a fi una de cercetare, și nu o metodă specială de supraveghere.

De lege ferenda, apreciem că nu este justificat caracterul de măsură specială de cercetare și se impune ca măsura să fie inclusă din nou în categoria supravegherii tehnice prin introducerea unei dispoziții expres cuprinse în art. 144 C.pr.pen. privind termenul maxim pentru care se poate dispune obținerea datelor privind tranzacțiile financiare ale unei persoane. Introducerea art. 146[1] C.pr.pen. constituie o fragmentare inutilă a dispozițiilor Codului de procedură penală, care nu este justificată, date fiind similaritățile cu măsura. Totodată, față de caracterul intruziv al măsurii, se impune limitarea folosirii acesteia numai la infracțiuni de o gravitate ridicată.

[1] *Ibidem*; *Gh. Mateuț*, Procedură penală, 2019, p. 709; *M. Bulancea, R. Slăvoiu*, în M. Udroiu (coord.), Codul de procedură penală, 2017, p. 715.

Capitolul III
Persoanele care pot fi chemate să comunice date privind tranzacțiile financiare ale unei persoane

Secțiunea 1. Instituțiile de credit

În strictă legătură cu utilitatea prevederii în legislația română a acestui procedeu probatoriu sunt instituțiile care pot fi obligate să contribuie la punerea în executare a măsurii prin transmiterea datelor privind tranzacțiile financiare ale unei persoane. Întrucât considerăm că măsura nu se poate dispune în mod universal, ci trebuie ca judecătorul de drepturi și libertăți să dispună expres față de fiecare entitate financiară în parte, va fi necesar ca atât acesta, cât și procurorul să cunoască ce instituții pot fi supuse măsurii speciale de cercetare.

Din cuprinsul art. 138 alin. (9) C.pr.pen. rezultă că, pentru aplicarea acestei măsuri, este necesar ca procurorul să se adreseze unei *instituții de credit* sau unei alte *entități financiare*.

Instituțiile de credit sunt reglementate de O.U.G. nr. 99/2006 privind instituțiile de credit și adecvarea capitalului, conform art. 3 din aceeași lege împărțindu-se în mai multe categorii: *i)* bănci, *ii)* organizații cooperatiste de credit, *iii)* bănci de economisire și creditare în domeniul locativ și *iv)* bănci de credit ipotecar. Toate aceste instituții se vor înființa și funcționa în conformitate cu legea anterior menționată, Banca Națională a României având un rol esențial, întrucât prin art. 4 alin. (1) din O.U.G. nr. 99/2006 se stabilește că aceasta reprezintă autoritatea de reglementare, autorizare și supraveghere prudențială a tuturor instituțiilor de credit. În același timp, Banca Națională a României este și autoritatea de stat în măsură să furnizeze organelor de urmărire penală informații cu privire la identitatea oricărei instituții de credit, acestea fiind înregistrate, conform art. 35 alin. (2) din O.U.G. nr. 99/2006, în registrul instituțiilor de credit ținut de Banca Națională a României[1].

Majoritatea măsurilor de cercetare privind tranzacțiile unei persoane vor viza o instituție de credit și, dintre acestea, aproape toate vor viza o bancă, datorită specificului larg al activității desfășurate de acestea. Specific acestor instituții este că informațiile referitoare la clienți sunt protejate de secretul bancar, în conformitate cu dispozițiile art. 111 alin. (1) din O.U.G. nr. 99/2006[2], acest tip de informație fiind o formă de secret profesional cu un grad de confidențialitate deosebit de ridicat. Apreciem că distincția dintre secretul bancar și un simplu

[1] Banca Națională a României ține un registru online pentru toate instituțiile de credit, instituțiile de plată, furnizorii specializați în servicii de informare cu privire la conturi, instituțiile emitente de monedă electronică, instituțiile financiare nebancare, ce poate fi consultat în mod liber pe *www.bnr.ro*

[2] Conform art. 111 din O.U.G. nr. 99/2006:

„(1) Instituția de credit este obligată să păstreze confidențialitatea asupra tuturor faptelor, datelor și informațiilor referitoare la activitatea desfășurată, precum și asupra oricărui fapt, dată sau informație, aflate la dispoziția sa, care privesc persoana, proprietatea, activitatea, afacerea, relațiile personale sau de afaceri ale clienților ori informații referitoare la conturile clienților – solduri, rulaje, operațiuni derulate –, la serviciile prestate sau la contractele încheiate cu clienții.

(2) În înțelesul prezentului capitol se consideră client al unei instituții de credit, orice persoană cu care, în desfășurarea activităților prevăzute la art. 18 și la art. 20, instituția de credit a negociat o tranzacție, chiar dacă respectiva tranzacție nu s-a finalizat și orice persoană care beneficiază de serviciile unei instituții de credit, inclusiv persoanele care au beneficiat în trecut de serviciile unei instituții de credit".

secret profesional este că o instituție de credit nu poate nici măcar să transmită faptul că o persoană este sau a fost vreodată clientul său, banca trebuind să refuze să pună la dispoziție toate aceste date, fără a exista o analiză dacă divulgarea acestor informații ar putea produce vreun prejudiciu clientului său.

În cazul instituțiilor de credit, aparte de dispozițiile Codului de procedură penală, însăși legea care reglementează cadrul general al activității acestora impune colaborarea cu procurorul în vederea transmiterii datelor privind tranzacțiile financiare ale unei persoane. Astfel, conform art. 114 din O.U.G. nr. 99/2006, „*instituțiile de credit sunt obligate să furnizeze **procurorului sau instanței de judecată**, la solicitarea acestora, informații de natura secretului bancar, dispozițiile privind metodele speciale de supraveghere sau cercetare din Codul de procedură penală aplicându-se în mod corespunzător*" (s.n.). Semnificația menționării exprese a procurorului sau instanței înseamnă că un organ de cercetare penală niciodată nu va putea solicita o informație ce constituie secret bancar. Textul de lege menționat se coroborează și cu dispozițiile art. 306 alin. (6) C.pr.pen., în care se arată că secretul bancar și cel profesional nu sunt opozabile procurorului, după începerea urmăririi penale, cu excepția secretului profesional al avocatului.

Secțiunea a 2-a. Entitățile financiare

Entitățile financiare vor fi mai greu de definit, întrucât Codul de procedură penală nu ne oferă suficientă claritate în a le determina. Doctrina este insuficientă în această privință, dând doar exemple pe alocuri de astfel de entități, precum Western Union și MoneyGram[1], acestea fiind instituțiile de plată[2] cel mai des folosite (în special când românii transferă bani câștigați în străinătate înapoi în țară). În realitate, numărul de entități financiare este deosebit de mare, pentru determinarea caracterului de entitate financiară trebuind să fie analizată legislația specială în domeniul bancar și financiar. Necesar a fi menționat este că o instituție de credit este și o entitate financiară, termenul folosit de legiuitor fiind suficient de general pentru a include orice instituție care ar putea activa în domeniul financiar și care ar putea fi obligată să transmită date privind tranzacțiile financiare efectuate de o persoană.

În acest sens, trebuie avute în vedere și definițiile date prin Regulamentul (UE) nr. 575/2013[3], la care se face deseori trimitere în legislația națională în domeniul financiar. Regulamentul european conține termeni foarte apropiați celui prevăzut în Codul de procedură penală, definind „entitatea din sectorul financiar", formulare pe care o considerăm sinonimă celei de „entitate financiară".

Potrivit art. 4 alin. (1) pct. 27 din Regulamentul (UE) nr. 575/2013, prin „entitate din sectorul financiar" vom înțelege oricare dintre următoarele:

a) o instituție[4]*;*

b) o instituție financiară[5]*;*

---

[1] *M. Udroiu*, Procedură penală, vol. I, 2019, p. 634.

[2] Instituțiile de plată sunt reglementate prin Legea nr. 209 din 8 noiembrie 2019 privind serviciile de plată și pentru modificarea unor acte normative (M. Of. nr. 913 din 13 noiembrie 2019).

[3] Publicat în J. Of., seria L, nr. 176/1 din 27 iunie 2013.

[4] Conform art. 4 alin. (1) pct. 3 din Regulamentul (UE) nr. 575/2013, prin „instituție" se va înțelege o instituție de credit sau o firmă de investiții.

[5] Conform art. 4 alin. (1) pct. 26 din Regulamentul (UE) nr. 575/2013, prin „instituție financiară" se va înțelege o „întreprindere, alta decât o instituție (de credit – n.n.), a cărei activitate principală constă în

c) o întreprindere prestatoare de servicii auxiliare inclusă în situația financiară consolidată a unei instituții[1]*;*

d) o întreprindere de asigurare;

e) o întreprindere de asigurare dintr-o țară terță;

f) o întreprindere de reasigurare;

g) o întreprindere de reasigurare dintr-o țară terță;

h) o societate holding de asigurare;

i) o societate holding cu activitate mixtă;

j) o societate holding de asigurare cu activitate mixtă, astfel cum este definită la articolul 212 alineatul (1) litera g) din Directiva 2009/138/CE;

k) o întreprindere exclusă din domeniul de aplicare al Directivei 2009/138/CE în conformitate cu articolul 4 din directiva menționată;

l) o întreprindere dintr-o țară terță cu o activitate principală comparabilă cu a oricăreia dintre entitățile menționate la literele (a)-(k) de mai sus.

Definiția dată de regulamentul european poate fi folosită în vederea determinării persoanei căreia i se va adresa organul de urmărire penală pentru sprijin în punerea în executare a măsurii de cercetare, însă trebuie să avem în vedere și specificul național în acest proces, dar și caracterul autonom al terminologiei legii penale. Pentru a defini noțiunea de „entitate financiară" în sensul art. 138 alin. (9) C.pr.pen., considerăm că se impune o abstractizare a definiției, bazându-ne pe trăsături esențiale ale unei asemenea entități.

În opinia noastră, pentru a fi considerată entitate financiară, se impune ca o persoană juridică (română sau străină) să îndeplinească următoarele condiții: să aibă ca obiect de activitate desfășurarea de operațiuni financiare cu monedă (inclusiv monedă electronică) sau operațiuni cu instrumente financiare[2], entitatea să se adreseze publicului și să fie autorizată și supravegheată de către o autoritate publică.

---

dobândirea de participații sau în desfășurarea uneia sau mai multor activități menționate la punctele 2-12 și la punctul 15 din anexa I la Directiva 2013/36/UE, inclusiv o societate financiară holding, o societate financiară holding mixtă, o instituție de plată în sensul Directivei 2007/64/CE a Parlamentului European și a Consiliului din 13 noiembrie 2007 privind serviciile de plată în cadrul pieței interne și o societate de administrare a activelor, dar cu excluderea societăților holding de asigurare și a societăților holding de asigurare cu activitate mixtă, astfel cum este definită la articolul 212 alineatul (1) litera (g) din Directiva 2009/138/CE".

[1] Conform art. 4 alin. (1) pct. 18 din Regulamentul (UE) nr. 575/2013, prin „întreprindere prestatoare de servicii auxiliare" se înțelege „o întreprindere a cărei activitate principală constă în deținerea sau administrarea de bunuri, administrarea de servicii de prelucrare a datelor sau o activitate similară care este auxiliară activității principale a uneia sau mai multor instituții".

[2] În sensul art. 4 alin. (1) pct. 50 din Regulamentul (UE) nr. 575/2013, „instrumentul financiar" poate fi definit ca oricare dintre următoarele:

„a) un contract care generează simultan un activ financiar, pentru una dintre părți, și un pasiv financiar sau un titlu de capital pentru cealaltă dintre părți;

b) un instrument menționat în secțiunea C din anexa I la Directiva 2004/39/CE;

c) un instrument financiar derivat;

d) un instrument financiar primar;

e) un instrument de numerar".

În sensul secțiunii C din Anexa I a Directivei nr. 2004/39/CE la care se face referire mai sus, prin „instrument financiar" se înțelege și unul dintre următoarele:

a) valorile mobiliare;

b) instrumentele pieței monetare;

c) unitățile de organisme de plasament colectiv;

Ținând cont de nevoia de reglementare a sistemului financiar, evidențiată mai ales în urma crizei economice produse în anul 2008, datorată lipsei de supraveghere a pieței de creditare ipotecare din S.U.A., în prezent, activitatea financiară este obligatoriu reglementată și supravegheată la nivel european, încercându-se uniformizarea legislației, sens în care legislația română a început să facă trimiteri la legislația europeană, fără a mai defini ea însăși concepte. Una dintre responsabilitățile naționale rămase este aceea de a autoriza și supraveghea entitățile financiare, obligație instituită prin art. 4 din Directiva 2013/36/UE și implementată de România prin modificările aduse O.U.G. nr. 99/2006, în care se prevăd două autorități de stat care vor exercita aceste atribuții: Banca Națională a României[1] și Autoritatea de Supraveghere Financiară[2].

Ca atare, vor constitui entități financiare următoarele categorii de instituții: instituțiile de plată (Western Union, MoneyGram etc.); furnizorii specializați în servicii de informare cu privire la conturi (în prezent nu operează niciunul); instituțiile emitente de monedă electronică (de exemplu, Orange Money); instituțiile financiare nebancare[3] (instituții ce oferă servicii de credite de consum, credite ipotecare și sau imobiliare, microcredite, finanțare de tranzacții comerciale, factoring, scontare, forfetare, leasing financiar, emitere de garanții și asumare de

---

d) contractele de opțiuni, contractele la termen, contractele swap, contractele la termen pe rata dobânzii și orice alte contracte derivate referitoare la valori mobiliare, monede, rate ale dobânzii sau ale rentabilității sau alte instrumente derivate, indici financiari sau măsuri financiare care pot fi regularizate prin livrare fizică sau în numerar;

e) contractele de opțiuni, contractele la termen, contractele swap, contractele la termen pe rata dobânzii și orice alte contracte derivate referitoare la materii prime care trebuie regularizate în numerar sau pot fi regularizate în numerar la cererea uneia dintre părți (altfel decât în caz de încălcare a obligațiilor sau de alt incident care conduce la reziliere);

f) contractele de opțiuni, contractele la termen, contractele swap și orice alt contract derivat referitor la materii prime care pot fi regularizate prin livrare fizică, cu condiția să fie tranzacționate pe o piață reglementată și/sau un MTF;

g) contractele de opțiuni, contractele la termen, contractele swap, contractele la termen fix („forwards") și orice alte contracte derivate referitoare la materii prime care pot fi regularizate prin livrare fizică, care nu au fost menționate în alt mod în secțiunea C punctul 6 și neavând scopuri comerciale, care prezintă caracteristicile altor instrumente financiare derivate ținând seama dacă, în special, sunt compensate și regularizate prin intermediul unor organisme de compensare recunoscute sau fac obiectul unor apeluri în marjă regulate;

h) instrumentele derivate care servesc la transferul riscului de credit;

i) contractele financiare pentru diferențe (*financial contracts for differences*);

j) contractele de opțiuni, contractele la termen, contractele swap, contractele la termen pe rata dobânzii și orice alte contracte derivate referitoare la variabile climatice, la taxe de navlu, la autorizații de emisiuni sau la rate ale inflației sau alte statistici economice oficiale care trebuie regularizate în numerar sau pot fi regularizate în numerar la cererea uneia dintre părți (altfel decât în caz de încălcare a obligațiilor sau de alt incident care conduce la reziliere), precum și orice alte contracte derivate privind active, drepturi, obligații, indici și măsuri care nu au fost menționate în alt mod în prezenta secțiune C, care prezintă caracteristicile altor instrumente financiare derivate ținând seama dacă, în special, sunt tranzacționate pe o piață reglementată sau un MTF, sunt compensate și regularizate prin intermediul unor organisme de compensare recunoscute sau fac obiectul unor apeluri în marjă regulate".

[1] Conform art. 4 alin. (1) din. O.U.G. nr. 99/2006, „Banca Națională a României este autoritatea competentă cu privire la reglementarea, autorizarea și supravegherea prudențială a instituțiilor de credit, potrivit prevederilor prezentei ordonanțe de urgență și ale Regulamentului (UE) nr. 575/2013".

[2] Conform art. 4[1] alin. (1) din O.U.G. nr. 99/2006, „Autoritatea de Supraveghere Financiară este autoritatea competentă cu privire la reglementarea și supravegherea prudențială a societăților de servicii de investiții financiare, potrivit prevederilor prezentei ordonanțe de urgență și ale Regulamentului (UE) nr. 575/2013".

[3] Reglementate prin Legea nr. 93 din 8 aprilie 2009 privind instituțiile financiare nebancare (M. Of. nr. 259 din 21 aprilie 2009). Definiția legală a „instituției financiare nebancare" este cuprinsă în art. 5 lit. c) din Legea nr. 93/2009, în care se arată că „instituții financiare nebancare" sunt entitățile, altele decât instituțiile de credit, ce desfășoară activitate de creditare cu titlu profesional, în condițiile stabilite de lege.

angajamente, alte forme de finanțare de natura creditului și activități multiple de creditare); organisme de plasament colectiv; societăți de administrare investiții; depozitari centrali; societăți de servicii de investiții financiare; societăți de asigurare și reasigurare; societăți ce administrează sisteme de pensii private.

În considerarea celor arătate mai sus, organele de urmărire penală nu vor trebui să se limiteze numai la instituțiile de credit, ci vor trebui să aibă în vedere și faptul că făptuitorul sau persoanele interpuse vor putea desfășura și o multitudine de alte tranzacții financiare decât cele desfășurate prin bănci.

De interes vor fi și tranzacțiile desfășurate cu instrumente financiare, nu doar cu sume de bani. Trebuie avut în vedere că o societate de administrare investiții cu regim deschis va încerca să atragă sume de bani de la populație în vederea sprijinirii cu capital a diverselor activități, în funcție de profilul de risc angajat de public. În general, portofoliile se constituie dintr-o combinație de titluri de stat și alte instrumente financiare private, inclusiv acțiuni. De pildă, diverse fonduri de investiții pot avea un specific – agricultură, tehnologie, energie, imobiliare – sau pot fi ghidate de tendințele pieței de capital analizate prin prisma unor indecși (sau indici) – fonduri index (de exemplu, BT RO Index al BT Asset Management S.A.I). Orice persoană fizică poate achiziționa o unitate de fond, a cărei valoare va crește în funcție de rentabilitatea investițiilor. În cadrul societăților de administrare investiții, fiecare investitor va avea un cont, similar cu cel bancar, în care se vor detalia unitățile de fond aflate în portofoliu ce vor fi evaluate în funcție da valoarea curentă pentru o unitate de fond. Aceste unități de fond pot fi achiziționate și, ulterior, răscumpărate, însă nu pot fi transmise unei alte persoane.

Chiar și tranzacțiile financiare realizate pe piața de capital vor intra sub incidența măsurii speciale de cercetare, întrucât și acestea se desfășoară prin entități financiare specializate de brokeraj – societăți de servicii de investiții financiare –, ce sunt înregistrate la nivelul burselor de valori din țară sau din străinătate. Cumpărarea și vânzarea de acțiuni sau alte instrumente financiare tranzacționate pe piața de capital se va face prin intermediul acestor societăți care intermediază relația investitorului cu emitentul acțiunilor sau cu partenerul de tranzacționare (după caz, oferind și consiliere). Investitorii vor deține, în mod obligatoriu, conturi la aceste societăți de investiții, în care se vor regăsi toate acțiunile sau instrumentele financiare din portofoliul acestora, putând fi tranzacționate oricând. Excepție de la această regulă o constituie situația în care acțiunile emise de societățile românești se regăsesc la Depozitarul Central, autoritate care nu este abilitată să tranzacționeze la bursă, ci numai să depoziteze acțiunile unei persoane într-un cont. La fel ca în cazul unităților de fond emise de societățile de administrare a investițiilor, acțiunile nu se pot tranzacționa direct între particulari, ele trebuind a fi supuse regulilor cererii și ofertei de pe piața de capital.

În privința existenței unui secret bancar în cazul entităților financiare, altele decât instituțiile de credit, apreciem că acestea vor trebui să aplice același standard ridicat ca în cazul celor din urmă, chiar dacă legislația specială care guvernează formele de entități financiare se referă doar la obligația păstrării secretului profesional.

Secțiunea a 3-a. Agenția Națională de Administrare Fiscală

Unele dintre instrumentele financiare cele mai stabile de pe piață sunt cele emise de autoritățile publice: titlurile de stat, obligațiunile și certificatele de trezorerie, operațiunile cu astfel de instrumente intrând, în mod evident, în obiectul măsurii de cercetare analizate. Ele sunt

considerate investiții cu un grad scăzut de risc, întrucât restituirea sumei investite la termen, alături de dobândă (numită „cupon") este garantată de stat. Emisiunea de astfel de instrumente financiare este realizată, de regulă, pentru finanțarea deficitului bugetului de stat și, mai rar, pentru realizarea de proiecte de investiție deosebite, fiind dispusă prin ordin al Ministrului Finanțelor Publice. Pentru ca o persoană să poată realiza astfel de operațiuni în mod direct (să fie titularul nominal al instrumentului financiar), este necesar să aibă un cont deschis la Trezoreria statului și să subscrie o sumă de bani, în condițiile stabilite de prospectul de emisiune.

În doctrină s-a ridicat problema ca datele privind tranzacțiile financiare ale unei persoane să fie obținute prin utilizarea bazelor electronice de date administrate de Agenția Națională de Administrare Fiscală, în temeiul art. 267 C.pr.pen., care permite accesarea acestor baze de date în scopul îndeplinirii procedurii de citare[1]. Opinia exprimată, cu care suntem de acord, este că nu se va putea proceda la obținerea de date privind tranzacțiile financiare ale unei persoane și nici la obținerea de date privind situația financiară a unei persoane decât prin folosirea procedeului probatoriu dedicat prevăzut de lege. Obținerea de probe prin intermediul accesului conferit organelor de urmărire penală, în temeiul art. 267 C.pr.pen., nu poate fi considerată decât ca o eludare a procedurii de obținere a probei prin deturnarea scopului articolului de lege antemenționat. Probele obținute vor fi nelegale, impunându-se constatarea nulității relative a procedeului probatoriu și, în măsura în care sunt îndeplinite și celelalte condiții legale, să se dispună excluderea probei.

Ceea ce s-a mai indicat în doctrină și considerăm că este o opțiune de avut în vedere de către procuror este îndreptarea solicitării de obținere a datelor privind tranzacțiile financiare ale unei persoane direct către Agenția Națională de Administrare Fiscală[2], în virtutea obligațiilor legale ale instituțiilor de credit de a raporta acestei instituții toate rulajele și soldurile conturilor deschise, precum și toate informațiile și documentele privind operațiunile desfășurate prin respectivele conturi[3]. Situația descrisă este incidentă atunci când organele fiscale au obținut deja datele privind tranzacțiile financiare în urma unei cereri formulate către instituția de credit și, chiar dacă informațiile sunt deținute de un organ al statului, acestea au fost transmise în baza legii pentru un scop anume, care nu poate fi deturnat de organele de urmărire penală. Într-adevăr, este un neajuns al legislației fiscale faptul că organele fiscale pot avea puteri mai extinse decât organele de urmărire penală, aspect care va trebui să fie reglementat în sensul introducerii autorizării judecătorului de drepturi și libertăți și pentru organele fiscale, nefiind permisă lipsa oricărei garanții a respectării dreptului la viață privată al persoanei. Nu este însă o chestiune de noutate, organele fiscale având acest drept inclusiv sub imperiul Codului de procedură fiscală anterior, în care același drept era cuprins în art. 54 alin. (4) C.pr.fisc. anterior încă din anul 2010[4].

[1] *M. Udroiu*, Procedură penală, vol. I, 2019, p. 624; *A.-R. Trandafir, G. Marin*, Obținerea de informații ori înscrisuri de la instituțiile de credit în cursul urmăririi penale, publicat pe *www.juridice.ro*

[2] *M. Udroiu*, Procedură penală, vol. I, 2019, p. 624 și p. 636.

[3] Potrivit art. 61 alin. (1) C.pr.fisc., „instituțiile de credit (...) au obligația ca, la solicitarea organului fiscal central, să comunice, pentru fiecare titular care face subiectul solicitării, toate rulajele și/sau soldurile conturilor deschise la acestea, precum și informațiile și documentele privind operațiunile derulate prin respectivele conturi".

[4] Introdus ca urmare a modificărilor suferite de Codul de procedură fiscală din 2010 prin adoptarea O.U.G. nr. 54 din 23 iunie 2010 (M. Of. nr. 421 din 23 iunie 2010).

În măsura în care s-ar solicita astfel de date și informații în temeiul art. 170 C.pr.pen., procedeul probatoriu ar fi nelegal, întrucât probele s-ar obține prin deturnarea dispozițiilor art. 146[1] C.pr.pen., care conferă un grad de protecție superior al vieții private. În sens contrar, s-a arătat în doctrină că problema nu ar fi una de legalitate, ci una de loialitate a obținerii probelor[1].

Referitor la situația financiară a unei persoane, observăm că dispozițiile Codului de procedură fiscală prevăd o obligație din partea instituțiilor de credit de a transmite organului fiscal central, zilnic, lista cu titularii tuturor conturilor deschise și a datelor de identificare a persoanelor care dețin drept de semnătură pe conturi[2], **fără a fi transmisă situația financiară**. Chiar și în aceste condiții, obținerea lor de către organele de urmărire penală va fi condiționată de emiterea unei ordonanțe de către procuror în temeiul dispozițiilor art. 153 C.pr.pen., întrucât măsura obținerii datelor privind situația financiară a unei persoane include informații și cu privire la existența conturilor la o anumită instituție de credit.

Secțiunea a 4-a. Persoanele fizice

O problemă aparte este dacă măsura poate consta în obligarea unei persoane fizice să dezvăluie date privind tranzacțiile financiare deținute despre o altă persoană. Aparent, răspunsul ar trebui să fie nu, întrucât nicio persoană fizică nu poate avea calitatea de instituție de credit, în conformitate cu art. 3 din O.U.G. nr. 99/2006, însă unele persoane fizice pot fi încadrate ca entități financiare ce pot fi supuse obligației comunicării datelor. Astfel cum am arătat mai sus, între entitățile financiare vor intra și instituțiile de plată, reglementate de Legea nr. 209/2019, entități financiare care pot avea agenți[3] persoane fizice sau juridice ce pot realiza servicii de plată[4], în sensul legii. Scopul acestor agenți este de a prelua sau remite sume de bani

[1] *A.-R. Trandafir, G. Marin*, Obținerea de informații ori înscrisuri de la instituțiile de credit în cursul urmăririi penale, publicat pe *www.juridice.ro*

[2] Potrivit art. 61 alin. (2) C.pr.fisc., instituțiile de credit sunt obligate să comunice organului fiscal central, zilnic, următoarele informații:

a) lista titularilor persoane fizice, juridice sau orice alte entități fără personalitate juridică ce deschid ori închid conturi, precum și datele de identificare ale persoanelor care dețin dreptul de semnătură pentru conturile deschise la acestea;

b) lista persoanelor care închiriază casete de valori, precum și încetarea contractului de închiriere.

[3] Art. 5 alin. (1) pct. 2 din Legea nr. 209/2019 definește ca „agent" o persoană fizică sau juridică care furnizează servicii de plată în numele și pe seama unei instituții de plată sau unui furnizor specializat în servicii de informare cu privire la conturi.

[4] Alin. (1) al art. 7 din Legea nr. 209/2019 definește ca fiind „servicii de plată" oricare dintre următoarele activități:

„a) servicii care permit depunerea de numerar într-un cont de plăți, precum și toate operațiunile necesare pentru funcționarea unui cont de plăți;

b) servicii care permit retrageri de numerar dintr-un cont de plăți, precum și toate operațiunile necesare pentru funcționarea unui cont de plăți;

c) efectuarea următoarelor operațiuni de plată în cazul în care fondurile nu sunt acoperite printr-o linie de credit: debitări directe, inclusiv debitări directe singulare, operațiuni de plată printr-un card de plată sau un dispozitiv similar, operațiuni de transfer-credit, inclusiv operațiuni cu ordine de plată programată;

d) efectuarea următoarelor operațiuni de plată în cazul în care fondurile sunt acoperite printr-o linie de credit deschisă pentru un utilizator al serviciilor de plată: debitări directe, inclusiv debitări directe singulare, operațiuni de plată printr-un card de plată sau un dispozitiv similar, operațiuni de transfer-credit, inclusiv ordine de plată programată;

și a le transmite mai departe instituțiilor în numele și pe seama cărora lucrează, pentru ca acestea să ajungă, într-un final, la un destinatar aflat la distanță. În urma consultării registrului specializat al Băncii Naționale a României al instituțiilor de plată[1], la momentul scrierii erau înregistrați un număr de 56 de agenți, majoritatea persoane fizice, cu adresa în localități din afara țării cu comunități semnificative de români. Întrucât desfășoară operațiuni financiare reglementate de lege și aflate sub supravegherea Băncii Naționale a României, chiar și acești agenți pot fi solicitați în baza unui mandat al judecătorului de drepturi și libertăți să transmită date privind tranzacțiile financiare ale unei persoane. Este drept că aceleași date vor putea fi obținute de la instituția de plată pe seama căreia aceștia lucrează, însă nimic nu împiedică procurorul să formuleze o cerere față de acești agenți – persoane fizice.

O problemă de nișă o constituie posibilitatea obligării unei persoane fizice să remită date privind tranzacțiile financiare ale unei alte persoane atunci când deține înscrisuri (de exemplu, extrase de cont) din care rezultă conținutul acestor tranzacții. Într-o atare situație, apreciem că măsura nu va putea fi întrebuințată, întrucât persoana fizică arătată nu va avea calitatea de entitate financiară, fiind doar o persoană care deține anumite înscrisuri, putând fi aplicate procedee probatorii obișnuite pentru obținerea acestora.

e) emiterea de instrumente de plată și/sau acceptarea de operațiuni de plată;
f) remiterea de bani;
g) servicii de inițiere a plății;
h) servicii de informare cu privire la conturi".

[1] A se consulta pe *www.bnr.ro*

Capitolul IV
Corelația dintre obținerea de date privind situația financiară a unei persoane și obținerea datelor privind tranzacțiile financiare ale unei persoane

Fără a intra în specificul fiecărei măsuri de cercetare în parte, trebuie să fie relevate diferențele atât de natură, cât și de scop între obținerea datelor privind tranzacțiile financiare ale unei persoane și măsura similară de obținere de date privind situația financiară a unei persoane.

Prima diferență între cele două măsuri este obiectul lor: prima se referă la *conținutul tranzacțiilor financiare ale unei persoane* și cealaltă privește doar *situația financiară a unei persoane*. Mai mult, referindu-ne la dispozițiile art. 138 alin. (9) C.pr.pen., observăm că, în cazul primei metode speciale de cercetare, pot face obiectul măsurii nu numai conținutul tranzacției, ci și înscrisurile aflate în posesia unei instituții de credit sau entități financiare referitoare la tranzacțiile și operațiunile unei persoane.

Din punctul de vedere al naturii juridice, ambele măsuri se pot încadra în categoria metodelor speciale de cercetare, cu mențiunile cuprinse mai sus privind prevalența caracteristicilor de măsură de supraveghere tehnică a obținerii datelor privind tranzacțiile financiare ale unei persoane. Asemenea tuturor metodelor speciale de supraveghere sau cercetare, dispunerea lor se poate face numai în cursul urmăririi penale. Cu toate acestea, în cazul obținerii datelor privind tranzacțiile financiare trecute ale unei persoane, dar și cu privire la datele privind situația financiară a unei persoane, considerăm că și instanța va putea încuviința administrarea acelorași probe, însă prin alte procedee probatorii, întrucât aceste probe s-ar referi la fapte ce s-au desfășurat anterior încuviințării administrării probei. În acest sens, menționăm că aflarea situației financiare a unei persoane nu este o măsură specifică procesului penal, fiind necesară în cazul majorității proceselor civile privind succesiunea unei persoane pentru determinarea masei succesorale cunoașterea situației conturilor defunctului la data decesului acestuia. În același sens, pentru dovedirea unei eventuale dosiri a bunurilor defunctului de către succesori[1] prin retragerea unor sume de bani din contul defunctului, se impune ca instanța să administreze probe din care să rezulte conținutul tranzacțiilor financiare desfășurate ulterior decesului[2]. Instanța, într-o asemenea situație, își va întemeia fundamentarea unei cereri către instituția de credit pe dispozițiile art. 113 alin. (2) lit. e) din O.U.G. nr. 99/2006[3], la care am mai făcut

[1] Potrivit alin. (1) al art. 1.119 C.civ.: „Succesibilul care, cu rea-credință, a sustras ori a ascuns bunuri din patrimoniul succesoral sau a ascuns o donație supusă raportului ori reducțiunii este considerat că a acceptat moștenirea, chiar dacă anterior renunțase la ea. El nu va avea însă niciun drept cu privire la bunurile sustrase sau ascunse și, după caz, va fi obligat să raporteze ori să reducă donația ascunsă fără a participa la distribuirea bunului donat".

[2] În acest sens, C. Ap. București, s. a IV-a civ., dec. civ. nr. 360 din 14 februarie 2006, prin care instanța a stabilit, prin intermediul analizării tranzacțiilor financiare ulterioare decesului lui *de cuius*, că o parte dintre moștenitori au retras sume de bani din cont, în baza împuternicirilor dobândite în cursul vieții defunctului.

[3] Conform art. 113 alin. (2) lit. e) din O.U.G. nr. 99/2006:

„Informații de natura secretului bancar pot fi furnizate, în măsura în care acestea sunt justificate de scopul pentru care sunt cerute ori furnizate, în următoarele situații: (...) e) la solicitarea instanței, în scopul soluționării diferitelor cauze deduse judecății".

referire într-un capitol precedent. De altfel, în practica judiciară, în cazul proceselor civile ce au ca obiect succesiuni, instituțiile de credit comunică un extras de cont pentru ziua decesului lui *de cuius* sau un extras de cont pentru o perioadă mai lungă, în funcție de preferințe. Cu toate acestea, nu va fi posibil ca instanța să dispună pentru viitor obținerea datelor privind tranzacțiile financiare ale unei persoane, deoarece această atribuție nu intră între funcțiile instanței, dar și pentru că o asemenea măsură nu ar putea face obiectul judecății unei instanțe, aceasta limitându-se numai la fapte trecute, cuprinse în mod limitativ în actul de sesizare a instanței.

Cea mai importantă diferență dintre cele două măsuri de cercetare este că una poate avea un caracter dinamic și pentru viitor, iar cealaltă are tot timpul un caracter static și pentru trecut. Prin măsura obținerii datelor privind tranzacțiile financiare ale unei persoane se vor putea obține probe cu privire la desfășurarea unor tranzacții în trecut, dar și în viitor pentru durata pentru care se emite mandatul. Dimpotrivă, în cazul măsurii de cercetare a obținerii datelor privind situația financiară a unei persoane, măsura se va putea emite numai pentru trecut, cele mai recente situații fiind cele de la data la care se procedează la comunicarea răspunsului către procuror.

Instituțiile care pot fi ținute să dea curs solicitărilor procurorului în cazul ambelor măsuri speciale de cercetare par a fi diferite, aparent în cazul măsurii obținerii situației financiare a unei persoane, ea putând fi dispusă față de orice *instituție*, nu doar față de entități financiare. În realitate, apreciem că vom avea aceleași persoane care vor fi ținute să comunice procurorului informațiile cerute, cu mențiunea că termenul de „instituție" este unul mult prea general. Totodată, nu este de conceput că legiuitorul a avut în vedere să includă în cadrul măsurii și alte instituții care nu au legătură cu sectorul financiar, întrucât șansele ca ele să dețină date și informații privind situația financiară a unei persoane, date care să nu fie deținute și de o entitate financiară, sunt practic inexistente.

Din punctul de vedere al procedurii de autorizare, obținerea datelor privind tranzacțiile financiare ale unei persoane se aseamănă cu procedura de autorizare a supravegherii tehnice, diferită față de măsura de cercetare a obținerii de date privind situația financiară a unei persoane, care nu prevede o procedură specifică sau alte condiții, decât începerea urmăririi penale față de faptă (implicită, de altfel).

Persoanele față de care se pot lua cele două măsuri sunt aceleași, cu mențiunea că există o discrepanță între dispozițiile art. 146[1] alin. (1) C.pr.pen. și art. 153 alin. (1) C.pr.pen. Dacă, în cazul măsurii obținerii datelor privind tranzacțiile financiare ale unei persoane, aceasta se poate dispune față de făptuitor, suspect, inculpat sau orice persoană, în privința obținerii de date privind situația financiară a unei persoane, măsura poate fi luată față de orice persoană. Considerăm că mai întemeiate sunt aceste din urmă dispoziții, deoarece ele sunt în același sens cu dispozițiile art. 140 C.pr.pen., în care se arată că, pentru emiterea mandatului de supraveghere tehnică, trebuie indicată doar persoana supusă măsurii, fără a avea vreo importanță calitatea sa procesuală. În plus, nu considerăm corectă includerea în cuprinsul art. 146[1] C.pr.pen. a calității de **făptuitor,** care nu este recunoscută de legislația procesuală penală ca o calitate procesuală.

Capitolul V
Condițiile legale pentru autorizarea metodei speciale de cercetare

Obținerea datelor privind tranzacțiile financiare ale unei persoane, asemenea celorlalte metode speciale de supraveghere sau cercetare, presupune restrângerea drepturilor și libertăților persoanei vizate de acest procedeu probatoriu, motiv pentru care legea condiționează folosirea acestuia numai când sunt îndeplinite anumite condiții și cu garantarea respectării proporționalității între interesul public și interesul persoanei.

Necesitatea încuviințării procedeului probatoriu servește un dublu scop, cel de a conferi organelor de urmărire penală puteri sporite în activitatea de administrare a probelor și cel de a garanta legalitatea administrării probei.

Organul competent să dispună asupra folosirii metodei speciale de cercetare este *judecătorul de drepturi și libertăți*, ca regulă. În mod excepțional, *procurorul*, potrivit art. 146[1] alin. (4) C.pr.pen., va putea dispune limitat, pentru o durată de maximum 48 de ore și cu controlul ulterior al judecătorului de drepturi și libertăți, obținerea datelor privind tranzacțiile financiare ale unei persoane. Astfel cum vom vedea într-o secțiune ulterioară[1], apreciem că măsura autorizării provizorii de către procuror se va putea aplica doar pentru tranzacțiile viitoare ale persoanei supuse măsurii, nu și pentru obținerea datelor privind tranzacțiile sale trecute.

Obținerea datelor privind tranzacțiile financiare ale unei persoane se va putea încuviința numai dacă sunt îndeplinite condițiile cumulative prevăzute de art. 146[1] alin. (1) C.pr.pen. O condiție implicită constă în necesitatea începerii urmăririi penale pentru o faptă prevăzută de legea penală. Această condiție reiese din faptul că începerea urmăririi penale este actul procesual care creează întreg cadrul pentru desfășurarea activităților de urmărire penală, inclusiv administrarea probelor, întrucât Codul de procedură penală actual nu mai recunoaște faza actelor premergătoare din Codul de procedură penală anterior.

Prima condiție specială pentru acest procedeu probatoriu este existența unei *suspiciuni rezonabile cu privire la pregătirea sau săvârșirea unei infracțiuni*. Prevederea acestei condiții este inutilă și reprezintă o lipsă de inspirație din partea legiuitorului, care a vrut să facă o distincție între această măsură de cercetare și metodele de supraveghere tehnică. În cazul condiției similare prevăzute pentru supravegherea tehnică la art. 139 alin. (1) lit. a) C.pr.pen., trebuie ca infracțiunea care se pregătește sau care s-a săvârșit să aibă o anumită gravitate și să fie dintre cele indicate la art. 139 alin. (2) C.pr.pen. În realitate, condiția prevăzută de art. 146[1] alin. (1) lit. a) este inutilă, deoarece orice procedeu probatoriu se va dispune numai atunci când există o suspiciune rezonabilă privind pregătirea săvârșirii sau săvârșirea unei infracțiuni, întrucât din coroborarea art. 305 alin. (1) C.pr.pen. cu art. 294 alin. (3) C.pr.pen. rezultă că începerea urmăririi penale se va dispune în toate cazurile în care există o suspiciune rezonabilă privind pregătirea sau săvârșirea unei infracțiuni, iar din actul de sesizare nu rezultă vreun caz de împiedicare dintre cele prevăzute de art. 16 C.pr.pen. Alegerea legiuitorului este cu atât mai nefericită, întrucât infracțiunile în care probarea existenței unor tranzacții financiare ar avea o relevanță este destul de restrânsă, fapt care rezultă și din predecesoarea măsurii, prevăzută în legislația specială anterioară intrării în vigoare a Codului de procedură penală[2].

[1] *V. infra*, Titlul VIII, Capitolul VI.

[2] Monitorizarea tranzacțiilor unei persoane, *v. supra*, Titlul VII, Capitolul I.2.

Ipotetic, măsura de cercetare ar putea fi aplicată în orice cauză, însă este greu de imaginat care ar fi relevanța administrării unui asemenea procedeu probatoriu într-o infracțiune de loviri sau alte violențe, ucidere din culpă, viol etc. Chiar dacă se poate susține argumentul că legiuitorul trebuie să lase o marjă de apreciere organelor de urmărire penală, ținând seama de inventivitatea deosebită a făptuitorilor și a dezvoltării tehnologice, apreciem că acest argument nu ar fi suficient pentru a justifica deschiderea acestei măsuri de cercetare oricărei urmăriri penale. În opinia noastră, pentru această măsură specială de cercetare, trebuie prevăzut un criteriu de gravitate al faptei, pentru a putea justifica folosirea ei numai în cauze care depășesc o anumită gravitate reflectată prin pedeapsa prevăzută de legea penală.

Măsura de cercetare poate fi întrebuințată numai în cursul urmăririi penale, împrejurare comună cu toate metodele speciale de supraveghere sau cercetare. Sub acest aspect, avem o rezervă în a susține că decizia legiuitorului este una înțeleaptă, întrucât această măsură de cercetare are un caracter de excepție, putând viza tranzacțiile financiare trecute ale unei persoane. Această ipoteză nu se poate regăsi la niciuna dintre celelalte măsuri speciale de supraveghere tehnică[1] sau cercetare care își pot regăsi aplicabilitatea în prezent[2]. Este indiscutabilă utilitatea administrării probei privind tranzacțiile financiare trecute ale unei persoane în faza de judecată, întrucât reprezintă fapte și împrejurări trecute care pot contribui la soluționarea cauzei. Mai mult decât atât, întrucât măsura de cercetare se referă și la înscrisuri referitoare la tranzacțiile sau operațiunile unei persoane, față de natura acestor mijloace de probă, nu vedem de ce o instanță ar putea fi oprită să le obțină. În realitate, lacuna legislativă reliefată va privi doar faza de judecată, impunându-se reglementarea situației prin care instanța va putea administra proba și în faza de judecată. Cu toate că dispozițiile legale necesare există în legislația specială, era necesar să se prevadă în Cod o procedură distinctă pentru faza de judecată. *De lege ferenda*, se impune ca obținerea datelor privind tranzacțiile financiare trecute ale unei persoane să poată fi dispusă prin încheierea instanței, entitățile financiare fiind obligate să transmită datele și înscrisurile solicitate. Până la o modificare legislativă viitoare, apreciem că instanța își va putea întemeia solicitarea pe dispozițiile art. 114 din O.U.G. nr. 99/2006, întrucât formularea acestui articol include atât procurorul, cât și instanța de judecată, „*metodele speciale de supraveghere sau cercetare din Codul de procedură penală aplicându-se* ***corespunzător***" (s.n.)[3].

A doua condiție care se impune a fi îndeplinită pentru autorizarea măsurii de cercetare este cea privitoare la *proporționalitatea măsurii cu restrângerea drepturilor și libertăților fundamentale*. Această condiție este prevăzută de art. 146[1] alin. (1) lit. b) C.pr.pen. și se impune a fi analizată de judecătorul de drepturi și libertăți prin prisma criteriilor prevăzute de textul de lege: *particularitățile cauzei, importanța informațiilor sau a probelor ce urmează a fi obținute ori gravitatea infracțiunii*.

[1] Cu o aparentă excepție în cazul accesului la un sistem informatic, însă, în cazul acestei măsuri, se vor descoperi probe create în trecut concomitent cu date informatice noi create în timpul realizării accesului la un sistem informatic. În ipoteza unui suport de stocare, datele vor fi tot timpul create în trecut, procedeul probatoriu care va trebui utilizat de instanță va fi percheziția informatică.

[2] Obținerea datelor de trafic și de localizare prelucrate de către furnizorii de rețele publice de comunicații electronice destinate publicului este o metodă specială de cercetare exclusiv pentru trecut, însă este inoperantă ca urmare a Deciziei Curții Constituționale nr. 440 din 8 iulie 2014 care a declarat neconstituțională Legea nr. 82/2012.

[3] Totodată, vor putea fi avute în vedere și dispozițiile art. 113 alin. (2) lit. e) din O.U.G. nr. 99/2006, prin care o instituție de credit poate transmite informații de natura secretului bancar, la solicitarea instanței, pentru soluționarea diferitelor cauze deduse judecății.

Proporționalitatea trebuie analizată prin raportare la gravitatea dreptului la viață privată al persoanei, judecătorul de drepturi și libertăți trebuind să constate că nu va exista o disproporție între acțiunile statului și dreptul la viață privată al persoanei. În cadrul analizei asupra ingerinței aduse dreptului la viață privată, judecătorul de drepturi și libertăți nu va avea în vedere numai activitățile personale sau cotidiene ale unei persoane, ci și activitățile sale comerciale sau profesionale[1]. Va trebui să se aibă în vedere și dacă se solicită o măsură de cercetare pentru trecut sau pentru viitor, întrucât, în opinia noastră, dispunerea obținerii tranzacțiilor financiare trecute ale unei persoane poate avea caracter mult mai invaziv față de o măsură dispusă pentru viitor. Dacă în cazul monitorizării tranzacțiilor viitoare, legea instituie o durată maximă pentru care poate opera măsura (6 luni), pentru tranzacțiile trecute, legea nu instituie nicio limită temporală. În acest sens, s-a constatat inclusiv în jurisprudența Curții Europene a Drepturilor Omului încălcarea dreptului la viață privată referitoare la obținerea de date privind tranzacțiile financiare ale unei persoane, reliefându-se și situația în care s-au obținut informații privind tranzacțiile unei persoane pentru o perioadă de peste doi ani dinainte de dispunerea măsurii[2]. Întrucât legea nu instituie nicio limită temporală pentru măsură, este necesar ca judecătorul de drepturi și libertăți să cântărească atent sub aspectul proporționalității luarea măsurii, trebuind să se limiteze cât mai strict cu privire la intervalul de timp pentru care pot fi obținute date privind tranzacțiile financiare ale unei persoane. În măsura în care procurorul nu ar menționa intervalul de timp pentru care dorește să afle conținutul tranzacțiilor financiare, apreciem că judecătorul de drepturi și libertăți se află în imposibilitatea de a analiza concret proporționalitatea măsurii, trebuind să respingă propunerea de autorizare a măsurii.

De plano, judecătorul de drepturi și libertăți nu ar trebui să admită obținerea datelor privind tranzacțiile financiare dintre avocat și suspect, inculpat sau orice persoană pe care o apără, decât în situația în care există date că avocatul săvârșește sau pregătește săvârșirea unei infracțiuni dintre cele prevăzute de art. 139 alin. (2) C.pr.pen.[3].

Prin „particularitățile cauzei" vom înțelege acele împrejurări specifice unei anumite cauze penale care vor impune utilizarea metodelor speciale de supraveghere sau cercetare pentru soluționarea cauzei, deoarece un altfel de mijloc nu ar fi propice pentru a stabili starea de fapt. De exemplu, în cazul infracțiunii de spălarea banilor, prevăzută de art. 49 din Legea nr. 129/2019[4], măsura va fi necesară atunci când fapta se realizează prin intermediul unor conturi deținute la entități financiare.

Prin „importanța informațiilor ori a probelor ce urmează a fi obținute" înțelegem contribuția pe care o pot avea informațiile sau probele obține pentru stabilirea împrejurărilor esențiale ale cauzei. Tot în cazul infracțiunilor de spălarea banilor, măsura își va găsi utilitatea maximă, fiind propice pentru obținerea de probe directe privind săvârșirea infracțiunii.

„Gravitatea infracțiunii" are în vedere o analiză a pericolului social concret pe care îl presupune săvârșirea infracțiunii care face obiectul urmăririi penale. Acest criteriu se va stabili de către organele judiciare și printr-un just echilibru între interesul public de a urmări o faptă și restrângerea dreptului la viață privată[5].

---

[1] CEDO, cauza *Niemietz c. Germania,* Hotărârea din 16 decembrie 1992, §29.

[2] CEDO, cauza *Sommer c. Germania*. În cauză au fost incidente mai multe probleme de drept, între care: autorizarea măsurii de către procuror, autorizarea măsurii față de un avocat, dar mai ales lipsa de informare a avocatului de către procuror, corelativă cu interzicerea expresă a băncii de a-l informa pe avocat cu privire la desfășurarea măsurii, precum și lipsa unui remediu legal pentru ingerința adusă vieții private.

[3] *F. Ciopec*, Drept procesual penal. Partea generală, Ed. C.H. Beck, București, 2017, p. 179.

[4] Publicată în M. Of. nr. 589 din 18 iulie 2019.

[5] A se vedea, în acest sens, CEDO, cauza *Ibrahim ș.a. c. Marea Britanie*, Hotărârea din 13 septembrie 2016, §274.

A treia condiție impusă de Codul de procedură penală pentru încuviințarea măsurii de cercetare este *necesitatea procedeului probatoriu* pentru obținerea probei. Cu alte cuvinte, condiția se referă și la *subsidiaritatea* măsurilor speciale de supraveghere sau cercetare față de orice alt procedeu probatoriu. Această condiție este prevăzută în cuprinsul art. 146[1] alin. (1) lit. c) C.pr.pen. și restrânge obținerea datelor privind tranzacțiile financiare ale unei persoane, cu excepția cazurilor în care „*probele nu ar putea fi obținute în alt mod sau obținerea lor ar presupune dificultăți deosebite ce ar prejudicia ancheta ori există un pericol pentru siguranța persoanelor sau a unor bunuri de valoare*". Această condiție este comună cu cea prevăzută în cazul supravegherii tehnice, iar măsura specială de cercetare nu prezintă caracteristici particulare în plus, astfel că facem trimitere la cele expuse mai devreme în prezenta lucrare[1].

[1] *V. supra*, Titlul III, Capitolul I.4.

Capitolul VI
Procedura autorizării obținerii datelor privind tranzacțiile financiare ale unei persoane

Secțiunea 1. Autorizarea măsurii de către judecătorul de drepturi și libertăți

În considerarea faptului că măsura specială de cercetare supusă analizei a făcut parte din supravegherea tehnică mai înainte de intrarea în vigoare a O.U.G. nr. 18/2016, procedura de autorizare a rămas de competența judecătorului de drepturi și libertăți.

Potrivit art. 146[1] alin. (3) C.pr.pen., dispozițiile art. 140 alin. (2)-(9) C.pr.pen. se vor aplica corespunzător, fapt care semnifică împrumutarea procedurii de autorizare de la măsurile de supraveghere tehnică. Considerăm că legiuitorul trebuia să includă aplicarea și a alin. (1) al art. 140 C.pr.pen., întrucât prevederea de la art. 146[1] alin. (2) C.pr.pen. putea fi dedusă prin aplicarea corespunzătoare a art. 140 alin. (1) C.pr.pen.

Pentru a se putea autoriza metoda specială de cercetare, este necesar ca procurorul să întocmească o cerere în acest sens, în care să fie cuprinse toate elementele legale prevăzute de art. 140 alin. (2) C.pr.pen., pe care să o transmită judecătorului de drepturi și libertăți. Observăm că legiuitorul alternează în terminologie atunci când se referă la actul procurorului, acesta constituind fie o *cerere* [art. 140 alin. (2) C.pr.pen.], fie o *propunere* [art. 146[1] alin. (1) C.pr.pen.]. Apreciem că această inconsecvență este una nefericită, în opinia noastră, impunându-se ca legiuitorul să întrebuințeze termenul de „propunere" pentru a exprima în mod unitar o solicitare adresată de un organ judiciar către un alt organ judiciar învestit prin lege cu soluționarea acesteia în cursul urmăririi penale.

Competența de judecare a propunerii revine judecătorului de drepturi și libertăți din cadrul instanței competente să judece cauza în primă instanță sau din cadrul instanței corespunzătoare în grad acesteia în a cărei circumscripție se află sediul parchetului din care face parte procurorul care a formulat cererea.

Pentru autorizarea obținerii datelor privind situația financiară a unei persoane de către judecătorul de drepturi și libertăți, se impune mai întâi verificarea de către acest organ judiciar a respectării condițiilor prevăzute de art. 146[1] alin. (1) C.pr.pen.

Această verificare se face pe baza propunerii depuse de către procuror și în urma verificării dosarului cauzei, care va fi înaintat de către procuror împreună cu propunerea de autorizare a măsurii speciale de cercetare. Procurorul trebuie să includă toate elementele prevăzute de art. 140 alin. (2) C.pr.pen.[1], trebuind să fie detaliată și sub aspectul întinderii acesteia, în sensul precizării caracterului temporal al măsurii: dacă solicitarea privește tranzacții financiare trecute ale persoanei, tranzacții financiare viitoare sau ambele, cu mențiunea că, în cazul tranzacțiilor din trecut, trebuie să se precizeze expres intervalul de timp pentru care se cere

[1] Conform acestui articol, cererea trebuie să cuprindă, printre altele: numele sau alte date de identificare a persoanei împotriva căreia se dispune măsura, dacă sunt cunoscute, indicarea probelor ori a datelor din care rezultă suspiciunea rezonabilă cu privire la săvârșirea unei infracțiuni, indicarea faptei și a încadrării juridice, motivarea caracterului proporțional și subsidiar al măsurii.

autorizarea măsurii[1]. Procurorul trebuie să indice, dacă sunt cunoscute, conturile persoanei care va fi supusă măsurii ori indicarea entității financiare care va fi obligată să transmită datele solicitate. Nu considerăm că lipsa nominalizării entității financiare ar putea afecta legalitatea măsurii sau că ar constitui o lipsă de proporționalitate dacă s-ar dispune față de unele categorii de entități la care o persoană are deschise conturi. Cu toate acestea, va constitui o ingerință în viața privată a unei persoane și o lipsă de proporționalitate autorizarea măsurii pentru orice entitate financiară, întrucât se impune ca judecătorul de drepturi și libertăți să analizeze specificul tranzacțiilor entității financiare vizate și fapta care face obiectul urmăririi penale. De pildă, dacă se urmărește o infracțiune de spălarea banilor desfășurată prin intermediul instituțiilor de credit, nu va fi proporțională măsura dacă se va autoriza și pentru societăți de asigurare, reasigurare sau societăți de pensii.

Judecarea propunerii procurorului are loc în aceeași zi cu formularea ei, în camera de consiliu, fără citarea părților și cu prezența obligatorie a procurorului. Soluțiile pe care le poate pronunța judecătorul de drepturi și libertăți sunt fie respingerea cererii, fie admiterea ei.

Respingerea cererii se va dispune conform art. 140 alin. (6) C.pr.pen., atunci când judecătorul de drepturi și libertăți va respinge în totalitate cererea procurorului, fie ca inadmisibilă, fie ca nefondată.

În cazul oricăreia dintre soluțiile adoptate de către judecătorul de drepturi și libertăți, aceasta nu va putea fi supusă niciunei căi de atac, însă procurorul va fi îndreptățit să formuleze o nouă cerere de încuviințare în cazul respingerii, dacă vor fi îndeplinite cerințele prevăzute de art. 140 alin. (8) C.pr.pen.[2].

În cazul admiterii cererii, judecătorul de drepturi și libertăți va dispune numai asupra persoanelor față de care s-a propus măsura – suspect, inculpat sau altă persoană, cu indicarea numelui acestuia, a tipului de tranzacții financiare avute în vedere, a entității financiare care va transmite datele privind conținutul tranzacțiilor financiare și, după caz, indicarea înscrisurilor cu privire la tranzacțiile sau operațiunile financiare, alături de mențiunile cuprinse de art. 140 alin. (5) C.pr.pen. Referitor la mențiunea cuprinsă la art. 140 alin. (5) lit. f) C.pr.pen., apreciem că, în cazul acestei măsuri de cercetare, va fi necesară indicarea numelui persoanei supuse măsurii, întrucât, în cazul tranzacțiilor financiare, aceasta va trebui identificată nominal. Nu poate fi imaginată nicio situație în care organele de urmărire penală să dețină numai informații cu privire la un anumit cont, fără a cunoaște și numele persoanei care deține contul.

În situația în care s-ar cunoaște numai contul unei persoane, s-ar impune ca organele de urmărire penală să procedeze prin intermediul procedurii prevăzute de art. 153 C.pr.pen. la aflarea titularului contului și, mai apoi, la formularea unei propuneri către judecătorul de drepturi și libertăți pentru ca acesta să poată analiza față de o persoană concretă luarea măsurii, dacă nu ar cunoaște aceste informații din orice altă sursă. Mai mult, ține și de o minimă obligație de diligență a organelor de urmărire penală să facă acest lucru, în condițiile în care nu ar avea minime date privind tranzacțiile desfășurate cu titularul respectivului cont – fiind de notorietate că nu pot exista tranzacții financiare anonime. Nu putem fi de acord cu o opinie exprimată în doctrină[3] potrivit căreia există obligația ca, înainte de a se formula propunerea privind obținerea datelor privind tranzacțiile financiare ale unei persoane, procurorul să

[1] *A.-R. Trandafir, G. Marin*, Obținerea de informații ori înscrisuri de la instituțiile de credit în cursul urmăririi penale, publicat pe *www.juridice.ro*

[2] Cu privire la formularea unei noi cereri de autorizare, *v. supra*, Titlul III, Capitolul II.2.

[3] *V. Trif*, op. cit., p. 253.

solicite, în temeiul art. 153 C.pr.pen., obținerea de date privind situația financiară a unei persoane. Această condiționare nu există în cuprinsul Codului de procedură penală și exclude posibilitatea ca organul de urmărire penală să cunoască atât contul persoanei, cât și persoana titulară din alte surse (de pildă, prin descoperirea unui extras de cont ori ordin de plată în urma unei percheziții domiciliare).

S-a susținut în doctrină o opinie jurisprudențială conform căreia în procedura autorizării măsurii se impune ca procurorul să indice datele de identificare a contului, nefiind suficientă indicarea instituției bancare la care persoanele vizate de măsură ar avea conturi, apreciindu-se că art. 140 alin. (5) lit. g) C.pr.pen. include o condiție în acest sens[1]. Nu putem fi de acord cu această susținere, întrucât reprezintă o interpretare defectuoasă a legii și conduce la tergiversarea urmăririi penale și văduvirea de obiect a măsurii de cercetare. În cuprinsul art. 140 alin. (5) lit. g) C.pr.pen. se impune indicarea, între altele, „*a oricăror **date cunoscute** pentru identificarea căii de comunicare sau a numărului de cont*" (s.n.); în măsura în care datele privitoare la cont nu sunt cunoscute, nu înseamnă că nu există date pentru identificarea numărului de cont, aceasta făcându-se în baza datelor de identificare a titularului[2]. Limitarea măsurii doar la un cont identificat prin numărul acestuia (IBAN, în cazul instituțiilor de credit) exclude posibilitatea furnizării datelor privind tranzacțiile de pe alte conturi deținute de persoana vizată la aceeași instituție de credit.

Admiterea cererii se face prin încheierea judecătorului de drepturi și libertăți, care va proceda la emiterea imediată a mandatului de obținere a datelor privind tranzacțiile financiare ale unei persoane, întocmind în mod obligatoriu o minută. În cuprinsul acestui mandat se va impune nominalizarea persoanei față de care s-a luat măsura, fără a se menționa calitatea ei procesuală sau obiectul urmăririi penale, întrucât mandatul se va transmite unei entități financiare care nu are niciun drept să cunoască aceste aspecte și ar putea lua măsuri de consemnare a acestei calități pe care o are clientul și să se folosească de aceste informații în relațiile viitoare cu acesta[3].

După admiterea cererii procurorului, judecătorul de drepturi și libertăți emite, conform art. 140 alin. (5) C.pr.pen., un mandat care trebuie să cuprindă mai multe elemente regăsite și în încheierea de admitere a cererii. Mandatul emis nu va fi un mandat de supraveghere tehnică (și nici nu ar trebui denumit astfel), ci un mandat de obținere a datelor privind tranzacțiile financiare ale unei persoane.

Elementele comune care nu pun probleme deosebite sunt cele privind *denumirea instanței*, *data, ora și locul emiterii*, *numele, prenumele* și *calitatea persoanei care a dat încheierea și a emis mandatul*, *semnătura judecătorului și ștampila instanței*. Un alt element comun care nu ridică probleme este perioada pentru care se dispune măsura de cercetare, aceasta putând fi de maximum 30 de zile.

Alături de acestea, în cuprinsul art. 140 alin. (5) lit. e) teza a II-a C.pr.pen., legiuitorul a prevăzut că este obligatorie menționarea *scopului* pentru care s-a încuviințat măsura. În

[1] Trib. București, s. I pen., încheierea din 2 martie 2017, dosar nr. 7229/3/2017, nepublicată, *apud V. Trif*, op. cit., p. 253.

[2] În acest sens, a se vedea *A.-R. Trandafir, G. Marin*, Obținerea de informații ori înscrisuri de la instituțiile de credit în cursul urmăririi penale, publicat pe *www.juridice.ro*

[3] *A.-R. Trandafir*, Obținerea de informații și înscrisuri de la instituțiile de credit în cursul urmăririi penale, prelegere susținută în cadrul Conferinței privind aspecte de practică neunitară intervenite de la intrarea în vigoare a Noului Cod penal și Noului Cod de procedură penală, București, 9-10 octombrie 2017, organizată de Institutul Național al Magistraturii – *www.youtube.com*

opinia noastră, acest element este inutil în cuprinsul unui mandat de obținere a datelor privind tranzacțiile financiare ale unei persoane, întrucât, fiind vorba de un procedeu probatoriu, scopul este subînțeles.

În privința *indicării concrete a măsurii încuviințate*, judecătorul de drepturi și libertăți va trebui să detalieze care sunt datele financiare sau înscrisurile pe care trebuie să le transmită instituția de credit sau entitatea financiară: extrasele de cont, tranzacțiile efectuate la bancomate, ordinele de plată semnate de o anumită persoană, contractele de credit, cumpărarea sau răscumpărarea de unități de fond, de acțiuni etc. Tot în această categorie va trebui indicat intervalul temporal pentru care se cer datele sau înscrisurile.

Astfel cum am menționat mai sus, *numele persoanei* supusă măsurii va trebui indicat pentru ca entitatea financiară să poată să identifice conturile ale căror tranzacții vor fi avute în vedere. În mod evident, dacă vor fi cunoscute datele de identificare ale persoanei față de care se ia măsura, acestea trebuie transmise.

Numărul de cont vizat de măsură va trebui să fie transmis numai în situația în care acesta este cunoscut de către organele de urmărire penală. În lipsa unor date de identificare complete (de exemplu, se cunoaște doar numele persoanei vizate), indicarea unui număr de cont deja cunoscut poate fi deosebit de utilă pentru entitatea financiară, în condițiile în care există mai mulți clienți cu același nume.

Măsura poate fi dispusă pentru o durată maximă de 30 de zile în cazul tranzacțiilor financiare care urmează a fi efectuate[1]. Legea nu prevede niciun termen de punere în executare a măsurii în cazul tranzacțiilor financiare deja realizate, ceea ce constituie un neajuns, întrucât nu se poate admite punerea în executare întârziată a unei măsuri de cercetare. În sens contrar, s-a susținut că ar trebui indicat și intervalul de timp în care metoda specială urmează a fi pusă în executare cu privire la tranzacțiile trecute, întrucât o autorizare *sine die* ar încălca în mod nejustificat dreptul la viață privată[2]. *De lege ferenda*, se impune ca, în cazul acestei măsuri de cercetare, termenul de 30 de zile de valabilitate al autorizării să fie aplicabil și tranzacțiilor financiare trecute, procurorul pierzând dreptul de a solicita aceste date după expirarea mandatului, nu și de a le primi.

Conform art. 146[1] alin. (4) C.pr.pen. raportat la art. 144 C.pr.pen., măsura de cercetare poate fi prelungită, fiecare prelungire neputând depăși 30 de zile. Totodată, conform art. 146[1] alin. (4) C.pr.pen., durata totală a măsurii de cercetare nu poate depăși 6 luni **în aceeași cauză cu privire la aceeași persoană**. Remarcăm două aspecte de interes cu privire la durata totală: lipsa cumulului cu durata maximă de autorizare a măsurilor de supraveghere tehnică și limitarea aplicării măsurii de cercetare prin raportare la persoană și cauză, nu prin raportare la persoană și faptă.

Întrucât măsura nu este considerată ca făcând parte din metodele de supraveghere tehnică, autorizarea anterioară a supravegherii tehnice pentru o anumită durată nu va împiedica dispunerea măsurii de cercetare și prelungirea acestei măsuri până la 6 luni. Astfel, măsurile de supraveghere tehnică și această măsură de cercetare pot fi autorizate succesiv, fiecare pentru o durată maximă de 6 luni[3].

---

[1] *Gh. Mateuț*, Procedură penală, 2019, p. 709; *M Bulancea, R. Slăvoiu*, în M. Udroiu (coord.), Codul de procedură penală, 2017, p. 715; *A.-R. Trandafir, G. Marin*, Obținerea de informații ori înscrisuri de la instituțiile de credit în cursul urmăririi penale, publicat pe *www.juridice.ro*; *V. Trif*, op. cit., p. 255.

[2] *M. Bulancea, R. Slăvoiu*, în M. Udroiu (coord.), Codul de procedură penală, 2017, p. 716.

[3] *Ibidem*; *M. Udroiu*, Procedură penală, vol. I, 2019, p. 631; *A.-R. Trandafir, G. Marin*, Obținerea de informații ori înscrisuri de la instituțiile de credit în cursul urmăririi penale, publicat pe *www.juridice.ro*

Limitarea prelungirii măsurii prin raportare la aceeași persoană și aceeași cauză este o particularitate a metodei speciale de cercetare, astfel se poate ca, pentru aceeași persoană, în aceeași cauză, să se dispună obținerea datelor privind tranzacțiile financiare ale unei persoane pentru o durată de maximum 6 luni, durată care va putea fi extinsă în măsura în care cauza se schimbă. În doctrină s-a arătat că va constitui aceeași cauză situația în care procurorul dispune extinderea urmăririi penale pentru o altă faptă, nefiind posibilă prelungirea peste 6 luni a măsurii[1]. Dimpotrivă, disjungerea cauzei va conduce la posibilitatea prelungirii pentru 30 de zile a măsurii în noua cauză chiar și dacă privește aceeași persoană[2], făcând posibilă curgerea unei durate maxime de autorizare de încă 6 luni.

Secțiunea a 2-a. Autorizarea provizorie a măsurii de către procuror

În mod excepțional și cu controlul ulterior al judecătorului de drepturi și libertăți, Codul de procedură penală permite procurorului să autorizeze provizoriu, pentru o perioadă care nu poate depăși 48 de ore, obținerea datelor privind tranzacțiile financiare ale unei persoane.

Această prevedere este una excepțională, putând fi utilizată de procuror numai atunci când sunt întrunite condițiile stricte ale art. 146[1] alin. (5) C.pr.pen., măsura fundamentându-se pe urgența efectuării actului. Urgența impune procurorului să procedeze direct la autorizarea măsurii de cercetare ca urmare a faptului că nu există timpul necesar pentru parcurgerea procedurii ordinare în fața judecătorului de drepturi și libertăți.

Procedura autorizării de către procuror este prevăzută în mod analog celei din cazul supravegherii tehnice, sens în care facem trimitere la explicațiile generale și criticile făcute mai devreme în prezenta lucrare[3].

Pentru autorizarea provizorie a obținerii datelor privind tranzacțiile financiare ale unei persoane vor trebui respectate condițiile generale despre care am discutat anterior, dar și condiții specifice, similare autorizării măsurilor de supraveghere tehnică pentru o durată de maximum 48 de ore (art. 141 C.pr.pen.). Astfel, pe lângă caracterul urgent, art. 146[1] alin. (5) C.pr.pen. adaugă drept condiții: „*întârzierea substanțială a cercetărilor, pierderea, alterarea sau distrugerea probelor ori ar pune în pericol siguranța victimei sau a altor persoane*".

În privința întârzierii substanțiale a cercetărilor, considerăm că legiuitorul a impus o condiție care nu se justifică raportat la durata relativ scurtă de timp în care se poate obține un mandat de la judecătorul de drepturi și libertăți, astfel simplul motiv că cercetarea ar fi întârziată cu o zi sau două nu apreciem că poate constitui motiv suficient[4]. În plus, ținând seama că măsura de cercetare nu se pune în executare decât cu sprijinul unei entități financiare, vor exista evidente întârzieri în punerea ei în aplicare, deoarece predarea înscrisurilor și datelor privind tranzacțiile financiare se va face în scris, ulterior momentului la care acestea au loc. De altfel, nici nu se poate pretinde ca un particular să depună un efort disproporționat în sprijinul organelor de urmărire penală, acesta fiind incident în cazul de față. Lesne poate fi imaginată situația emiterii unei ordonanțe de autorizare care să presupună transmiterea unui original al ordinului de plată întocmit de o persoană cu mult timp înainte, acesta putând fi arhivat deja de bancă și neputând fi pus la dispoziția imediată a organelor de urmărire penală.

[1] *Gh. Mateuț*, Procedură penală, 2019, p. 709.
[2] *Ibidem*; *M. Bulancea, R. Slăvoiu*, în M. Udroiu (coord.), Codul de procedură penală, 2017, p. 715.
[3] *V. supra*, Titlul III, Capitolul II.3.
[4] *S. Grădinaru*, Supravegherea tehnică, 2014, p. 37.

Cazul pierderii, alterării sau distrugerii probelor este inaplicabil, întrucât datele și înscrisurile solicitate sunt deținute de o instituție de credit sau de o altă entitate financiară față de care nu se ridică suspiciuni că ar putea exercita astfel de acțiuni care să conducă la pierderea probelor. Mai mult decât atât, instituțiile de credit trebuie să arhiveze toate datele și înscrisurile privind relația cu clienții.

Cea de-a treia situație prevăzută de lege este aplicabilă atunci când obținerea întârziată a mandatului ar pune în pericol siguranța victimei sau a altor persoane. Din nou ne aflăm într-o situație în care este discutabilă posibilitatea emiterii unei astfel de ordonanțe, întrucât obținerea datelor privind tranzacțiile financiare ale unei persoane nu ar putea releva informații prin care să se poată asigura siguranța persoanelor amintite mai sus. Cert este că ar exista mijloace mai eficiente de a preveni producerea rezultatului pe care legiuitorul îl dorește evitat sau pentru identificarea infractorului decât această măsură de cercetare specială dispusă provizoriu.

Specifică măsurii de cercetare a obținerii datelor privind tranzacțiile financiare ale unei persoane este problema obținerii tranzacțiilor financiare trecute ale unei persoane prin ordonanța procurorului de autorizare provizorie. În doctrină s-a arătat că pare de neînțeles opțiunea legiuitorului de a permite procurorului să obțină datele privind tranzacțiile financiare trecute ale unei persoane, neputându-se susține caracterul de urgență al măsurii[1], întrucât probele nu s-ar putea pierde ca urmare a obligației entităților financiare de a păstra și arhiva tranzacțiile. Într-o asemenea situație, apreciem că autorizarea măsurii de către procuror ar avea un evident caracter ilegal, întrucât ar permite acestuia să obțină conținutul tranzacțiilor trecute ale unei persoane pentru o durată nelimitată în timp, în condițiile în care nu s-ar putea pierde aceste probe și, ținând seama de caracterul lor trecut, obținerea lor nu ar putea fi justificată pe temeiul urgenței.

Autorizarea de către procuror a obținerii datelor privind tranzacțiile financiare ale unei persoane se dispune prin ordonanță, aceasta trebuind să conțină toate elementele prevăzute de art. 140 alin. (5) C.pr.pen., adică să aibă un conținut identic cu mențiunile obligatorii din mandatul și încheierea care se emit, în procedura obișnuită, de judecătorul de drepturi și libertăți.

Conform art. 141 alin. (3) C.pr.pen., procurorul are obligația ca, în termen de cel mult 24 de ore de la expirarea măsurii, să sesizeze judecătorul de drepturi și libertăți competent în vederea confirmării măsurii. Deși textul art. 141 indică existența unui proces-verbal de redare rezumativă a activităților de supraveghere tehnică efectuate și dosarul cauzei, în cazul acestei măsuri de cercetare specială, nu se poate vorbi despre un asemenea proces-verbal, nefiind incidentă o supraveghere tehnică. Situația este oarecum aparte, fiind posibil ca, după expirarea măsurii, instituția de credit sau entitatea financiară să nu aibă suficient timp să comunice datele și înscrisurile solicitate de procuror, întrucât, în orice situație, sesizarea judecătorului de drepturi și libertăți va trebui să se facă în termen de 24 de ore la expirarea măsurii sub sancțiunea decăderii[2]. Suntem de acord cu corectitudinea identificării de către doctrină a acestei sancțiuni, deoarece textul de lege impune urgența acestei sesizări, prevăzând posibilitatea ca judecătorul de drepturi și libertăți să dispună, prin aceeași încheiere, autorizarea măsurilor de supraveghere tehnică. S-a susținut că, fiind incidentă decăderea, cererea procurorului de confirmare a măsurii formulată peste termen nu poate conduce la o soluție de confirmare și nici de infirmare a măsurii într-o asemenea situație, impunându-se anularea ordonanței

[1] *V. Trif*, op. cit., p. 257.

[2] *M. Udroiu*, Procedură penală, vol. I, 2019, p. 580.

procurorului și a probelor obținute, în condițiile art. 282 C.pr.pen. privind nulitățile relative[1]. În ipoteza în care entitatea financiară solicitată nu a comunicat datele și înscrisurile solicitate de procuror prin ordonanță, judecătorul de drepturi și libertăți va fi ținut să analizeze cererea de confirmare a procurorului și în absența acestora, întrucât este nevoit să respecte termenul de pronunțare de 24 de ore, prevăzut de art. 141 alin. (4) C.pr.pen. Ținând seama de natura măsurii de cercetare, lipsa de la dosarul cauzei a datelor și înscrisurilor solicitate prin ordonanța procurorului de autorizare a măsurii constituie o dovadă a lipsei de urgență a măsurii, întrucât dacă, după trecerea a 72 de ore de la punerea în executare a măsurii, organele de urmărire penală nu au obținut probe suplimentare, este evident că procurorul ar putea proceda la propunerea luării măsurii de către judecătorul de drepturi și libertăți.

În cazul acestei măsuri de cercetare, se reflectă cel mai bine opinia din doctrină potrivit căreia instituția autorizării de către procuror a măsurilor de supraveghere tehnică (implicit și acelor de cercetare care urmează aceeași procedură) ar trebui eliminată, deoarece intră în contradicție cu funcția judiciară atribuită judecătorului de drepturi și libertăți[2].

Cu ocazia formulării cererii de confirmare a măsurii, procurorul poate să ceară autorizarea în continuare a măsurii de cercetare, în condițiile art. 140 C.pr.pen.

Judecătorul de drepturi și libertăți, fiind sesizat de procuror în vederea confirmării măsurii de cercetare, are posibilitatea de a *infirma* sau *confirma* măsura efectuată în baza autorizației emise de procuror.

În situația în care judecătorul de drepturi și libertăți va constata că au fost încălcate dispozițiile art. 146[1] alin. (5) C.pr.pen. privind autorizarea de către procuror a obținerii datelor privind tranzacțiile financiare ale unei persoane, măsura va fi infirmată și se va dispune distrugerea probelor obținute. Față de această încheiere, procurorul nu poate exercita nicio cale de atac, fiind obligat să procedeze la distrugerea probelor obținute, consemnând operațiunea într-un proces-verbal. În măsura în care s-au transmis înscrisuri originale de către o entitate financiară, acestea nu vor fi distruse, trebuind să fie restituite acesteia.

În cazul în care judecătorul de drepturi și libertăți va aprecia că autorizarea măsurilor de supraveghere tehnică dispuse de procuror s-a făcut în conformitate cu prevederile art. 146[1] alin. (5) C.pr.pen., va proceda la confirmarea măsurii prin încheiere.

[1] *Ibidem*, p. 580.

[2] *Gh. Mateuț*, Procedură penală, 2019, p. 689.

Capitolul VII
Punerea în executare a metodei speciale de cercetare

Secțiunea 1. Transmiterea mandatului și obligațiile instituției solicitate

Spre deosebire de măsurile de supraveghere tehnică, obținerea datelor privind tranzacțiile financiare ale unei persoane va presupune concursul unei instituții de credit sau unei alte entități financiare, acestea reprezentând sursa de informare a organelor de urmărire penală. Sub acest aspect, procedeul probatoriu se aseamănă cu predarea voluntară de obiecte, înscrisuri sau date informatice prevăzută de art. 170 C.pr.pen.

După ce judecătorul de drepturi și libertăți se pronunță asupra încuviințării măsurii și emite mandatul de obținere a datelor privind tranzacțiile financiare ale unei persoane, procurorul va proceda la transmiterea acestui mandat către fiecare instituție de credit sau entitate financiară vizată. Nu va fi necesar să emită o ordonanță privind punerea în executare a măsurii, fiind suficientă transmiterea mandatului (în original sau în copie certificată pentru conformitate cu originalul[1]), întrucât procurorul nu poate depăși autorizarea dată de judecătorul de drepturi și libertăți. Ceea ce poate fi inclus alături de mandat, eventual printr-o adresă emisă de procuror, este cadrul în care se va realiza măsura de cercetare: modul de transmitere a datelor și informațiilor, împuternicirea ridicării de către organele de cercetare a rezultatelor măsurii de cercetare, ritmicitatea transmiterii acestora[2] etc. Nu va fi suficientă menționarea printr-o adresă a existenței unui mandat emis de judecătorul de drepturi și libertăți, acesta trebuind să fie transmis în mod efectiv[3]. Acesta a fost sensul pentru care legiuitorul stabilește, în cazul procedeelor probatorii intruzive, existența unei *încheieri* – act procesual de autorizare cu caracter nepublic, ce cuprinde toate elementele care au stat la baza autorizării măsurii, dar și a unui *mandat* – un act procedural cu caracter sumar, emis cu scopul de a certifica existența autorizării cerute de lege față de terți participanți. În lipsa transmiterii mandatului către instituțiile financiare solicitate, emiterea de către judecător a mandatului nu ar avea nicio finalitate, întrucât la dosarul cauzei va exista oricum încheierea judecătorului de drepturi și libertăți care cuprinde toate elementele din mandat.

Deși nu se specifică în cuprinsul art. 146[1] C.pr.pen., apreciem că, prin raportare la caracterul intruziv al măsurii, procurorul este obligat să dispună prin ordonanță încetarea măsurii de cercetare înainte de expirarea mandatului, dacă nu mai există temeiurile care au justificat măsura, aplicându-se dispozițiile art. 142 alin. (4) C.pr.pen.

Potrivit art. 146[1] alin. (7) C.pr.pen., „*instituțiile de credit sau entitățile financiare care efectuează tranzacțiile financiare sunt obligate să predea înscrisurile sau informațiile la care se face referire în mandatul dispus de judecător sau în autorizația emisă de procuror*". Legiuitorul

[1] *M. Udroiu*, Procedură penală, vol. I, 2019, p. 634.

[2] *Ibidem*.

[3] *A.-R. Trandafir*, Obținerea de informații și înscrisuri de la instituțiile de credit în cursul urmăririi penale, prelegere susținută în cadrul Conferinței privind aspecte de practică intervenite de la intrarea în vigoare a Noului Cod penal și Noului Cod de procedură penală, București, 9-10 octombrie 2017, organizată de Institutul Național al Magistraturii – *www.youtube.com*

a prevăzut în mod expres prin acest articol că orice instituție financiară solicitată va fi ținută să comunice datele și înscrisurile pe care le deține, nefiind opozabil secretul profesional sau secretul bancar[1]. Credem că această dispoziție legală era necesară, întrucât secretul bancar este aplicabil numai instituțiilor de credit, nu și celorlalte entități financiare, prin aceasta atrăgându-se atenția oricărei persoane solicitate că are această obligație potrivit legii. Totodată, dispoziția legală cu care trebuie întotdeauna să fie coroborată este cea cuprinsă în art. 306 alin. (6) C.pr.pen., în care se arată că „*secretul bancar și cel profesional, cu excepția secretului profesional al avocatului, nu sunt opozabile procurorului, după începerea urmăririi penale*".

În ceea ce privește termenul în care instituția solicitată trebuie să răspundă, legiuitorul nu prevede vreo lămurire, sub acest aspect reieșind că datele și înscrisurile solicitate trebuie transmise în cel mai scurt timp posibil pentru instituția financiară sau în ritmul indicat de procuror, în cazul tranzacțiilor viitoare. Într-o opinie s-a considerat că, pentru tranzacțiile financiare trecute, instituția solicitată trebuie să răspundă în termenul de valabilitate al mandatului, respectiv în cele 30 de zile, în cazul transmiterii acestora după expirarea termenului, proba trebuind să fie constatată ca fiind nelegal administrată și exclusă[2]. Nu putem fi de acord cu această susținere, întrucât nu are nicio importanță momentul în care instituțiile de credit transmit datele și înscrisurile solicitate de procuror și cuprinse în mandatul emis de judecătorul de drepturi și libertăți. Ceea ce se autorizează este obținerea de date privind tranzacțiile financiare trecute, termenul de 30 de zile fiind prevăzut de art. 146[1] alin. (2) C.pr.pen. doar pentru tranzacții financiare viitoare. Mai mult decât atât, sancțiunile procesuale se vor aplica numai în cazul actelor efectuate de participanți la procesul penal, nu și de alte persoane care intervin întâmplător. În consecință, chiar dacă informațiile și înscrisurile privind tranzacțiile financiare sunt transmise după expirarea duratei mandatului emis de judecătorul de drepturi și libertăți, ele vor rămâne valabil administrate, singura sancțiune care poate interveni fiind amendarea, după caz, a entității financiare solicitate, în conformitate cu dispozițiile art. 283 alin. (4) lit. o[1]) C.pr.pen.[3].

Secțiunea a 2-a. Informațiile și înscrisurile care pot fi transmise de entitățile financiare

După transmiterea mandatului emis de judecătorul de drepturi și libertăți, instituția de credit sau entitatea financiară solicitată va trebui să pună la dispoziția organelor de urmărire penală datele, informațiile și înscrisurile solicitate cu privire la tranzacțiile sau operațiunile financiare realizate de o persoană sau care urmează a fi realizate în perioada de valabilitate a mandatului.

Din punct de vedere istoric, primele persoane juridice care au adoptat tehnologii de calcul și tehnologii de transmitere la distanță a informațiilor scrise au fost entitățile financiare, în special bursele, pentru care comunicarea în timp real a valorii acțiunilor era esențială. Odată

[1] După cum am mai arătat în prezentul titlu, potrivit art. 114 din O.U.G. nr. 99/2006, instituțiile de credit sunt obligate să transmită datele și înscrisurile solicitate.

[2] *V. Trif*, op. cit., p. 259.

[3] Conform art. 283 alin. (4) lit. o1) C.pr.pen., va constitui abatere judiciară și se va sancționa cu amendă de la 500 lei la 5.000 lei: neîndeplinirea obligației prevăzute la art. 1461 alin. (7) C.pr.pen. de către instituțiile de credit sau entitățile financiare care efectuează tranzacțiile financiare.

cu dezvoltarea tehnologiei, viteza cu care se desfășurau tranzacțiile și numărul lor din ce în ce mai mare a impus automatizarea lor și, odată cu automatizarea, a impus nevoia stocării lor într-un alt format decât cel scris. În prezent, este greu de imaginat că o instituție de credit va ține registre scrise cu privire la tranzacțiile financiare ale unui client, tendința modernă fiind de a digitaliza toate informațiile și de a reduce consumul de hârtie la un minimum necesar, astfel că informațiile privind tranzacțiile financiare ale unei persoane se vor arhiva digital după ce au fost procesate de sistemele informatice ale entității financiare.

Avantajul care trebuie avut în vedere de organele de urmărire penală este că datele privind tranzacțiile financiare pot fi obținute facil de la entitățile financiare, putând fi transmise în câteva zile de primirea solicitării fie în format scris, fie în format digital. Pentru o entitate financiară, în special o bancă, oferirea de informații către organele de urmărire penală reprezintă o operațiune ușoară atunci când se solicită un extras de cont – un document generat automat de sistemul informatic pentru orice cont la momentul la care un operator emite o comandă în sistem. Simpla tipărire a acestor date este o operațiune materială care poate fi lăsată la latitudinea entității financiare solicitate, fiind acceptabilă transmiterea în format digital a informațiilor.

Pentru a profita de celeritatea maximă, organele de urmărire penală trebuie să înțeleagă că o bancă poate furniza cel mai repede date care sunt generate automat, însă, dacă se cer informații mai precise care nu pot fi extrase din sistemul informatic, răspunsul va putea fi dat după procesarea lor manuală. S-a arătat în doctrină că solicitarea unor rulaje ale conturilor[1], deși poate părea limitativă prin raportare la solicitarea extraselor de cont, va pune o bancă în imposibilitate de a răspunde cererii, întrucât va impune extragerea manuală doar a informației privind rulajul pe cont din extrasele de cont din sistemul informatic. Or, nu considerăm că o astfel de practică ar trebui să fie îngăduită, deoarece reprezintă un efort disproporțional al băncii față de solicitările organelor de urmărire penală. Dacă acestea doresc extragerea unei situații privind rulajele, apreciem că respectiva problemă va apărea în cadrul unor cauze mai complexe în care oricum se va impune efectuarea unei expertize care să aibă ca obiect respectivele tranzacții, astfel că problema rulajelor poate fi elucidată de expert.

În ceea ce privește înscrisurile care pot face obiectul măsurii de cercetare, acestea vor fi într-un număr mai redus, întrucât tranzacțiile financiare se desfășoară electronic, și nu considerăm că înscrisurile care stau la baza unei tranzacții financiare vor putea fi obținute prin această măsură, decât dacă ar conține elemente privind conținutul unei tranzacții financiare.

În continuare vom trata anumite categorii de informații și înscrisuri care pot fi transmise către organele de urmărire penală prin punerea în executare a măsurii speciale de cercetare.

a) Extrasele de cont;

Solicitarea transmiterii extraselor de cont este cea mai ușoară metodă de a obține informații privind tranzacțiile financiare trecute ale unei persoane, pe baza unor documente generate automat de sistemul informatic al entității financiare. Extrasele de cont trebuie să fie considerate informații, și nu înscrisuri în sensul art. 138 alin. (9) C.pr.pen., deoarece ele se emit din sistemul informatic al entității și pot fi transmise procurorului și în format digital (după cum se solicită)[2]. Extrasele de cont pot fi utile și atunci când măsura de cercetare nu se desfășoară în timp real, ci informațiile sunt transmise cu o anumite periodicitate (zilnic,

[1] *A.-R. Trandafir, G. Marin*, Obținerea de informații ori înscrisuri de la instituțiile de credit în cursul urmăririi penale, publicat pe *www.juridice.ro*

[2] *Ibidem*.

săptămânal etc.). Distincția făcută are importanță numai în situația în care extrasele de cont se solicită unei entități financiare; în cazul în care ele se solicită unei alte persoane – persoană vătămată, terț –, atunci vor avea valoarea unui înscris și vor putea fi obținute prin procedeele probatorii obișnuite, precum predarea de obiecte sau înscrisuri prevăzută de art. 170 C.pr.pen.[1].

Sub aspectul conținutului, s-a arătat în mod corect că extrasul de cont bancar oferă „*o imagine completă asupra tranzacțiilor desfășurate de client (nume/denumire titular, CUI/CNP, număr de identificare a titularului în sistemul informatic al băncii, număr de cont, sold, detalii privind fiecare tranzacție – sumă, dată, persoana cu care s-a desfășurat tranzacția, ce reprezintă respectivele sume, existența unor popriri/sume blocate etc., limită credit/overdraft, suma creditului neutilizată)*"[2]. Datele cuprinse în extrasul de cont au și un caracter continuu, deoarece, în funcție de intervalul pentru care s-a autorizat măsura, procurorul va putea vedea întreaga cronologie a tranzacțiilor din respectiva perioadă și, astfel, va putea stabili proveniența unor sume de bani aflate în prezent în contul unei persoane, virate la o dată anterioară, sau va putea dovedi, prin conținutul unei tranzacții, săvârșirea unei infracțiuni.

Alături de extrasele de cont bancar, trebuie să fie avute în vedere și extrasele de cont de la alte entități financiare – societăți de administrare a investițiilor, societăți de servicii de investiții financiare, depozitari de părți sociale etc. –, de unde se vor putea afla date privind numele titularului, datele sale de identificare, numărul de cont, numărul de unități de fond, acțiuni sau alte instrumente financiare, tipul acestora, la care fond de investiții sau societate pe acțiuni aparțin și momentul când acestea au fost cumpărare, vândute sau răscumpărate, după caz.

b) Obținerea în timp real a tranzacțiilor financiare ale unei persoane;

În funcție de circumstanțele cauzei, poate fi utilă organelor de urmărire penală aflarea în timp real a desfășurării tranzacțiilor financiare ale unei persoane, sens în care se impune ca procurorul, odată cu transmiterea mandatului (sau ordonanței de autorizare), să comunice acest aspect entității financiare solicitate, pentru a fi informat de îndată când se realizează o cerere de procesare a unei tranzacții.

Informarea în timp real a organelor de urmărire penală se mai realizează și atunci când sunt incidente situațiile reglementate prin Legea nr. 129/2019 și acestea sunt sesizate de Oficiul Național de Prevenire și Combatere a Spălării Banilor. În esență, în cazul unor tranzacții suspecte, entitățile raportoare prevăzute la art. 5 din Legea nr. 129/2019[3] au obligația de a notifica în cel mai scurt timp O.N.P.C.S.B., suspendând pentru 24 de ore procesarea tranzacției. La rândul său, O.N.P.C.S.B. va analiza tranzacția și, dacă va constata că există indicii cu privire la săvârșirea unei infracțiuni, va sesiza, potrivit art. 34 alin. (1) și (3) din Legea nr. 129/2019, după caz, P.I.C.C.J. (pentru infracțiuni de spălarea banilor și finanțarea terorismului) și alte organe de urmărire penală. Astfel, chiar și în absența unui mandat emis de judecătorul de drepturi și libertăți, există o monitorizare continuă a tranzacțiilor financiare realizată de entitățile raportoare.

---

[1] *Ibidem*.

[2] *Ibidem*.

[3] Alin. (3) al art. 9 din Legea nr. 129/2019 prevede că inclusiv avocații, notarii, executorii judecătorești și alte persoane care exercită profesii juridice liberale vor avea această obligație „numai în măsura în care nu sunt avute în vedere informațiile pe care acestea le primesc de la unul dintre clienții lor sau le obțin în legătură cu aceștia în cursul evaluării situației juridice a clientului în cadrul unor proceduri judiciare sau al îndeplinirii obligației de apărare sau de reprezentare a clientului în proceduri judiciare sau în legătură cu aceste proceduri, inclusiv de consiliere juridică privind inițierea sau evitarea procedurilor, indiferent dacă aceste informații sunt primite sau obținute înaintea procedurilor, în timpul acestora sau după acestea". În același sens, a se vedea CEDO, cauza *Michaud c. Franța*, Hotărârea din 6 martie 2013, §90-92.

c) Obținerea înscrisurilor referitoare la tranzacțiile sau operațiunile financiare ale unei persoane.

Alături de datele privind tranzacțiile financiare, prin metoda specială de cercetare a obținerii datelor privind tranzacțiile financiare ale unei persoane pot fi solicitate înscrisuri referitoare la tranzacțiile sau operațiunile financiare.

Vor avea această caracteristică înscrisurile care conțin elemente privind tranzacțiile financiare concrete realizate sau care vor fi realizate și care vor furniza informații cu privire la: existența operațiunii, procesarea acesteia, destinatarul sumei de bani (după caz), semnificația tranzacției financiare, condițiile prin care se realizează etc. S-a susținut că vor avea astfel de caracteristici următoarele înscrisuri: un contract de vânzare care a stat la baza unei tranzacții, o factură fiscală, borderouri de achiziție materiale, mandatul prin care o persoană a fost autorizată să efectueze o anumită plată, certificatul de moștenitor al persoanei care a retras sume de bani din contul persoanei decedate, un stat de plată a salariilor, un formular completat la ghișeul unei bănci pentru retragerea/depunerea de numerar ori formularul primit pentru schimbul valutar[1]. Menționăm că nu este obligatoriu ca unele exemple, precum un contract de vânzare sau o factură fiscală, nu este obligatoriu să fie în posesia băncii prin care s-a realizat tranzacția, putându-se face plăți doar în temeiul indicării ca justificare a respectivului contract sau a facturii.

Alături de cele amintite mai sus, s-a pus problema care dintre înscrisurile care stau la baza acordării unui credit pot fi considerate ca fiind supuse măsurii speciale de cercetare și care nu, putând fi solicitate de procuror în temeiul art. 170 C.pr.pen. S-a stabilit că dacă prin această formulare se urmărește obținerea numai a înscrisurilor care au fost prezentate de client pentru a solicita creditul[2], nu va fi necesară prezentarea unui mandat, întrucât aceste înscrisuri nu reflectă conținutul unei tranzacții financiare. O altă situație este cea în care se va solicita contractul de credit, înscris care conține tranzacțiile financiare negociate între instituția de credit și client, pentru obținerea lor fiind necesară obținerea unui mandat de la judecătorul de drepturi și libertăți.

Secțiunea a 3-a. Informarea persoanei supuse metodei speciale de cercetare

Odată cu încetarea duratei pentru care a fost încuviințată măsura de cercetare, procurorului îi va reveni obligația de a încunoștința fiecare subiect al mandatului cu privire la măsura care a fost luată. În conformitate cu art. 146[1] alin. (8) C.pr.pen., în termen de cel mult 10 zile de la efectuarea măsurii de cercetare, procurorul va realiza această informare în scris, indicând persoanelor că au dreptul de a lua la cunoștință de activitățile desfășurate.

Dată fiind natura unor tranzacții financiare, nu va fi afectată doar viața privată a persoanei față de care s-a dispus metoda specială de cercetare, ci și cea a persoanei cu care s-a desfășurat tranzacția. Deși în prezenta lucrare am pledat pentru necesitatea încunoștințării și a persoanelor care au fost afectate tangențial, în situația aceasta, apreciem că intruziunea cauzată

[1] *A.-R. Trandafir, G. Marin*, Obținerea de informații ori înscrisuri de la instituțiile de credit în cursul urmăririi penale, publicat pe *www.juridice.ro*; *M. Udroiu*, Procedură penală, vol. I, 2019, p. 626.

[2] *A.-R. Trandafir, G. Marin*, Obținerea de informații ori înscrisuri de la instituțiile de credit în cursul urmăririi penale, publicat pe *www.juridice.ro*

va fi minimă ca urmare a naturii măsurii obținerii datelor financiare ale unei persoane. Dacă, pentru persoana vizată, ingerința în viața privată poate fi deosebită, trebuie să ținem seama că această ingerință devine din ce în ce mai gravă pe măsură ce persoana vizată realizează diverse tranzacții financiare cu mai multe persoane, putându-se descoperi aspecte intime din viața acesteia. Pe de altă parte, partenerul său din fiecare tranzacție poate fi foarte variat și va fi, de regulă, un comerciant pentru care datele privind o tranzacție (vânzarea unui bun la o anumită dată și la un anumit preț) nu va avea o însemnătate deosebită.

Raportând art. 146[1] alin. (9) C.pr.pen. la art. 145 alin. (4) C.pr.pen., procurorul va putea să amâne motivat efectuarea informării persoanei numai în situația în care aceasta ar duce la perturbarea sau periclitarea bunei desfășurări a urmăririi penale în cauză. Această amânare are o durată maximă expusă de art. 145 alin. (5) C.pr.pen., respectiv până la terminarea urmăririi penale sau la clasarea cauzei.

Capitolul VIII
Obținerea datelor privind tranzacțiile financiare ale avocatului

O problemă particulară în punerea în executare a măsurii de cercetare este interdicția de a o aplica tranzacțiilor financiare dintre suspect, inculpat sau orice altă persoană vizată de măsură și avocatul acestora. Potrivit art. 146[1] alin. (6) C.pr.pen., este interzisă aplicarea metodei speciale asupra acestor tranzacții financiare, cu excepția situației în care avocatul săvârșește sau pregătește săvârșirea unei infracțiuni dintre cele prevăzute la art. 139 alin. (2) C.pr.pen. Această interdicție este identică celor prevăzute la alte metode speciale de supraveghere sau cercetare din Codul de procedură penală și subliniază gradul ridicat de protecție a secretului profesional al avocatului instituit de legiuitor.

Cu privire la protejarea secretului profesional al avocatului în cazul autorizării metodei speciale de cercetare a obținerii datelor privind tranzacțiile financiare ale unei persoane, apreciem că vor fi protejate tranzacțiile financiare ale clientului cu avocatul (clientul său fiind persoana supusă măsurii speciale de cercetare), dar mai ales tranzacțiile financiare realizate de avocat atât de pe conturile cabinetului (sau oricărei alte forme de exercitare a profesiei), cât și de pe conturile sale personale (în măsura în care au legătură cu activitatea profesională).

Mai înainte de a analiza aplicabilitatea acestei interdicții, trebuie să înțelegem ce a dorit să exprime legiuitorul prin calitatea de avocat în cadrul dispozițiilor art. 146[1] alin. (6) C.pr.pen. Potrivit art. 88 alin. (1) C.pr.pen., „*avocatul asistă sau reprezintă, în procesul penal, părțile ori subiecții procesuali principali, în condițiile legii*". O asemenea prevedere nu va fi completă, deoarece art. 146[1] C.pr.pen. permite aplicarea măsurii de cercetare și **altor persoane** care nu au nicio calitate în procesul penal, astfel că nu își pot angaja un avocat în cauza penală respectivă. Credem că, prin interdicția inserată în art. 146[1] alin. (6) C.pr.pen., prin „avocat al suspectului, inculpatului sau al unei alte persoane" vom înțelege avocatul care realizează asistarea sau reprezentarea persoanei în orice cauză pe care ar avea-o aceasta, nu numai procesul penal în cadrul căruia se dispune obținerea datelor privind tranzacțiile financiare ale unei persoane.

O consecință aparte a dispozițiilor amintite mai sus este că, și în contextul în care avocatul va fi singura persoană cercetată într-o cauză penală, nu va fi posibilă autorizarea obținerii datelor privind tranzacțiile sale financiare, decât dacă acuzația privește una dintre faptele prevăzute la art. 139 alin. (2) C.pr.pen., deci un standard mai ridicat decât cel prevăzut de lege la art. 146[1] alin. (1) lit. a) C.pr.pen. Explicația constă în faptul că viața privată a unui avocat este indisolubil legată de activitatea sa profesională, astfel că o autorizare asupra conturilor personale ale acestuia va constitui și o ingerință adusă secretului profesional dintre avocat și clienții săi.

Ținând seama de cele arătate mai sus, putem să imaginăm mai multe situații care pot fi incidente în cazul obținerii datelor privind tranzacțiile financiare ale avocatului: obținerea datelor privind tranzacțiile financiare ale avocatului atunci când acesta face obiectul urmăririi penale; obținerea accidentală a datelor privind tranzacțiile financiare ale avocatului; obținerea nelegală a datelor privind tranzacțiile financiare ale avocatului.

a) Obținerea datelor privind tranzacțiile financiare ale avocatului atunci când acesta face obiectul urmăririi penale;

Dacă procurorul va dori să obțină date privind tranzacțiile financiare ale avocatului persoanei cercetate în cauză, s-ar impune ca față de avocat să existe deja începută urmărirea

penală pentru una dintre infracțiunile prevăzute la art. 139 alin. (2) C.pr.pen. și ca acea infracțiune să aibă legătură cu cauza în care se dispune măsura de cercetare. Ca atare, avocatul va deveni una dintre persoanele față de care se ia măsura și se va impune ca judecătorul de drepturi și libertăți din cadrul instanței competente să se pronunțe asupra măsurii.

Pentru luarea măsurii față de avocat, este necesar ca judecătorul de drepturi și libertăți să analizeze dacă acuzațiile formulate de procuror cu privire la fapta cercetată în legătură cu activitatea avocatului au un caracter clar și dacă există suficiente temeiuri pentru a susține o asemenea acuzație. Această condiție nu rezultă din lege, însă, în cazul autorizării unei metode speciale de cercetare față de un avocat în legătură cu activitatea sa profesională desfășurată cu o persoană ce face obiectul urmăririi penale, este necesar un standard mai ridicat pentru a proteja de orice inferență arbitrată. În jurisprudența Curții Europene a Drepturilor Omului s-a constatat că cercetarea unor fapte vagi și neclare referitoare la implicarea avocatului în infracțiunile reținute în sarcina clientului său nu este suficientă pentru autorizarea unei asemenea măsuri[1].

O altă situație este atunci când, ulterior încuviințării metodei speciale de cercetare, se descoperă probe cu privire la infracțiunea care se pregătește a fi săvârșită de avocat sau care a fost săvârșită de acesta. În această situație, apreciem că, odată cunoscută calitatea de avocat a persoanei și existând suspiciuni privind pregătirea sau săvârșirea unei infracțiuni de către aceasta, va fi necesară reautorizarea măsurii față de avocat, după ce, în prealabil, se va începe urmărirea penală față de faptele acestea.

Cu toate că se poate dispune o asemenea măsură față de avocat, apreciem că, față de specificul metodei speciale de cercetare, tranzacțiile financiare care nu au legătură cu cauza vor fi protejate în continuare de secretul profesional, nefiind permisă păstrarea acestora la dosarul cauzei, fiindcă ar afecta relațiile corecte dintre avocat și restul clientelei sale. Simpla existență la dosarul cauzei a tranzacțiilor financiare ale avocatului cu persoane care nu fac obiectul urmăririi penale constituie o încălcare a vieții private a avocatului în sensul art. 8 Conv.EDO, întrucât dosarul cauzei poate fi consultat de orice parte și subiect procesual principal[2].

b) Obținerea accidentală a datelor privind tranzacțiile financiare ale avocatului;

În situația în care, în cursul punerii în executare a măsurii, procurorul descoperă că s-au realizat tranzacții financiare de către suspect, inculpat sau altă persoană față de care s-a luat măsura și avocatul acesteia, procurorul nu va avea dreptul să folosească probele obținute în procesul penal. Situația este posibilă atunci când o instituție de credit comunică extrasele de cont privind tranzacțiile unei persoane pe un interval mai lung de timp, putând fi incluse și tranzacțiile financiare ale clientului cu avocatul său. Aceasta ar constitui o obținere accidentală a datelor privind tranzacțiile financiare cu avocatul, care se vor regăsi, cel mai probabil, în extrasul de cont transmis în formă scrisă de instituția de credit. Nu va fi culpabil organul de urmărire penală care realizează acest act decât dacă va proceda la folosirea probei în procesul penal, fiind suficient ca datele privind tranzacția financiară cu avocatul să se afle la dosarul cauzei. Credem că trecerea metodei speciale între metodele de cercetare a afectat aplicabilitatea dispozițiilor art. 139 alin. (4) C.pr.pen., care stipulau obligația procurorului de a distruge toate rezultatele de supraveghere tehnică care au vizat relația dintre suspectul și inculpatul pe care îl apără. Totuși, ținând seama atât de necesitatea protejării secretului profesional al avocatului,

[1] CEDO, cauza *Sommer c. Germania*, Hotărârea din 27 iulie 2017, §61.
[2] *Ibidem*, §57.

cât și a dezlegărilor date în jurisprudența Curții Europene a Drepturilor Omului[1], se va impune ca procurorul să distrugă datele și informațiile care au avut în vedere relația dintre persoana care a fost subiectul metodei speciale de cercetare și avocatul său.

O particularitate constă în faptul că desfășurarea unor astfel de tranzacții se face, de regulă, prin conturile cabinetului de avocat, și nu prin conturile personale ale avocatului[2], astfel că, în extrasul de cont, se va evidenția că beneficiarul este un cabinet de avocat, și nu o persoană fizică, fiind greu de imaginat că un organ de urmărire penală nu va sesiza acest aspect. Cu toate acestea, va trebui să fie avută în vedere și explicația tranzacției financiare cu avocatul, neintrând sub protecția secretului profesional acele tranzacții financiare care nu au legătură cu activitatea profesională, ci sunt rezultate în urma altor convenții (de pildă, plata unei chirii de către cabinetul de avocat). Această particularitate este importantă, deoarece este posibil ca persoana supusă măsurii să nu aibă nicio calitate procesuală și nici avocatul să nu aibă o împuternicire avocațială depusă la dosarul cauzei, organul de urmărire penală neavând nicio altă posibilitate de a stabili relația dintre persoana vizată de metoda de cercetare și avocat, decât explicația tranzacției financiare.

În cazul în care s-a procedat în mod accidental la obținerea datelor privind tranzacțiile financiare ale suspectului, inculpatului sau unei alte persoane cu avocatul său, considerăm că se va impune și încunoștințarea avocatului. Vor intra sub incidența secretului profesional dintre client și avocat și tranzacțiile financiare realizate între aceștia (plata onorariului și a cheltuielilor), cu toate că legislația care reglementează organizarea și exercitarea profesiei de avocat nu a avut în vedere și această ipoteză[3].

Încunoștințarea avocatului, în cazul în care se obțin date privind tranzacțiile sale financiare cu un client care fac obiectul metodei speciale de cercetare, o apreciem ca fiind obligatorie, în conformitate cu art. 146[1] alin. (8) C.pr.pen., chiar dacă avocatul nu era un subiect al mandatului emis de judecătorul de drepturi și libertăți.

Legiuitorul nu a prevăzut o procedură specială pentru încunoștințarea avocatului în situația descrisă mai sus, fiind posibil ca încunoștințarea acestuia să fie amânată în conformitate cu art. 145 alin. (4) C.pr.pen., singurul temei al acestei amânări putând fi o eventuală *perturbare sau periclitare a bunei desfășurări a urmăririi penale în cauză*. Suntem ferm convinși că o asemenea situație nu poate reprezenta un impediment pentru desfășurarea urmăririi penale atât timp cât avocatului i se asigură inclusiv dreptul de a consulta dosarul cauzei.

c) Obținerea nelegală a datelor privind tranzacțiile financiare ale avocatului.

În nicio situație nu se poate dispune în mod voit obținerea datelor privind tranzacțiile financiare ale unui avocat în relația cu clientul său, o asemenea măsură fiind interzisă de lege, dar fără precizarea concretă a sancțiunii aplicabile, obligația încunoștințării avocatului sau posibilitatea de a contesta măsura de către avocat și de a obține distrugerea probelor obținute.

---

[1] CEDO, cauza *M.N. și alții c. San Marino*, Hotărârea din 7 octombrie 2015, §54; cauza *Sommer c. Germania,* Hotărârea din 27 iulie 2017, §7-8.

[2] Deși această posibilitate nu trebuie exclusă de organele de urmărire penală, după cum s-a putut constata la CEDO, cauza *Brito Ferrinho Bexiga Villa-Nova c. Portugalia*, Hotărârea din 1 decembrie 2015. Totuși, Curtea a constatat că secretul profesional va fi aplicabil și acestor conturi.

[3] Potrivit art. 34 alin. (3) din Legea nr. 51/1995 privind organizarea și exercitarea profesiei de avocat, „nu vor putea fi ascultate și înregistrate, cu niciun fel de mijloace tehnice, convorbirile telefonice ale avocatului și nici nu va putea fi interceptată și înregistrată corespondența sa cu caracter profesional, decât în condițiile și cu procedura prevăzute de lege". Textul de lege nu este actualizat încât să privească toate metodele speciale de supraveghere sau cercetare.

În prezent, stadiul legislației este deficitar, impunându-se completarea acesteia de legiuitor pentru a conferi o mai bună protecție a secretului profesional al avocatului.

În jurisprudența Curții Europene a Drepturilor Omului au fost identificate mai multe situații în care s-a constatat încălcarea secretului profesional al avocatului ca urmare a întrebuințării procedeelor probatorii similare cu obținerea datelor privind tranzacțiile financiare ale unei persoane, remarcându-se cauzele *Michaud c. Franța*[1], *M.N. și alții c. San Marino*[2], *Brito Ferrinho Bexiga Villa-Nova c. Portugalia*[3] și *Sommer c. Germania*[4].

O astfel de situație a fost analizată de către Curtea Europeană a Drepturilor Omului în cauza *Sommer c. Germania*, la care am făcut deja referiri, aceasta reprezentând cel mai clar exemplu de imixtiune nelegală al organelor de urmărire penală în derularea relației dintre client și avocat prin obținerea datelor privind tranzacțiile financiare ale avocatului, ceea ce impune analizarea acestui caz în prezenta secțiune.

În cauză se reține că domnul avocat Ulrich Sommer a apărat într-o cauză penală un client care, la finalul procesului penal, a fost condamnat la o pedeapsă privativă de libertate și încarcerat, astfel că plata unei părți din onorariul domnului avocat s-a realizat de către logodnica clientului prin intermediul unei operațiuni financiare din a cărei explicație rezulta că plata reprezenta onorariul avocațial pentru respectivul client. La ceva timp după aceasta, un procuror care efectua urmărirea penală pentru infracțiuni de criminalitate organizată și față de clientul domnului avocat Sommer a obținut date privind tranzacțiile financiare desfășurate de fostul client și de logodnica sa, în care a descoperit că logodnica primise de la fostul client o sumă de bani suspectată ca provenind de pe urma săvârșirii de infracțiuni. O parte din această sumă de bani a fost transferată în contul domnului avocat Sommer cu titlu de onorariu. Văzând această tranzacție, procurorul a solicitat băncii avocatului comunicarea tuturor datelor privind tranzacțiile financiare ale acestuia pentru o perioadă de aproximativ 2 ani, cerând ca avocatul să nu fie încunoștințat de cele întâmplate. La aproximativ un an de la aceasta, avocatul Sommer, care își reprezenta fostul client și în noua cauză penală, a obținut admiterea cererii sale de a consulta dosarul, descoperind că la dosarul cauzei se aflau date privind 53 de tranzacții desfășurate de acesta cu alți clienți, apreciate de procuror ca fiind suspecte. Întrucât procurorul a considerat că acestea reprezintă probe, datele privind tranzacțiile financiare se aflau la dosarul de urmărire penală și puteau fi consultate de toate părțile. Deși domnul avocat Sommer a încercat să obțină distrugerea acestora atât prin cereri adresate procurorului, cât și instanței, a reușit să obțină doar ca aceste tranzacții să nu poată fi văzute de ceilalți participanți decât cu încuviințarea prealabilă a instanței. Domnul avocat nu a fost niciodată pus sub acuzare pentru săvârșirea vreunei fapte penale.

În cauza arătată mai sus se observă mai multe probleme pe care le vom aborda în cele ce urmează.

În primul rând, apreciem că organele de urmărire penală nu puteau considera că avocatul ar fi făcut parte dintr-o grupare de criminalitate organizată doar ca urmare a faptului că ar fi fost plătit din sume suspectate ca provenind din activități ilegale. Simpla proveniență a sumelor din surse nelegale nu poate constitui un temei pentru a bănui un avocat de săvârșirea unei infracțiuni.

[1] CEDO, cauza *Michaud c. Franța*, Hotărârea din 6 martie 2013, pe *hudoc.echr.coe.int*

[2] CEDO, cauza *M.N. și alții c. San Marino*, Hotărârea din 7 octombrie 2015, pe *hudoc.echr.coe.int*

[3] CEDO, cauza *Brito Ferrinho Bexiga Villa-Nova c. Portugalia*, Hotărârea din 1 martie 2016, pe *hudoc.echr.coe.int*

[4] CEDO, cauza *Sommer c. Germania*, Hotărârea din 27 iulie 2017, pe *hudoc.echr.coe.int*

În al doilea rând, a fost nelegală solicitarea procurorului de a obține date privind tranzacțiile financiare ale avocatului pentru o durată de peste doi ani, pornind de la o singură plată făcută în numele unui client. Astfel cum a reținut și Curtea, acuzațiile la care făcea referire procurorul, care nu s-au formalizat niciodată, nu erau decât vagi și nu puteau fi încadrate într-o infracțiune anume[1]. Spre deosebire de Codul de procedură penală român, nu exista obligația începerii urmăririi penale față de fapta avocatului, condiție care rezultă implicit din dispozițiile art. 139 alin. (2) C.pr.pen.

În al treilea rând, măsura dispusă față de avocat s-a făcut printr-o simplă solicitare din partea procurorului, fără ca măsura să fie autorizată de o instanță[2]. O atare situație nu poate fi incidentă în legislația română, întrucât măsura se va dispune de către judecătorul de drepturi și libertăți, și doar în mod excepțional de către procuror.

În al patrulea rând, Curtea a constatat că atât lipsa posibilității legale de a-l încunoștința pe avocat despre măsura la care a fost supus, cât și solicitarea procurorului față de bancă de a nu divulga clientului său transmiterea datelor privind tranzacțiile financiare au influențat aptitudinea sa de a ataca măsura[3]. Curtea amintește că eficacitatea unui recurs în fața unei instanțe asupra măsurii dispuse este în mod obligatoriu legată de obligația organelor judiciare de a informa persoana despre măsura la care a fost supusă. În această privință, observăm că avocatul nu a fost încunoștințat nici de prima tranzacție, descoperită accidental, și nici de cele 53 care au fost obținute ulterior. Sub acest aspect, credem că legea română este la fel de deficitară, impunându-se încunoștințarea avocatului în situația în care organele de urmărire penală descoperă conținutul tranzacțiilor sale financiare cu un client.

În al cincilea rând, în cauză s-a constatat lipsa unor măsuri efective prin care să fie înlăturată ingerința la viață privată realizată prin folosirea ca probe a tranzacțiilor financiare ale avocatului. Legea română se află într-o situație similară, întrucât în cuprinsul art. 146[1] C.pr.pen. nu se reglementează o procedură similară cu cea din cadrul supravegherii tehnice de distrugere a oricăror probe obținute ca urmare a relației dintre client și avocat.

Ținând seama de cele expuse mai sus, apreciem că, în cazul lacunelor legislative evidențiate mai sus, se impune ca organele de urmărire penală să dea efect jurisprudenței Curții Europene a Drepturilor Omului până la o reglementare corectă a ipotezelor arătate. *De lege ferenda*, se impune ca probele obținute privind tranzacțiile financiare ale unei persoane cu avocatul său să fie excluse din procesul penal, rezultatul metodei de cercetare să fie distrus de către procuror și avocatul să fie încunoștințat de această măsură. În plus, se impune reglementarea unei proceduri unitare de contestare a legalității măsurilor de cercetare de către orice persoană care a făcut obiectul acestora, chiar dacă nu a avut calitatea de suspect sau inculpat în cauză.

[1] *Ibidem*, §61.
[2] *Ibidem*, §62.
[3] *Ibidem*.

Capitolul IX
Concluzii

Obținerea datelor privind tranzacțiile financiare ale unei persoane constituie o metodă specială de cercetare utilă în descoperirea și probarea unor infracțiuni, putând să conducă la obținerea de probe în procesul penal, inclusiv probe directe, prin raportare la specificul infracțiunii. Prin intermediul ei, organele de urmărire pot cunoaște conținutul tranzacțiilor financiare ale unei persoane, putând obține și înscrisuri care au stat la baza realizării lor, sub rezerva că acestea trebuie să conțină aspecte privind însăși tranzacția. Dacă organele de urmărire penală vor dori să afle doar situația financiară a unei persoane, vor putea recurge la o altă metodă specială, obținerea de date privind situația financiară a unei persoane, care va constitui o ingerință mai mică adusă vieții private a unei persoane.

Deși metoda este considerată una de cercetare, ea prezintă caracteristici care o apropie foarte mult de supravegherea tehnică. Cu toate acestea, o diferență notabilă o reprezintă posibilitatea aflării conținutului tranzacțiilor trecute ale unei persoane.

Întrucât Codul de procedură penală nu definește termenii de „instituție de credit" și „entitate financiară", pentru înțelegerea măsurii, va fi necesar să ne raportăm la legislația europeană și națională în domeniul financiar, unde lesne pot fi identificate persoanele care pot comunica datele solicitate.

Autorizarea măsurii se va face de către judecătorul de drepturi și libertăți, la propunerea procurorului, trebuind să fie analizată măsura prin raportare la toate condițiile legale, în special cea a proporționalității. Sub acest aspect, este de preferat ca judecătorul de drepturi și libertăți să fie exigent în a determina perioada din trecut pentru care se vor obține date privind tranzacțiile financiare.

Un minus al legislației actuale este posibilitatea ca procurorul să autorizeze provizoriu metoda specială de cercetare, aspect pe care îl considerăm vătămător pentru viața privată a unei persoane, date fiind particularitățile măsurii, dar și posibilitatea teoretică a aflării tranzacțiilor financiare trecute ca urmare a acestei autorizări provizorii.

Pentru punerea în executare a mandatului judecătorului de drepturi și libertăți, acesta va trebui să fie trimis entității financiare solicitate, care va transmite datele și înscrisurile solicitate.

În ultimul rând, metoda specială de cercetare prezintă grave lacune privind autorizarea ei față de avocat, mai ales în contextul în care tranzacțiile financiare ale persoanei cercetate le pot include și pe cele desfășurate cu avocatul său, acestea fiind protejate de secretul profesional al avocatului. Legiuitorul va trebui să găsească un mecanism prin care să excludă obligatoriu tranzacțiile efectuate cu avocatul și să instituie obligația încunoștințării acestuia despre măsură, chiar și atunci când acesta l-a vizat doar incidental.

Titlul IX
Obținerea de date privind situația financiară a unei persoane

Capitolul I
Aspecte generale

Secțiunea 1. Utilitatea reglementării metodei speciale de cercetare a obținerii de date privind situația financiară a unei persoane

Printre metodele speciale de cercetare prevăzute de legiuitor pentru cercetarea aspectelor financiare din viața unei persoane, regăsim și obținerea de date privind situația financiară a unei persoane prevăzută de art. 153 C.pr.pen.

În opinia noastră, este cea mai ușor de înțeles măsură dintre metodele speciale de cercetare și supraveghere și cea care produce cea mai mică ingerință în viața privată a unei persoane. Simplitatea ei constă în faptul că metoda specială nu cunoaște o procedură specifică de autorizare, prevede condiții largi pentru întrebuințarea ei și, odată cunoscută metoda similară a obținerii datelor privind tranzacțiile financiare ale unei persoane, se poate facil determina locul și scopul ei în legislația procesuală penală.

Obiectul măsurii speciale de cercetare este de a reglementa un procedeu probatoriu privind situația financiară a unei persoane prin care să se înlăture, dincolo de orice dubiu, obligația unor entități financiare de a transmite procurorului date financiare ce ar constitui secret bancar sau, după caz, secret profesional. Altfel, metoda specială pare a fi înrudită cu predarea obiectelor, înscrisurilor și a datelor informatice prevăzută de art. 170 C.pr.pen. Totodată, măsura este utilă pentru a contrabalansa metoda specială a obținerii datelor privind tranzacțiile financiare ale unei persoane, oferind procurorului o metodă specială mai puțin intruzivă prin care să realizeze probațiunea în cauză[1]. În consecință, măsura va avea o cuprindere limitată, putând fi obținute probe cu privire la o arie restrânsă de împrejurări.

Întrebuințarea metodei speciale de cercetare poate să își găsească utilitatea în mai multe situații – de la dovedirea situației financiare a unei persoane în prezent sau la un moment determinat din trecut, în vederea dovedirii unor împrejurări necesare pentru justa soluționare a cauzei, sau până la cunoașterea situației prezente a unei persoane, în vederea luării unei măsuri asigurătorii față de patrimoniul acesteia.

Prin folosirea metodei speciale de cercetare, procurorul poate obține probe cu privire la *existența conturilor* și *conținutul conturilor unei persoane*. Nu pot fi solicitate înscrisuri în legătură cu aceste conturi ori cu tranzacțiile efectuate, pentru aceasta fiind nevoie de emiterea unei ordonanțe de predare de înscrisuri, potrivit art. 170 C.pr.pen., sau autorizarea

[1] *G.C. Militaru*, Considerații asupra mandatului de supraveghere tehnică privind obținerea datelor referitoare la tranzacțiile financiare ale unei persoane și analiza comparativă cu instituția obținerii de date privind situația financiară a unei persoane, în Dreptul nr. 9/2016, p. 123.

obținerii datelor privind tranzacțiile financiare ale unei persoane, prevăzută de art. 138 alin. (9) C.pr.pen.[1].

Prin „existența conturilor", legiuitorul a avut în vedere ipoteza în care în cursul urmăririi penale nu se cunosc entitățile financiare la care un inculpat ar deține conturi, impunându-se verificarea instituțiilor unde s-ar bănui că persoana ar deține conturi. Prin „conturi" nu vom înțelege numai conturile la o instituție de credit, ci conturi deschise la orice entitate financiară, indiferent ce natură ar avea acestea (cont de investiții, cont de acțiuni etc.)[2]. În sensul legii, pentru relevarea existenței conturilor, va trebui să se indice și dacă acestea sunt deschise sau închise. Apreciem că, pentru informarea completă a procurorului, entitatea financiară va trebui să transmită implicit și data la care s-a deschis contul și, după caz, data la care acesta a fost închis.

Această metodă specială de cercetare va putea fi aplicată singură sau împreună cu orice alt procedeu probatoriu, astfel că nu putem fi de acord cu opinia că s-ar impune folosirea ei în mod obligatoriu atunci când nu se cunosc conturile unei persoane[3] și se dorește obținerea datelor privind tranzacțiile financiare ale unei persoane.

În doctrină s-a arătat că s-ar putea face o distincție teoretică între situația în care procurorul ar solicita identitatea împuternicitului de pe contul unei anumite persoane, situație care nu ar cădea sub incidența art. 153 C.pr.pen., și situația în care s-ar solicita informații cu privire la conturile pe care o anumită persoană este împuternicită, caz în care s-ar impune utilizarea metodei speciale prevăzute de art. 153 C.pr.pen.[4].

Prin „conținutul conturilor" vom înțelege suma de bani – exprimată în moneda în care este deschis contul – sau instrumentele financiare – unități de fond, acțiuni, instrumente derivate – care se află în contul persoanei pentru care se solicită date. Această situație va trebui să fie comunicată procurorului fără a divulga tranzacțiile financiare care au condus la formarea respectivului sold al contului, întrucât ar impune autorizarea judecătorului de drepturi și libertăți, în conformitate cu art. 146[1] C.pr.pen. Cu alte cuvinte, nu se va putea solicita extrasul de cont[5]. În același timp, metoda specială nu se va putea folosi pentru a afla rulajul contului, cel mai des organele de urmărire penală folosind termenul în mod impropriu pentru a se referi la informații care vor rezulta din extrasul de cont, astfel că nici aceste informații nu vor putea fi transmise în absența prezentării mandatului judecătorului de drepturi și libertăți obținut în urma parcurgerii procedurii prevăzute de art. 146[1] C.pr.pen.

Fiind o măsură specială de cercetare, aceasta va putea fi întrebuințată numai în cursul urmăririi penale, neputând fi dispusă de instanță în faza de judecată. Instanța, într-o asemenea situație, își va întemeia fundamentarea unei cereri către instituția de credit pe dispozițiile art. 113 alin. (2) lit. e) din O.U.G. nr. 99/2006[6].

---

[1] *A. Crișu*, Drept procesual penal. Partea generală (conform noului Cod de procedură penală), ed. a 3-a, revizuită și actualizată, Ed. Hamangiu, București, 2018, p. 387.

[2] *V. supra*, Titlul VIII, Capitolul III.

[3] *V. Trif*, op. cit., p. 253.

[4] *A.-R. Trandafir, G. Marin*, Obținerea de informații ori înscrisuri de la instituțiile de credit în cursul urmăririi penale, publicat pe *www.juridice.ro*

[5] *M. Udroiu*, Procedură penală, vol. I, 2019, p. 634.

[6] Conform art. 113 alin. (2) lit. e) din O.U.G. nr. 99/2006: „Informații de natura secretului bancar pot fi furnizate, în măsura în care acestea sunt justificate de scopul pentru care sunt cerute ori furnizate, în următoarele situații: (...) e) la solicitarea instanței, în scopul soluționării diferitelor cauze deduse judecății (...)".

Distinct față de alte metode speciale de supraveghere sau cercetare, obținerea de date privind situația financiară a unei persoane poate viza numai situații trecute sau, cel mult, situația financiară curentă a unei persoane, măsura neputându-se dispune pentru viitor. Totodată, probele care vor rezulta vor reflecta o stare de fapt statică, și nu o dinamică cronologică a situației financiare a unei persoane.

Secțiunea a 2-a. Introducerea obținerii de date privind situația financiară a unei persoane prin Legea de punere în aplicare a Codului de procedură penală

Spre deosebire de metoda specială de cercetare a obținerii datelor privind tranzacțiile financiare ale unei persoane, această metodă de cercetare nu era reglementată distinct în Codul de procedură penală anterior și nici în legislația specială, pentru obținerea probelor privind situația financiară a unei persoane folosindu-se procedeele probatorii obișnuite. Chiar și la momentul adoptării Legii nr. 135/2010 privind Codul de procedură penală, metoda specială de cercetare nu se regăsea prevăzută distinct, întrucât făcea parte din metoda specială de cercetare a „*solicitării și obținerii, potrivit legii, a datelor referitoare la tranzacțiile financiare, precum și a datelor financiare ale unei persoane*", prevăzută de art. 138 alin. (1) lit. g) din Codul de procedură penală (formă adoptată care nu a intrat în vigoare niciodată).

Prin Legea nr. 255/2013 pentru punerea în aplicare a Legii nr. 135/2010 privind Codul de procedură penală și pentru modificarea și completarea unor acte normative care cuprind dispoziții procesual penale s-a încercat o delimitare între cele două metode speciale de cercetare pe care le cunoaștem în prezent, metoda de cercetare anterior prevăzută la art. 153 C.pr.pen. fiind înlocuită cu obținerea de date privind situația financiară a unei persoane.

În forma sa inițială, metoda specială de cercetare a produs confuzii în practică, deoarece nu se făcea o distincție suficientă între ea și măsura de supraveghere tehnică (la acel moment) a obținerii datelor privind tranzacțiile financiare ale unei persoane. Motivul care a generat această confuzie a fost reglementarea încuviințării prealabile a judecătorului de drepturi și libertăți în cazul obținerii de date privind situația financiară a unei persoane, fără a se detalia distinct, ori făcea trimitere la o procedură de autorizare.

Inițial, textul art. 153 alin. (1) C.pr.pen. era următorul: „*procurorul poate solicita, cu încuviințarea prealabilă a judecătorului de drepturi și libertăți, unei instituții de credit sau oricărei alte instituții care deține date privind situația financiară a unei persoane comunicarea datelor privind existența și conținutul conturilor și a altor situații financiare ale unei persoane în cazul în care există indicii temeinice cu privire la săvârșirea unei infracțiuni și există temeiuri pentru a se crede că datele solicitate constituie probe*". Trebuie remarcat și faptul că exprimarea era confuză, deoarece se face referire la existența conturilor și a altor situații financiare, fără să se indice expres că se va obține și conținutul conturilor unei persoane.

Ceea ce a contribuit la dificultatea în aplicarea acestei metode speciale de cercetare a fost că, în cuprinsul art. 153 alin. (2) C.pr.pen. (care a rămas nemodificat), se arăta că măsura urma să se dispună din oficiu sau la cererea organului de cercetare penală prin **ordonanță**, ceea ce contravenea cu cele arătate mai sus, din care reiese că măsura se va autoriza de judecătorul de drepturi și libertăți.

Întrucât metoda specială era inaplicabilă în forma sa de la momentul intrării în vigoare a Codului de procedură penală, prin O.U.G. nr. 18/2016, legiuitorul delegat a procedat la modificarea conținutului art. 153 alin. (1) C.pr.pen., ajungându-se la forma în vigoare a metodei speciale de cercetare.

Forma în vigoare a art. 153 alin. (1) C.pr.pen. este: „*procurorul poate solicita unei instituții de credit sau oricărei altei instituții care deține date privind situația financiară a unei persoane comunicarea datelor privind existența și conținutul conturilor unei persoane, în cazul în care există indicii temeinice cu privire la săvârșirea unei infracțiuni și există temeiuri pentru a se crede că datele solicitate constituie probe*". Remarcăm că, prin forma actuală, competența de a dispune întrebuințarea acestui procedeu probatoriu aparține procurorului și că măsura va fi limitată numai la existența și conținutul conturilor unei persoane (soldul conturilor).

Capitolul II
Procedura autorizării obținerii de date privind situația financiară a unei persoane

Procedura de autorizare a metodei speciale de cercetare este una simplificată, fiind comună cu efectuarea oricărui act de administrare a unei probe în procesul penal, cu anumite particularități pe care le vom trata în prezenta secțiune.

Încă de la început trebuie subliniat faptul că această măsură este necesar să aibă în vedere interesul particular – reprezentat de secretul situației financiare – ca un element ce ține de viața privată a unei persoane și nevoia asigurării unei eficiente represiuni a săvârșirii infracțiunilor. Legiuitorul s-a concentrat mai mult pe latura represivă, permițând procurorului să obțină în mod facil informații privind situația financiară a unei persoane, dând prilej unor abuzuri. Trebuie avut în vedere că persoana față de care se dispune măsura nu trebuie să fie bănuită că ar fi săvârșit vreo infracțiune, dându-se prilej procurorului să verifice averea unei persoane, într-un mod similar comisiilor controlului provenienței bunurilor care funcționau înainte de evenimentele din decembrie 1989[1].

Pentru a se putea dispune metoda specială de cercetare, este necesar a fi îndeplinite câteva condiții legale, mult mai puține față de cele prevăzute în cazul supravegherii tehnice.

Prima condiție de autorizare constă în existența unei urmăriri penale începute, întrucât metoda specială de cercetare reprezintă un procedeu probatoriu, astfel că nu poate fi administrat fără existența cadrului procesual creat prin începerea urmăririi penale față de o faptă, în conformitate cu art. 305 alin. (1) C.pr.pen.

A doua condiție constă în împrejurarea că există indicii temeinice cu privire la săvârșirea unei infracțiuni, astfel că urmărirea penală trebuie să aibă ca obiect orice faptă prevăzută de legea penală. Această condiție nu are o existență proprie în realitate, însă o menționăm pentru a releva faptul că legiuitorul nu a dorit limitarea procedeului probatoriu la o anumită categorie de infracțiuni, apreciind că restrângerea dreptului la viață privată este una minoră.

Observăm că lipsesc condițiile legale privind *necesitatea și proporționalitatea probelor*, dar și al caracterului *subsidiar*. Acest lucru semnifică faptul că procurorul are posibilitatea de a dispune măsura fără a aprecia dacă măsura va fi proporțională cu restrângerea dreptului la viață privată al persoanei, legiuitorul prezumând deja că această ingerință va fi una proporțională față de interesul public al aflării adevărului. O atare situație este problematică, deoarece orice ingerință în viața privată a unei persoane necesită îndeplinirea condiției proporționalității, sens în care textul legal se află în contradicție cu art. 8 Conv.EDO. De pildă, într-o cauză care are ca obiect o infracțiune economică, obținerea situației financiare a suspectului sau chiar a persoanei bănuite sau la care se face referire prin actul de sesizare a organelor de urmărire

[1] Legea nr. 18 din 24 iunie 1968 privind controlul provenienței unor bunuri ale persoanelor fizice, care nu au fost dobândite în mod licit (B. Of. nr. 81 din 24 iunie 1968). În esență, fie la sesizarea unui particular, a conducerii organizațiilor socialiste, fie la sesizarea unor organe financiare, de urmărire penală sau a instanței, se desfășura o procedură a verificării caracterului nejustificat al averii în fața unei comisii formate din doi judecători și un procuror, care putea decide asupra trimiterii în judecată a unei persoane care deține bunuri pentru care nu poate justifica proveniența. Scopul era impozitarea bunurilor dobândite în mod nejustificat cu 80%, dar putea conduce la desfășurarea unei urmăriri penale dacă averea era dobândită ilicit.

penală poate fi apreciată ca fiind proporțională, însă nu va mai fi dacă măsura se extinde și asupra rudelor sau prietenilor acestuia.

Subsidiaritatea este o condiție care lipsește, permițând procurorului ca, pentru obținerea situației financiare a unei persoane, să aibă în vedere metoda specială de cercetare prevăzută de art. 153 C.pr.pen. ca primă măsură care poate fi luată pentru administrarea probei. Suntem de acord că un criteriu al subsidiarității ar fi unul ciudat în prezenta situație, întrucât prin metoda de cercetare este cel mai facil și complet mod de a obține situația financiară a unei persoane, dar și cel mai puțin intruziv mijloc (de pildă, prin raportare la obținerea datelor privind tranzacțiile financiare ale unei persoane ori percheziția domiciliară).

Competența de autorizare a metodei speciale de cercetare revine procurorului, în conformitate cu art. 153 alin. (1) C.pr.pen., fiind exclusă posibilitatea ca aceasta să fie dispusă de un organ de cercetare penală. Prin aceasta diferă de administrarea altor probe în cursul urmăririi penale care, în funcție de competența materială și personală, ar putea fi administrate la dispoziția organului de cercetare penală. Motivul pentru care numai procurorul poate dispune, dincolo de faptul că, în cazul metodelor speciale de supraveghere sau cercetare, organele de cercetare penală nu au niciodată putere de autorizare, este că, prin obținerea de date privind situația financiară a unei persoane, se va înfrânge secretul bancar și, după caz, secretul profesional al unei instituții de credit sau al unei alte entități financiare. Astfel, dispozițiile art. 153 C.pr.pen. se coroborează cu dispozițiile art. 306 alin. (6) C.pr.pen.[1] și cu dispozițiile art. 114 din O.U.G. nr. 99/2006[2]. Întrucât toate dispozițiile mai sus arătate se referă doar la procuror, și nu la organe de urmărire penală, apreciem că nu se va putea dispune nici delegarea organelor de cercetare penală să dispună asupra obținerii de date privind situația financiară a unei persoane. În plus, observăm că situația în care un organ de cercetare penală constată necesitatea administrării probei prin acest procedeu probatoriu, conform art. 153 alin. (2) C.pr.pen., acesta trebuie să formuleze procurorului o propunere în acest sens. Menționăm că textul legal face referire la *cererea organului de cercetare penală*, însă expresia este folosită impropriu, întrucât organul de cercetare penală va face propuneri procurorului, nu va adresa cereri, astfel cum rezultă din art. 306 alin. (5) C.pr.pen.[3].

Actul prin care se va dispune administrarea probei prin metoda specială de cercetare este *ordonanța procurorului*, care va conține, în mod obligatoriu, mențiunile cuprinse la art. 286 alin. (2) C.pr.pen. Alături de acestea, potrivit art. 153 alin. (2) C.pr.pen., se impune ca ordonanța să cuprindă instituția care este în posesia datelor sau care are sub control datele, numele suspectului sau inculpatului, motivarea îndeplinirii condițiilor prevăzute la art. 153 alin. (1) C.pr.pen., menționarea obligației instituției de a comunica imediat, în condiții de confidențialitate, datele solicitate.

---

[1] Potrivit art. 306 alin. (6) C.pr.pen., „secretul bancar și cel profesional, cu excepția secretului profesional al avocatului, nu sunt opozabile **procurorului**, după începerea urmăririi penale" (s.n.).

[2] Conform art. 114 din O.U.G. nr. 99/2006: „Instituțiile de credit sunt obligate să furnizeze **procurorului** sau instanței de judecată, la solicitarea acestora, informații de natura secretului bancar, dispozițiile privind metodele speciale de supraveghere sau cercetare din Codul de procedură penală aplicându-se în mod corespunzător" (s.n.).

[3] Potrivit art. 306 alin. (5) C.pr.pen., „când organul de cercetare penală apreciază că este necesară administrarea unor mijloace de probă sau folosirea unor metode speciale de supraveghere, care pot fi autorizate ori dispuse, în faza de urmărire penală, numai de procuror sau, după caz, de judecătorul de drepturi și libertăți, **formulează propuneri motivate**, care trebuie să cuprindă datele și informațiile care sunt obligatorii în cadrul acelei proceduri. Referatul este trimis procurorului împreună cu dosarul cauzei" (s.n.).

Instituția care este în posesia datelor sau care are sub control datele este necesară pentru ca ordonanța să justifice obligarea respectivei instituții să transmită datele; fără această mențiune, apreciem că ordonanța nu va fi suficient de clară. Nimic nu îl împiedică pe procuror să emită o ordonanță față de mai multe entități financiare ori să emită pentru fiecare entitate financiară în parte câte o ordonanță.

Numele suspectului sau inculpatului reprezintă un element care ridică anumite probleme. Dincolo de faptul că art. 286 alin. (2) lit. c) C.pr.pen. cuprinde deja această mențiune, există o neconcordanță între dispozițiile art. 153 alin. (1) C.pr.pen. și art. 153 alin. (2) C.pr.pen., întrucât cea din urmă dispoziție pare a restrânge măsura numai la suspect sau inculpat, contrar primei care o face aplicabilă oricărei persoane. Apreciem că legiuitorul a dovedit lipsă de claritate în limbaj, sensul real al mențiunii respective fiind de a se indica entității financiare *persoana față de care s-a luat măsura și pentru care trebuie să comunice situația financiară*. Sub acest aspect, credem că legiuitorul a dorit înlocuirea mențiunii cuprinse de art. 286 alin. (2) lit. c) C.pr.pen. cu cea din art. 153 alin. (2) C.pr.pen. Considerăm că nu va prezenta utilitate pentru entitatea financiară calitatea procesuală a persoanei, putând fi dăunătoare acesteia mențiunea calității în viitoarele sale relații cu o bancă, de pildă[1]. În plus, trebuie avut în vedere că urmărirea penală are caracter nepublic și că ordonanța de autorizare nu este transmisă entității financiare spre analiză, ci pentru punere în aplicare. Similar în acest sens, mandatul judecătorului de drepturi și libertăți (în cazul supravegherii tehnice ori al unor metode speciale de cercetare) nu va cuprinde elemente care să divulge aspecte privind urmărirea penală și se emite pentru a fi pus în executare.

Motivarea îndeplinirii condițiilor prevăzute la art. 153 alin. (1) C.pr.pen. reprezintă o condiție care nu este suplimentară, fiind prevăzută în mod inutil de lege în cazul dispunerii metodei speciale de cercetare, întrucât, potrivit art. 286 alin. (2) lit. d) C.pr.pen., ordonanța procurorului trebuie să cuprindă motivele de fapt și de drept pentru emiterea actului. Ținând seama că metoda specială de cercetare se emite în aceleași condiții ca orice ordonanță de administrare a unei probe, nu se impunea ca legiuitorul să menționeze că trebuie motivată îndeplinirea condițiilor prevăzute de art. 153 alin. (1) C.pr.pen.

Menționarea obligației instituției de a comunica imediat, în condiții de confidențialitate, datele solicitate o apreciem ca fiind utilă, întrucât obligă procurorul să încunoștințeze entitatea financiară că are obligația cuprinsă în art. 153 alin. (3) C.pr.pen. Ceea ce suscită un interes este mențiunea privind transmiterea datelor în condiții de confidențialitate, fapt care este aparent inutil în condițiile în care entitățile financiare sunt obligate prin secretul bancar sau prin secretul profesional să nu divulge date cu privire la clienții lor. În realitate, mențiunea nu se referă la aceasta, ci la obligația entității financiare de a se asigura de confidențialitatea măsurii față de client, fiindu-i interzisă comunicarea către client a împrejurării că procurorul a dispus obținerea de date privind situația sa financiară.

Alături de mențiunile expuse mai sus, apreciem că se impune ca procurorul să indice *momentul de referință pentru situația financiară a unei persoane*, fiind posibilă solicitarea atât a situației financiare curente, cât și a unei situații financiare trecute.

[1] *A.-R. Trandafir*, Obținerea de informații și înscrisuri de la instituțiile de credit în cursul urmăririi penale, prelegere susținută în cadrul Conferinței privind aspecte de practică intervenite de la intrarea în vigoare a Noului Cod penal și Noului Cod de procedură penală, București, 9-10 octombrie 2017, organizată de Institutul Național al Magistraturii – *www.youtube.com*

Capitolul III
Punerea în executare a obținerii de date privind situația financiară a unei persoane

Punerea în executare a metodei speciale de cercetare a obținerii de date privind situația financiară a unei persoane se va face cu concursul entității financiare solicitate prin ordonanța procurorului. Pentru aceste motiv se va impune comunicarea ordonanței către entitatea financiară solicitată, în caz contrar, aceasta putând refuza transmiterea datelor privind situația financiară a unei persoane[1]. S-a mai arătat în doctrină că entitatea financiară este ținută să analizeze dacă prin datele solicitate nu se excedează obiectul metodei speciale de cercetare, sens în care se va impune refuzul pentru informații care presupun obținerea unui mandat de la judecătorul de drepturi și libertăți, în conformitate cu dispozițiile art. 146[1] C.pr.pen.[2].

În ceea ce privește instituțiile care vor fi ținute să comunice datele privind situația financiară a unei persoane, observăm că legiuitorul nu a fost constant în modul în care le-a enunțat în cuprinsul Codului. Astfel, potrivit art. 153 alin. (1) C.pr.pen., vor fi obligate să furnizeze date privind situația financiară a unei persoane *instituțiile de credit* sau *oricare alte instituții*.

Instituțiile de credit nu ridică nicio problemă, întrucât ele sunt definite de art. 3 din O.U.G. nr. 99/2006[3] și pot fi lesne identificate prin consultarea registrului ținut de Banca Națională a României. Întrucât am analizat această categorie în titlul cu privire la obținerea datelor privind tranzacțiile financiare ale unei persoane, facem trimitere la explicațiile date cu ocazia abordării respectivei metode speciale de cercetare[4].

Credem că, prin „oricare alte instituții", legiuitorul a creat o aparentă diferență între această metodă specială de cercetare și obținerea datelor privind tranzacțiile financiare ale unei persoane. Formularea este oarecum neclară, aparent permițând procurorului să obțină aceste date de la orice instituție care ar deține asemenea date sau care ar avea sub control astfel de date. Totuși, este parțial justificată, deoarece, spre deosebire de tranzacțiile financiare, există instituții care pot furniza date privind situația financiară, altele decât entitățile financiare propriu-zise. Termenul de „instituție" nu este unul adecvat, întrucât legiuitorul nu este consecvent în utilizarea unui set terminologic coerent. În acest sens, amintim că terminologia folosită este raportată la Regulamentul (UE) nr. 575/2013, pentru care termenul de „instituție" este sinonim cu cel de „instituție de credit".

Referirea la „instituții" are în vedere instituțiile publice, în special Agenția Națională de Administrare Fiscală, care are rolul de a colecta date privind situația tuturor conturilor deschise

---

[1] *M. Udroiu*, Procedură penală, vol. I, 2019, p. 640.

[2] *Ibidem*.

[3] Conform art. 3 din O.U.G. nr. 99/2006, instituțiile de credit se pot constitui și funcționa, în una din următoarele categorii:

a) bănci;

b) organizații cooperatiste de credit;

c) bănci de economisire și creditare în domeniul locativ;

d) bănci de credit ipotecar.

[4] *V. supra*, Titlul VIII, Capitolul III.1.

la instituțiile de credit din România, nu și în ceea ce privește alte tipuri de conturi deschise la altfel de entități financiare[1].

Pe de altă parte, considerăm că nu este justificată omisiunea din partea legiuitorului a includerii noțiunii de „entitate financiară", întrucât ar pune în discuție posibilitatea descoperirii situației financiare a unei persoane prin aflarea de date privind instrumentele financiare deținute. Până la o modificare legislativă, apreciem că prin termenul de „instituții" vom înțelege orice *entitate financiară*. Cu privire la explicarea noțiunii de „entitate financiară", facem trimitere la explicațiile date în prezenta lucrare în titlul privind obținerea datelor privind tranzacțiile financiare ale unei persoane[2]. *De lege ferenda*, credem că expresia cea mai completă ar fi „instituții de credit, entități financiare și instituții publice".

Odată primită ordonanța procurorului, entitatea financiară solicitată va trebui să pună la dispoziție de îndată datele solicitate în forma cerută de procuror – fie în format electronic, fie în format scris, în conformitate cu dispozițiile art. 153 alin. (3) C.pr.pen. Trebuie reamintit faptul că va trebui să se limiteze doar la informațiile privind existența conturilor și conținutul acestora, neputându-se transmite un extras de cont, acesta conținând și tranzacțiile financiare ale unei persoane.

O particularitate amintită într-o secțiune precedentă este obligarea entității financiare solicitate de a transmite datele în condiții de confidențialitate, în opinia noastră, aceasta însemnând nedivulgarea operațiunii către propriul său client. O atare situație pare ca fiind firească, întrucât este posibil ca persoana față de care se ia măsura să nu cunoască împrejurarea că este cercetată penal sau să nu i se fi adus la cunoștință calitatea procesuală. Chiar dacă are calitate procesuală, încunoștințarea sa de către entitatea financiară ar putea permite acesteia să retragă sume de bani sau să înstrăineze instrumente financiare, mai înainte de a se institui o măsură asigurătorie asupra acestora.

Ceea ce constituie o omisiune din partea legiuitorului este lipsa instituirii unei obligații a procurorului de a încunoștința persoana față de care s-a dispus metoda specială de cercetare. Chiar dacă măsura este minim intruzivă, apreciem că va exista o restrângere a dreptului la viață privată al persoanei, sens în care se va impune încunoștințarea persoanei în condițiile art. 145 C.pr.pen., indiferent cât de redusă este restrângerea. În mod evident, odată fiind încunoștințată, persoana vizată de măsură va trebui să aibă dreptul de a contesta legalitatea măsurii, chiar dacă nu va avea calitatea de suspect sau inculpat în cauză. Fiind un act al procurorului, acesta poate fi atacat în cursul urmăririi penale, potrivit art. 339 C.pr.pen. În acest sens, am amintit într-o secțiune anterioară că în jurisprudența Curții Europene a Drepturilor Omului s-a constatat că încunoștințarea persoanei supuse unei măsuri care restrânge dreptul la viață privată este o condiție esențială pentru ca aceasta să poată contesta legalitatea măsurii[3]. Prin raportare la această jurisprudență, chiar și în absența unui text legal, se va impune încunoștințarea persoanei față de care s-a dispus măsura, în aceleași condiții ca în cazul metodei speciale de cercetare a obținerii datelor privind tranzacțiile financiare ale unei persoane.

---

[1] Potrivit art. 61 alin. (2) C.pr.fisc., instituțiile de credit sunt obligate să comunice organului fiscal central, zilnic, următoarele informații:

a) lista titularilor persoane fizice, juridice sau orice alte entități fără personalitate juridică ce deschid ori închid conturi, precum și datele de identificare ale persoanelor care dețin dreptul de semnătură pentru conturile deschise la acestea;

b) lista persoanelor care închiriază casete de valori, precum și încetarea contractului de închiriere.

[2] *V. supra*, Titlul VIII, Capitolul III.2.

[3] CEDO, cauza *Sommer c. Germania*, Hotărârea din 27 iulie 2017, §62.

Capitolul IV
Concluzii

Metoda specială de cercetare a obținerii de date privind situația financiară a unei persoane constituie un procedeu probatoriu prin care procurorul poate obține probe privind situația financiară a unei persoane, concretizată în identificarea conturilor deținute și a soldului acestora.

Din punctul de vedere al ingerinței aduse dreptului la viață privată, metoda specială este mai puțin invazivă decât alte metode, precum obținerea de date privind tranzacțiile financiare ale unei persoane, sens în care legiuitorul a permis folosirea acesteia în cazul oricărei cauze care face obiectul urmăririi penale.

Procedura de autorizare este una simplificată, fiind obligatorie emiterea unei ordonanțe de către procuror pentru a fi administrată, nefiind specificate condiții legale speciale pentru autorizarea măsurii. Cu toate acestea, măsura este în mod corect aptă să fie întrebuințată doar de procuror, nu și de organele de cercetare penală, întrucât secretul bancar și secretul profesional nu îi sunt opozabile procurorului, în condițiile legii.

Metoda specială de cercetare este criticabilă sub aspectul modalității de reglementare, în ceea ce privește elementele care trebuie să fie conținute în ordonanța procurorului, cât mai ales din perspectiva dreptului persoanei vizate de măsură de a fi informată asupra desfășurării acesteia. *De lege ferenda*, se impune ca persoana care a făcut obiectul metodei speciale de cercetare să fie informată de procuror, în conformitate cu art. 145 C.pr.pen., și să aibă un drept efectiv de a contesta legalitatea măsurii luate împotriva sa.

Titlul X
Obținerea datelor de trafic și de localizare prelucrate de către furnizorii de rețele publice de comunicații electronice ori furnizorii de servicii de comunicații electronice destinate publicului

Capitolul I
Aspecte generale

Secțiunea 1. Obținerea datelor de trafic și de localizare de la intrarea în vigoare a Codului de procedură penală până la Decizia Curții Constituționale nr. 440/2014 privind neconstituționalitatea Legii nr. 82/2012

În acord cu evoluția tehnologiei și a legislației europene dezvoltate în scopul prevenirii criminalității[1], legislația română a adoptat măsuri pentru întrebuințarea judiciară a datelor prelucrate în vederea asigurării serviciilor de comunicații electronice. În mod adevărat s-a reținut chiar în preambulul Directivei care a stat la baza legislației pentru retenția datelor: „*Deoarece păstrarea datelor s-a dovedit a fi un instrument de investigare atât de necesar și eficace pentru aplicarea legii în mai multe state membre și, în special, în ceea ce privește problemele grave, cum sunt criminalitatea organizată și terorismul, este necesară asigurarea că datele păstrate sunt puse la dispoziția autorităților de aplicare a legii pentru o anumită perioadă, sub rezerva condițiilor prevăzute de prezenta directivă*"[2]. După cum vom vedea în prezenta lucrare, necesitatea și eficiența unui procedeu probatoriu nu pot fi considerate criterii suficiente pentru restrângerea dreptului la viață privată, condiția principală care trebuie să fie îndeplinită pentru folosirea oricărei metode speciale de supraveghere sau cercetare fiind proporționalitatea sa.

Față de momentul adoptării Directivei 2006/24/CE, societatea a cunoscut schimbări majore odată cu conștientizarea gravelor ingerințe pe care le poate aduce supravegherea automată și în masă a tuturor persoanelor, tendința actuală fiind de a se interzice introducerea unor măsuri intruzive până la o analiză în detaliu a nivelului de restrângere a vieții private și pentru a se adopta un cadru legal unitar[3]. Colectarea unor date despre toate persoanele, chiar

[1] Directiva 2006/24/CE privind păstrarea datelor generate sau prelucrate în legătură cu furnizarea serviciilor de comunicații electronice accesibile publicului sau de rețele de comunicații publice și de modificare a Directivei 2002/58/CE (J. Of., seria L, nr. 105/54 din 13 aprilie 2006).

[2] Alin. (9) din preambulul Directivei 2006/24/CE.

[3] De exemplu, în prezent, Comisia Europeană analizează oportunitatea interzicerii pentru o durată de 5 ani a tehnologiei de recunoaștere facială pentru camerele de supraveghere publice, până se vor putea determina mai bine consecințele permiterii folosirii unei astfel de tehnologii, în contextul în care unele state membre au implementat complexe sisteme de monitorizare a publicului în orașele principale. A se vedea: Facial recognition: EU considers ban of up to five years, pe *www.bbc.com/news/technology*; EU mulls five-year ban on facial recognition tech in public areas, pe *www.reuters.com*

și în scopuri legitime, conduce la o restrângere a drepturilor și libertăților fundamentale ale acestora, chiar dacă s-ar putea dovedi utilă ulterior și chiar dacă datele prezintă sau nu un caracter sensibil sau vătămător[1]. Stocarea acestora pentru o perioadă de timp va constitui, de asemenea, o ingerință adusă vieții private[2]. După cum spunea scriitorul englez George Orwell în cartea sa, intitulată *1984*: „*omenirea are de ales între libertate și fericire și, pentru marea majoritate a oamenilor, fericirea este preferabilă*". Bunăoară, scopurile legitime și caracterul legal al unei astfel de supravegheri sunt supuse unor particularități culturale și sociale, ceea ce ar fi inacceptabil într-o societate vestică, putând fi normal într-una asiatică[3].

Prin Legea nr. 82/2012[4], România a transpus în legislația națională Directiva 2006/24/CE, creând cadrul legal pentru retenția datelor în scopul obținerii de probe în cursul urmăririi penale. La momentul adoptării Legii nr. 135/2010 privind Codul de procedură penală, nu erau prevăzute metode speciale de supraveghere sau cercetare prin care să se obțină toate datele a căror reținere a fost stipulată prin Legea nr. 82/2012, fiind posibilă doar identificarea abonatului, proprietarului sau utilizatorului unui sistem de telecomunicații ori a unui punct de acces la un sistem informatic sau obținerea listei convorbirilor telefonice. Neexistând cadrul procesual penal care să poată folosi informațiile prelucrate și reținute de furnizorii de rețele publice de comunicații electronice ori furnizorii de servicii de comunicații electronice destinate publicului, prin Legea nr. 255/2013 de punere în aplicare a Codului de procedură penală a fost introdusă, la art. 152 C.pr.pen., metoda specială de cercetare denumită „obținerea datelor generate sau prelucrate de către furnizorii de rețele publice de comunicații electronice sau furnizorii de servicii de comunicații electronice destinate publicului, altele decât conținutul comunicațiilor, și reținute de către aceștia".

Conform art. 152 alin. (1) C.pr.pen. în forma de la intrarea în vigoare a Codului de procedură penală, „*organele de urmărire penală, cu autorizarea prealabilă a judecătorului de drepturi și libertăți, pot solicita unui furnizor de rețele publice de comunicații electronice sau unui furnizor de servicii de comunicații electronice destinate publicului transmiterea datelor reținute, în baza legii speciale privind reținerea datelor generate sau prelucrate de furnizorii de rețele publice de comunicații electronice și de furnizorii de servicii de comunicații electronice destinate publicului, altele decât conținutul comunicațiilor, în cazul în care există o suspiciune rezonabilă cu privire la săvârșirea unei infracțiuni și există temeiuri pentru a se crede că datele solicitate constituie probe, pentru categoriile de infracțiuni prevăzute de legea privind reținerea datelor generate sau prelucrate de furnizorii de rețele publice de comunicații electronice și de furnizorii de servicii de comunicații electronice destinate publicului*".

[1] CJUE, cauzele reunite C-465/00, C-138/01 și C-139/01, *Österreichischer Rundfunk și alții*, Hotărârea din 20 mai 2003, §75.

[2] CJUE, cauzele reunite C-293/12 și C-594/12, *Digital Rights Ireland și alții*, Hotărârea din 8 aprilie 2014, §34.

[3] Exemplul Chinei este unul negativ în acest sens, unde sisteme de recunoaștere facială sunt folosite pentru controlul minorităților. A se vedea Inside China's Massive Surveillance Operation, pe *www.wired.com*

[4] Legea nr. 82/2012 privind reținerea datelor generate sau prelucrate de furnizorii de rețele publice de comunicații electronice și de furnizorii de servicii de comunicații electronice destinate publicului, precum și pentru modificarea și completarea Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice (republicată în M. Of. nr. 211 din 25 martie 2014, ieșită din vigoare ca urmare a Deciziei Curții Constituționale nr. 440 din 8 iulie 2014).

Din definiția dată de legiuitor, reieșeau mai multe caracteristici importante ale metodei speciale de cercetare, o parte dintre acestea constituind lipsuri care vor fi constatate ulterior de Curtea de Justiție a Uniunii Europene, după cum vom vedea într-o secțiune ulterioară[1].

În primul rând, metoda specială impunea încuviințarea măsurii de către judecătorul de drepturi și libertăți, la propunerea organelor de urmărire penală (a procurorului).

În al doilea rând, metoda specială de cercetare era aplicabilă atunci când exista o suspiciune rezonabilă privind săvârșirea unei infracțiuni, desemnând posibilitatea folosirii sale indiferent de gravitatea faptei care făcea obiectul urmăririi penale.

În al treilea rând, legiuitorul a fost contradictoriu în abordare, întrucât în același alineat, deși admite ca o condiție existența suspiciunii rezonabile pentru săvârșirea oricărei infracțiuni, impune folosirea metodei numai atunci când se vor obține probe cu privire la categoriile de infracțiuni prevăzute în Legea nr. 82/2012[2]. Textul era criticabil, întrucât transfera din legea procesuală penală în legislația specială dispoziția legală care prevedea categoriile de infracțiuni pentru care putea fi întrebuințată măsura. Acesta reprezenta un regres al legiuitorului, întrucât, prin reglementarea unitară în Codul de procedură penală a metodelor speciale de supraveghere sau cercetare, s-a urmărit crearea unei legislații unitare pentru aceste măsuri, anterior prevăzute prin legi speciale.

În al patrulea rând, Codul de procedură penală cuprindea că vor putea fi obținute toate datele reținute de furnizori în baza legii speciale, mai puțin conținutul comunicațiilor, pentru că acesta nu era reținut și putea fi obținut numai pentru viitor prin supravegherea tehnică [art. 138 alin. (1) lit. a) C.pr.pen.].

În al cincilea rând, dispozițiile Codului de procedură penală erau legate în mod indisolubil de dispozițiile Legii nr. 82/2012, întrucât art. 152 alin. (1) C.pr.pen. arăta că datele obținute de organele de urmărire penală vor fi acele date reținute „*în baza legii speciale privind reținerea datelor generate sau prelucrate de furnizorii de rețele publice de comunicații electronice și de furnizorii de servicii de comunicații electronice destinate publicului, altele decât conținutul comunicațiilor*". O atare limitare este importantă, întrucât dispozițiile legale menționate au devenit

[1] *V. infra*, Titlul X, Capitolul III.

[2] Potrivit art. 1 din Legea nr. 82/2012, datele prelucrate erau reținute și stocate și în scopul descoperirii și urmăririi penale a infracțiunilor grave. Prin „infracțiuni grave", în sensul legii, se vor înțelege următoarele categorii de infracțiuni cuprinse în art. 2 alin. (1) lit. e) din Legea nr. 82/2012:

„1. infracțiunile prevăzute la art. 2 lit. b) din Legea nr. 39/2003 privind prevenirea și combaterea criminalității organizate, cu modificările ulterioare, săvârșite sau nu de un grup infracțional organizat;

2. infracțiunile prevăzute în cap. IV din Legea nr. 535/2004 privind prevenirea și combaterea terorismului, cu modificările și completările ulterioare;

3. următoarele infracțiuni prevăzute de Legea nr. 286/2009 privind Codul penal, cu modificările și completările ulterioare: infracțiunile contra securității naționale a statului, uciderea ori vătămarea nou-născutului săvârșită de către mamă, vătămare corporală, viol, tâlhărie și tâlhărie calificată, actul sexual cu un minor, distrugerea și distrugerea calificată, ultrajul, evadarea și înlesnirea evadării, infracțiunile de falsuri în înscrisuri, constituirea unui grup infracțional organizat, furtul calificat, înșelăciunea și înșelăciunea privind asigurările, falsificarea de titluri de credit sau instrumente de plată atunci când privește un instrument de plată electronică, șantajul și pornografia infantilă;

4. infracțiunile de corupție, infracțiunile asimilate acestora, precum și infracțiunile împotriva intereselor financiare ale Uniunii Europene, prevăzute de Legea nr. 78/2000 pentru prevenirea, descoperirea și sancționarea faptelor de corupție, cu modificările și completările ulterioare;

5. infracțiuni de evaziune fiscală prevăzute la art. 9 din Legea nr. 241/2005 pentru prevenirea și combaterea evaziunii fiscale, cu modificările ulterioare".

inaplicabile odată cu pronunțarea Deciziei Curții Constituționale nr. 440/2014[1], practic, metoda specială de cercetare a devenit inaplicabilă din acel moment.

Potrivit art. 3 din Legea nr. 82/2012, se reținеau mai multe categorii de date într-o bază de date electronică, care puteau fi puse la dispoziția organelor de urmărire penală în urma obținerii încuviințării din partea judecătorului de drepturi și libertăți. Aceste date se împărțeau în următoarele categorii, care erau detaliate în cuprinsul Legii nr. 82/2012: date necesare pentru urmărirea și identificarea sursei unei comunicări[2]; date necesare pentru identificarea destinației unei comunicări[3]; date necesare pentru a determina data, ora și durata comunicării[4]; date necesare pentru identificarea tipului de comunicare[5]; date necesare pentru identificarea echipamentului de comunicație al utilizatorului sau a dispozitivelor ce servesc utilizatorului drept echipament[6]; date necesare pentru identificarea locației echipamentului

[1] Astfel cum se arată în considerentele Dec. CCR nr. 440/2014, §80: „Este evident că, în condițiile inexistenței unei legi care să reglementeze procedura reținerii și stocării datelor, art. 152 din Codul de procedură penală rămâne fără aplicabilitate practică, dar această împrejurare nu se constituie într-un viciu de neconstituționalitate, textul urmând a deveni incident imediat ce este adoptată o nouă lege referitoare la reținerea datelor".

[2] Conform art. 4 din Legea nr. 82/2012, această categorie de date cuprinde:

„a) în cazul rețelelor de telefonie fixă și de telefonie mobilă: numărul de telefon apelant, precum și numele și adresa abonatului sau ale utilizatorului înregistrat;

b) în cazul serviciilor de acces la internet, poștă electronică și telefonie prin internet:

1. identificatorul alocat;

2. identificatorul de utilizator și numărul de telefon alocat pentru efectuarea oricărei comunicări prin rețeaua publică de telefonie;

3. numele și adresa abonatului sau ale utilizatorului înregistrat, căruia i s-a alocat o adresă Internet Protocol, denumită în continuare adresă IP, un identificator de utilizator sau un număr de telefon, la momentul comunicării".

[3] Conform art. 5 din Legea nr. 82/2012, această categorie de date cuprinde:

„a) în cazul rețelelor de telefonie fixă și de telefonie mobilă:

1. numărul format sau apelat și, în cazurile care includ servicii suplimentare precum redirecționarea sau transferul apelului, numărul către care este direcționat apelul;

2. numele și adresa abonatului ori ale utilizatorului înregistrat;

b) în cazul serviciilor de acces la internet, poștă electronică și telefonie prin internet:

1. identificatorul utilizatorului sau numărul de telefon al destinatarului unui apel telefonic prin internet;

2. numele și adresa abonatului sau ale utilizatorului înregistrat și identificatorul utilizatorului destinatar al comunicării".

[4] Conform art. 6 din Legea nr. 82/2012, această categorie de date cuprinde:

„a) în cazul rețelelor de telefonie fixă și de telefonie mobilă: data și ora inițierii și încheierii unei comunicări;

b) în cazul serviciilor de acces la internet, poștă electronică și telefonie prin internet:

1. data și ora conectării și deconectării de la serviciul de acces la internet, adresa IP alocată dinamic sau static unei comunicări de furnizorul de servicii de acces la internet, precum și identificatorul abonatului sau al utilizatorului înregistrat;

2. data și ora conectării și deconectării de la serviciul de poștă electronică sau de telefonie prin internet".

[5] Conform art. 7 din Legea nr. 82/2012, prin „date necesare pentru identificarea tipului de comunicare" se înțeleg:

„a) în cazul rețelelor de telefonie fixă și de telefonie mobilă: informații privind serviciul de telefonie utilizat;

b) în cazul comunicărilor prin serviciul de poștă electronică și de telefonie prin internet: informații privind serviciul de acces la internet utilizat".

[6] Conform art. 8 din Legea nr. 82/2012, această categorie de date cuprinde:

„a) în cazul rețelelor de telefonie fixă: numărul de telefon al apelantului și numărul de telefon al apelatului;

b) în cazul rețelelor de telefonie mobilă:

1. numărul de telefon al apelantului și numărul de telefon al apelatului;

2. identitatea internațională de abonat mobil, denumită în continuare IMSI, a apelantului;

3. identitatea internațională a echipamentului mobil, denumită în continuare IMEI, a apelantului;

de comunicații mobile[1]. Toate aceste date erau reținute și stocate de furnizori pentru o durată de 6 luni, conform art. 3 alin. (2) din Legea nr. 82/2012. Cu alte cuvinte, organele de urmărire penală puteau obține date, cu încuviințarea prealabilă a judecătorului de drepturi și libertăți, cu până la 6 luni anterior momentului punerii în executare a măsurii.

După cum se poate lesne observa, numărul datelor colectate în legătură cu comunicarea este foarte mare, permițând să se descopere aspecte intime din viața privată a unei persoane, precum obiceiurile sale, locațiile frecventate, persoanele cu care intră în legătură, abilitatea sa informatică etc., factori în funcție de care organele de urmărire penală își pot forma un profil al persoanei și să reușească, inclusiv, să prezică mișcările și acțiunile sale[2]. Tocmai din acest motiv, credem că și în Directiva 2006/24/CE s-a menționat cât sunt de importante aceste date în cazurile de criminalitate organizată sau terorism, deoarece ele fac posibilă dovedirea unor legături între persoane, ierarhii, roluri etc., putând foarte ușor justifica extinderea unei supravegheri tehnice [în sensul art. 138 alin. (1) lit. a)-d) C.pr.pen.] față de un grup de persoane pentru obținerea de noi probe, în speță, date conținut.

Dispozițiile art. 152 alin. (2) și (3) C.pr.pen. nu au suferit modificări de la pronunțarea Deciziei Curții Constituționale nr. 440/2014, astfel că ele vor fi analizate în secțiuni subsecvente. Prin această decizie, Curtea Constituțională a constatat neconstituționalitatea în întregime a Legii nr. 82/2012, sfârșind posibilitatea de întrebuințare a metodei speciale de cercetare, până la modificarea legislativă care a avut loc în parte, cu mențiunile ce vor fi avute în vedere în secțiunea următoare.

Secțiunea a 2-a. Forma în vigoare a metodei speciale a obținerii datelor de trafic și localizare

Ca urmare a pronunțării Deciziei Curții Constituționale nr. 440/2014, metoda specială de cercetare avea nevoie de modificări legislative pentru a putea fi folosită în continuare de organele de urmărire penală. Măsurile luate de legiuitor au fost să modifice conținutul art. 152 alin. (1) C.pr.pen. și să reglementeze un nou cadru privind reținerea datelor. Totodată, metoda specială de cercetare a fost redenumită în „obținerea datelor de trafic și de localizare prelucrate de către furnizorii de rețele publice de comunicații electronice ori furnizorii de servicii de comunicații electronice destinate publicului", indicând în mod corect prin denumirea marginală noul obiect al măsurii.

---

4. identitatea IMSI a apelatului;

5. identitatea IMEI a apelatului;

6. în cazul serviciilor anonime preplătite: data și ora activării inițiale a serviciului, precum și identificatorul celulei de la care a fost activat serviciul;

c) în cazul serviciilor de acces la internet, poștă electronică și telefonie prin internet: numărul de telefon al apelantului în cazul accesului prin dial-up; linia DSL sau alt punct terminal al celui care inițiază comunicarea".

[1] Conform art. 9 din Legea nr. 82/2012, prin „datele necesare pentru identificarea locației echipamentului de comunicații mobile" se vor înțelege:

„a) identificatorul celulei la începutul comunicării;

b) datele care permit stabilirea localizării geografice a celulelor, prin referire la identificatorul acestora, pe durata în care datele comunicării sunt reținute".

[2] CJUE, cauzele reunite C-293/12 și C-594/12, *Digital Rights Ireland și alții*, Hotărârea din 8 aprilie 2014, §27.

Prin forma ulterioară a art. 152 alin. (1) C.pr.pen.[1], metoda specială de cercetare este definită astfel: „*Organele de urmărire penală, cu autorizarea prealabilă a judecătorului de drepturi și libertăți, pot solicita date de trafic și localizare prelucrate de către furnizorii de rețele publice de comunicații electronice ori furnizorii de servicii de comunicații electronice destinate publicului dacă sunt îndeplinite, cumulativ, următoarele condiții:*

a) există o suspiciune rezonabilă cu privire la săvârșirea unei infracțiuni dintre cele prevăzute la art. 139 alin. (2) sau a unei infracțiuni de concurență neloială, de evadare, de fals în înscrisuri, infracțiuni privind nerespectarea regimului armelor, munițiilor, materialelor nucleare și al materiilor explozive, a unei infracțiuni privind nerespectarea dispozițiilor privind introducerea în țară de deșeuri și reziduuri, a unei infracțiuni privind organizarea și exploatarea jocurilor de noroc ori a unei infracțiuni privind regimul juridic al precursorilor de droguri, și infracțiuni referitoare la operațiuni cu produse susceptibile de a avea efecte psihoactive asemănătoare celor determinate de substanțele și produsele stupefiante sau psihotrope;

b) există temeiuri justificate pentru a se crede că datele solicitate constituie probe;

c) probele nu ar putea fi obținute în alt mod sau obținerea lor ar presupune dificultăți deosebite ce ar prejudicia ancheta ori există un pericol pentru siguranța persoanelor sau a unor bunuri de valoare;

d) măsura este proporțională cu restrângerea drepturilor și libertăților fundamentale, date fiind particularitățile cauzei, importanța informațiilor ori a probelor ce urmează a fi obținute sau gravitatea infracțiunii".

Structura definiției metodei speciale de cercetare s-a extins și asupra condițiilor de autorizare prin modificările aduse de legiuitor. Întrucât condițiile de autorizare le vom trata separat într-o secțiune distinctă, facem trimitere la explicațiile care urmează a fi date[2]. Cea mai importantă distincție față de forma precedentă a art. 152 alin. (1) C.pr.pen., din punctul de vedere al definiției, este că măsura va putea privi numai **date de trafic și de localizare** și nu va putea fi aplicată și la alte date care sunt prelucrate și reținute de furnizorii de rețele publice de comunicații electronice ori furnizorii de servicii de comunicații electronice destinate publicului.

În lipsa cadrului legal conferit prin Legea nr. 82/2012, pentru a da eficiență metodei speciale de cercetare, legiuitorul a utilizat noțiunile de „date de trafic" și „date de localizare", care se regăsesc în cuprinsul Legii nr. 506/2004[3]. Această lege exista la momentul adoptării Legii nr. 82/2012, termenii de „date de trafic" și „date de localizare" regăsindu-se încă de atunci cuprinși în aceasta, însă legea avea un alt scop decât cel al combaterii infracționalității[4]. Ceea ce a făcut legiuitorul a fost să mute cadrul de reținere și colectare a datelor de pe o lege ieșită din vigoare pe o lege care nu a fost supusă controlului de constituționalitate, reprezentând un procedeu neconform cu jurisprudența Curții de Justiție a Uniunii Europene pronunțată ulterior Deciziei Curții Constituționale nr. 440/2014, prin care se stabilește că un mecanism de retenție a datelor cu caracter personal contravine dreptului european[5].

---

[1] Forma arătată este cea instituită prin Legea nr. 75 din 28 aprilie 2016 privind aprobarea Ordonanței de urgență a Guvernului nr. 82/2014 pentru modificarea și completarea Legii nr. 135/2010 privind Codul de procedură penală (M. Of. nr. 334 din 29 aprilie 2016).

[2] *V. infra*, Titlul X, Capitolul IV.

[3] Legea nr. 506 din 17 noiembrie 2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice (M. Of. nr. 1101 din 25 noiembrie 2004).

[4] *S. Șandru*, Scurte considerații privind monitorizarea datelor de trafic și drepturile de proprietate intelectuală. Abordări europene, în Revista Română de Drept European nr. 4/2013, p. 29.

[5] CJUE, cauzele reunite C-203/15 și C-698/15, *Tele2 Sverige AB, Secretary of State for the Home Department și alții*, soluționate prin Hotărârea din 21 decembrie 2016.

Ca urmare a modificărilor Legii nr. 506/2004, survenite prin intrarea în vigoare a Legii nr. 253/2015[1], legiuitorul român a reglementat în cuprinsul primei legi posibilitatea de a fi întrebuințate datele de trafic și localizare și pentru alte scopuri decât cele pentru care erau reținute în mod automat și fără a fi necesar consimțământul utilizatorului. Anterior, datele erau reținute și stocate numai pentru realizarea comunicării și pentru facturare[2]. Practic, legiuitorul a menținut scopurile legitime pentru colectarea datelor și a inclus scopul cuprins de Legea nr. 82/2012, modificând și dispozițiile privind durata maximă a colectării. În cele ce urmează vom analiza modificările aduse, prin care s-a încercat crearea contextului legal pentru aplicarea metodei speciale a obținerii de date de trafic și localizare.

Potrivit art. 5 alin. (1) din Legea nr. 506/2004 în forma sa în vigoare, „*datele de trafic referitoare la abonați și la utilizatori, prelucrate și stocate de către furnizorul unei rețele publice de comunicații electronice sau de către furnizorul unui serviciu de comunicații electronice destinat publicului, trebuie să fie șterse ori transformate în date anonime, atunci când nu mai sunt necesare la transmiterea unei comunicări, dar nu mai târziu de 3 ani de la data efectuării comunicării, cu excepția situațiilor prevăzute la alin. (2), (3) și (5)*". Dispozițiile par a fi deopotrivă, în conformitate cu respectarea dreptului la viață privată, dar și în contradicție cu acesta, din cauza reglementării a două durate de retenție a datelor diferite.

În realitate, nu putem să considerăm că legiuitorul a fost inspirat atunci când a stipulat că datele de trafic referitoare la abonați și utilizatori[3] trebuie să fie șterse ori transformate în date anonime când nu mai sunt necesare la transmiterea unei comunicări, dar nu mai târziu de trei ani, deoarece datele de trafic sunt o formă de date informatice a căror existență nu trebuie să fie decât foarte scurtă, strict până la realizarea respectivei comunicări. Modul în care este formulat textul de lege conduce la obligația distrugerii lor sau anonimizării lor după ce s-a realizat transmiterea comunicării – ceea ce în situația datelor informatice înseamnă și momentul la care s-a realizat finalizarea comunicării. Din punct de vedere tehnic, datele de trafic necesare transmiterii unei comunicări își pierd utilitatea în momentul în care fiecare pachet de informații este confirmat ca fiind primit de beneficiar sau, cel târziu, când se va deconecta echipamentul de la rețea (fie prin deconectare de la internet, fie prin încheierea apelului telefonic). Paradoxal, pentru datele de trafic care ar trebui să persiste doar câteva secunde, se prevede un termen maxim de retenție de trei ani, cu mult mai lung decât termenul prevăzut de Legea nr. 82/2012 (6 luni). *De lege ferenda*, se impune înlăturarea termenului de maximum trei ani pentru care se pot reține și stoca datele de trafic în scopul realizării transmiterii comunicării. Nu există nicio justificare tehnică pentru care datele trebuie să fie stocate o asemenea perioadă de timp, ele trebuind a fi șterse de îndată ce nu mai sunt necesare comunicării sau să fie anonimizate. Această ultimă posibilitate este firească, întrucât unele date de trafic pot fi utile furnizorului pentru îmbunătățirea serviciului, însă ele se impun a fi selectate, și dacă sunt informații utile trebuie păstrate anonimizate. De exemplu, pentru îmbunătățirea calității apelurilor telefonice,

[1] Legea nr. 235 din 12 octombrie 2015 pentru modificarea și completarea Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice (M. Of. nr. 767 din 14 octombrie 2015).

[2] Astfel cum rezultă din dispozițiile art. 4 alin. (6) și art. 5 alin. (3) din Legea nr. 506/2004, care preced adoptarea Legii nr. 82/2012.

[3] Dacă termenul de „abonat" nu este unul care să cauzeze probleme, termenul de „utilizator" poate fi apreciat neclar, motiv pentru care legea definește ca fiind utilizator, în art. 2 alin. (1) lit. a): „orice persoană fizică ce beneficiază de un serviciu de comunicații electronice destinat publicului, fără a avea în mod necesar calitatea de abonat al acestui serviciu".

este firesc ca furnizorul să prelucreze și să stocheze situațiile în care apelurile s-au încheiat ca urmare a lipsei de semnal, putând suplimenta echipamentele sale din respectiva locație, în beneficiul clienților, însă, cu această ocazie, informațiile trebuie de îndată anonimizate (aduse într-o stare în care nu se poate identifica abonatul, utilizatorul sau echipamentul) și să fie folosite în această formă. Este evident că pentru un furnizor nu contează dacă o persoană anume a suferit o întrerupere de semnal, dar va fi util să constate că toate persoanele, oricare ar fi identitatea lor, suferă de aceste pierderi de semnal într-o anumită zonă.

Un alt scop pentru care se pot reține și stoca datele privind traficul este cel de facturare. Astfel, potrivit art. 5 alin. (2) din Legea nr. 506/2004, „*prelucrarea datelor de trafic efectuată în scopul facturării abonaților sau al stabilirii obligațiilor de plată pentru interconectare este permisă doar până la împlinirea unui termen de 3 ani de la data scadenței obligației de plată corespunzătoare*". Prevederea unui asemenea scop va urmări și cuantumul datelor de trafic care se impun reținute și stocate, nefiind necesare toate datele de trafic pentru realizarea acestuia. Termenul de 3 ani este în acord cu legislația europeană și se referă la posibilitatea contestării sau urmăririi facturii emise, cu alte cuvinte, se referă la conservarea respectivelor date pe durata termenului de prescripție al acțiunii civile[1]. Orice date de trafic care nu pot fi utile pentru facturare vor trebui distruse sau anonimizate de îndată ce nu mai sunt necesare pentru realizarea transmiterii comunicării.

În concluzie, regimul datelor de trafic stabilit prin Legea nr. 506/2004 este unul deficitar, întrucât nu oferă suficiente garanții că datele de trafic vor fi șterse imediat ce ele nu vor mai fi utile pentru scopul legitim al prelucrării lor, legea nu prevede categorii și subcategorii de date de trafic care sunt apte a fi folosite la facturare și nici nu prevede sortarea acestor categorii în date care pot fi stocate în vederea facturării și date care nu pot fi stocate, lăsând la latitudinea furnizorului această problemă. Referitor la datele de trafic necesare pentru transmiterea comunicării și care nu sunt utile în scopul facturării, ele se impun a fi distruse (sau anonimizate) de îndată ce ele nu mai sunt utile transmiterii comunicării, adică imediat după încetarea comunicării. În privința datelor de trafic prelucrate și stocate în vederea facturării, ele nu se identifică cu toate datele de trafic care pot fi prelucrate, ci doar cu acea parte care este relevantă pentru facturare, celelalte date trebuind să fie distruse de îndată ce ele nu mai sunt utile transmiterii comunicării.

În privința *datelor privind localizarea*, Legea nr. 506/2004 nu instituie un termen maxim pentru stocarea acestora, lăsând o situație de aparentă incertitudine, stipulând doar că acestea vor putea fi prelucrate și reținute numai în anumite situații. Conform alin. (1) al art. 8 din Legea nr. 506/2004, „*prelucrarea datelor de localizare, altele decât datele de trafic, referitoare la utilizatorii sau abonații rețelelor publice de comunicații electronice sau ai serviciilor de comunicații electronice destinate publicului, atunci când este posibilă, este permisă numai în unul dintre următoarele cazuri:*

a) datele în cauză sunt transformate în date anonime;

b) cu consimțământul expres prealabil al utilizatorului sau abonatului la care se referă datele respective, în măsura și pentru durata necesare furnizării unui serviciu cu valoare adăugată[2]*;*

[1] CJUE, cauzele reunite C-203/15 și C-698/15, *Tele2 Sverige AB, Secretary of State for the Home Department și alții*, Hotărârea din 21 decembrie 2016, §86.

[2] Conform art. 2 alin. (1) lit. f) din Legea nr. 506/2004, prin „serviciu cu valoare adăugată" se va înțelege „orice serviciu care necesită prelucrarea datelor de trafic sau a datelor de localizare, în alte scopuri decât transmiterea comunicării ori facturarea contravalorii acestei operațiuni". Acest tip de servicii este oferit de furnizorul de servicii de comunicații și/sau partenerii săi, reprezintă servicii suplimentare serviciilor de bază

c) atunci când serviciul cu valoare adăugată cu funcție de localizare are ca scop transmiterea unidirecțională și nediferențiată a unor informații către utilizatori".

Condițiile arătate mai sus par a fi incompatibile cu posibilitatea prelucrării stocării datelor în cele mai multe situații. De pildă, datele de localizare anonimizate vor fi inutile pentru un organ de urmărire penală, deoarece nu vor putea spune nimic despre persoana cercetată. Cele necesare furnizării unui serviciu cu valoare adăugată nu vor putea fi folosite decât dacă sunt necesare serviciului și pentru durata acestuia, după care vor trebui șterse sau anonimizate. Concluzia este că, în cazul datelor de localizare, nu se poate identifica nicio situație în care datele să fie stocate pentru o perioadă de timp mai lungă ori să poată exista în toate situațiile. Spre deosebire de reglementarea anterioară (Legea nr. 82/2012), datele de localizare nu se vor colecta într-o aceeași măsură și nu vor fi prelucrate și stocate pentru o perioadă de timp îndelungată, concluzia firească fiind că nu va exista nicio oportunitate de a fi transmise organelor de urmărire penală.

Considerăm suspecte dispozițiile art. 8 alin. (6) din Legea nr. 506/2004, întrucât par a conduce la posibilitatea transmiterii către organele de urmărire penală a datelor de localizare, fără ca acest lucru să fie afectat de restul dispozițiilor art. 8, la care am făcut referire deja[1]. Dacă am admite că organele de urmărire penală nu sunt limitate la situațiile în care se prelucrează și stochează datele de localizare, atunci unde sunt stabilite limitele legale ale acestei colectări atunci când scopul este unul judiciar? Răspunsul nostru este că, în funcție de modul în care este redactată Legea nr. 506/2004, nu va putea fi aplicată metoda specială de cercetare prevăzută de art. 152 C.pr.pen., întrucât nu ar trebui să existe date de localizare individualizate, iar, în cazul în care acestea ar exista, furnizorul de servicii de comunicații le-a prelucrat și stocat în mod nelegal.

Atât în cazul datelor de trafic, cât și în cazul datelor privind localizarea, ca urmare a Deciziei Curții Constituționale nr. 440/2014, legiuitorul a inclus proceduri și condiții suplimentare de transmitere a datelor de trafic și de localizare în vederea recreerii posibilității de aplicare a dispozițiilor art. 152 C.pr.pen. Dacă sub aspectul autorizării și punerii în executare, dispozițiile art. 12[1] din Legea nr. 506/2004 vor fi amintite în secțiuni ulterioare, trebuie observat că, față de Legea nr. 82/2012, a fost instituită o procedură de conservare a datelor de trafic și localizare peste termenele prevăzute de lege, la solicitarea organelor judiciare. Astfel, potrivit art. 12[1] alin. (5) din Legea nr. 506/2004, „*datele de trafic, datele de identificare a echipamentului și datele de localizare solicitate conform alin. (1) nu fac obiectul ștergerii sau anonimizării de către furnizori, atunci când solicitarea formulată în temeiul alin. (1) este însoțită ori urmată de o notificare cu privire la necesitatea menținerii lor, în scopul identificării și conservării probelor sau indiciilor temeinice, în cadrul investigațiilor pentru combaterea infracțiunilor ori în domeniul apărării și securității naționale, atât timp cât subzistă motivele care au stat la baza solicitării, dar nu mai mult de 5 ani de la data solicitării sau, după caz, până la pronunțarea unei hotărâri definitive a instanței de judecată*".

Această dispoziție a fost corect criticată în doctrină ca având grave probleme de proporționalitate[2], în condițiile în care termenul de retenție a datelor poate fi extins până la o perioadă de

(de ex.: e-mail, mesagerie vocală, portal, SMS, MMS) și oferă acces la informații și/sau servicii de divertisment sau de altă natură.

[1] Conform art. 8 alin. (6) din Legea nr. 506/2004, „dispozițiile prezentului articol nu aduc atingere posibilității organelor de urmărire penală, instanțelor de judecată și organelor de stat cu atribuții în domeniul securității naționale de a avea acces la datele generate sau prelucrate și păstrate de furnizorii de rețele publice de comunicații și de furnizorii de servicii de comunicații electronice destinate publicului, în condițiile legii".

[2] *G. Zlati*, în M. Udroiu (coord.), Codul de procedură penală, 2017, p. 746.

8 ani sau până la pronunțarea unei hotărâri definitive a unei instanțe. Din această perspectivă, întregul alineat citat va permite accesarea datelor de trafic și localizare după ce acestea ar fi trebuit să fie șterse ca urmare a unei simple notificări din partea unui organ de stat, în ceea ce ne privește, organele de urmărire penală. Practic, în situația în care organele de urmărire penală consideră că nu există temeiuri prezente pentru accesarea datelor de trafic și localizare prin intermediul unui mandat emis de judecătorul de drepturi și libertăți, vor putea notifica furnizorii să conserve datele de trafic și localizare pentru viitor, în caz că totuși va fi nevoie de accesarea lor. În condițiile în care constituie o ingerință chiar și prelucrarea și colectarea datelor de la un număr nedeterminat de persoane, fără a exista criterii obiective și fără un control de proporționalitate, dispoziția vine în contradicție flagrantă cu jurisprudența Curții de Justiție a Uniunii Europene, care va fi analizată în secțiunile ulterioare[1].

Dacă vom compara limitele minime și cele maxime pentru care se pot stoca datele – cel minim fiind de îndată ce nu mai sunt utile transmiterii comunicării; cel maxim de 8 ani [3 ani plus 5 ani, conform art. 12[1] alin. (5) din Legea nr. 506/2004] sau până la pronunțarea unei hotărâri definitive (care poate depăși chiar și termenul de 8 ani) –, vom constata că durata de stocare a datelor este vădit disproporțională cu interesul general protejat (prevenirea și descoperirea săvârșirii unor infracțiuni, nu toate putând fi considerate grave) și provoacă o ingerință excesivă asupra vieții private a persoanei, motive pentru care se impune, *de lege ferenda*, abrogarea acestor dispoziții legale. Apreciem că aceste dispoziții nu ar putea supraviețui unui control de constituționalitate, în eventualitatea invocării unei excepții bazate pe jurisprudența Curții de Justiție a Uniunii Europene ulterioară pronunțării Deciziei Curții Constituționale nr. 440/2014.

Secțiunea a 3-a. Utilitatea reglementării metodei speciale de cercetare a obținerii datelor de trafic și de localizare

Am ales să tratăm problema utilității acestei metode speciale de cercetare după analiza legislației, pentru a se înțelege mai bine că, deși prezintă o utilitate ipotetică, în concret, cadrul legislativ nu poate conduce la o aplicare care să fie în conformitate cu respectarea dreptului la viață privată.

Metoda specială de cercetare a fost introdusă de legiuitor în speranța în care va putea furniza probe în procesul penal prin exploatarea datelor colectate conform Legii nr. 82/2012, abrogată și inaplicabilă în prezent. Inițial, metoda avea în vedere o categorie mult mai largă de date, astfel cum am văzut într-o secțiune precedentă[2]. În prezent, măsura are o utilitate mai scăzută, limitându-se doar la datele de trafic și la cele de localizare, care pot fi obținute de la furnizorii de rețele publice de comunicații electronice sau furnizorii de servicii de comunicații electronice destinate publicului.

Din punctul de vedere al tipului de probe care pot fi obținute, considerăm că se vor limita numai la probe indirecte[3], fiindcă se vor obține probe numai cu privire la realizarea unei comunicări și locul de unde a fost realizată (sau unde se afla persoana vizată), fără a se cunoaște conținutul acesteia.

[1] *V. infra*, Titlul X, Capitolul II.1 și II.3.
[2] *V. supra*, Titlul X, Capitolul I.1.
[3] *Gh. Mateuț*, Tratat, vol. II, 2012, p. 34.

Prin metoda specială de cercetare, organele de urmărire penală pot avea acces la informații privind comunicațiile trecute ale persoanei, fără a putea cunoaște conținutul acestora, însă, prin intermediul datelor de trafic și de localizare, pot să cunoască ce anume făcea persoana vizată la momentul colectării datelor. Fiind restrânsă față de obiectul inițial, aparent, măsura ar constitui o ingerință mai redusă adusă vieții private a persoanei. În doctrină s-a arătat că datele privind traficul se pot dovedi mai intruzive decât datele conținut[1]. Și noi apreciem că măsura a rămas la fel de invazivă, întrucât, prin analizarea unor date privind traficul informațional (*traffic data*), se pot cunoaște elemente privind persoana cercetată, uneori mai precise, dacă se va proceda la analizarea datelor privind conținutul comunicării. De pildă, analizând apelurile unei persoane, se vor putea identifica aspecte privind starea sa de sănătate, în cazul în care are apeluri repetate către un medic cardiolog ori în cazul în care realizează apeluri repetate către o clinică specializată în avorturi și apoi, brusc, acestea încetează[2]. În același fel, se va putea determina raportul dintre două persoane în funcție de identitatea lor, frecvența comunicărilor și durata acestora (stabilindu-se inclusiv dacă relațiile sunt apropiate, dacă persoanele formează un cuplu și dacă se vor despărți). Trebuie subliniat și faptul că folosirea acestei metode de cercetare este mai facilă decât interceptarea comunicațiilor unei persoane, întrucât nu va fi necesară ascultarea și redarea conținutului convorbirilor sau comunicărilor, ci va trebui doar să se analizeze datele trafic pentru a afla detalii importante despre viața unei persoane.

În domeniul comunicațiilor prin internet, devine din ce în ce mai greu ca doar prin datele privind traficul să se identifice acțiunile persoanei supravegheate. De pildă, în prezent, se vor putea cunoaște adresele de internet pe care le accesează o persoană prin datele de trafic (cererile de pagini web prin D.N.S.-uri se transmit necriptat), însă această posibilitate va deveni din ce în ce mai restrânsă odată cu avansurile tehnologice care conduc nu numai la criptarea datelor conținut (paginile de internet au devenit prevalent criptate HTTPS prin TLS – transport layer security), ci și la criptarea datelor de trafic (DNS over TLS[3] și DNSCrypt[4]). În plus, utilizarea din ce în ce mai prevalentă a serviciilor de comunicație de tip WhatsApp, Signal, Facebook Messenger, iMessages tinde să facă mai puțin utile datele de trafic, întrucât nu vor releva decât folosirea acestor servicii și nu vor putea furniza informații despre destinatar, comunicațiile trecând prin servere în calea lor către destinatar. În orice caz, furnizorii de astfel de servicii nu cad sub incidența legii și nu vor putea face obiectul metodei speciale de cercetare prevăzute de art. 152 C.pr.pen.

Ținând seama de capacitățile tehnologice curente, prin folosirea datelor trafic, organele de urmărire penală vor putea cunoaște obiceiurile persoanei supuse măsurii (tipul de servicii folosite, dacă folosește anumite aplicații de internet), cercul său de prieteni, natura relațiilor cu aceștia, aspecte privind sănătatea sa, probleme financiare (de pildă, este sunată de instituții de credit în mod regulat), dacă vizitează site-uri cu conținut pornografic, xenofob, rasist, dacă obișnuiește să consume conținut video prin internet și care este sursa acestui material (licită – YouTube sau ilicită – site-uri de pornografie infantilă). Ca atare, măsura va fi una deosebit de intruzivă chiar dacă nu se va descoperi conținutul comunicărilor, acesta putând fi intuit prin intermediul datelor trafic.

---

[1] *G. Zlati*, în M. Udroiu (coord.), Codul de procedură penală, 2017, p. 743; *C. Harfield, K. Harfield*, Covert Investigation, 2018, p. 165.

[2] *P. Mutchler, J. Mayer*, MetaPhone: The Sensitivity of Telephone Metadata, publicat pe Web Policy, 12 martie 2014, disponibil pe *webpolicy.org*

[3] *S. Gallagher*, How to keep your ISP's nose out of your browser history with encrypted DNS, pe *arstechnica.com*

[4] *www.opendns.com*

Situațiile și problemele prezentate mai sus sunt importante în stabilirea proporționalității în utilizarea metodei speciale a obținerii datelor de trafic și localizare, întrucât relevă că această metodă de cercetare va putea fi exploatată numai în cazurile în care atât complexitatea și importanța cauzei, cât și gravitatea faptelor cercetate justifică analizarea comportamentului unei persoane. Utilizarea ei limitativă, prin întrebuințarea numai a anumitor date de trafic, își poate găsi o utilitate mai largă – de pildă, verificarea existenței unei convorbiri telefonice între două persoane. Neajunsul metodei de cercetare este că organele de urmărire penală vor obține toate datele privind traficul informațional colectate, ceea ce presupune probleme de proporționalitate, mai ales în situațiile în care starea de fapt care se urmărește a fi dovedită nu este esențială pentru probarea infracțiunii.

Din perspectiva localizării, metoda specială de cercetare se dovedește a avea o utilitate mare, deoarece permite stabilirea locației trecute a unei persoane pe baza datelor provenite de la furnizorul de servicii de comunicații electronice, de regulă, furnizorul de telefonie mobilă. Este evident că prezența unei persoane într-o arie geografică poate constitui o probă indirectă care să servească aflării adevărului, putându-se stabili cu certitudine că o persoană ar fi fost, de pildă, la locul săvârșirii unei infracțiuni a cărei comitere o contestă.

Specific datelor privind localizarea este caracterul lor continuu pentru toată durata înregistrării unui terminal de telefonie mobilă (sau orice alt dispozitiv conectat la o rețea de telefonie mobilă) într-o anumită rețea. Ținând cont de specificațiile tehnologice ale rețelelor de telefonie mobilă, se va putea cunoaște locația pe care a avut-o un terminal la un moment dat și se vor putea cunoaște mișcările acestea, implicit și cele ale persoanei care poartă acest terminal asupra sa. Este lesne de identificat traseul unei persoane, locurile unde poposește, indiferent dacă aceasta va realiza comunicări. Bunăoară, datele de trafic vor exista doar în situația unei comunicări, dar pentru generarea datelor de localizare este necesar numai ca terminalul persoanei care face obiectul măsurii să fie pornit și în raza de acoperire a furnizorului de servicii de comunicații electronice. În mod corect s-a observat că între metoda specială de cercetare analizată și metoda specială de supraveghere a localizării sau urmăririi prin mijloace tehnice există o diferență de gravitate a ingerinței vieții private ca urmare a diferenței de precizie în localizarea persoanei prin cele două metode, cea din urmă remarcându-se printr-o precizie mult mai mare (de regulă – n.n.)[1] și prin caracterul prezent al supravegherii[2].

Datele privind localizarea unei persoane sunt extrem de intruzive, fapt care reprezintă o problemă de proporționalitate a luării măsurii față de o persoană determinată și, în opinia noastră, limitează autorizarea măsurii numai în cazul unor infracțiuni grave.

În final, arătăm că utilitatea metodei speciale de cercetare este limitată mai ales prin legislația extrapenală care reglementează procedura colectării și stocării datelor de trafic și localizare, aceasta fiind supusă unor critici binemeritate. Utilitatea măsurii va trebui să fie pusă în balanță cu proporționalitatea ei sub două aspecte – colectarea informațiilor și obținerea acestora de către organele de urmărire penală.

Considerăm că prima problemă este cea mai importantă, întrucât legislația extrapenală nu oferă suficiente garanții pentru a preveni o supraveghere în masă a întregii populații prin colectarea și stocarea datelor și informațiilor pentru o perioadă de timp care poate fi mai lungă decât cea prevăzută prin Legea nr. 82/2012, care a fost declarată neconstituțională.

[1] *M. Bulancea, G. Zlati, R. Slăvoiu*, în M. Udroiu (coord.), Codul de procedură penală, 2017, pp. 660-661.
[2] *Ibidem*, p. 661.

A doua problemă – proporționalitatea obținerii de către organele de urmărire penală a datelor de trafic și localizare – va fi una subsidiară primei, întrucât un examen de proporționalitate din partea judecătorului de drepturi și libertăți, prin prisma unor criterii clare stabilite de legiuitor, nu va putea compensa ingerința adusă prin colectarea datelor de la întreaga populație.

Capitolul II
Noțiunile de „furnizori", „date de trafic" și „date de localizare"

Secțiunea 1. Persoanele care pot fi chemate să comunice date de trafic și localizare

Măsura de cercetare specială nu poate fi înțeleasă pe deplin decât în măsura în care se va cunoaște semnificația termenilor cu care se operează și contextul legislativ al acestora. Dispozițiile art. 152 C.pr.pen. nu includ definiții cu privire la datele care pot fi obținute prin întrebuințarea măsurii, acestea trebuind să fie interpretate prin prisma legislației speciale în domeniu. În strictă legătură cu datele, sunt și persoanele care procedează la reținerea și stocarea acestora și care mai apoi pot fi chemate de organele de urmărire penală să comunice aceste date.

Întrucât se pune în discuție obținerea unor date care au fost procesate de un sistem informatic, observăm că există foarte multe legături între această metodă specială de cercetare și accesul la un sistem informatic ca formă de supraveghere tehnică. O parte dintre explicațiile pe care le-am inclus la analizarea accesului la un sistem informatic vor fi incidente, în special cele date în cazul terminologiei specifice[1], motiv pentru care facem trimitere la partea din lucrare în care am analizat accesul la un sistem informatic. În esență, datele de trafic și de localizare vor fi colectate de furnizorii de servicii de comunicații electronice și furnizorii de rețele de comunicații electronice, dintre care cei mai comuni vizați sunt furnizorii de internet (ISP) și cei de telecomunicații (Telekom, Orange, Vodafone etc.).

Potrivit art. 4 alin. (1) pct. 6 din O.U.G. nr. 111/2011, prin „rețea de comunicații electronice" vom înțelege „*sistemele de transmisie și, acolo unde este cazul, echipamentele de comutare sau rutare și alte resurse, inclusiv elementele de rețea care nu sunt active, care permit transportul semnalelor prin cablu, prin unde radio, prin mijloace optice ori alte mijloace electromagnetice, incluzând rețelele de comunicații electronice prin satelit, rețelele terestre fixe, cu comutare de circuite și cu comutare de pachete, inclusiv internet, și mobile, rețelele electrice, în măsura în care sunt utilizate pentru transmiterea de semnale, rețelele utilizate pentru transmisia serviciilor de programe audiovizuale și rețelele de televiziune prin cablu, indiferent de tipul de informație transmisă*". În esență, furnizorul de rețele de comunicații electronice este acela care deține infrastructura necesară pentru a permite funcționarea comunicațiilor electronice. De pildă, va fi un astfel de furnizor persoana juridică – proprietarul unui tronson de fibră optică, pe care îl pune la dispoziția furnizorilor de servicii pentru transmisia comunicațiilor. În general, persoanele fizice nu stabilesc relații contractuale cu un astfel de furnizor, dar vor beneficia de accesul la rețea prin intermediul unui furnizor de servicii de comunicații electronice.

Conform art. 4 alin. (1) pct. 9 din O.U.G. nr. 111/2011, prin „serviciu de comunicații electronice" vom înțelege „*un serviciu, furnizat, de regulă, contra cost, care constă, în întregime sau în principal, în transmiterea semnalelor prin rețelele de comunicații electronice, incluzând serviciile de telecomunicații și pe cele prin rețelele utilizate pentru transmisia serviciilor de programe audiovizuale, dar fără a include serviciile prin care se furnizează conținutul*

[1] Pentru explicații privind termenii de „sistem informatic", „furnizor de rețele de comunicații electronice", „furnizor de servicii de comunicații electronice", „date referitoare la conținutul informațional", a se vedea Titlul V, Capitolul I.

informației transmise prin intermediul rețelelor ori serviciilor de comunicații electronice sau se exercită controlul editorial asupra acestui conținut; de asemenea, nu se includ serviciile societății informaționale, definite la art. 1 pct. 1 din Legea nr. 365/2002 privind comerțul electronic, republicată, care nu constau, în întregime sau în principal, în transmiterea semnalelor prin rețelele de comunicații electronice". Spre deosebire de furnizorul de rețele de comunicații, furnizorul de serviciu de comunicații electronice va fi cel care va gestiona comunicațiile desfășurate printr-o rețea fizică, constituindu-și o rețea virtuală prin care se desfășoară comunicații și care este interconectată cu alte rețele. Nu este exclus ca furnizorul de servicii de comunicații electronice să fie și cel care este proprietarul rețelei de comunicații electronice[1]. Nu vor fi considerați furnizori de servicii de comunicații electronice aceia care oferă servicii, precum e-mail[2], sau de comunicații, prin mesaje tip Skype/WhatsApp/Viber sau Signal[3], decât în măsura în care realizează o interconectare plătită cu un serviciu de comunicații electronice prin sistem VoIP[4].

Ipoteza de la care a plecat legiuitorul în reglementarea metodei speciale a fost că acești furnizori prelucrează anumite date în momentul în care prestează serviciul specific, putând constitui o sursă de probe pentru organele de urmărire penală.

Activitatea de prelucrare a datelor de trafic și localizare, precum și a altor tipuri de date care nu fac obiectul metodei speciale de cercetare prevăzute de art. 152 C.pr.pen., este reglementată de Legea nr. 506/2004[5]. Importanța ei este că stabilește contextul legal în care un operator va obține informațiile care pot fi puse la dispoziția organelor de urmărire penală, cu criticile la care am făcut deja referire în secțiunile precedente.

Întrucât persoanele care pot fi supuse metodei speciale de cercetare vor avea calitatea de clienți ai unui furnizor de servicii de comunicații electronice, apreciem că procurorul va trebui să aibă în vedere transmiterea solicitărilor de obținere de date privind traficul și localizarea către acești furnizori.

Prin Legea nr. 506/2004 se stabilesc și unele definiții legale pentru „datele de trafic și de localizare" la care face referire art. 152 C.pr.pen., care se apreciază ca fiind definitorii pentru măsura de cercetare analizată[6]. În opinia noastră, cel puțin în cazul datelor de trafic, există probleme sub aspectul definiției, întrucât Legea nr. 506/2004 nu este singura care definește datele de trafic. Mai mult, trebuie să avem în vedere și dacă definiția dată de Legea nr. 506/2004 este conformă cu tratatele internaționale la care România a aderat.

Secțiunea a 2-a. Datele de trafic

În prezenta lucrare am mai tratat problema definiției „datelor privind traficul" în secțiunea dedicată accesului la un sistem informatic, din perspectiva art. 35 alin. (1) pct. 1 lit. f) din

[1] CJUE, cauza C-193/18, *Google c. Germania*, Hotărârea din 13 iunie 2019, §32; cauza C-475/12, *UPC DTH*, Hotărârea din 30 aprilie 2014, §43.

[2] CJUE, cauza C-193/18, *Google c. Germania*, Hotărârea din 13 iunie 2019, §41.

[3] CJUE, cauza C-142/18, *Skype Communications c. IBPT*, Hotărârea din 5 iunie 2019, §42.

[4] *Ibidem*, §49. Curtea a apreciat că serviciul SkypeOut care permite unui utilizator Skype să poată contacta, contra cost, un număr de telefonie constituie temei pentru ca Skype să fie considerat furnizor de servicii de comunicații electronice.

[5] Legea nr. 506 din 17 noiembrie 2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice (M. Of. nr. 1101 din 25 noiembrie 2004).

[6] *G. Zlati*, în M. Udroiu (coord.), Codul de procedură penală, 2017, p. 750.

Legea nr. 161/2003[1] și a art. 1 lit. d) din Convenția de la Budapesta privind criminalitatea informatică, în care datele privind traficul informațional (*traffic data*) sunt definite ca: „*orice date informatice referitoare la o comunicare realizată printr-un sistem informatic, generate de un sistem informatic care a format o parte din lanțul de comunicare, indicând originea comunicării, destinația, ruta folosită, data comunicării, mărimea informațiilor comunicate, durata transmiterii datelor și tipul serviciului utilizat pentru comunicare*".

Față de datele informatice conținut, datele privind traficul informațional **nu presupun cunoașterea conținutului comunicării, ci numai a unor elemente accesorii acestuia**. În general, datele privind traficul informațional sunt efemere, fiind reținute de către furnizorii de servicii informatice numai pentru perioade scurte de timp, mai apoi fiind șterse.

Spre deosebire de definiția dată mai sus, prin art. 2 alin. (1) lit. a) din Legea nr. 506/2004, prin „date de trafic" se vor înțelege „*date prelucrate în scopul transmiterii unei comunicări printr-o rețea de comunicații electronice sau în scopul facturării contravalorii acestei operațiuni*". Pe bună dreptate s-a constatat că dispozițiile menționate mai sus din Legea nr. 506/2004 sunt insuficiente și neclare față de reglementarea anterioară, respectiv art. 3-9 din Legea nr. 82/2012[2], și că, pentru relevarea sensului „datelor de trafic", se va impune interpretarea dispozițiilor legale inclusiv prin prisma normelor abrogate. În opinia noastră, credem că, deși argumentul este unul valid, situația legislativă curentă cunoaște două definiții ale „datelor de trafic informatic", care nu sunt sincronizate, fapt care pune în discuție prioritatea uneia dintre definiții. Cu toate că recunoaștem că Legea nr. 506/2004 reprezintă cadrul legal pentru prelucrarea datelor cu caracter personal în sectorul comunicațiilor electronice, apreciem că, pentru explicarea „datelor de trafic", va avea prioritate definiția din cuprinsul art. 35 alin. (1) pct. 1 lit. f) din Legea nr. 161/2003, deoarece prin această lege se transpune definiția dată în cuprinsul art. 1 lit. d) din Convenția de la Budapesta privind criminalitatea informatică. Considerăm acceptabilă soluția din mai multe motive pe care le vom expune mai jos.

În primul rând, nu se pot accepta două definiții diferite în aplicarea legii procesuale penale, noțiunea de „date de trafic" având importanță deosebită și în cazul măsurii de supraveghere a accesului la un sistem informatic. Cu alte cuvinte, nu putem să folosim sensul din Legea nr. 161/2003 atunci când vom întrebuința accesul la un sistem informatic și nici pe cel din Legea nr. 506/2004 când întrebuințăm metoda specială de cercetare prevăzută de art. 152 C.pr.pen., fiind necesar ca noțiunea să aibă un înțeles unitar.

În al doilea rând, ratificarea Convenției de la Budapesta privind criminalitatea informatică de către țara noastră obliga la reglementarea elementelor din convenție în mod coerent în legislația noastră, inclusiv definiția unor termeni și expresii.

În al treilea rând, prin compararea celor două definiții se observă că nu există contradicții între acestea, cea din Legea nr. 506/2004 fiind o suprapunere nefericită a unor elemente din definiția din Legea nr. 161/2003. Sub acest aspect, Legea nr. 82/2012 era superioară, creând un cadru derogatoriu de la Legea nr. 506/2004, prin care se afirmau anumite trăsături ale datelor de trafic, fără a fi dată o definiție propriu-zisă.

În al patrulea rând, cele două definiții se referă la date informatice, întrucât, în prezent, toate comunicațiile se realizează prin intermediul unor rețele create prin sisteme informatice.

[1] Legea nr. 161 din 19 aprilie 2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice și în mediul de afaceri, prevenirea și sancționarea corupției (M. Of. nr. 279 din 21 aprilie 2003).

[2] *G. Zlati*, în M. Udroiu (coord.), Codul de procedură penală, 2017, p. 750.

Până și simplul telefon cu fir se va conecta în mod analog la un sistem informatic care, din semnal electric analog, îl va converti într-un semnal digital, codat, care va fi transmis mai departe prin rețea. Telefoanele mobile sunt toate sisteme informatice, realizând transmisiunea de date criptate (cu mențiunea că această criptare este una rudimentară, în special în cazul rețelelor 2G) între acestea și turnurile de recepție care transmit mai departe convorbirile, mesajele și internetul ca date informatice.

În al cincilea rând, definiția dată prin Legea nr. 506/2004 este în mod nefericit concisă, însă poate fi interpretată în sensul definiției mai largi propuse. Astfel, vor intra în cadrul datelor prelucrate în scopul transmiterii unei comunicări printr-o rețea de comunicații electronice următoarele informații cuprinse în definiția propusă: originea comunicării, destinația, ruta folosită, data comunicării, mărimea informațiilor comunicate, durata transmiterii datelor și tipul de serviciu. Fără aceste elemente nu se poate realiza comunicarea în mediul digital – originea și destinația sunt necesare, deoarece comunicarea este bidirecțională întotdeauna (se trimite o cerere, mai apoi se răspunde cu informațiile solicitate, se transmite confirmarea primirii ș.a.m.d.); ruta folosită este esențială, deoarece definește legăturile din rețea prin care trebuie să treacă semnalul pentru a ajunge la destinație (internetul fiind un sistem interconectat de sisteme informatice, datele informatice vor face mici popasuri la fiecare echipament de rutare pe măsură ce trec din echipament, prin cabluri, către un alt echipament ș.a.m.d. până la destinație); data comunicării este esențială din motive tehnice multiple; mărimea informațiilor transmise este importantă, deoarece informația circulă sub forma unor pachete între origine și destinație, la ambele puncte verificându-se integritatea pachetelor mai ales prin prisma mărimii lor (în caz de eroare, pachetul se va recomunica); tipul serviciului sau protocolul folosit poate defini natura comunicării – voce, sms sau internet, în cazul acestuia din urmă, va defini serviciul folosit – web, mail, DNS, VoIP, FTP etc.). O importanță deosebită o va avea adresa IP alocată de furnizorul de servicii de internet, întrucât aceasta va identifica în mod unic un utilizator, mai puțin în situația în care serviciul va fi oferit prin intermediul unui punct de acces rezidențial[1]. Această din urmă situație este regăsită atunci când, într-o locuință, societate, instituție există o rețea internă cu adrese IP locale și care va folosi adresa IP alocată de furnizorul de servicii de internet numai pentru comunicațiile din afara rețelei interne. În cazul alocării de adrese IP telefoanelor mobile, din cauza costului ridicat al achiziționării adreselor IP, în ultimii ani, furnizorii de servicii de comunicații electronice preferă să nu aloce o adresă unică fiecărui terminal, ci să îi integreze într-o rețea proprie[2] și să folosească pentru mai mulți utilizatori aceeași adresă[3], aspect care trebuie să fie ținut minte de către organele de urmărire penală, întrucât nu va exista nicio legătură între utilizatorii care vor partaja aceeași adresă IP[4].

Din perspectiva informațiilor necesare facturării contravalorii, vor avea cea mai mare importanță mărimea informațiilor transmise, durata comunicării și tipul serviciului folosit

[1] *Ibidem*, p. 751.

[2] Acest lucru se realizează fără știrea clientului și are în vedere că majoritatea comunicațiilor prin dispozitivele mobile sunt simple și nu necesită cerințe speciale (precum în cazul serverelor). Echipamentele folosite sunt routere cu Carrier-grade NAT (CGN). Pentru detalii, a se vedea What is Carrier-grade NAT (CGN/CGNAT)?, pe *www.a10networks.com/blog*

[3] Faptul acesta este ușor verificabil de către orice utilizator de telefon: pentru verificarea adresei IP externe, se va accesa un site, precum *www.whatismyipaddress.com*, care va furniza adresa IP externă a dispozitivului, ulterior, căutându-se în setările dispozitivului telefonic (variază în funcție de model) adresa alocată de furnizor, aceasta urmând a fi diferită de prima, semnificând că mai mulți utilizatori împart o adresă IP externă unică.

[4] *L. Polcak, R. Hranick, T. Martinek*, On Identities in Modern Networks, în Journal of Digital Forensics, Security and Law, vol. 9, no. 2/2014, pp. 9-10.

(voce, sms sau internet – cu toate subcategoriile sale), dar și destinația și originea, în cazul serviciilor de voce și SMS.

În consecință, chiar și în lipsa clarității reglementării actuale în domeniul prelucrării datelor de către furnizorii de rețele publice de comunicații electronice și furnizorii de servicii de comunicații electronice destinate publicului, vom ajunge la concluzia că, în realitate, datele de trafic presupun aceleași informații conținute în definiția dată prin Legea nr. 161/2003 și, pe cale de interpretare, se va ajunge la aplicarea ei.

Secțiunea a 3-a. Datele de localizare

Legiuitorul a fost mai inspirat atunci când a reglementat datele de localizare în cuprinsul art. 2 alin. (1) lit. c) din Legea nr. 506/2004, prin astfel de date înțelegându-se „*orice date prelucrate într-o rețea de comunicații electronice sau prin intermediul unui serviciu de comunicații electronice, care indică poziția geografică a echipamentului terminal al utilizatorului unui serviciu de comunicații electronice destinat publicului*".

Credem că datele de localizare au cea mai mare utilitate pentru organele de urmărire penală, întrucât pot plasa persoana vizată de măsură într-o arie geografică suficient de precisă pentru a dovedi prezența sa într-o anumită locație la un moment dat. Utilitatea lor pleacă de la premisa stocării unor astfel de date[1] de către furnizorii de servicii de comunicații electronice pe o perioadă mai lungă de timp, diferențiindu-se astfel de supravegherea tehnică a localizării sau urmăririi prin mijloace tehnice care va prevedea numai pentru viitor.

Deși datele de localizare pot fi incidente și în cazul în care terminalul utilizatorului este unul fix (telefon fix), situația nu se impune a fi analizată, deoarece locația acestuia va corespunde cu locul în care acesta a fost instalat. Credem că textul a fost inserat pentru terminalele mobile, precum telefoane mobile, tablete, ceasuri inteligente, laptopuri și orice dispozitiv care folosește servicii de comunicații electronice mobile.

Din perspectiva tehnică a problemei, rețelele de telefonie mobilă se bazează pe echipamente de radiotransmisie care sunt menite să acopere un spațiu geografic definit. În funcție de numărul de utilizatori, de întinderea zonei vizate, de tehnologia folosită (2G, 3G, 4G etc.) și elementele geografice, densitatea unor astfel de echipamente va fi mai mare sau mai mică. În general, în mediul urban, densitatea va fi mult mai mare ca urmare a numărului mai mare de utilizatori, dar și a clădirilor care afectează propagarea undelor radio.

Un terminal conectat la o rețea de telefonie mobilă va fi dotat cu o cartelă SIM (subscriber identification module) sau esim (cartelă SIM conținută de terminal) prin care va identifica rețelei terminalul ca fiind al unui anumit abonat (sau utilizator) și, prin intermediul acesteia, va permite terminalului să se înregistreze în rețea cu un număr de telefon, aprobând desfășurarea comunicațiilor.

Prin „conectare la o rețea de telefonie mobilă" vom înțelege că un terminal a intrat în raza radio a unui turn de recepție al unui furnizor de servicii de comunicații publice și a comunicat acestuia datele sale de identificare, înregistrându-se pe acel turn care va transmite mai departe întregii rețele că are în aria sa respectivul terminal. Un terminal de telefonie mobilă (sau dispozitiv similar) va transmite regulat starea sa către rețea, indicând că acesta există și este

[1] Legalitatea unei astfel de stocări, dar și posibilitatea curentă de a stoca astfel de date vor fi tratate într-o secțiune subsecventă, *v. infra*, Titlul X, Capitolul II.I.

activ. Pentru optimizarea semnalului, este necesară recepționarea de mai multe turnuri de recepție (dacă sunt mai multe în zona respectivă), care vor calcula distanța dintre terminal și acestea și vor stabili, pe bază de triangulație, poziția sa față de aceste turnuri[1]. În cazul în care terminalul se va afla mai aproape de un turn, acesta va prelua sarcina comunicațiilor cu terminalul. Acest sistem explică în practică de ce se solicită celula în care se află terminalul, respectiv în care arie geografică definită de un furnizor se află echipamentul utilizatorului. Întrucât pozițiile geografice ale echipamentelor de emisie-recepție ale furnizorilor de servicii de comunicații electronice (sau ale furnizorilor de rețele de comunicații electronice, în cazul în care furnizorii de comunicații nu dețin și echipamentele de rețea) sunt cunoscute precis, se va putea stabili poziția terminalului. Mai mult, fiind important pentru optimizarea funcționării întregii rețele, se impune ca, pentru o perioadă scurtă de timp, rețeaua să cunoască și ultimele poziții trecute ale utilizatorului[2].

Așa cum în mod corect s-a arătat, „*prin aceste date se poate identifica locația (identificator celular) echipamentului terminal folosit de către persoana supravegheată la începerea comunicației – de exemplu, locația aproximativă de unde a fost transmis un SMS ori inițiat un apel telefonic*"[3]; astfel, vom afla o locație aproximativă, în funcție de densitatea rețelei din acea zonă. Precizia poate varia de la o rază de peste 1 km în mediul rural, la situații în care se pot identifica strada și numărul aproximativ la care se află terminalul.

[1] *D. Perera*, Cellphone network upgrades make location tracking almost as precise as GPS, în FierceGovernmentIT, 28 aprilie 2013; *J. Beck, C. Magana, E.J. Imwinkelried*, The Use of Global Position System (GPS) and Cell Tower Evidence to Establish A Person's Location – Part-I, în Criminal Law Bulletin, vol. 49, no. 1/2013, p. 160.

[2] *R.M. Bloom, W.T. Clark*, Small Cells, Big Problems: The Increasing Precision of Cell Site Location Information and The Need For Fourth Amendment Protections, în Journal of Criminal Law & Criminology, vol. 106, nr. 2/2016, p. 182.

[3] *G. Zlati*, în M. Udroiu (coord.), Codul de procedură penală, 2017, p. 753.

Capitolul III
Importanța deciziilor Curții de Justiție a Uniunii Europene și ale Curții Constituționale în aplicabilitatea metodei speciale de cercetare

Secțiunea 1. Hotărârea Curții de Justiție a Uniunii Europene în cauza *Digital Rights Ireland și alții* pentru invalidarea Directivei 2006/24/CE privind reținerea și stocarea datelor cu caracter personal în contextul comunicațiilor electronice

Întrucât legislația națională privind reținerea și stocarea datelor cu caracter personal de către furnizorii de rețele publice și comunicații și furnizorii de servicii de comunicații electronice destinate publicului constituie implementarea directivelor europene în domeniul telecomunicațiilor, sunt deosebit de importante deciziile Curții de Justiție a Uniunii Europene în privința acestora, găsindu-și aplicabilitate și asupra legislației naționale.

Legea nr. 82/2012, la care am făcut referire în numeroase rânduri, a constituit transpunerea în legislația națională a Directivei 2006/24/CE, fapt care face relevantă decizia Curții de Justiție a Uniunii Europene prin care s-a constatat neconformitatea directivei cu Carta Drepturilor Fundamentale a Uniunii Europene și a dus la invalidarea ei de către Curte în cauza *Digital Rights Ireland*[1] *și alții* (denumită în continuare „Hotărârea Digital Rights"). Subsecvent acestei decizii și pe baza ei, Curtea Constituțională a constatat, prin Decizia nr. 440/2014, neconstituționalitatea Legii nr. 82/2012. La câțiva ani după aceasta, Curtea de Justiție a Uniunii Europene a intervenit în continuare asupra problemei retenției datelor personale prin Hotărârea Tele2 Sverige AB, Secretary of State for the Home Department și alții[2] (denumită în continuare „Hotărârea Tele2"), stabilind un standard de apreciere mai înalt decât cel al Curții Constituționale, motiv pentru care se impune explicarea tuturor acestor decizii pentru a se înțelege problemele curente ale metodei speciale de cercetare.

În Hotărârea Digital Rights, Curtea a constatat că, prin Directiva 2006/24/CE, furnizorilor de servicii de comunicații electronice accesibile publicului sau rețelelor de comunicații publice li s-a instituit obligația acestora de a păstra, pentru o anumită perioadă de timp, dar nu mai puțin de 6 luni și nu mai mult de 2 ani, informații referitoare la viața privată a persoanelor și comunicațiile acestora. De la bun început, Curtea a constatat că însăși colectarea informațiilor respective constituie o ingerință adusă vieții private a persoanei[3].

În plus față de colectarea și stocarea datelor, Curtea a reținut că va constitui o ingerință suplimentară adusă dreptului la viață privată și împrejurarea că autoritățile naționale competente, inclusiv organele de urmărire penală, vor putea avea acces la aceste date[4].

---

[1] CJUE, cauzele reunite C-293/12 și C-594/12, *Digital Rights Ireland și alții*, Hotărârea din 8 aprilie 2014.

[2] CJUE, cauzele reunite C-203/15 și C-698/15, *Tele2 Sverige AB, Secretary of State for the Home Department și alții*, Hotărârea din 21 decembrie 2016.

[3] CJUE, cauzele reunite C-293/12 și C-594/12, *Digital Rights Ireland și alții*, Hotărârea din 8 aprilie 2014, §34.

[4] *Ibidem*, §35.

Deși aceste ingerințe au fost constatate, existența lor nu împiedica aplicabilitatea directivei europene, cât timp această măsură era una necesară și proporțională cu restrângerea drepturilor cetățenilor. Scopul pentru care se realiza retenția datelor a fost considerat ca fiind unul legal, întrucât procedeele probatorii care puteau fi întrebuințate prin raportare la respectivele date erau de natură a preveni și combate săvârșirea infracțiunilor grave, mai ales ținând seama de necesitatea unor tehnici moderne de anchetă pentru combaterea în special a criminalității organizate și a terorismului[1]. Cu toate acestea, chiar dacă acest obiectiv fundamental este unul legal, el nu poate justifica *per se* instituirea unei colectări a datelor precum cea impusă prin Directiva 2006/24/CE. Cu alte cuvinte, chiar dacă o măsură de acest fel poate fi utilă în cazul cercetării infracțiunii, doar prin prisma eficienței procedeului probatoriu nu se poate constata că adoptarea sa este justificată.

Curtea a constatat că este problematică o colectare generalizată a datelor care privesc toate persoanele care utilizează servicii de comunicații electronice, fără ca acestea să fie bănuite de săvârșirea vreunei infracțiuni sau să fie într-o legătură cu persoane care comit astfel de fapte. De altfel, colectarea de date generalizată nu distingea între persoane care ar putea face obiectul unei urmăriri penale și alte persoane, inclusiv persoane obligate la păstrarea secretului profesional (de pildă, avocații), neexistând niciun standard minim prin care să se aprecieze asupra căror persoane se poate aplica măsura[2]. Totodată, colectarea datelor nu era în legătură cu o activitate infracțională determinată, care să se realizeze într-o anumită perioadă, o arie geografică sau de către un grup de persoane determinabile.

Una dintre cele mai importante constatări ale Curții este că Directiva 2006/24/CE nu prevede niciun criteriu obiectiv pentru accesul la informațiile colectate, fiind necesară o limitare a numărului de persoane care poate avea acces, trebuind să existe un control prealabil realizat de o instanță sau de o entitate administrativă independentă. Este necesar astfel un control de proporționalitate[3] între datele accesate și drepturile fundamentale ale persoanei vizate pentru ca datele accesate să se limiteze strict la informațiile necesare în desfășurarea urmăririi penale[4].

A fost criticată și durata de păstrare a datelor și informațiilor colectate potrivit Directivei 2006/24/CE, întrucât toate informațiile colectate erau păstrate pe o perioadă de cel puțin 6 luni, fără a se face vreo distincție între datele care se pot dovedi utile în cursul urmăririi penale[5] și cele care nu ar fi putut avea această calitate. Sub acest aspect, astfel cum am arătat într-o secțiune precedentă, metoda specială de cercetare prevăzută de art. 152 C.pr.pen. avea în vedere totalitatea datelor colectate, nu doar cele care puteau fi definite ca date de trafic și de localizare.

Întrucât Curtea a constatat că Directiva 2006/24/CE nu prevedea norme clare, precise și nici criterii obiective prin care să se reglementeze limitarea ingerințelor aduse respectării dreptului la viață privată și protejarea datelor cu caracter personal atât din perspectiva colectării datelor (colectarea fiind una generală), a termenului de stocare (sunt stocate pentru o perioadă de la 6 luni la 2 ani), a omisiunii limitării colectării numai la date necesare urmăririi penale, cât și

[1] *Ibidem*, §49-51.

[2] *Ibidem*, §58.

[3] *G. Fábián*, Accesul la datele stocate de furnizorii serviciilor de comunicații electronice și influența jurisprudenței Curții de Justiție a Uniunii Europene, adoptată în cazul „Digital Rights", în aplicarea dreptului național în acest domeniu, în Dreptul nr. 5/2016, p. 159.

[4] CJUE, cauzele reunite C-293/12 și C-594/12, *Digital Rights Ireland și alții*, Hotărârea din 8 aprilie 2014, §62.

[5] *Ibidem*, §63.

din lipsa instituirii unor garanții privind accesul la datele respective prin intermediul unui organ independent, s-a impus invalidarea Directivei, întrucât constituia o ingerință de mare amploare și gravitate deosebită adusă acestor drepturi fundamentale.

Secțiunea a 2-a. Decizia Curții Constituționale nr. 440/2014 referitoare la excepția de neconstituționalitate a dispozițiilor Legii nr. 82/2012 (Legea retenției datelor)

La scurt timp după pronunțarea Hotărârii Digital Rights de către Curtea de Justiție a Uniunii Europene, Curtea Constituțională a fost chemată să analizeze o excepție de neconstituționalitate a Legii nr. 82/2012, dar și a dispozițiilor art. 152 C.pr.pen. în forma în vigoare la acel moment. Deși avea posibilitatea să se axeze pe cele reținute în Hotărârea Digital Rights, Curtea Constituțională a preferat să preia numai o parte dintre argumente și, în opinia noastră, a preluat argumentele care erau cel mai puțin importante și a respins argumente care erau valide atât din punctul de vedere al Hotărârii Digital Rights, cât și din perspectiva hotărârii subsecvente, Hotărârea Tele2. Ca atare, deși este singura decizie a Curții Constituționale pronunțată până în prezent cu implicații privind metoda specială de cercetare prevăzută de art. 152 C.pr.pen., atât interpretarea ei, cât și a reglementării în vigoare a metodei speciale și a legislației aferente va trebui să se facă prin raportare la Hotărârea Tele2, despre care urmează să detaliem într-o secțiune subsecventă.

Pornind de la faptul că, prin Legea nr. 82/2012, a fost transpusă în legislația națională Directiva 2006/24/CE, Curtea a constatat că, prin Hotărârea Digital Rights, Curtea de Justiție a Uniunii Europene a declarat invalidă această directivă, întrucât încălca dispozițiile art. 7, art. 8 și art. 52 alin. (1) din Carta drepturilor fundamentale a Uniunii Europene. Ținând seama de dezlegările din hotărârea amintită, Curtea a constatat că, prin prelucrarea și stocarea datelor personale ale abonaților și utilizatorilor, există o ingerință de mare amploare și deosebit de gravă adusă drepturilor fundamentale privind viața intimă, familială și privată, secretului corespondenței și libertății de exprimare, datele reținute fiind apte să conducă la „*concluzii foarte precise privind viața privată a persoanelor ale căror date au fost păstrate, concluzii ce pot viza obiceiurile din viața cotidiană, locurile de ședere permanentă sau temporară, deplasările zilnice sau alte deplasări, activitățile desfășurate, relațiile sociale ale acestor persoane și mediile sociale frecventate de ele*”[1]. Totodată, Curtea preia argumentele privind lipsa de previzibilitate și claritate a Legii nr. 82/2012 prin raportare la limitările aduse drepturilor fundamentale ca urmare a conținutului măsurii reținerii, stocării și utilizării datelor.

Este criticată și lipsa de criterii obiective prin care să se limiteze în mod strict persoanele care pot avea acces, întrucât nu este limitată în toate cazurile ingerința prin acces, de controlul unei instanțe de judecată sau de o entitate administrativă independentă[2]. Dacă, până la acest punct, Curtea Constituțională a preluat argumentele din Hotărârea Digital Rights, de la acest moment, adoptă o opinie discordantă, prin care pune accentul pe accesarea informațiilor stocate, acesta fiind, după cum vom vedea, motivul pronunțării soluției de admitere.

[1] CCR, Dec. nr. 440 din 8 iulie 2014, §56 (M. Of. nr. 653 din 4 septembrie 2014).
[2] *Ibidem*, §57.

Curtea Constituțională separă discuția asupra Legii nr. 82/2012 în două etape: *i)* reținerea și stocarea datelor; *ii)* accesarea și folosirea lor. Totodată, face o limitare a discuției la date de trafic, de localizare și la cele de identificare a unui abonat sau utilizator.

În analiza *primei etape*, Curtea Constituțională reține că, din moment ce legiuitorul a considerat necesară reținerea și stocarea datelor, prin ea însăși, nu contravine dreptului la viața intimă, familială și privată, astfel reținând că nici Constituția și nici jurisprudența sa nu ar interzice această colectare. În mod corect s-a apreciat în doctrină că, prin aceasta, Curtea a mutat analiza de constituționalitate pe a doua etapă[1]. O atare abordare vine în contradicție cu Hotărârea Digital Rights, întrucât în acea cauză s-a pus accentul pe etapa de reținere și stocare a datelor, aceasta fiind socotită a fi o ingerință gravă adusă drepturilor fundamentale ale persoanei. Mai grav este că toate criticile noastre privind dispozițiile art. 5 și 12[1] din Legea nr. 506/2004 privesc tocmai acea parte din Hotărârea Digital Rights pe care Curtea Constituțională o ignoră, efectul fiind mutarea cadrului de reglementare de pe Legea nr. 82/2012 pe Legea nr. 506/2004, fără a crea garanții suficiente pentru a împiedica reținerea datelor într-un mod abuziv sau pentru o perioadă de timp care excedează scopul legal al respectivei legi.

În cea *de-a doua etapă*, Curtea Constituțională reține că, potrivit dispozițiilor art. 1 din Legea nr. 82/2012, au acces la datele reținute, conform prevederilor acestei legi, organele de urmărire penală, instanțele de judecată și organele de stat cu atribuții în domeniul siguranței naționale, însă numai organele de urmărire penală sunt ținute să obțină o autorizare prealabilă din partea judecătorului de drepturi și libertăți, în conformitate cu dispozițiile art. 152 C.pr.pen., nu și organele de stat din domeniul siguranței naționale, astfel lipsind garanția unei protecții eficiente a datelor păstrate împotriva unui abuz sau acces și utilizare ilicită[2]. Ca atare, deși ignoră complet problema lipsei de proporționalitate a reținerii și colectării, reține în mod corect că se impune ca și organele din domeniul securității naționale să fie obligate să treacă printr-o procedură judiciară pentru a putea obține datele de la furnizorii de servicii de comunicații electronice sau de rețele publice de comunicații electronice.

Ca efect al celor reținute de Curte, Legea nr. 82/2012 este neconstituțională în ansamblul ei, Curtea subliniind că vor putea fi totuși colectate anumite date în baza Legii nr. 506/2004, dar numai cele necesare pentru facturare sau plăți de interconectare ori alte scopuri pentru care există consimțământul abonatului sau utilizatorului[3]. Or, astfel cum am arătat într-o secțiune anterioară, tocmai acest tip de date mai pot fi exploatate, ținând seama de caracterul subsidiar al Legii nr. 506/2004.

Ca o soluție la vidul legislativ lăsat în urma declarării neconstituționale a Legii nr. 82/2012, Curtea Constituțională a arătat că este necesară o nouă lege privind reținerea datelor, până la acel moment, datele colectate neputând să mai fie folosite nici de organele de urmărire penală, nici de organele de stat din domeniul securității naționale. Curtea reține următoarele: „*de asemenea, organele judiciare și cele cu atribuții în domeniul siguranței naționale nu au temei legal și constituțional nici pentru accesarea și utilizarea datelor reținute de către furnizori pentru facturare, plăți pentru interconectare ori în alte scopuri comerciale, pe care să le folosească în cadrul activităților de prevenire, de cercetare, de descoperire și de urmărire penală a infracțiunilor*

[1] *G. Zlati*, în M. Udroiu (coord.), Codul de procedură penală, 2017, p. 739.

[2] CCR, Dec. nr. 440 din 8 iulie 2014, §62-63 (M. Of. nr. 653 din 4 septembrie 2014).

[3] *G. Negruț*, Neconstituționalitatea dispozițiilor privind reținerea datelor generate sau prelucrate de furnizorii de rețele publice de comunicații electronice și de furnizorii de servicii de comunicații electronice destinate publicului, în Pro Patria Lex, vol. 15, nr. 2/2015, p. 113.

grave sau pentru rezolvarea cauzelor cu persoane dispărute ori pentru punerea în executare a unui mandat de arestare sau de executare a pedepsei, tocmai datorită caracterului, naturii și scopului diferit al acestora, așa cum este prevăzut de Directiva 2002/58/CE. De altfel, chiar Legea nr. 82/2012 stabilește în art. 11 că aceste ultime date reținute sunt exceptate de la prevederile legii, având un alt regim juridic, fiind supuse prevederilor Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice"[1]. În mod clar arată Curtea Constituțională că Legea nr. 506/2004 nu poate fi acceptată ca fiind temei pentru a furniza aceleași date ca Legea nr. 82/2012, dar, cu toate acestea, legiuitorul a mers peste voința Curții atunci când, prin Legea nr. 235/2015, a modificat două articole din lege (art. 2 și art. 5) și a introdus unul nou (art. 12[1]), socotind că prin aceasta poate reînvia metoda specială de cercetare prevăzută de art. 152 C.pr.pen. Sub acest aspect, apreciem că Legea nr. 235/2015 este neconstituțională în ansamblul ei, întrucât contrazice Decizia Curții Constituționale nr. 440/2014. Într-o opinie contrară, s-a considerat că o atare măsură luată de legiuitor este una suficientă pentru a asigura legalitatea metodei speciale de cercetare, prin Legea nr. 235/2015 fiind pusă în acord legislația penală cu decizia Curții Constituționale[2].

Suntem de acord cu concluzia Curții privind necesitatea unei noi legi referitoare la reținerea datelor, în condițiile în care Legea nr. 506/2004 are un alt obiect și alte scopuri, fiind un regres folosirea ei în locul unei legi dedicate prevenirii și combaterii criminalității. Posibilitatea adoptării unei legi speciale în domeniu este încă discutabilă, mai ales în contextul Hotărârii Tele2 din 21 decembrie 2016, a cărei analiză a vizat Directiva 2002/58/CE, care a fost transpusă în legislația națională prin Legea nr. 506/2004.

Analizând dispozițiile art. 152 C.pr.pen. din perspectiva problemei deduse judecății sale, Curtea Constituțională a apreciat că acestea nu încălcau prevederile Constituției, situație pe care o apreciem nefirească, ținând cont de constatările Curții de Justiție a Uniunii Europene din Hotărârea Digital Rights privind nevoia aplicării metodei speciale de cercetare numai la infracțiuni grave, în condițiile în care art. 152 alin. (1) C.pr.pen. în forma de la acel moment nu condiționa de gravitatea faptei întrebuințarea procedeului probatoriu[3].

Mutând analiza de constituționalitate pe etapa accesării și folosirii datelor colectate, credem că se putea ajunge numai la constatarea neconstituțională a articolelor care prevedeau posibilitatea obținerii de date și de alte instituții ale statului, fără o încuviințare prealabilă din partea judecătorului de drepturi și libertăți ori a instanței. Numai acestea puteau fi socotite neconstituționale, nu întreaga lege și nicidecum dispozițiile care se refereau la folosirea datelor în procesul penal. Cu toate acestea, credem că soluția paradoxală a Curții Constituționale a fost dată pentru că nu se puteau ignora efectele invalidării Directivei 2006/24/CE, ceea ce impunea declararea neconstituțională a Legii nr. 82/2012 în întregimea sa.

[1] CCR, Dec. nr. 440 din 8 iulie 2014, §79 (M. Of. nr. 653 din 4 septembrie 2014).

[2] *A.-N. Volintiru*, Aspecte privind obținerea datelor de trafic și de localizare prelucrate de către furnizorii de rețele publice de comunicații ori furnizorii de servicii de comunicații electronice destinate publicului, în Revista Universul Juridic nr. 9/2016, p. 82.

[3] CCR, Dec. nr. 440 din 8 iulie 2014, §80-81 (M. Of. nr. 653 din 4 septembrie 2014).

Secțiunea a 3-a. Hotărârea Curții de Justiție a Uniunii Europene în cauzele reunite C-203/15 și C-698/15, *Tele2 Sverige AB, Secretary of State for the Home Department și alții*, privind imposibilitatea folosirii Directivei 2002/58/CE în vederea reținerii datelor privind comunicațiile electronice

În contextul invalidării Directivei 2006/24/CE, Curtea de Justiție a Uniunii Europene a fost învestită cu judecarea a două cauze reunite sub numele de *Tele2 Sverige AB, Secretary of State for the Home Department și alții*, cauzele reunite C-203/15 și C-698/15[1], în care s-a pus în discuție aplicabilitatea reținerii stocării și apoi a accesării datelor privind comunicațiile electronice ale unei persoane din perspectiva Directivei 2002/58/CE. Această Directivă avea un caracter subsidiar față de Directiva 2006/24/CE, însă conținea și dispoziții care permiteau ca, în cazul în care era posibil, datele colectate (datele de trafic și de transfer) să poată fi folosite și de organele de urmărire penală.

După cum am arătat, transpunerea în legislația națională a Directivei 2002/58/CE este făcută prin Legea nr. 506/2004, actuala reglementare care stabilește posibilitatea reținerii și stocării datelor de trafic și de localizare, precum și accesul autorităților statului la acestea. Ca atare, dezlegările date de Curte prin Hotărârea Tele2 vor trebui să aibă o aplicabilitate directă în modul în care sunt reținute și stocate datele și mai apoi sunt puse la dispoziția organelor de urmărire penală.

Deși Directiva 2002/58/CE a fost gândită cu scopul principal al protejării vieții private a persoanelor, ca urmare a prelucrării datelor personale ale acestora, potrivit dispozițiilor sale finale, datele obținute vor putea fi folosite și în alte scopuri, inclusiv combaterea infracționalității, fapt care a fost constatat de Curtea de Justiție a Uniunii Europene, astfel că este posibilă reținerea și stocarea unor astfel de date și, ulterior, să fie permis accesul la acestea[2]. Cu toate acestea, stocarea respectivelor date se va putea face numai pentru durata minimă necesară facturării, comercializării sau furnizării serviciilor, cu condiții mai limitative în cazul datelor de trafic și localizare[3]. Faptul că datele pot fi folosite în cursul unei urmăriri penale nu va putea să deturneze legislația de scopul său inițial[4].

Ținând seama de cuprinsul art. 5 și art. 12[1] din Legea nr. 506/2004, observăm că introducerea unor termene mai lungi de timp ar sugera posibilitatea de a se stoca date pentru o durată peste cea necesară, ceea ce contravine cu Hotărârea Tele2, în special sub aspectul că stocarea datelor trebuie să constituie o excepție, și nu o regulă, astfel vor fi lipsite de conținut dispozițiile Directivei privind confidențialitatea datelor cât timp legislația națională prevede în mod diferit.

Deși Curtea admite posibilitatea folosirii unor date colectate, a apreciat că o reglementare națională care nu limitează această colectare de date și care permite stocarea lor peste limitele strictului necesar nu poate fi considerată justificată într-o societate democratică, astfel cum se prevede la art. 15 alin. (1) din Directiva 2002/58/CE, interpretat în lumina art. 7, 8 și 11, precum și a art. 52 alin. (1) din Cartă[5]. Această concluzie este deosebit de importantă, deoarece,

[1] CJUE, cauzele reunite C-203/15 și C-698/15, *Tele2 Sverige AB, Secretary of State for the Home Department și alții*, Hotărârea din 21 decembrie 2016.

[2] *Ibidem*, §74-76.

[3] *Ibidem*, §86.

[4] *G. Fábián*, op. cit., p. 160.

[5] CJUE, cauzele reunite C-203/15 și C-698/15, *Tele2 Sverige AB, Secretary of State for the Home Department și alții*, Hotărârea din 21 decembrie 2016, §107.

deși recunoaște posibilitatea existenței unui scop legitim al reținerii de date, dar și posibilitatea ca acestea să fie folosite în scopul prevenirii și combaterii infracționalității, Directiva 2002/58/CE nu va putea fi interpretată în sensul în care ar permite ca datele să fie stocate pe o durată mai mare de timp decât e strict necesar pentru transmiterea comunicării și facturare. Luând în considerare această situație, apare mai clar că direcția vizată de Decizia Curții Constituționale nr. 440/2014 a fost una eronată, prin aprecierea ideii că prima etapă – reținerea și stocarea datelor – ar fi constituțională, fapt contrazis clar de Curtea de Justiție a Uniunii Europene.

În vederea reglementării corecte a posibilității de a reține și stoca datele personale ale abonaților și utilizatorilor, se impune introducerea unor criterii obiective. Mergând pe firul de raționament al Hotărârii Digital Rights, Curtea de Justiție a Uniunii Europene a expus în Hotărârea Tele2 că, pentru supravegherea unui public larg, trebuie să existe o legătură între datele acestuia și acte de infracționalitate gravă, o atare delimitare putând fi făcută prin intermediul unui criteriu obiectiv, geografic, locațiile trebuind să vizeze zone cu un risc ridicat de comitere de infracțiuni[1]. Or, legislația română nu prevede niciun criteriu de delimitare în colectarea datelor de trafic și datelor de localizare în cuprinsul Legii nr. 506/2004. Din acest punct de vedere, sunt importante concluziile Curții privind prima întrebare preliminară analizată în Hotărârea Tele2: „*Având în vedere toate considerațiile care precedă, trebuie să se răspundă la prima întrebare în cauza C-203/15 că articolul 15 alineatul (1) din Directiva 2002/58, citit în lumina articolelor 7, 8 și 11, precum și a articolului 52 alineatul (1) din cartă, trebuie interpretat în sensul că se opune unei reglementări naționale care prevede, în scopul combaterii infracționalității, o păstrare generalizată și nediferențiată a ansamblului datelor de transfer și al datelor de localizare ale tuturor abonaților și utilizatorilor înregistrați în ceea ce privește toate mijloacele de comunicare electronică*"[2].

În ceea ce privește accesarea datelor stocate, este important a sublinia că în Hotărârea Tele2 s-a stabilit că, în materie de prevenție, cercetare, detectare și urmărire penală a infracțiunilor, numai combaterea infracțiunilor grave poate justifica un astfel de acces, întrucât un acces general la aceste date ar veni în contradicție cu necesitatea unui acces limitat la strictul necesar și numai atunci când acesta se ia față de persoane care sunt bănuite că pregătesc, săvârșesc sau au săvârșit o infracțiune gravă ori că ar fi implicate într-o astfel de infracțiune[3]. Legea română este în dezacord cu Hotărârea Tele2, întrucât permite întrebuințarea măsurii și în cazul în care obiectul urmăririi penale îl constituie infracțiuni a căror gravitate nu poate fi una ridicată, de exemplu, infracțiunile de fals în înscrisuri sau cele contra patrimoniului. Din acest punct de vedere, legislația română este excesiv de permisivă prin raportare la standardul impus de Uniunea Europeană prin Directiva 2002/58/CE, astfel că asigură o protecție insuficientă dreptului la viață privată al persoanelor sub aspectul posibilității organelor de urmărire penală de a obține accesul la datele de trafic și localizare. În contextul Hotărârii Tele2, nu putem să

[1] Putem să ne imaginăm situația unor cartiere cu rată de criminalitate crescută, cartiere locuite de imigranți sau de anumite etnii minoritare. Credem că formularea utilizată de Curte a avut în vedere criterii etnice de fapt, însă exprimarea directă a unor asemenea îngrijorări sau criterii putea fi interpretată ca rasistă sau să dea prilejul aplicării unor asemenea măsuri la o anumită minoritate, situație pentru care China este blamată (în relația statului cu minoritarii uiguri).

[2] CJUE, cauzele reunite C-203/15 și C-698/15, *Tele2 Sverige AB, Secretary of State for the Home Department și alții*, Hotărârea din 21 decembrie 2016, §112.

[3] *Ibidem*, §115, §119.

fim de acord cu opinia mai veche exprimată în doctrină, conform căreia legiuitorul național are libertatea de a reglementa în orice mod retenția datelor în urma Hotărârii Digital Rights[1].

Ulterior accesării datelor de către organele de urmărire penală sau de către orice altă autoritate națională competentă, Curtea a constatat că este necesară informarea persoanei care a fost supusă măsurii, aceasta fiind necesară pentru a-i permite să conteste acțiunea statului[2]. Este lesne de observat că legislația procesuală penală română este deficitară sub acest aspect, întrucât nu prevede nicio obligație ca organele de urmărire penală să procedeze la informarea persoanei față de care s-a întrebuințat metoda specială de cercetare a obținerii datelor de trafic și de localizare.

Din cele arătate mai sus, putem concluziona că legislația română cunoaște grave carențe atât sub aspectul modului în care este reglementată metoda specială de cercetare, cât și sub aspectul legislației speciale în domeniul reținerii și colectării datelor. Chiar și dacă prin Legea nr. 235/2015, legiuitorul a încercat să reintroducă posibilitatea concretă ca organele de urmărire penală să apeleze la dispozițiile art. 152 C.pr.pen., prin raportare la considerentele și concluziile Curții de Justiție a Uniunii Europene din Hotărârea Tele2, considerăm, alături de alți autori[3], că măsura este inaplicabilă din punct de vedere legal la acest moment și ne exprimăm rezerve că aceasta ar putea fi vreodată făcută viabilă[4].

[1] *G. Fábián*, op. cit., p. 164.

[2] CJUE, cauzele reunite C-203/15 și C-698/15, *Tele2 Sverige AB, Secretary of State for the Home Department și alții*, Hotărârea din 21 decembrie 2016, §121.

[3] *M. Udroiu*, Procedură penală, vol. I, 2019, p. 620; *G. Zlati*, în M. Udroiu (coord.), Codul de procedură penală, 2017, pp. 742-743; *M. Petroiu*, Epopeea accesului organelor de stat la datele de trafic, de identificare a echipamentelor și de localizare, în Pandectele Române nr. 3/2016, p. 26.

[4] În sens contrar, *G. Fábián*, op. cit., p. 164.

Capitolul IV
Condițiile legale pentru autorizarea metodei speciale

Mai înainte de a trata autorizarea metodei speciale de cercetare, se impune analizarea condițiilor legale de autorizare a acesteia, condiții care seamănă în proporție foarte mare cu condițiile legale de autorizare a metodelor de supraveghere tehnică. Întrucât am abordat deja gravele probleme ce țin de încălcarea dreptului la viață privată din perspectiva colectării și stocării datelor de trafic și localizare, ne vom referi în prezenta secțiune doar la aspectele de proporționalitate și necesitate strict din perspectiva dispozițiilor Codului de procedură penală.

Obținerea datelor de trafic și de localizare prelucrate de către furnizorii de rețele publice de comunicații electronice ori furnizorii de servicii de comunicații electronice destinate publicului, asemenea celorlalte metode speciale de supraveghere sau cercetare, presupune restrângerea drepturilor și libertăților persoanei vizate de acest procedeu probatoriu, motiv pentru care legea condiționează folosirea acestuia numai când sunt îndeplinite anumite condiții și cu garantarea respectării proporționalității între interesul public și interesul persoanei.

Necesitatea încuviințării procedeului probatoriu servește un dublu scop, cel de a conferi organelor de urmărire penală puteri sporite în activitatea de administrare a probelor și cel de a garanta legalitatea administrării probei.

Obținerea datelor privind traficul informațional și a datelor de localizare se va putea încuviința numai dacă sunt îndeplinite condițiile cumulative prevăzute de art. 152 alin. (1) C.pr.pen. Mai înainte de orice condiție prevăzută expres de lege, este necesar să fi fost începută urmărirea penală pentru o faptă prevăzută de legea penală. Această condiție reiese din faptul că începerea urmăririi penale este actul procesual care creează întreg cadrul pentru desfășurarea activităților de urmărire penală, inclusiv administrarea probelor.

Prima condiție specială pentru acest procedeu probatoriu este existența unei *suspiciuni rezonabile cu privire la săvârșirea unei infracțiuni* dintre cele enumerate la art. 152 alin. (1) lit. a) C.pr.pen. Spre deosebire de alte metode de supraveghere tehnică, nu este inclusă ipoteza existenței unei suspiciuni rezonabile cu privire la pregătirea săvârșirii unei infracțiuni, ceea ce este firesc, întrucât datele de trafic și localizare vor fi obținute pentru trecut.

Criteriul acesta privește o analiză de proporționalitate *in abstracto* făcută de legiuitor pentru a limita măsurile invazive numai la anumite categorii de infracțiuni, ea fiind necesară în cazul metodei speciale de obținere de date de trafic și localizare. În jurisprudența Curții de Justiție a Uniunii Europene s-a arătat că obținerea unora dintre datele prelucrate de furnizori de servicii de comunicații electronice nu va constitui o ingerință gravă care să justifice limitarea măsurii numai la infracțiuni grave, în opinia Curții, astfel de date fiind identificarea titularilor cartelelor SIM activate cu un telefon, numele, prenumele și adresa acestor titulari[1].

Spre deosebire de alte metode speciale de supraveghere sau cercetare, legiuitorul a inclus o sferă mai largă de infracțiuni care pot justifica întrebuințarea acestui procedeu probatoriu. Astfel, potrivit art. 152 alin. (1) lit. a) C.pr.pen., este necesar ca fapta cercetată să fie încadrată ca fiind o infracțiune de „*concurență neloială, de evadare, de fals în înscrisuri, infracțiuni privind nerespectarea regimului armelor, munițiilor, materialelor nucleare, al materiilor explozive și al*

[1] CJUE, cauza C-207/16, *Ministerio Fiscal*, Hotărârea din 2 octombrie 2018, §63.

precursorilor de explozivi restricționați, a unei infracțiuni privind nerespectarea dispozițiilor privind introducerea în țară de deșeuri și reziduuri, a unei infracțiuni privind organizarea și exploatarea jocurilor de noroc ori a unei infracțiuni privind regimul juridic al precursorilor de droguri, și infracțiuni referitoare la operațiuni cu produse susceptibile de a avea efecte psihoactive asemănătoare celor determinate de substanțele și produsele stupefiante sau psihotrope". Totodată, legiuitorul a menționat că vor fi incluse în această categorie și toate infracțiunile cuprinse în art. 139 alin. (2) C.pr.pen.[1]. Prevederea legislativă ridică probleme de compatibilitate cu Carta drepturilor fundamentale a Uniunii Europene (implicit și Convenția Europeană a Drepturilor Omului) prin raportare la includerea unor infracțiuni care nu au un caracter grav între cele care pot face obiectul măsurii. O astfel de măsură contravine cu jurisprudența constantă a Curții de Justiție a Uniunii Europene, întrucât numai combaterea infracționalității grave poate justifica un acces al organelor de urmărire penală la datele de trafic și localizare colectate[2]. Deși se face referire chiar la textul art. 139 alin. (2) C.pr.pen., nu putem să nu remarcăm din nou că această dispoziție legală nu se referă numai la infracțiuni grave, ci și la unele care, prin numărul lor, pot fi socotite ca infracțiuni obișnuite. În această privință, ne referim în principal la cea mai des întâlnită infracțiune contra patrimoniului – furtul – pentru care, în anul 2018, au fost trimise în judecată 8.053 de persoane[3] dintr-un total de 58.737 de persoane trimise în judecate în acel an. Nu considerăm că această infracțiune ar putea justifica gradul de ingerință în viața privată a unei persoane, incident în cazul metodei speciale de cercetare prevăzute de art. 152 C.pr.pen. Mergând mai departe pe aceeași linie de gândire, deși legiuitorul instituie un criteriu subsidiar al pedepsei de cel puțin 5 ani pentru întrebuințarea metodelor speciale de supraveghere tehnică [implicit, prin dispozițiile art. 152 alin. (1) lit. a) C.pr.pen. și a metodei de cercetare a obținerii de date de trafic și de localizare], se vor putea aplica astfel de măsuri maxim intruzive și în cazul infracțiunilor contra siguranței circulației pe drumurile publice, în care limita maximă de pedeapsă este, de regulă, de 5 ani[4]. Aceste infracțiuni sunt, în prezent, cel mai des întâlnite; potrivit bilanțului Ministerului Public pe anul 2018, au fost trimise în judecată 22.047 de persoane pentru comiterea unor asemenea fapte dintr-un total de 58.737. Dacă vom aduna

[1] Conform art. 139 alin. (2) C.pr.pen., „supravegherea tehnică se poate dispune în cazul infracțiunilor contra securității naționale prevăzute de Codul penal și de legi speciale, precum și în cazul infracțiunilor de trafic de droguri, de efectuare de operațiuni ilegale cu precursori sau cu alte produse susceptibile de a avea efecte psihoactive, infracțiunilor privind nerespectarea regimului armelor, muniților, materialelor nucleare, al materiilor explozive și al precursorilor de explozivi restricționați, de trafic și exploatarea persoanelor vulnerabile, acte de terorism, de spălare a banilor, de falsificare de monede, timbre sau de alte valori, de falsificare de instrumente de plată electronică, în cazul infracțiunilor care se săvârșesc prin sisteme informatice sau mijloace de comunicare electronică, contra patrimoniului, de șantaj, de viol, de lipsire de libertate în mod ilegal, de evaziune fiscală, în cazul infracțiunilor de corupție și al infracțiunilor asimilate infracțiunilor de corupție, infracțiunilor împotriva intereselor financiare ale Uniunii Europene ori în cazul altor infracțiuni pentru care legea prevede pedeapsa închisorii de 5 ani sau mai mare".

[2] CJUE, cauzele reunite C-203/15 și C-698/15, *Tele2 Sverige AB, Secretary of State for the Home Department și alții*, Hotărârea din 21 decembrie 2016, §115; CJUE, cauza C-746/18, *H.K./Prokuratuur*, Hotărârea din 2 martie 2021.

[3] Raportul activității desfășurate de Ministerul Public în anul 2018, disponibil pe *www.mpublic.ro*

[4] Astfel, metoda specială de cercetare se va putea aplica următoarelor infracțiuni contra siguranței pe drumurile publice: punerea în circulație sau conducerea unui vehicul neînmatriculat [prevăzută de art. 334 alin. (2) C.pen.], conducerea unui vehicul fără permis de conducere [prevăzută de art. 335 alin. (1) C.pen.], conducerea unui vehicul sub influența alcoolului sau a altor substanțe (prevăzută de art. 336 C.pen.), refuzul sau sustragerea de la prelevarea de mostre biologice (prevăzută de art. 337 C.pen.), părăsirea locului accidentului ori modificarea sau ștergerea urmelor acestuia (prevăzută de art. 338 C.pen.), nerespectarea atribuțiilor privind verificarea tehnică ori efectuarea reparațiilor [prevăzută de art. 340 alin. (2) C.pen.].

infracțiunile de furt și infracțiunile contra siguranței circulației pe drumurile publice, vom ajunge la concluzia că majoritatea infracțiunilor săvârșite în România sunt infracțiuni pentru care se poate autoriza metoda specială de cercetare a obținerii datelor de trafic și de localizare. Din acest punct de vedere, ele nu pot fi socotite ca fiind grave și apreciem că aplicarea metodei speciale de cercetare în cazul acestora va constitui o ingerință disproporționată a dreptului la viață privată al unei persoane, în lumina jurisprudenței Tele2 și a cauzelor subsecvente ale Curții de Justiție a Uniunii Europene. Cea mai recentă cauză o constituie cauza *H.K./Prokuratuur*, în care Curtea a constatat că accesul în scopuri penale la un ansamblu de date de transfer sau de localizare care permit deducerea unor concluzii precise cu privire la viața privată nu este autorizat decât în vederea combaterii infracționalității grave sau a prevenirii amenințărilor grave la adresa siguranței naționale[1]. Această analiză va trebui făcută de un organ independent, și nicidecum de procuror, fiind de remarcat că, în cauza menționată, obiectul urmăririi penale a constituit un concurs de infracțiuni de furt, utilizarea fără drept a cardului bancar al unui terț și fapte de violență față de persoane care participă la o procedură judiciară.

Cu această ocazie, trebuie să observăm că numai în cursul urmăririi penale se poate folosi această măsură de cercetare, legiuitorul renunțând la posibilitatea folosirii sale în cursul judecății. S-a arătat într-o opinie că, și în cursul judecății, instanța poate solicita datele de trafic, datele de identificare a echipamentului și datele de localizare de la furnizorii de servicii de comunicații electronice destinate publicului și furnizorii de rețele publice de comunicații electronice prin încheiere[2].

A doua condiție prevăzută de lege constă în *existența unor temeiuri justificate pentru a se crede că datele solicitate constituie probe*. Această condiție este oarecum subînțeleasă în situația administrării oricărei probe în procesul penal, procurorul trebuind oricum să își justifice propunerea prin raportare la probele care consideră că vor putea fi obținute ca urmare a punerii în executare a metodei speciale de cercetare.

A treia condiție impusă de Codul de procedură penală pentru încuviințarea măsurii de cercetare este *necesitatea procedeului probatoriu* pentru obținerea probei. Cu alte cuvinte, condiția se referă la *subsidiaritatea*[3] metodelor speciale de supraveghere tehnică și cercetare față de orice alt procedeu probatoriu. Această condiție este prevăzută în cuprinsul art. 152 alin. (1) lit. c) C.pr.pen. și limitează folosirea, reținerea, predarea și percheziționarea trimiterilor poștale, cu excepția cazurilor în care „*probele nu ar putea fi obținute în alt mod sau obținerea lor ar presupune dificultăți deosebite ce ar prejudicia ancheta ori există un pericol pentru siguranța persoanelor sau a unor bunuri de valoare*". În realitate, există două situații prevăzute în care se poate considera ca fiind necesară autorizarea măsurii de cercetare: imposibilitatea (absolută sau relativă) obținerii probelor în alt mod și existența unui pericol pentru siguranța persoanei sau a unor bunuri de valoare.

În prima situație, necesitatea este determinată de imposibilitatea obținerii probei în orice alt mod, adică prin utilizarea unui alt procedeu probatoriu, or, obținerea probei prin utilizarea unui alt mijloc de probă ar aduce serioase impedimente anchetei. Prin această prevedere, legiuitorul subliniază faptul că, în cursul urmăririi penale, trebuie folosite, ca regulă, alte mijloace mai

[1] CJUE, cauza C-746/18, *H.K./Prokuratuur*, Hotărârea din 2 martie 2021.

[2] *M. Udroiu*, Procedură penală, vol. I, 2019, p. 623.

[3] *Gh. Mateuț*, Observații critice privind noua reglementare a supravegherii tehnice într-o prezentare comparativă, în Caiete de Drept Penal nr. 3/2015, p. 24.

puțin intruzive, dacă ele sunt apte să conducă la aceleași rezultate[1]. Sensul dispozițiilor legale privind autorizarea măsurii este cel de utilizare a acestor mijloace doar în situația în care proba s-ar obține în condiții dificile, printr-un efort deosebit al organelor de urmărire penală. În această din urmă situație, se impune ca obținerea probei să fie o certitudine pentru organul de urmărire penală, deoarece nu se poate admite folosirea unor astfel de mijloace în speranța obținerii unei eventuale probe sau a descoperirii vreunei infracțiuni.

Cea de-a doua situație prevede utilizarea obținerii datelor de trafic și localizare în cazul în care există un *pericol pentru siguranța persoanelor sau pentru unele bunuri de valoare*. Avem dubii serioase că o astfel de condiție este compatibilă cu natura măsurii, în special având în vedere că datele colectate se vor referi la fapte și împrejurări trecute.

A patra condiție care se impune a fi îndeplinită este cea privitoare la *proporționalitatea măsurii cu restrângerea drepturilor și libertăților fundamentale*. Această condiție este prevăzută de art. 152 alin. (1) lit. b) C.pr.pen. și se impune a fi analizată de judecătorul de drepturi și libertăți prin prisma criteriilor prevăzute de textul de lege: *particularitățile cauzei*, *importanța informațiilor ori a probelor ce urmează a fi obținute sau gravitatea infracțiunii*.

Proporționalitatea trebuie analizată prin raportare la gravitatea restrângerii dreptului persoanei la viață privată, judecătorul de drepturi și libertăți trebuind să constate că nu va exista o disproporție între acțiunile statului și dreptul persoanei vizate de a-i fi protejate aceste drepturi. În analiza proporționalității, va trebui să se aibă în vedere dacă se solicită datele de trafic și de localizare sau numai una dintre aceste componente și pentru ce interval de timp. Întrucât art. 152 C.pr.pen. nu specifică față de ce persoane se poate lua măsura, va fi important ca judecătorul de drepturi și libertăți să stabilească, pe baza propunerii procurorului și a dosarului cauzei, care este implicarea persoanei în infracțiunile săvârșite. Mai mult, va trebui să se acorde atenție sporită atunci când măsura va privi un avocat, chiar dacă textul legal nu include condiții specifice sau o interdicție de a se lua măsura față de avocatul persoanei împotriva căreia se desfășoară urmărirea penală sau bănuită de organele de urmărire penală că ar fi comis o infracțiune.

Prin „particularitățile cauzei" vom înțelege acele împrejurări specifice unei anumite cauze penale care vor impune utilizarea supravegherii tehnice pentru soluționarea cauzei, deoarece un altfel de mijloc nu ar fi propice pentru a stabili starea de fapt.

Prin „importanța informațiilor ori a probelor ce urmează a fi obținute" înțelegem contribuția pe care o pot avea informațiile sau probele obținute pentru stabilirea împrejurărilor esențiale ale cauzei. Proporționalitatea trebuie stabilită raportat la utilitatea probei ce urmează a fi obținută și în funcție de împrejurarea concretă care se urmărește a se dovedi.

„Gravitatea infracțiunii" presupune, în opinia noastră, o analiză a pericolului social concret pe care îl presupune săvârșirea infracțiunii care face obiectul urmăririi penale.

[1] *M. Udroiu, O. Predescu*, Protecția europeană, 2008, p. 829.

Capitolul V
Procedura autorizării obținerii datelor de trafic și de localizare

Obținerea datelor de trafic și de localizare este o metodă specială de cercetare a cărei procedură de autorizare este incompletă, legiuitorul omițând să prevadă cel puțin un element prin care să se cunoască modul de autorizare a măsurii. Ceea ce se poate determina este organul competent și termenul în care se pronunță, lipsind detalii privind modul în care trebuie formulată propunerea de autorizare a măsurii, elementele care trebuie să le conțină, desfășurarea ședinței de judecată (lipsind inclusiv mențiunile privind caracterul public sau nepublic, prezența procurorului etc.), cuprinsul încheierii de autorizare, emiterea unui mandat etc. Dacă, în cazul unor metode speciale de cercetare, omisiunile pot fi complinite printr-o analogie de bun-simț și în acord cu nevoia respectării dreptului la viață privată și al secretului profesional (de exemplu, lipsa mențiunii din cuprinsul art. 153 C.pr.pen. privind interzicerea obținerii situației financiare a avocatului), multitudinea de omisiuni în a legifera metoda de cercetare ridică probleme privind posibilitatea aplicării în mod coerent și printr-o jurisprudență unitară a acesteia.

Propunerea de autorizare a metodei speciale de cercetare aparține *organelor de urmărire penală*, conform art. 152 alin. (1) C.pr.pen. [coroborat și cu art. 152 alin. (2) C.pr.pen.]. Aceasta reprezintă o anomalie în domeniul metodelor speciale de supraveghere sau cercetare, unde regula presupune că procurorul este cel care propune autorizarea măsurii de către judecătorul de drepturi și libertăți. O parte a doctrinei nu semnalează o atare problemă, reținând întocmai ca legiuitorul că propunerea poate fi făcută de organele de urmărire penală[1], ceea ce semnifică inclusiv organele de cercetare penală. Cealaltă opinie exprimată, cu care suntem de acord, arată că, deși legiuitorul a menționat organele de urmărire penală ca putând fi titularii propunerii, acesta s-a referit doar la procuror, întrucât numai acesta poate sesiza judecătorul de drepturi și libertăți[2]. De altfel, dispozițiile art. 55 alin. (3) lit. b) C.pr.pen. cuprind în mod expres atribuția funcțională exclusivă a procurorului de a sesiza judecătorul de drepturi și libertăți și instanța de judecată. Este greu de crezut că legiuitorul ar fi avut vreun motiv ca, numai în cazul acestei metode speciale de cercetare, să permită unui organ de cercetare penală să sesizeze judecătorul de drepturi și libertăți, trecând peste procurorul care supraveghează urmărirea penală.

O omisiune flagrantă a legiuitorului era de a se prevedea și intervalul de timp pentru care se solicita datele privind traficul și localizarea, ținând seama de caracterul intruziv al măsurii care trebuie să fie limitat în timp, chiar dacă măsura se va autoriza pentru date obținute în trecut. În mod similar cu măsura obținerii datelor privind tranzacțiile financiare ale unei persoane, intervalul de timp pentru care sunt solicitate datele va influența gradul de intruziune în viața privată a unei persoane. Va fi necesar ca procurorul să precizeze intervalul pentru care solicită datele și, în consecință, judecătorul de drepturi și libertăți să se pronunțe numai asupra acestuia, nefiind de conceput să se admită autorizarea unei măsuri pentru toate datele deținute de furnizori.

[1] *G. Zlati*, în M. Udroiu (coord.), Codul de procedură penală, 2017, p. 753; *M. Udroiu*, Procedură penală, vol. I, 2019, p. 621.

[2] *Gh. Mateuț*, Procedură penală, 2019, p. 735.

Organul competent să dispună asupra folosirii metodei speciale de cercetare a obținerii datelor de trafic și de localizare este *judecătorul de drepturi și libertăți*. Deși textul art. 152 alin. (1) C.pr.pen. instituie o autorizație prealabilă a judecătorului de drepturi și libertăți, aceasta nu va însemna că organele de urmărire penală vor avea posibilitatea să dispună asupra măsurii și că actul de autorizare va rămâne cel al judecătorului[1]. Acest aspect va avea relevanță asupra identificării actului care va trebui comunicat furnizorului solicitat. De altfel, în jurisprudența Curții de Justiție a Uniunii Europene s-a statuat că un control al instanței sau al unei autorități administrative independente este necesar pentru a se asigura limitarea accesului la datele colectate[2].

Într-un mod ciudat, legiuitorul nu a prevăzut posibilitatea ca procurorul să dispună autorizarea provizorie a măsurii pe o durată de 48 de ore, cum este posibil în cazul măsurilor de supraveghere tehnică și a altor metode speciale de cercetare. Chiar ținând cont de faptul că procedura autorizării unor asemenea măsuri a fost considerată în mod corect ca fiind neconstituțională[3], raportat la dispozițiile art. 21 alin. (3) din Constituție, nu putem să atribuim vreun merit legiuitorului, întrucât nu credem că această omisiune are un caracter intenționat, fiind doar una dintr-un lanț de omisiuni pe care le-am evidențiat deja în lucrare în ceea ce privește reglementarea metodelor speciale de supraveghere sau cercetare.

Judecarea propunerii se va face în termen de 48 de ore de la înregistrarea acesteia la instanță, un termen mai lung decât în cazul supravegherii tehnice, iar judecătorul de drepturi și libertăți trebuie să se pronunțe în aceeași zi. Judecata va avea loc în camera de consiliu, dispozițiile art. 152 alin. (2) C.pr.pen. neindicând dacă prezența procurorului va fi obligatorie. În lipsa unei dispoziții legale, se poate concluzia că judecata se va desfășura și fără prezența procurorului[4]. Totuși, o atare situație ar constitui o excepție nejustificată în cazul metodelor speciale de supraveghere sau cercetare, astfel că opinăm în sensul în care procurorul va fi dator să participe la judecarea propunerii, întrucât, odată ce sesizează judecătorul de drepturi și libertăți, el este obligat să își susțină propunerea în fața acestuia.

Judecătorul de drepturi și libertăți se va pronunța printr-o încheiere, al cărei conținut nu este stabilit de Codul de procedură penală, așa cum nu este stabilit nici conținutul propunerii. De altfel, nu se menționează nici obligația ca judecătorul de drepturi și libertăți să emită un mandat, ci doar să dispună asupra autorizării măsurii. În opinia noastră, aceste omisiuni vor trebui completate cu dispozițiile art. 140 C.pr.pen., pentru a se crea un cadru coerent de aplicare a metodelor speciale de supraveghere tehnică și cercetare. Mai mult, apreciem că emiterea unui mandat este necesară, întrucât, potrivit art. 285 alin. (2) C.pr.pen., urmărirea penală are caracter nepublic și nu se poate admite divulgarea către persoanele care vor contribui la punerea în executare a măsurii a întreg conținutului încheierii. Nu va fi suficient ca furnizorii de rețele publice de comunicații electronice și furnizorii de servicii de comunicații electronice destinate publicului să păstreze secretul operațiunii efectuate, întrucât aceștia nu sunt participanți în procesul penal încât să li se poată permite accesul să cunoască orice act al dosarului, mai ales unul care face referire la faptele cercetate, la persoanele față de care se strâng probe, ce probe există în prezent etc.

---

[1] *V. Trif*, op. cit., p. 271.

[2] CJUE, cauzele reunite C-293/12 și C-594/12, *Digital Rights Ireland și alții*, Hotărârea din 8 aprilie 2014, §62.

[3] *Gh. Mateuț*, Observații critice privind noua reglementare a supravegherii tehnice într-o prezentare comparativă, în Caiete de Drept Penal nr. 3/2015, pp. 31-32.

[4] *M. Udroiu*, Procedură penală, vol. I, 2019, p. 623.

Chiar dacă metoda specială de cercetare nu prevede posibilitatea întrebuințării sale în cursul judecății, în legislația specială s-a instituit posibilitatea instanței de a solicita datele de trafic, datele de identificare a echipamentului și datele de localizare[1]. Într-o asemenea situație, administrarea probei se va dispune prin încheierea instanței. Dincolo de aspectele de neconstituționalitate a modalității de reținere a datelor respective, observăm că, asemenea altor metode speciale de cercetare ce privesc fapte și împrejurări din trecut, legislația specială prevede o procedură paralelă pentru ca instanța să obțină datele solicitate. *De lege ferenda*, considerăm că este preferabil ca o astfel de posibilitate să fie inclusă în Codul de procedură penală, distinct de metodele speciale de supraveghere sau cercetare, prin care instanța să poată obține, după caz, aceleași probe ca în situația în care proba ar fi fost administrată de organul de urmărire penală, cu mențiunea că procedeul probatoriu va putea privi numai fapte și împrejurări trecute (de exemplu, tranzacțiile financiare trecute ale unei persoane).

[1] Conform art. 12[1] alin. (1) din Legea nr. 506/2004, „la solicitarea instanțelor de judecată sau la solicitarea organelor de urmărire penală ori a organelor de stat cu atribuții în domeniul apărării și securității naționale, cu autorizarea prealabilă a judecătorului stabilit potrivit legii, furnizorii de servicii de comunicații electronice destinate publicului și furnizorii de rețele publice de comunicații electronice pun la dispoziția acestora, de îndată, dar nu mai târziu de 48 de ore, datele de trafic, datele de identificare a echipamentului și datele de localizare, în conformitate cu prevederile referitoare la protecția datelor cu caracter personal”.

Capitolul VI
Punerea în executare a obținerii datelor de trafic și de localizare

Secțiunea 1. Transmiterea mandatului și obligația de confidențialitate a furnizorului solicitat

În virtutea celor arătate în secțiunea precedentă, apreciem că se va impune ca judecătorul de drepturi și libertăți să emită un mandat pentru autorizarea metodei speciale de cercetare, acesta fiind remis procurorului care va realiza punerea în executare.

În punerea în executare a măsurii, procurorul poate dispune el însuși ca mandatul să fie transmis furnizorilor solicitați sau poate dispune delegarea organelor de cercetare să realizeze acest lucru. Practic, punerea în executare nu va presupune decât transmiterea mandatului și primirea datelor de la furnizori, legea neprevăzând alte obligații subsecvente pentru organele de urmărire penală.

Ceea ce poate fi inclus alături de mandat, eventual printr-o adresă emisă de procuror, este cadrul în care se va realiza măsura de cercetare: modul de transmitere a datelor și informațiilor, împuternicirea ridicării de către organele de cercetare a rezultatelor măsurii de cercetare etc.

În conformitate cu dispozițiile art. 152 alin. (3) C.pr.pen., furnizorii de rețele de comunicații electronice și furnizorii de servicii de comunicații electronice destinate publicului sunt obligați să păstreze secretul operațiunii solicitate. Ca atare, nu vor putea divulga informații despre împrejurarea că datele de trafic sau de localizare au fost solicitate de organele de urmărire penală, că acestea au fost transmise, perioada pentru care au fost transmise etc. Măsura are în vedere relația dintre client (abonat sau utilizator) și furnizor, întrucât natura datelor transmise – date personale – oricum ar fi impus nedivulgarea lor. Corelativ, art. 12^1 alin. (4) din Legea nr. 506/2004 impune furnizorilor să proceseze solicitările organelor de urmărire penală în condiții de confidențialitate, ceea ce înseamnă, în plus față de cele cuprinse în Codul de procedură penală, că accesarea și apoi transmiterea datelor trebuie să nu fie divulgate decât unui număr restrâns de persoane din cadrul furnizorului.

Secțiunea a 2-a. Transmiterea datelor de trafic și de localizare

Odată cu trimiterea mandatului, este necesar ca procurorul să indice modalitatea în care va dori să fie transmise datele de trafic și de localizare, în funcție de preferințe (electronic sau în format scris), dar și în conformitate cu Legea nr. 506/2004, care prevede dispoziții pentru ambele posibilități.

Deși Codul de procedură penală nu stipulează un termen pentru transmiterea de către furnizori a datelor de trafic și de localizare, Legea nr. 506/2004 impune un termen în cuprinsul art. 12^1 alin. (1), în care se stabilește că datele vor fi transmise *de îndată*, dar nu mai târziu de 48 de ore de la primirea solicitării. În plus față de acestea, atunci când datele se vor transmite pe cale electronică, va fi obligatorie semnarea acestora cu o semnătură electronică bazată pe un certificat calificat eliberat de un furnizor de certificare acreditat. O atare obligație vine

în conflict cu nivelul de reglementare al metodelor speciale de supraveghere tehnică, unde semnarea acestor informații este facultativă, conform art. 142[1] C.pr.pen. Nu considerăm că această prevedere aduce vreo vătămare intereselor furnizorilor ca urmare a costurilor scăzute ale unui astfel de certificat. Transmiterea electronică a datelor de trafic și de localizare o apreciem a fi preferabilă transmiterii în format scris, întrucât se va putea realiza cu mai mare rapiditate și constituie formatul specific în care deja se află datele de trafic și de localizare. Prin „accesul la date în format electronic", organele de urmărire penală pot întrebuința un sistem informatic pentru a sorta și a găsi mai repede informațiile solicitate.

Secțiunea a 3-a. Informarea persoanei supuse metodei speciale de cercetare

Informarea persoanei care a fost supusă metodei speciale de cercetare nu este prevăzută de dispozițiile art. 152 C.pr.pen., legiuitorul apreciind că nu ar fi necesară o astfel de obligație care să incumbe organelor de urmărire penală. O atare omisiune o considerăm a fi neconstituțională, prin raportare la dezlegările date de Curtea Constituțională prin Decizia nr. 244/2017[1], în care s-a stabilit că dispozițiile art. 145 C.pr.pen. sunt neconstituționale în măsura în care nu dau posibilitatea contestării măsurii de către o persoană care nu are calitate de inculpat. În cazul art. 152 C.pr.pen., lipsa oricărei prevederi din partea legiuitorului asupra informării persoanei supravegheate împiedică posibilitatea reală ca o persoană să conteste măsura[2].

În același timp, o atare prevedere era necesară și din punctul de vedere al dreptului Uniunii Europene, deoarece lipsa ei împiedica exercitarea posibilității persoanei de a ataca măsura, în conformitate cu dispozițiile art. 15 alin. (2) din Directiva 2002/58/CE coroborat cu art. 22 din Directiva 95/46/CE[3], fapt care a fost subliniat în jurisprudența Tele2[4]. Or, această încunoștințare, fiind obligatorie în sensul deciziei arătate și fiind menționată și de Directiva 2002/58/CE (preluată în legislația națională prin Legea nr. 506/2004) omisiunea de a prevedea obligativitatea informării, constituie o încălcare a țării noastre de a-și însuși acquis-ul comunitar și de a aplica deciziile Curții de Justiție a Uniunii Europene. *De lege ferenda*, se impune ca procedura aplicabilă în cazul metodelor de supraveghere tehnică să fie aplicată și în cazul obținerii datelor de trafic și de localizare.

[1] CCR, Dec. nr. 244 din 6 aprilie 2017 (M. Of. nr. 529 din 6 iulie 2017).

[2] CEDO, cauza *Sommer c. Germania*, Hotărârea din 27 iulie 2017, §62.

[3] Conform art. 22 din Directiva 95/46/UE, „fără să aducă atingere oricărei căi administrative de atac care poate fi prevăzută, *inter alia*, în fața autorității de supraveghere menționată la articolul 28, anterior sesizării autorității judecătorești, statele membre prevăd dreptul oricărei persoane la o cale atac în justiție în caz de încălcare a drepturilor garantate prin dreptul intern aplicabil prelucrării în cauză".

[4] CJUE, cauzele reunite C-203/15 și C-698/15, *Tele2 Sverige AB, Secretary of State for the Home Department și alții*, Hotărârea din 21 decembrie 2016, §121.

Capitolul VII
Concluzii

Metoda specială de cercetare a obținerii datelor de trafic și de localizare prevăzută de Codul de procedură penală a cunoscut o existență zbuciumată datorată repetatelor probleme de legalitate a reținerii și stocării datelor de către furnizorii de servicii de comunicații electronice. Deși a suferit modificări, atât aceasta, cât și legislația specială care creează cadrul pentru aplicarea ei cunosc probleme care nu pot fi soluționate decât printr-o intervenție mai amplă a legiuitorului.

Legea română cunoaște incoerențe terminologice, dar și contradicții privind durata maximă de stocare a datelor, sens în care nu se va putea realiza o stocare legală a datelor și, în consecință, ele nu se vor putea comunica în mod legal organelor de urmărire penală pentru a constitui probe în procesul penal. *De lege ferenda*, se impune înlăturarea termenului de maximum trei ani pentru care se pot reține și stoca datele de trafic în scopul realizării transmiterii comunicării. Nu există nicio justificare tehnică pentru care datele trebuie să fie stocate o asemenea perioadă de timp, ele trebuind a fi șterse de îndată ce nu mai sunt necesare comunicării sau să fie anonimizate.

Din perspectiva jurisprudenței Curții de Justiție a Uniunii Europene, apreciem că nu se va mai putea continua folosirea acestei metode speciale de cercetare în forma sa actuală, întrucât nu mai este permisă o acțiune de reținere și stocare a datelor privind un număr nedeterminat de persoane, trebuind să fie găsite mecanisme prin care numai anumite categorii de persoane să fie afectate.

De lege ferenda, se impune ca metoda specială de cercetare să fie transformată într-o metodă specială de supraveghere prin care, pentru anumite persoane și numai pentru viitor, să se autorizeze ca datele de trafic și de localizare să fie colectate în scopul strângerii de probe, neputând fi acceptată desfășurarea pentru trecut a acestei activități, întrucât ar contrazice necesitatea limitării colectării datelor doar la anumite persoane.

În ultimul rând, apreciem că se impune reglementarea unei proceduri de informare a persoanei care a făcut obiectul metodei de cercetare, în aceleași condiții ca pentru supravegherea tehnică.

Titlul XI
Reținerea, predarea și percheziționarea trimiterilor poștale[1]

Capitolul I
Aspecte generale și istorice

Printre metodele speciale de supraveghere sau cercetare reglementate de legiuitor în Codul de procedură penală, regăsim și una dintre cele mai vechi forme de obținere a informațiilor (*lato sensu*) cunoscute de om – interceptarea, deschiderea și citirea corespondenței. Transmiterea informației la distanță este de mult timp esențială pentru stabilitatea oricărui stat, noile tehnici de comunicație la distanță păstrând nevoia omului de a comunica semenilor săi sentimente și idei.

Siguranța și secretul mesajului purtat prin corespondență sunt esențiale și au stat la bazele făuririi marilor imperii antice, permițând unei conduceri centrale să delege resurse, armate, în funcție de nevoile curente, și să administreze zone întinse de teritoriu. Inițial, corespondența era livrată de mesageri (soli) ai regilor, împăraților, care purtau mesajele direct către destinatar, fără a avea intermediari.

Cu toate că obiceiul de a transmite la distanță decretele regelui era mai vechi, cea mai veche scrisoare datează din anul 255 î.Hr. și aparține unui faraon egiptean[2]. În perioada antică, poșta era rezervată conducătorilor statului sau personalului din administrație, primul serviciu de poștă și curierat propriu-zis, denumit *cursus publicus*, fiind înființat de împăratul Augustus. Sistemul roman de poștă era adaptat unui imperiu cu o mare întindere, astfel că era structurat pe o rețea de puncte de tranzit, de regulă, castre sau orașe din imperiu, călăreții care transportau mesajele oficiale trebuind să ducă corespondența de la un punct la altul și să o predea următorului călăreț. Inițial, acest serviciu poștal era rezervat doar împăratului, ulterior, ca urmare a abuzurilor funcționarilor din teritoriu care se foloseau de el pentru interes personal, a fost extins funcționarilor din administrația imperiului și, mai apoi, persoanelor particulare.

Dezvoltarea sistemului modern de poștă este atribuită trecerii de la acordurile bilaterale între state la adoptarea unor standarde internaționale, primul pas în acest sens având loc la Conferința de la Berna din data de 15 septembrie 1874. La data de 9 octombrie 1874, a fost semnat Tratatul de la Berna prin care se înființa Uniunea Generală Poștală (ulterior devenită Uniunea Poștală Universală), compusă inițial din 22 de state membre. Principatele Unite ale Moldovei și Țării Românești au aderat la acest tratat la data de 1 iulie 1875. În prezent, Uniunea Poștală Universală are 192 de state membre și servește ca organism internațional de reglementare în domeniul trimiterilor poștale.

Răspândirea posibilității oamenilor obișnuiți de a comunica la distanță prin intermediul corespondenței a dus la posibilitatea comunicării și a mesajelor care nu sunt conforme cu spiritul legii sau care pot servi aflării adevărului într-o cauză penală. Față de metodele primitive

[1] Prezentul titlu a fost publicat în Revista Penalmente Relevant nr. 2/2018, sub denumirea „Unele aspecte privind reținerea, predarea și percheziționarea trimiterilor poștale", pe *www.revista.penalmente.ro*

[2] Uniunea Poștală Universală, istoric, pe *www.upu.int*

de a obține probatoriul într-o cauză penală – constrângerea unei persoane de a recunoaște o faptă prevăzută de legea penală –, percheziționarea corespondenței acesteia prezintă avantajul descoperirii gândurilor persoanei vizate, expuse într-un moment de libertate, și poate servi mai bine la aflarea adevărului. Acest avantaj este unul deosebit, deoarece dovedește existența celui mai important element constitutiv al infracțiunii – vinovăția. În plus, față de mijloacele de obținere a informațiilor mai intruzive și contestate (de pildă, testarea poligraf), corespondența unei persoane va constitui un mijloc de probă greu de combătut, tocmai pentru că el exprimă gândurile persoanei, fără ca aceasta să aibă bănuiala că frazele scrise vor putea fi folosite pentru a o incrimina.

Citirea corespondenței unei persoane reprezintă, în mod neîndoielnic, o intruziune în viața privată a acesteia, la fel de gravă ca folosirea oricărei măsuri de supraveghere tehnică aptă să dezvăluie comunicările unei persoane sau să o surprindă desfășurându-și viața în ipostazele cele mai intime. Chiar dacă vom admite că urmărirea penală ar avea în mod efectiv un caracter secret, iar organele de urmărire penală ar fi de o integritate exemplară și ar respecta pe deplin secretul profesional, citirea corespondenței unei persoane produce o intruziune în viața privată a persoanei indiferent dacă o singură persoană deschide și află conținutul acesteia. În mod neîndoielnic, este o faptă de neiertat citirea corespondenței amoroase a unei domnișoare (sau chiar a unui bărbat, după caz) și nicio trăsătură pozitivă de caracter a persoanei care o citește nu va putea să repare această intruziune. Și dacă vom transpune această problemă în contextul în care diverse scrisori pot ajunge la dosarul cauzei să fie consultate și de alte persoane (părți, subiecți procesuali, avocați), este lesne de văzut cum viața unei persoane poate fi marcată de o astfel de măsură.

Chiar și în cadrul unei familii funcționale și fericite, membrii acesteia au dreptul la viața lor privată, care trebuie ținută secretă de orice persoană, nu pentru a ascunde ceva, ci pentru a putea asigura dezvoltarea personală a fiecăruia și de a menține un climat armonios. Dacă am fi conștienți că suntem urmăriți ori ne-am teme că toate acțiunile noastre vor putea fi disecate ulterior, nu ne-am mai comporta la fel, ceea ce ne va afecta dezvoltarea personală, a gândurilor și a opiniilor noastre politice[1].

Pericolul dezvăluirii unor informații care țin de viața privată a unei persoane a fost îndelung legat de ideea de domiciliu a persoanei, ca urmare a caracterului tradițional al corespondenței private, fiind foarte dificil de pus în aplicare o formă de supraveghere eficientă. Ca atare, până în secolul al XX-lea, problema deschiderii corespondenței se discuta în cadrul percheziției bunurilor unei persoane aflate asupra sau în domiciliul său. Sub acest ultim aspect, dreptul englez a recunoscut, încă de la 1604, că „*domiciliul oricărei persoane este pentru ea propriul său castel și fortăreață*"[2]. Un element esențial care decurge din acest drept asupra domiciliului constă în dreptul oricărei persoane de a decide pe cine primește în sfera sa intimă și ce informații dorește să îi împărtășească[3]. Or, sub acest aspect, considerăm că preceptele enunțate nu se vor aplica numai în cazul domiciliului persoanei, dar și asupra corespondenței sale, prin care aceasta își manifestă personalitatea în mod nerestricționat.

Garantarea vieții private a unei persoane, sub aspectul secretului corespondenței, a fost recunoscută în legislația autohtonă începând cu Constituția Principatelor Unite ale Moldovei și Țării Românești din anul 1866, în care, la art. 25, se prevedea că: „*Secretul scrisorilor și al*

[1] *L.K. Donohue*, The Future of Foreign Intelligence, 2016, p. 172.
[2] *Ibidem*, p. 76.
[3] *Ibidem*, p. 102.

depeșelor telegrafice este neviolabil. Ua lege va determina responsabilitatea agenților guvernului pentru violarea secretului scrisorilor și depeșelor încredințate poștei și telegrafului". Prin Legea telegrafo-poștală din 27 iunie 1871 s-a introdus sancționarea funcționarului care va încălca secretul corespondenței, însă această prevedere cu caracter penal nu rezolva necesitatea unui cadru procedural pentru administrarea probelor în procesul penal.

Ca în cazul dreptului englez și al legiuirilor continentale de la acea vreme, și în dreptul românesc antebelic, problema percheziților și a ridicării corespondenței s-a pus în contextul identificării asupra persoanei cercetate sau în cadrul locuinței sale a *ceva hârtii*, în sensul art. 84 din C.pr.pen. 1864, tocmai cu privire la scrisorile care pot servi aflării adevărului. În această privință, judecătorul de instrucție era abilitat să dispună ridicarea lor[1] de la prevenit. În aceeași perioadă se punea în discuție calitatea pe care o avea funcționarul poștal în reținerea și predarea corespondenței, subliniindu-se că, deși acesta avea calitatea de depozitar al scrisorii (considerată un bun, întocmai ca în dreptul englez[2]) și era ținut să protejeze secretul corespondenței, interesul superior al descoperirii săvârșirii unei infracțiuni va prima și va impune încălcarea lui[3].

Astfel, se permitea agenților statului să procedeze la deschiderea scrisorilor și depeșelor (telegramelor) trimise, evident fiind subînțeles că acești agenți vor avea și dreptul de a intercepta și obține această corespondență prin orice mijloc.

Prin Constituția Regatului României din 1923[4] se stabilea că secretul scrisorilor, telegramelor, dar și al convorbirilor telefonice, era inviolabil. Spre deosebire de legea constituțională anterioară, pentru prima dată se reglementează că se va putea proceda la restrângerea dreptului persoanei în scopul aflării adevărului într-o cauză judiciară. Potrivit art. 27 alin. (2) din Constituția de la 1923: „*o lege specială va stabili cazurile în cari justiția, în interesul instrucțiunii penale, va putea face excepțiune la dispozițiunea de față*". Restrângerea secretului corespondenței se putea face, așa cum am evidențiat deja, doar în cazul în care avem de-a face cu urmărirea penală a unei persoane și numai cu încuviințarea judecătorului de instrucție.

Cu toate acestea, în România, până la adoptarea Codului de procedură penală Carol al II-lea[5], nu a existat o delimitare clară a procedeelor probatorii prin care se putea proceda la predarea și deschiderea corespondenței unei persoane, scrisorile fiind considerate simple înscrisuri care urmau să fie supuse procedurii obișnuite de ridicare (sau percheziție, după caz). În acest sens, doctrina interbelică punea în discuție *sechestrarea* corpurilor delicte, precum și a *obiectelor, efectelor, lucrurilor, hârtiilor, actelor, documentelor, scrisorilor și corespondenței*[6], în fapt considerând că vor fi aplicate regulile privind percheziția.

Abia prin dispozițiile art. 251 și 252 C.pr.pen. Carol al II-lea se instituie o procedură distinctă a obținerii corespondenței unei persoane și întrebuințarea acesteia într-un proces penal.

Conform art. 251 C.pr.pen. Carol al II-lea, „*judecătorul de instrucție este în drept a cere să i se remită de către administrațiile publice sau private telegramele, scrisorile și orice alte lucruri trimise de inculpat sau adresate, sau destinate lui, fie direct, fie pe adresa unui terțiu*". Se poate observa că, pentru prima oară, legiuitorul prevede o metodă specifică pentru ridicarea

[1] *I. Tanoviceanu*, Curs de procedură penală română, Ed. Atelierele Grafice SOCEC & Co., București, 1913, p. 251.

[2] *L.K. Donohue*, The Future of Foreign Intelligence, 2016, p. 80.

[3] *I. Tanoviceanu*, op. cit., p. 253.

[4] Constituția României din 1923 (M. Of. nr. 282 din 29 martie 1923).

[5] Codul de procedură penală din 17 martie 1936 Carol al II-lea (M. Of. nr. 66 din 19 martie 1936).

[6] *Tr. Pop*, op. cit., p. 463.

corespondenței, cu particularitatea că, încă de la început, a introdus implementarea față de persoană a măsurii, și nu față de un obiect determinat. Aceasta o deosebește de alte forme de percheziție care au în vedere un obiect, un lucru sau o urmă digitală (în cazul percheziției informatice).

Legiuitorul avea în trecut un respect mai mare asupra vieții private a individului, în condițiile în care se sublinia că numai judecătorul de instrucție era îndreptățit să deschidă și să afle conținutul corespondenței reținute și predate, iar, în situația în care trimiterea era destinată inculpatului, dar era trimisă pe numele unui terț, deschiderea trimiterii se putea face numai în fața terțului[1]. Această abordare a trebuit abandonată, deoarece se punea în pericol caracterul secret al desfășurării actelor de urmărire penală, fiind evident că un terț căruia i se va trimite o scrisoare sau o altă trimitere poștală va avea deja o legătură preexistentă cu persoana care face obiectul unei cercetări penale și ar putea dezvălui cel puțin faptul că i-a fost deschisă corespondența.

Codul de procedură penală din 1968[2], în forma sa inițială, a înlăturat rolul judecătorului de instrucție (instituție desființată prin înglobarea atribuțiilor sale în cele ale procurorului) din încuviințarea măsurii, instituind că organul de cercetare penală putea dispune *reținerea și predarea corespondenței și a obiectelor*. Cu toate acestea, o asemenea măsură trebuia să fie autorizată de către procuror. Totodată, prin art. 98 C.pr.pen. 1968 se introducea posibilitatea folosirii acestui procedeu probatoriu și în cursul judecății, posibilitate care nu a mai fost inclusă în prezentul Cod, întrucât o asemenea măsură restrictivă de drepturi și libertăți nu se justifica în cursul judecății, lipsind elementul de surpriză necesar. Cu alte cuvinte, prin trimiterea în judecată a unei persoane scade covârșitor posibilitatea ca aceasta să comunice în scris aspecte legate de fapta de care este acuzată, care să contribuie la condamnarea sa. Corelativ, reținerea și predarea corespondenței unei persoane trimise în judecată pentru săvârșirea unei infracțiuni nu se poate folosi ca procedeu nici în dovedirea nevinovăției sale, orice corespondență (în special dacă provine de la inculpat) fiind cel mai probabil preconstituită *pro causa*. Totodată, dacă această corespondență cu caracter exonerator ar exista, interesul inculpatului ar fi să o prezinte voluntar instanței. Dintr-o altă perspectivă, prin pronunțarea asupra reținerii și predării corespondenței inculpatului în faza de judecată s-ar ajunge automat la incompatibilitatea judecătorului (sau judecătorilor), întrucât s-ar pronunța asupra restrângerii dreptului inculpatului cu scopul de a strânge probe strict în defavoarea sa. Lipsa de imparțialitate ar fi fost incidentă și din cauză că, spre deosebire de un înscris, corespondența putea numai să fie una viitoare, astfel că este lesne de probat că instanța ar avea o opinie formată cu privire la producerea în viitor a unor probe în defavoarea inculpatului, pe care ar vrea să le administreze. În cazul corespondenței reținute de la alte persoane, procedeul era inutil, întrucât instanța ar fi putut dispune efectuarea unei percheziții domiciliare prin care să se ridice trimiterile poștale, asemenea oricărei corespondențe.

---

[1] Art. 252 din C.pr.pen. Carol al II-lea stipula:

„(1) Numai judecătorul de instrucție ia cunoștința de conținutul scrisorilor și telegramelor ce i se remit. El reține pe cele necesare instrucției și restitue inculpatului sau destinatarului pe cele care nu ar fi de folos.

(2) Scrisorile și telegramele adresate unui terțiu nu pot fi deschise decât în prezența acestuia, după ce a fost legalmente încunoștințat.

(3) În cazul când telegramele și scrisorile ridicate sînt necesare instrucției, conținutul lor se aduce la cunoștința inculpatului sau destinatarului, afară de cazul cînd această încunoștiințare ar fi contrară interesului instrucției".

[2] Publicat în B. Of. nr. 145-146 din 12 noiembrie 1968.

În prezent, principiul respectării vieții intime a cetățeanului este reglementat prin art. 26 alin. (1) din Constituție, însă legiuitorul a considerat că se impune dedicarea unui articol separat pentru apărarea secretului corespondenței. Potrivit art. 28 din Constituție, „*secretul scrisorilor, al telegramelor, al altor trimiteri poștale, al convorbirilor telefonice și al celorlalte mijloace legale de comunicare este inviolabil*".

Până în anul 2003, nu s-a conferit un grad de protecție cuvenit secretului corespondenței și vieții private prin raportare la procedura prin care se încuviința măsura, până când, prin Legea nr. 281/2003 privind modificarea și completarea Codului de procedură penală și a unor legi speciale[1], s-a trecut la încuviințarea măsurii de către instanță. Potrivit art. 98 C.pr.pen. 1968, procurorul propunea instanței reținerea, predarea corespondenței și a obiectelor conform aceleiași proceduri ca pentru încuviințarea interceptărilor și înregistrărilor audiovideo și cu respectarea acelorași condiții. Considerăm că acest moment este deosebit de important, deoarece s-a revenit la o stare de normalitate din punctul de vedere al atribuțiilor funcționale ale organelor judiciare, care urma să se desăvârșească prin Codul de procedură penală actual, prin crearea instituției judecătorului de drepturi și libertăți.

În opinia noastră, din comoditate, legiuitorul a prevăzut, în anul 2003, o procedură comună cu interceptările și înregistrările, fapt care, în prezent, a condus la o greșită considerare a procedeului probatoriu ca fiind o metodă specială de cercetare.

În scopul unei mai bune protejări a secretului corespondenței, s-a urmărit ca, prin Codul de procedură penală din 2010[2], să se mențină caracteristicile protecției oferite de Codul de procedură penală privind autorizarea unor procedee probatorii excepționale prin care să poată fi obținute probe. Aici ne referim la procedura de încuviințare a măsurii în Codul de procedură penală, care impune aplicarea condițiilor și procedurii specifice încuviințării supravegherii tehnice. Cu toate că vom trata în secțiunile următoare modul în care se autorizează procedeul probatoriu, apreciem că, dintr-o similitudine în procedură, legiuitorul a reconsiderat natura măsurii.

Această modificare de optică a legiuitorului este bizară, în contextul în care, prin folosirea mai rară a trimiterilor poștale pentru împărtășirea gândurilor (nu și a bunurilor, în special cele de consum), măsura analizată reprezintă o modalitate de strângere a probelor mai puțin aptă să contribuie la aflarea adevărului ca urmare a perfecționării unor noi metode de comunicații. De altfel, aceasta explică și rara ei folosire în practică.

În mod firesc, orice modificare legislativă este specifică momentului istoric în care se află o societate. În cazul Codului de procedură din 1968, acesta era cel al trecerii de la un sistem axat pe respectarea drepturilor individului la unul axat pe binele social și menținerea ordinii și siguranței publice în detrimentul libertăților persoanei.

Paradoxal, ușurința cu care se emit mandatele de supraveghere tehnică în prezent nu face mai puțin invaziv setul de metode speciale de supraveghere sau cercetare prevăzut de Codul de procedură penal actual, ci, din contră, duce la posibilitatea controlării în cel mai mic detaliu al vieții persoanei. În ceea ce privește rezultatul, un stat totalitar nu diferă față de un stat democratic liberal, dus în forma sa cea mai extremă, precum modelul S.U.A., unde dreptul la viață privată și dreptul la demnitate sunt puse pe un plan secundar față de libertatea de exprimare[3]. Și tocmai această libertate de exprimare dusă la paroxism (încurajarea distribuirii inclusiv a elementelor banale din viața unei persoane în mediul online), coroborată cu

[1] Publicată în M. Of. nr. 468 din 1 iulie 2003.

[2] Legea nr. 135/2010 privind Codul de procedură penală (M. Of. nr. 486 din 15 iulie 2010).

[3] *R.J. Krotoszynski, Jr.*, Privacy Revisited, 2016, p. 36.

posibilitatea colectării automatizate de informații (Big Data) asupra unei singure persoane, permite profilajul deosebit de precis al acesteia și este mai invazivă decât mijlocul tradițional al reținerii corespondenței unei persoane[1]. Dacă, prin mijloacele tradiționale, putem cunoaște, cel mult, gândurile unei persoane la un moment dat, prin metode moderne, putem cunoaște aspecte despre viața unei persoane de care nici aceasta nu este conștientă, putem să prezicem cum se va comporta într-o anumită împrejurare, cum își petrece timpul și, inclusiv, ce a făcut în trecut, cu cine s-a asociat și care este cercul său de prieteni.

Credem că legiuitorul va trebui în viitor să se concentreze pe realitățile lumii digitale, în care informațiile utile cauzei nu sunt date numai de conținutul comunicărilor, ci mai ales de modul în care se desfășoară, regularitatea lor și cu cine se desfășoară. Analiza apelurilor efectuate de o persoană, fără analiza conținutului, ori a site-urilor frecventate ne poate da detalii mult mai invazive în viața unei persoane. Un exemplu poate fi surprinderea cronologică a apelurilor desfășurate, fără a se cunoaște conținutul convorbirilor: o femeie sună și vorbește îndelung la telefon cu sora ei; după două zile, sună la o clinică specializată în avorturi; după o săptămână, sună la acea clinică de mai multe ori; apoi, la o altă săptămână, mai sună o singură dată, fără ca alte apeluri să fie efectuate la acea clinică. În același fel, să presupunem că un bărbat sună la un spital și vorbește îndelung cu un medic cardiolog; apoi, apelează un laborator specializat în aparate medicale; apoi, primește apeluri de la o farmacie și, ulterior, apelează un număr hotline de monitorizare permanentă a funcționării unui aparat de monitorizare a aritmiei. Toate aceste exemple fac parte dintr-un studiu desfășurat de cercetători în domeniul informatic din cadrul Universității din Stanford[2] și reflectă în mod îngrijorător noile amenințări la viața privată, pe care legiuitorul român le ignoră în continuare. În măsura în care s-ar implementa un sistem de înregistrare obligatorie a tuturor trimiterilor poștale, cu detalii privind expeditorul și destinatarul, credem că, și fără să aflăm conținutul corespondenței, se vor putea strânge date cu privire la obiceiurile persoanei, care să stea la baza încuviințării unor alte măsuri de supraveghere sau cercetare mai restrictive.

Deși, într-o societate democratică, în general, ocrotirea libertății de exprimare, a vieții private a individului și a secretului corespondenței este regula, protejarea acestor drepturi nu este una absolută și poate fi restrânsă pentru a garanta atât drepturile celor din jur, cât și menținerea ordinii publice. Față de posibilitățile facile de a restrânge viața privată a persoanei într-un mod cu mult mai brutal ca în trecut, reținerea, predarea și percheziționarea trimiterilor poștale reprezintă un procedeu probatoriu clasic, care ar trebui utilizat ca un procedeu subsidiar unor alte măsuri de supraveghere sau cercetare mai invazive.

[1] *Ibidem*, p. 37; *L.K. Donohue*, The Future of Foreign Intelligence, 2016, p. 45.

[2] *P. Mutchler, J. Mayer*, MetaPhone: The Sensitivity of Telephone Metadata, publicat pe Web Policy, 12 martie 2014, disponibil pe *webpolicy.org*

Capitolul II
Noțiunea de „trimitere poștală" și reglementarea activității de poștă în România

Stabilirea obiectului măsurii de cercetare tratate în prezentul capitol se va face prin intermediul legislației speciale extrapenale din domeniul serviciilor poștale, în condițiile în care legiuitorul nu a conferit prin Codul de procedură penală un sens propriu al noțiunii de „trimitere poștală".

În cazul unei analize superficiale, având ca fundament numai Codul de procedură penală, vom putea constata că obiectul măsurii îl reprezintă nu numai trimiterile poștale, ci și scrisorile și obiectele trimise de o persoană. Aparent, ar trebui să existe un element de diferențiere între scrisori, obiecte și trimiteri poștale, ele să reprezinte categorii diferite. Însă, la o analiză mai atentă, vom semnala că legiuitorul suferă de o eroare de logică, deoarece enumeră două elemente – scrisori și obiecte – care sunt incluse în categoria mai generală a trimiterilor poștale.

Comparativ cu legislația procesuală penală anterioară, legislația actuală constituie un regres în stabilirea cu claritate a obiectului măsurii de cercetare. Conform art. 98 alin. (1) C.pr.pen. 1968, republicat[1], obiectul procedeului probatoriu al *reținerii și predării corespondenței și a obiectelor* era reprezentat de *scrisorile, telegramele și oricare altă corespondență ori a obiectelor trimise sau primite*, situație în care observăm că legiuitorul a folosit exemplificativ noțiunile de „scrisori" și „telegrame" alături de menționarea categoriei mai generale a corespondenței, precum și de tratarea separată a coletelor poștale (obiecte). Este de neînțeles de ce legiuitorul actual nu a menținut modelul Codului de procedură penală din 1968, *de lege ferenda*, impunându-se reformularea obiectului măsurii în sensul înlăturării „scrisorilor" și „obiectelor" din enumerare ca fiind superfluă.

Revenind la categoria amintită mai sus, noțiunea de „trimitere poștală" este reglementată prin O.U.G. nr. 13/2013 privind serviciile poștale[2], în care, la art. 2 pct. 13, este definită ca: „*bun adresat, aflat în formă finală în care urmează să fie transportat și livrat la adresa indicată de expeditor pe trimiterea în sine, pe ambalaj sau într-o listă de distribuție. Pe lângă trimiterile de corespondență, în această categorie sunt incluse, de exemplu, imprimatele, sacii «M», pachetele mici, coletele poștale care conțin bunuri cu sau fără valoare comercială și mandatele poștale pe suport hârtie. În această categorie nu sunt incluse trimiterile hibrid*".

În mod evident, noțiunea de „trimitere poștală" acoperă întreaga plajă de trimiteri la care se poate adresa măsura specială de cercetare, incluzând și termenul de „corespondență" la care făcea referire Codul de procedură penală anterior. Observăm că, din punctul de vedere al legii supreme, Constituția României include în cadrul noțiunii de „corespondență" orice fel de trimitere poștală, alături de convorbirile personale și celelalte mijloace legale de comunicare.

Ca atare, termenul de „corespondență", în sensul său constituțional, este mai larg decât cel prevăzut în lege, în care, la art. 2 pct. 11 din O.U.G. nr. 13/2013, „trimiterea de corespondență" este definită ca o „*comunicare în formă scrisă pe orice fel de suport fizic, care urmează să fie transportată și livrată la adresa indicată de expeditor chiar pe trimiterea în sine sau pe ambalajul acesteia. Cărțile, cataloagele, ziarele, periodicele nu sunt considerate trimiteri de corespondență*".

[1] Republicat în M. Of. nr. 78 din 30 aprilie 1997.

[2] O.U.G. nr. 13 din 6 martie 2013 privind serviciile poștale (M. Of. nr. 139 din 15 martie 2013).

Din punct de vedere istoric, observăm că termenul de „corespondență" a fost folosit numai în legătură cu comunicările în formă scrisă, convorbirile telefonice și celelalte mijloace de comunicare legale, fiind, în opinia noastră, asimilate corespondenței. În același sens, amintim că, prin Constituția Republicii Socialiste România din 1965[1], art. 33 din legea fundamentală garanta *secretul corespondenței* și al *convorbirilor telefonice*.

Distincția dintre corespondență și alte mijloace legale de comunicație a fost avută în vedere și în structura Codului de procedură penală în vigoare, în care sunt tratate distinct acele procedee probatorii care afectează comunicările persoanei prin alte căi decât forma scrisă. Ne referim aici în special la supravegherea tehnică prin interceptarea comunicațiilor ori a oricărui tip de comunicare la distanță, însă este posibilă și, uneori, necesară folosirea concertată și a accesului la un sistem informatic pentru realizarea acestei interceptări.

Odată lămurit termenul de „corespondență", pentru înțelegerea deplină a măsurii speciale de cercetare, trebuie să avem în vedere cui i se poate adresa aceasta, cu alte cuvinte, cine poate fi obligat să își dea concursul în executarea măsurii. Potrivit art. 147 alin. (5) C.pr.pen., își vor da concursul *unitățile poștale* sau de *transport*, precum și *orice persoană fizică sau juridică* implicată în activități de transport sau transfer de informații.

Legislația procesuală penală diferă semnificativ față de cea din domeniul poștal, unde fundamentul este serviciul poștal, orice persoană autorizată pentru a desfășura astfel de activități – fie persoană fizică sau juridică – fiind denumită „furnizor de servicii poștale". Codul de procedură penală nu condiționează expres ca persoana fizică sau juridică să fie autorizată legal să desfășoare serviciile poștale, însă această caracteristică se va deduce implicit, deoarece nu putem concepe obligarea unei persoane să ajute organele de urmărire penală prin desfășurarea unei activități lucrative în afara legii[2].

Credem că legiuitorul trebuia să aibă în vedere, odată cu intrarea în vigoare a Codului de procedură penală, diferența terminologică și să o aducă la standardul din domeniul serviciilor poștale. Formularea generică folosită de legislația specială este de „servicii poștale", care, potrivit art. 2 pct. 1 din O.U.G. nr. 13/2003 privind serviciile poștale, constau în *colectarea, sortarea, transportul și livrarea trimiterilor poștale*. Vom detalia semnificația fiecăreia dintre aceste etape în partea dedicată punerii în executare a măsurii.

Furnizorul de servicii poștale poate fi de două tipuri: furnizor de serviciu universal și alți furnizori de servicii poștale. Specificul legislației poștale este că, deși este posibil ca orice persoană să fie autorizată să realizeze servicii poștale, numai o singură persoană juridică poate să dețină calitatea de furnizor de serviciu universal. În prezent, furnizorul de serviciu universal este Compania Națională Poșta Română S.A. (în continuare, C.N.P.R.) desemnat în baza Deciziei nr. 1158/2013 a Președintelui Autorității Naționale pentru Administrare și Reglementare în Comunicații (în continuare, A.N.C.O.M.).

Furnizorul de serviciu universal are un rol deosebit în asigurarea comunicației pentru cetățeni printr-un set de servicii de bază care intră în cadrul serviciului universal[3], prestate

[1] Constituția Republicii Socialiste România din anul 1965 (republicată în B. Of. nr. 65 din 29 octombrie 1986).

[2] În condițiile în care o persoană desfășoară servicii poștale fără autorizație, nu va fi incidentă numai legislația din domeniul poștal, ci și cea penală, întrucât veniturile obținute din această activitate nu ar putea fi înregistrate în mod legal în contabilitatea societății ori persoanei fizice.

[3] Potrivit art. 1 alin. (2) din Decizia Președintelui A.N.C.O.M. nr. 1158/2013: „CNPR are obligația să furnizeze, pe întregul teritoriu al României, în condițiile stabilite de legislația din domeniul serviciilor poștale și de prezenta decizie, următoarele servicii poștale din sfera serviciului universal:

în condiții de continuitate (5 zile pe săptămână), în mod neîntrerupt (cu excepția cazurilor de forță majoră), în fiecare localitate de pe teritoriul României, în condiții de celeritate (85% dintre trimiterile poștale trebuind livrate în cel mult o zi lucrătoare[1]), 97% dintre trimiterile poștale trebuind livrate în cel mult 3 zile lucrătoare[2]), cu asigurarea punctelor de acces permanente (cutii poștale sau unități poștale) și la tarife accesibile cetățenilor[3] (ținând seama de costuri și avându-se în vedere dreptul de acces la serviciul universal). Cu alte cuvinte, furnizorul de serviciu universal are rolul de a fi fundamentul atât al comunicațiilor scrise, cât și al transportului de obiecte de dimensiuni reduse pe tot teritoriul țării. În calitate de furnizor de serviciu universal, C.N.P.R. poate încheia convenții cu alte asemenea entități internaționale. Subliniem că acest furnizor va fi cel mai sever controlat de către stat, mai ales sub aspectul prețurilor, pentru că, deși trăim într-o societate democratică și tindem către o economie de piață, serviciile poștale trebuie să fie accesibile și celor mai săraci cetățeni, întrucât, prin serviciul poștal universal, se poate asigura libera exercitare a unor importante drepturi ale cetățenilor, mai ales dreptul de petiționare și liberul acces la justiție.

Ceilalți furnizori de servicii poștale sunt liberi să își stabilească propriile seturi de servicii pe care le vor furniza, fără a fi îngrădiți de necesitatea unei rețele publice la nivel național, de timpi de livrare mai scurți sau de limitarea prețurilor practicate. Cei mai importanți furnizori de servicii poștale din România sunt societățile comerciale specializate în curierat – Fan Courier, UrgentCargus, Sameday, Nemo Courier etc. Acești furnizori au apărut ca urmare a lipsei de flexibilitate a C.N.P.R. de a furniza servicii de livrare bunuri pentru consumatori în

---

a) colectarea, sortarea, transportul și livrarea trimiterilor poștale interne și internaționale, în greutate de până la 2 kg (inclusiv), având ca obiect:

1. trimiteri de corespondență, cu excepția trimiterilor de corespondență în număr mare;

2. imprimate, cu excepția imprimatelor în număr mare;

3. pachete mici, astfel cum acestea sunt prevăzute în Convenția Poștală Universală și Regulamentul poștei de scrisori, cu excepția pachetelor mici în număr mare;

b) colectarea, sortarea, transportul și livrarea coletelor poștale interne și internaționale, în greutate de până la 10 kg (inclusiv), cu excepția coletelor în număr mare;

c) distribuirea coletelor poștale cu limite de greutate între 10 kg și 20 kg (inclusiv) expediate din afara teritoriului României către o adresă aflată pe teritoriul acesteia;

d) serviciul de trimitere recomandată având ca obiect trimiteri poștale interne și internaționale în greutate de până la 2 kg (inclusiv) prevăzute la lit. a);

e) serviciul de trimitere cu valoare declarată având ca obiect:

1. trimiteri poștale interne și internaționale în greutate de până la 2 kg (inclusiv) prevăzute la lit. a);

2. colete poștale interne și internaționale în greutate de până la 10 kg (inclusiv), cu excepția coletelor în număr mare;

3. colete poștale cu limite de greutate între 10 și 20 kg (inclusiv) expediate din afara teritoriului României către o adresă aflată pe teritoriul acesteia;

f) colectarea, sortarea, transportul și livrarea cecogramelor interne și internaționale”.

[1] Conform art. 30 alin. (2) din O.U.G. nr. 13/2013: „Furnizorul de serviciu universal are obligația de a respecta cumulativ următoarele condiții: a) de a asigura livrarea la destinatari, în 3 zile lucrătoare de la data depunerii trimiterilor de corespondență intracomunitare din sfera serviciului universal din cea mai rapidă categorie standard la punctele de acces, a 85% din aceste trimiteri”.

[2] Conform art. 30 alin. (2) din O.U.G. nr. 13/2013: „Furnizorul de serviciu universal are obligația de a respecta cumulativ următoarele condiții: (...) b) de a asigura livrarea la destinatari, în 5 zile lucrătoare de la data depunerii trimiterilor de corespondență intracomunitare din sfera serviciului universal din cea mai rapidă categorie standard la punctele de acces, a 97% din aceste trimiteri”.

[3] Conform art. 8 alin. (1) din O.U.G. nr. 13/2013: „Dreptul de acces la serviciul universal reprezintă dreptul de a beneficia de furnizarea permanentă a serviciilor poștale incluse în sfera serviciului universal, la un anumit nivel de calitate, în orice punct de pe teritoriul României, la tarife accesibile tuturor utilizatorilor”.

condiții de comoditate pentru destinatar. Într-o societate consumeristă, este foarte important ca bunul vândut să fie preluat cât mai repede de la vânzător fără ca acesta să trebuiască să își asigure propria infrastructură de transport (autovehicule specializate, personal) pentru a duce marfa la cea mai apropiată unitate poștală. În același timp, și cumpărătorul va fi avantajat să i se livreze acasă produsul, decât să trebuiască să îl preia de la o unitate poștală.

Deși puțin probabil, atât legea specială privind serviciile poștale, cât și Codul de procedură penală admit posibilitatea ca o persoană fizică să fie autorizată în domeniul serviciilor poștale, caz în care și aceasta poate fi obligată prin mandatul emis de judecătorul de drepturi și libertăți să rețină și să predea corespondența unei persoane. În condițiile în care traficul devine din ce în ce mai intens în marile orașe ale țării, nu trebuie excluse serviciile de curierat desfășurate de o persoană fizică cu condiție fizică bună, care să se deplaseze pe bicicletă pentru a livra mai rapid scrisori sau pachete mici pentru diverse firme.

Capitolul III
Corelația dintre reținerea, predarea și percheziționarea trimiterilor poștale și alte procedee probatorii

Noțiunea de „corespondență" trebuie să fie înțeleasă și în contextul altor procedee probatorii prevăzute de Codul de procedură penală, prin care se pot obține obiecte sau înscrisuri. În această privință, așa cum vom vedea, metoda specială de cercetare se aseamănă cu percheziția domiciliară sub aspectul gravității afectării drepturilor persoanei, dar și în privința modalității de punere în executare. Aceeași rațiune o diferențiază de procedura predării obiectelor, înscrisurilor sau datelor informatice prevăzută de art. 170 C.pr.pen., procedeu probatoriu care nu afectează într-o asemenea măsură drepturile persoanei.

Măsura de cercetare are în vedere orice trimitere poștală, nu numai scrisorile, situație care impune detalierea posibilității folosirii alternative a procedurii ridicării de obiecte, înscrisuri sau date informatice. În cazul obiectelor transmise prin servicii poștale – colete sau pachete mici – care conțin un obiect, apreciem că, odată deschise, conținutul acestora – un obiect – va putea fi supus procedeului probatoriu prevăzut de art. 170 C.pr.pen. Secretul corespondenței apără, în principal, trimiterea poștală în sensul de capsulă sau recipient care poate purta în interiorul său orice bun sau mesaj. Această capsulă este protejată sub aspectul integrității sale și a secretului conținutului său pe tot timpul cât aceasta se află în circuitul său, dar și după ce a fost primită de destinatar. Textul art. 147 alin. (1) C.pr.pen. nu impune condiția ca trimiterile poștale să fie în tranzit, ci acestea pot fi deja primite de destinatar.

În cazul obiectelor primite prin serviciile poștale, se va putea dispune predarea în temeiul art. 170 C.pr.pen., deoarece procedeul probatoriu impune identificarea obiectului care urmează a fi predat, astfel că nu se mai discută despre respectarea secretului corespondenței cât timp organele de urmărire penală cunosc conținutul coletului și formulează o ordonanță prin care solicită acest bun. Nu va fi legală o măsură prin care obiectul supus predării este definit ca un colet sau pachet mic primit de o anumită persoană, întrucât s-ar eluda în mod nelegal procedura prevăzută de art. 147 C.pr.pen. și s-ar încălca secretul corespondenței. Or, așa cum am arătat deja, Codul de procedură penală conferă o protecție sporită acestui drept prin abilitarea judecătorului de drepturi și libertăți să dispună asupra măsurii. Pe de altă parte, în cazul procedurii predării de obiecte, înscrisuri sau date informatice, organul de urmărire penală (sau instanța) va fi în măsură să dispună asupra măsurii, deoarece este vizată doar proprietatea în cazul obiectelor.

Toate cele arătate mai sus sunt relevante în cazul coletelor și pachetelor mici deja primite, întrucât, în cazul în care vorbim de corespondență care urmează să fie trimisă ori este în circuitul poștal, se va putea utiliza numai procedura reținerii, predării și percheziționării trimiterilor poștale.

În cazul unor scrisori – „trimiteri de corespondență" în sensul art. 2 pct. 11 din O.U.G. nr. 13/2013 privind serviciile poștale –, aparent, s-ar putea ajunge la concluzia că orice scrisoare primită și deschisă este o specie de înscris și să cadă sub incidența dispozițiilor art. 170 C.pr.pen., fiind posibil ca organul de urmărire penală (sau instanța) să dispună predarea acesteia. Spre deosebire de coletele și pachetele mici care pot conține obiecte, trimiterile de corespondență vor conține un mesaj scris al cărui conținut nu este, de regulă, cunoscut de

organele de urmărire penală. În măsura în care ar cunoaște că o persoană deține o scrisoare care ar putea constitui un mijloc de probă în procesul penal, organul de urmărire penală ar trebui să individualizeze scrisoarea în ordonanță pentru a fi considerată ca înscris. În cazul trimiterilor de corespondență, nu este posibil din punct de vedere lingvistic să se găsească o formulă prin care organul de urmărire penală să se refere la o scrisoare decât ca „scrisoare", astfel că nu poate fi întrebuințat procedeul prevăzut de art. 170 C.pr.pen., deoarece nelegalitatea lui ar fi una manifestă.

Alături de problema semantică, chiar dacă, printr-o situație specială, organul de urmărire penală ar avea o copie a scrisorii primite de suspect, inculpat sau terț, tot nu este posibilă întrebuințarea procedeului probatoriu prevăzut de art. 170 C.pr.pen., deoarece ar reprezenta o încălcare ilicită a secretului corespondenței pentru care organul de urmărire penală nu are o încuviințare a judecătorului de drepturi și libertăți. Încălcarea secretului corespondenței va produce efecte asupra persoanei din momentul în care va fi obligată să predea scrisorile sale, indiferent dacă procurorul va fi cunoscut conținutul mai înainte, deoarece, din perspectiva persoanei, situația va fi egală și vătămarea se va produce.

Așa cum s-a arătat în doctrină, funcția de instrucție deținută de judecătorul de instrucție din perioada interbelică s-a transformat într-o formă de instrucție modernă prin judecătorul de drepturi și libertăți, care se va pronunța asupra actelor care restrâng drepturile și libertățile fundamentale ale persoanei[1].

Procedura prevăzută de art. 147 C.pr.pen. pune în valoare rolul judecătorului de drepturi și libertăți de a analiza proporționalitatea măsurii de cercetare, de a pune în balanță importanța probelor, necesitatea administrării lor, gravitatea faptei cercetate cu severitatea restrângerii drepturilor fundamentale ale persoanei. Nu numai că judecătorul de drepturi și libertăți are o altă poziție față de urmărirea penală decât organele de urmărire penală, dar și procedurii predării obiectelor, înscrisurilor sau a datelor informatice îi lipsește cu desăvârșire analiza de necesitate, proporționalitate și subsidiaritate a procedeului probatoriu, care este obligatorie în cazul reținerii, predării și percheziționării trimiterilor poștale.

Cu toate acestea, prin predarea obiectelor, înscrisurilor sau a datelor informatice se pot afla informații despre trimiterile poștale ale unei persoane, în afara conținutului acestora. Ne referim aici la „metadate" (în sens general), adică acele date informatice referitoare la transmiterea unor informații, cu mențiunea că metadatele acestea se referă la o transmitere a corespondenței unei persoane. Anumite tipuri de trimiteri poștale presupun înregistrarea lor la unitatea poștală de la care se face trimiterea – coletele, scrisorile recomandate, scrisorile transmise prin PrioriPost, scrisorile sau pachetele transmise prin curieri –, ceea ce generează informații despre acea trimitere, precum: data prezentării, expeditorul, destinatarul, tipul trimiterii, greutatea și data la care a fost primită trimiterea. În cazul în care se dorește probarea unor trimiteri anterioare sau a descoperirii persoanelor la care au fost trimise anumite scrisori sau colete, organele de urmărire penală nu sunt obligate să obțină un mandat, ele putând solicita direct furnizorului de servicii poștale date informatice relevante, potrivit art. 170 alin. (2) lit. a) C.pr.pen. Considerăm că acest procedeu își are relevanța atunci când se transmit colete conținând obiecte interzise prin intermediul furnizorilor de servicii poștale, organele de urmărire penală putând descoperi atât furnizorii persoanei cercetate, cât și potențialii clienți. În acest sens, în S.U.A., F.B.I. are posibilitatea de a verifica existența și traseul oricărei trimiteri

[1] *M. Udroiu (coord.)*, Codul de procedură penală, 2017, p. 13.

poștale, întrucât plicul în care se află aceasta nu este protejat de al patrulea amendament la Constituția S.U.A.[1].

În privința corelației cu percheziția domiciliară, reținerea, predarea și percheziționarea corespondenței se aseamănă foarte mult la nivelul severității restrângerii drepturilor și libertăților fundamentale ale persoanei. Procedura de încuviințare a percheziției domiciliare prezintă similarități sub aspectul condițiilor care vor trebui să fie avute în vedere de judecătorul de drepturi și libertăți, fapt pentru care considerăm că, dacă se va proceda la efectuarea unei percheziții domiciliare, organele de urmărire penală vor fi îndreptățite să ridice toată corespondența descoperită la persoana percheziționată, să o deschidă și să rețină toate trimiterile poștale care ar putea servi ca mijloace de probă în procesul penal.

Motivăm acest lucru prin prisma identității de organ judiciar care se pronunță asupra măsurii – judecătorul de drepturi și libertăți, prin identitatea condițiilor de necesitate, proporționalitate și subsidiaritate, precum și prin previzibilitatea descoperirii de corespondență în cursul efectuării unei percheziții domiciliare.

[1] *B. Snider*, Can police read or search through your mail?, publicat la data de 16 aprilie 2014, pe *blogs.findlaw.com*

Capitolul IV
Natura măsurii

În Codul de procedură penală, reținerea, predarea și percheziționarea trimiterilor poștale este prevăzută în Capitolul IV al Titlului IV, denumit „Metode speciale de supraveghere sau cercetare", astfel că legiuitorul a considerat că acest procedeu probatoriu este o specie de astfel de măsură.

Specificul acestor procedee probatorii este dependența lor de autoritatea statului, manifestată prin restrângerea drepturilor persoanei față de care se dispune folosirea metodelor speciale de supraveghere. Considerăm că aceste procedee probatorii sunt cele mai restrictive cu privire la viața privată a individului, motiv pentru care folosirea lor trebuie să fie văzută ca o *ultima ratio*, iar nu ca un mod comod de realizare a urmăririi penale.

Prin dispozițiile art. 138 alin. (13) C.pr.pen. se arată că vor constitui măsuri de supraveghere tehnică interceptarea comunicațiilor ori a oricărui tip de comunicare la distanță, accesul la un sistem informatic, supravegherea video, audio sau prin fotografiere și localizarea sau urmărirea prin mijloace tehnice. Prin urmare, legiuitorul a considerat că procedeul probatoriu în discuție nu va putea fi încadrat ca o metodă specială de supraveghere, ci va constitui o măsură specială de cercetare. Aceasta constituie o schimbare de viziune din partea legiuitorului, care a modificat, față de Codul de procedură penală din 1968, încadrarea acestui procedeu probatoriu într-o categorie mai largă. Anterior, legiuitorul considera că reținerea, predarea și percheziționarea trimiterilor poștale era o formă particulară de percheziție, și nu o metodă specială de supraveghere sau cercetare, deși era supusă aceleiași proceduri de încuviințare.

În opinia noastră, legiuitorul a greșit prin includerea reținerii, predării și percheziționării trimiterilor poștale în cadrul măsurilor speciale de cercetare, întrucât măsura are similarități mai mari cu formele de percheziție, în special cu percheziția domiciliară. În stabilirea naturii măsurii, nu vom ține seama de procedura prin care aceasta este încuviințată, întrucât nu are semnificație asupra aplicării practice a sa. Așa cum am arătat deja, de-a lungul timpului, legiuitorul și-a schimbat optica privind organul judiciar care dispunea asupra măsurii, dar această împrejurare nu a dus la modificarea locului în Cod a măsurii.

Pentru stabilirea naturii măsurii, va trebui să avem în vedere modalitatea în care se va pune în executare măsura, altfel spus, cum se va realiza în mod concret procedeul probatoriu. Dacă pentru măsurile de supraveghere tehnică intervine un element tehnologic care restrânge foarte mult viața privată a unei persoane, în cazul reținerii, predării și percheziționării trimiterilor poștale, aceasta are un caracter oarecum mai restrâns, deoarece presupune ca o persoană să se manifeste într-un mod tradițional – în scris. Ca atare, nu vom avea un element de noutate care să presupună tehnologii avansate sau folosirea unor tehnici aparte (precum utilizarea investigatorilor sub acoperire). În realitate, măsura de cercetare analizată pare banală, deoarece presupune obținerea corespondenței prin furnizorul de servicii poștale (ori orice altă persoană fizică sau juridică autorizată în domeniul poștal) și deschiderea acesteia pentru a-i afla conținutul. Nu este necesară implicarea unor organe specializate ale statului care să își ofere concursul tehnic, ca în situația interceptării comunicațiilor ori a oricărui tip de comunicare la distanță.

O formă evoluată a acestei măsuri o reprezintă livrarea supravegheată care reprezintă mai mult decât o percheziție, anume urmărirea unui transport de către organele de urmărire penală, inclusiv transfrontalier.

Credem că denumirea aleasă de legiuitor pentru această măsură de cercetare este criticabilă ca urmare a caracterului prea detaliat al enumerării operațiunilor care vor fi efectuate în detrimentul elementului esențial: percheziționarea trimiterilor poștale. În cazul oricărui procedeu probatoriu, organele de urmărire penală vor trebui să realizeze acte prin care să pregătească logistic desfășurarea procedeului. Așa cum vom vedea, reținerea și predarea corespondenței sunt acțiuni simple care nu sunt realizate de organele de urmărire penală și nu reprezintă o atingere veritabilă la secretul corespondenței. În schimb, acțiunea de percheziționare se poate realiza numai de către organele de urmărire penală și, prin aceasta, se aduce atingere secretului corespondenței. Or, este evident că, pentru a se realiza percheziționarea corespondenței, aceasta trebuie să fie în posesia organelor de urmărire penală.

Un alt argument în sensul naturii măsurii ca formă de percheziție este însăși folosirea cuvântului „percheziție" în denumirea măsurii, ceea ce face cu atât mai inexplicabilă alegerea legiuitorului de a nu încadra în Cod această măsură ca o formă de percheziție.

De aceea, considerăm că, *de lege ferenda*, se impune ca măsura să fie menționată, ca înainte, între formele de percheziție prevăzute de Cod și să fie redenumită „percheziționarea trimiterilor poștale".

Capitolul V
Condițiile legale pentru autorizarea reținerii, predării și percheziționării trimiterilor poștale

Reținerea, predarea și percheziționarea trimiterilor poștale, asemenea celorlalte metode speciale de supraveghere sau cercetare, presupune restrângerea drepturilor și libertăților persoanei vizate de acest procedeu probatoriu, motiv pentru care legea condiționează folosirea acestuia numai când sunt îndeplinite anumite condiții și cu garantarea respectării proporționalității între interesul public și interesul persoanei.

Necesitatea încuviințării procedeului probatoriu servește un dublu scop, cel de a conferi organelor de urmărire penală puteri sporite în activitatea de administrare a probelor și cel de a garanta legalitatea administrării probei.

Organul competent să dispună asupra folosirii măsurilor de supraveghere tehnică și, în consecință, asupra reținerii, predării și percheziționării corespondenței este *judecătorul de drepturi și libertăți*, ca regulă. În mod excepțional, *procurorul*, potrivit art. 147 alin. (4) C.pr.pen., va putea dispune limitat, pentru o durată de maximum 48 de ore și cu controlul ulterior al judecătorului de drepturi și libertăți, reținerea, predarea și percheziționarea trimiterilor poștale. Această din urmă procedură a fost considerată în mod corect ca fiind neconstituțională[1] raportat la dispozițiile art. 21 alin. (3) din Constituție, aspect care va fi reluat în prezentul articol.

Reținerea, predarea și percheziționarea trimiterilor poștale se va putea încuviința numai dacă sunt îndeplinite condițiile cumulative prevăzute de art. 147 alin. (1) C.pr.pen. Mai înainte de orice condiție prevăzută expres de lege, este necesar să fi fost începută urmărirea penală pentru o faptă prevăzută de legea penală. Această condiție reiese din faptul că începerea urmăririi penale este actul procesual care creează întreg cadrul pentru desfășurarea activităților de urmărire penală, inclusiv administrarea probelor.

Prima condiție specială pentru acest procedeu probatoriu este existența unei *suspiciuni rezonabile cu privire la pregătirea sau săvârșirea unei infracțiuni*. Prevederea acestei condiții este inutilă și reprezintă o lipsă de inspirație din partea legiuitorului, care a vrut să facă o distincție între această măsură de cercetare și supravegherea tehnică. În cazul condiției similare prevăzute pentru supravegherea tehnică, la art. 139 alin. (1) lit. a) C.pr.pen., trebuie ca infracțiunea care se pregătește sau care s-a săvârșit să aibă o anumită gravitate și să fie dintre cele indicate la art. 139 alin. (2) C.pr.pen. În realitate, condiția prevăzută de art. 147 alin. (1) lit. a) C.pr.pen. este inutilă, deoarece orice procedeu probatoriu se va dispune numai atunci când există o suspiciune rezonabilă privind pregătirea săvârșirii sau săvârșirea unei infracțiuni, dat fiind faptul că, din coroborarea art. 305 alin. (1) C.pr.pen. cu art. 294 alin. (3) C.pr.pen., rezultă că începerea urmăririi penale se va dispune în toate cazurile în care există o suspiciune rezonabilă privind pregătirea sau săvârșirea unei infracțiuni și din actul de sesizare nu rezultă vreun caz de împiedicare dintre cele prevăzute de art. 16 C.pr.pen. Or, dacă, în cazul în care pentru orice infracțiune sesizată se va dispune începerea urmăririi penale, înseamnă că pentru orice procedeu probatoriu trebuie să existe o suspiciune rezonabilă cu privire la pregătirea sau săvârșirea unei infracțiuni, indiferent de gravitatea acesteia.

[1] *Gh. Mateuț*, Observații critice privind noua reglementare a supravegherii tehnice într-o prezentare comparativă, în Caiete de Drept Penal nr. 3/2015, pp. 31-32.

Cu această ocazie, trebuie să observăm că numai în cursul urmăririi penale se poate folosi această măsură de cercetare, legiuitorul renunțând la posibilitatea folosirii sale în cursul judecății, fapt care este în conformitate cu modul în care se desfășoară procesul penal în prezent.

A doua condiție care se impune a fi îndeplinită este cea privitoare la *proporționalitatea măsurii cu restrângerea drepturilor și libertăților fundamentale*. Această condiție este prevăzută de art. 147 alin. (1) lit. b) C.pr.pen. și se impune a fi analizată de judecătorul de drepturi și libertăți prin prisma criteriilor prevăzute de textul de lege: *particularitățile cauzei, importanța informațiilor ori a probelor ce urmează a fi obținute sau gravitatea infracțiunii*.

Proporționalitatea trebuie analizată prin raportare la gravitatea restrângerii secretului corespondenței și dreptului persoanei la viață privată, judecătorul de drepturi și libertăți trebuind să constate că nu va exista o disproporție între acțiunile statului și dreptul persoanei de a-i fi protejate aceste drepturi. În analiza proporționalității, va trebui să se aibă în vedere dacă se solicită o măsură de cercetare care să afecteze întreaga corespondență a persoanei, în special dacă aceasta nu este bănuită de săvârșirea unei infracțiuni, ci este un terț care primește corespondență pentru suspect sau inculpat. În atare situație, va fi preferabil ca judecătorul de drepturi și libertăți să autorizeze reținerea, predarea și percheziționarea trimiterilor poștale care provin numai de la o anumită persoană către terț[1].

De plano, judecătorul de drepturi și libertăți nu ar trebui să admită percheziționarea corespondenței dintre avocat și suspect sau inculpat, ci ar trebui să procedeze, din oficiu, la excluderea din sfera corespondenței supuse măsurii de cercetare a corespondenței purtate cu avocatul. Motivăm acest lucru, deoarece, dacă s-ar admite ca toată corespondența suspectului sau a inculpatului să fie supusă verificării, persoana care ar trebui să decidă asupra existenței unor date privind pregătirea săvârșirii de către avocat a uneia dintre infracțiunile prevăzute de art. 139 alin. (2) C.pr.pen. ar fi organul de urmărire penală, ceea ce nu este permis, în condițiile în care numai judecătorul trebuie să decidă asupra autorizării măsurii de cercetare. Altfel spus, numai judecătorul de drepturi și libertăți ar putea decide asupra măsurii. A considera altfel ar conduce la încălcarea competenței funcționale a judecătorului de drepturi și libertăți, în plus, ar exista pericolul să se încalce și competența după calitatea persoanei, întrucât dispoziția asupra unei asemenea măsuri privind un avocat ar reveni judecătorului de drepturi și libertăți din cadrul Curții de Apel.

Prin „particularitățile cauzei" vom înțelege acele împrejurări specifice unei anumite cauze penale care vor impune utilizarea supravegherii tehnice pentru soluționarea cauzei, deoarece un altfel de mijloc nu ar fi propice pentru a stabili starea de fapt. De exemplu, în cazul infracțiunii de constituire a unui grup infracțional organizat, prevăzută de art. 367 C.pen., poate fi oportună măsura, raportat la particularitățile cauzei constând în necesitatea de a obține conținutul trimiterilor unor colete transmise între membrii grupului. Într-o asemenea situație, este posibil ca administrarea probelor să nu poată fi făcută prin audierea persoanelor.

Prin „importanța informațiilor ori a probelor ce urmează a fi obținute" înțelegem contribuția pe care o pot avea informațiile sau probele obține pentru stabilirea împrejurărilor esențiale ale cauzei. Proporționalitatea trebuie stabilită raportat la utilitatea probei ce urmează a fi obținută și în funcție de împrejurarea concretă care se urmărește a se dovedi.

„Gravitatea infracțiunii" presupune, în opinia noastră, o analiză a pericolului social concret pe care îl presupune săvârșirea infracțiunii care face obiectul urmăririi penale. Deși gravitatea unei infracțiuni se manifestă în limitele de pedeapsă prevăzute de lege, ca pericol social

[1] *V. supra*, Titlul III, Capitolul I.3.

abstract[1], considerăm că acest criteriu a fost avut în vedere de legiuitor în privința măsurii de cercetare.

A treia condiție impusă de Codul de procedură penală pentru încuviințarea măsurii de cercetare este *necesitatea procedeului probatoriu* pentru obținerea probei. Cu alte cuvinte, condiția se referă la *subsidiaritatea*[2] măsurilor de supraveghere tehnică față de orice alt procedeu probatoriu. Această condiție este prevăzută în cuprinsul art. 147 alin. (1) lit. c) C.pr.pen. și limitează folosirea reținerii, predării și percheziționării trimiterilor poștale, cu excepția cazurilor în care „*probele nu ar putea fi obținute în alt mod sau obținerea lor ar presupune dificultăți deosebite ce ar prejudicia ancheta ori există un pericol pentru siguranța persoanelor sau a unor bunuri de valoare*". În realitate, există două situații prevăzute în care se poate considera ca fiind necesară autorizarea măsurii de cercetare: imposibilitatea (absolută sau relativă) a obținerii probelor în alt mod și existența unui pericol pentru siguranța persoanei sau a unor bunuri de valoare.

În prima situație, necesitatea este determinată de imposibilitatea obținerii probei în orice alt mod, adică prin utilizarea unui alt procedeu probatoriu, or, obținerea probei prin utilizarea unui alt mijloc de probă ar aduce serioase impedimente anchetei. Prin această prevedere, legiuitorul subliniază faptul că, în cursul urmăririi penale, trebuie folosite, ca regulă, alte mijloace mai puțin intruzive, dacă ele sunt apte să conducă la aceleași rezultate[3]. Considerăm că simpla celeritate a desfășurării procesului penal nu poate justifica apelarea la măsuri de cercetare care restrâng drepturile și libertățile cetățenești ca o soluție pentru obținerea facilă de probe. Sensul dispozițiilor legale privind autorizarea măsurii este cel de utilizare a acestor mijloace doar în situația în care proba s-ar obține în condiții dificile, printr-un efort deosebit al organelor de urmărire penală. În această din urmă situație, se impune ca obținerea probei să fie o certitudine pentru organul de urmărire penală, deoarece nu se poate admite folosirea unor astfel de mijloace în speranța obținerii unei eventuale probe sau a descoperirii vreunei infracțiuni.

Cea de-a doua situație prevede utilizarea reținerii, predării și percheziționării trimiterilor poștale în cazul în care există *un pericol pentru siguranța persoanelor sau pentru unele bunuri de valoare*. Necesitatea este dată de însăși valoarea socială ocrotită de infracțiunea care se urmărește a fi săvârșită. Spre deosebire de supravegherea tehnică, este greu de imaginat cum autorizarea acestei măsuri de cercetare ar putea înlătura un asemenea pericol, deoarece conținutul trimiterilor poștale va fi cunoscut organelor de urmărire penală cu întârziere, mai ales dacă trimiterea sau primirea se face într-o altă localitate decât cea în care își are sediul organul de urmărire penală. În cazul supravegherii tehnice, este posibilă urmărirea în timp real a persoanei, astfel că este probabil ca organele de urmărire penală să intervină în timp util pentru salvgardarea siguranței unei persoane sau pentru salvarea unui bunuri de valoare.

Includerea, fără rost, a acestei condiții este prejudiciabilă pentru autorizarea măsurii de cercetare, întrucât impune procurorului să motiveze existența unei situații improbabile față de efectul pe care l-ar putea avea măsura.

---

[1] *M. Basarab*, op. cit., p. 140.

[2] *Gh. Mateuț*, Observații critice privind noua reglementare a supravegherii tehnice într-o prezentare comparativă, în Caiete de Drept Penal nr. 3/2015, p. 24.

[3] *M. Udroiu, O. Predescu*, Protecția europeană, 2008, p. 829.

Capitolul VI
Procedura autorizării reținerii, predării și percheziționării trimiterilor poștale

În mod asemănător altor elemente procedurale din cadrul acestui procedeu probatoriu, legiuitorul a ales să împrumute un număr semnificativ de prevederi în cazul reținerii, predării și percheziționării trimiterilor poștale. O parte dintre acestea, așa cum am văzut în cazul condițiilor, sunt impropriu utilizate și creează mai multă confuzie în etapa obținerii mandatului prin care se autorizează această măsură de cercetare.

Potrivit art. 147 alin. (3) C.pr.pen., dispozițiile art. 140 C.pr.pen. se vor aplica corespunzător, fapt care semnifică împrumutarea procedurii de autorizare de la măsurile de supraveghere tehnică.

Pentru a se dispune reținerea, predarea și percheziționarea trimiterilor poștale, este necesar ca procurorul să întocmească o cerere în acest sens, în care să fie cuprinse toate elementele legale prevăzute de art. 140 alin. (2) C.pr.pen., pe care să o transmită judecătorului de drepturi și libertăți. Competența revine judecătorului de drepturi și libertăți din cadrul instanței competente să judece cauza în primă instanță sau din cadrul instanței corespunzătoare în grad acesteia în a cărei circumscripție se află sediul parchetului din care face parte procurorul care a formulat cererea.

În privința încuviințării supravegherii tehnice de către judecătorul de drepturi și libertăți, procedura este prevăzută de art. 140 C.pr.pen. și impune, mai întâi, verificarea de către acest organ judiciar a respectării condițiilor prevăzute de art. 147 alin. (1) C.pr.pen.

Această verificare se face pe baza cererii depuse de către procuror și în urma verificării dosarului cauzei, care va fi înaintat de către procuror împreună cu cererea prin care solicită să se dispună supravegherea tehnică. În cuprinsul cererii, procurorul trebuie să includă toate elementele prevăzute de art. 140 alin. (2) C.pr.pen.[1].

Judecarea cererii formulate de procuror are loc în aceeași zi cu formularea ei, în camera de consiliu, fără citarea părților și cu prezența obligatorie a procurorului. Soluțiile pe care le poate pronunța judecătorul de drepturi și libertăți sunt fie respingerea cererii, fie admiterea ei.

Respingerea cererii se va dispune conform art. 140 alin. (6) C.pr.pen., atunci când judecătorul de drepturi și libertăți va respinge în totalitate cererea procurorului, fie ca inadmisibilă, fie ca nefondată.

În cazul oricăreia dintre soluțiile adoptate de către judecătorul de drepturi și libertăți, aceasta nu va putea fi supusă niciunei căi de atac, însă procurorul va fi îndreptățit să formuleze o nouă cerere de încuviințare în cazul respingerii, dacă vor fi îndeplinite cerințele prevăzute de art. 140 alin. (8) C.pr.pen. Formularea unei a doua cereri de încuviințare a reținerii, predării și percheziționării trimiterilor poștale va putea fi făcută numai în măsura în care au apărut sau s-au descoperit fapte sau împrejurări noi, necunoscute la momentul soluționării cererii anterioare. Considerăm că această condiție nu trebuie să fie considerată una formală, ea trebuind să fie

[1] Conform acestui articol, cererea trebuie să cuprindă, printre altele: numele sau alte date de identificare a persoanei împotriva căreia se dispune măsura, dacă sunt cunoscute, indicarea probelor ori a datelor din care rezultă suspiciunea rezonabilă cu privire la săvârșirea unei infracțiuni, indicarea faptei și a încadrării juridice, motivarea caracterului proporțional și subsidiar al măsurii.

verificată în mod temeinic de către judecătorul de drepturi și libertăți, raportat la starea de fapt descrisă în cuprinsul primei cereri de încuviințare. Astfel, nu va putea constitui **descoperirea unei fapte noi** simpla schimbare a încadrării juridice, deoarece, în această situație, starea de fapt rămâne aceeași, doar semnificația sa juridică este schimbată.

Pentru ca faptele și împrejurările noi să poată justifica formularea unei noi cereri de încuviințare, este necesar ca acestea să nu fi fost cunoscute de judecătorul de drepturi și libertăți la soluționarea primei cereri de încuviințare. Semnificația acestei prevederi este bazată pe faptul că, dacă faptele sau împrejurările erau cunoscute de către judecătorul de drepturi și libertăți la momentul în care a respins prima cerere de încuviințare, acesta le-a avut în vedere atunci când a dispus respingerea cererii.

În cazul admiterii cererii, judecătorul de drepturi și libertăți va dispune numai asupra persoanelor față de care s-a propus măsura, cu indicarea tipului de trimiteri poștale care sunt supuse măsurii: primite sau trimise. Această mențiune o socotim obligatorie, deoarece asigură o mai bună protejare a secretului corespondenței dacă nu vor fi urmărite toate trimiterile poștale și previne obținerea unor trimiteri care să nu aibă relevanță cu cauza. *De lege ferenda*, considerăm că legiuitorul trebuie să prevadă expres această obligație în cadrul procedurii de încuviințare a măsurii de cercetare.

O metodă mai bună de acțiune ar fi dacă procurorul ar reuși să contureze un cerc de persoane între care există o corespondență pe care o consideră utilă cauzei și doar trimiterile poștale dintre aceste persoane să fie supuse măsurii.

Admiterea cererii se face prin încheierea judecătorului de drepturi și libertăți, care va proceda la emiterea imediată a mandatului de reținere, predare și percheziționare a trimiterilor poștale, întocmind în mod obligatoriu o minută. Măsura poate fi dispusă pentru o perioadă maximă de 30 de zile, însă, conform art. 144 C.pr.pen., poate fi prelungită, fiecare prelungire neputând depăși 30 de zile. Totodată, conform art. 147 alin. (9) C.pr.pen., durata totală a măsurilor de supraveghere tehnică cu privire la aceeași persoană nu poate depăși 6 luni.

După admiterea cererii procurorului, judecătorul de drepturi și libertăți emite, conform art. 140 alin. (5) C.pr.pen., un mandat care trebuie să conțină mai multe elemente cuprinse și în încheierea de admitere a cererii, motiv pentru care le vom aborda unitar.

Elementele comune care nu pun probleme deosebite sunt cele privind denumirea instanței, data, ora și locul emiterii, numele, prenumele și calitatea persoanei care a dat încheierea și a emis mandatul, semnătura judecătorului și ștampila instanței. Un alt element comun care nu ridică probleme este perioada pentru care se dispun măsurile de supraveghere tehnică, aceasta putând fi de maximum 30 de zile.

Alături de acestea, în cuprinsul art. 140 alin. (5) lit. e) teza a II-a C.pr.pen., legiuitorul a prevăzut că este obligatorie menționarea *scopului* pentru care s-a încuviințat măsura. În opinia noastră, aceste element este inutil în cuprinsul unui mandat de reținere, predare și percheziționare a trimiterilor poștale, fiind vorba de un procedeu probatoriu, scopul măsurilor de supraveghere tehnică este subînțeles, la fel ca în cazul oricărui procedeu probatoriu.

În mod excepțional și cu controlul ulterior al judecătorului de drepturi și libertăți, Codul de procedură penală permite procurorului să autorizeze temporar, pentru o perioadă care nu poate depăși 48 de ore, reținerea, predarea și percheziționarea trimiterilor poștale.

Această prevedere este una excepțională, putând fi utilizată de procuror numai atunci când sunt întrunite condițiile stricte ale art. 147 alin. (4) C.pr.pen., măsura fundamentându-se pe urgența efectuării actului. Urgența impune procurorului să procedeze direct la autorizarea

supravegherii tehnice ca urmare a faptului că nu există timpul necesar pentru parcurgerea procedurii ordinare în fața judecătorului de drepturi și libertăți.

Procedura autorizării de către procuror a măsurii este prevăzută în mod analog celei din cazul supravegherii tehnice. Motivul pentru menținerea acestei instituții este găsirea unei soluții pentru acele situații în care procedura ordinară ar duce la pierderea momentului operativ și s-ar pierde oportunitatea de a obține anumite probe. În doctrina recentă s-a arătat că, deși instituția autorizării temporare de către procuror a unor măsuri a rămas neschimbată, ca urmare a modificării fundamentale a procesului penal, dispozițiile art. 141 C.pr.pen. [*mutatis mutandis* și ale 147 alin. (4) C.pr.pen.] sunt neconstituționale prin raportare la art. 21 alin. (3) din Constituție, având în vedere că *„procurorul nu prezintă garanții suficiente de independență și imparțialitate pentru luarea unor măsuri prin care se aduce atingere gravă drepturilor și libertăților persoanei*"[1]. În același timp, se arată, în mod corect, că instituția judecătorului de drepturi și libertăți a fost creată pentru a soluționa probleme urgente[2], inclusiv dispunerea întrebuințării metodelor speciale de supraveghere, iar dispozițiile art. 141 C.pr.pen. dă prerogative identice procurorului, contrar principiului separării funcțiilor judiciare în procesul penal.

Așa cum am arătat, specificul autorizării de către procuror a măsurii este urgența, or, noul Cod de procedură penală a creat deja un organ care să soluționeze chestiunile urgente care țin de restrângerea drepturilor și libertăților fundamentale ale persoanei: judecătorul de drepturi și libertăți.

Considerăm că, dintre toate măsurile speciale de supraveghere sau cercetare, reținerea, predarea și percheziționarea trimiterilor poștale este cea mai puțin susceptibilă caracterului de urgență la care se referă legiuitorul. Așa cum am menționat mai sus, măsura de cercetare nu este aptă să furnizeze probe în timp real, ci impune punerea ei în executare de către un furnizor de servicii poștale care să trebuiască să fie încunoștințat. Aplicarea considerentului de urgență presupune ca procurorul să cunoască despre actul de primire sau trimitere a unei scrisori, colet sau altă formă de corespondență, astfel că este posibilă utilizarea unor metode alternative pentru a se obține proba. În special, în cazul trimiterilor poștale, procurorul va putea să apeleze la metoda specială de cercetare a livrării supravegheate, prevăzută de art. 151 C.pr.pen., care se va autoriza prin ordonanța acestuia, fără a fi nevoie de un act din partea judecătorului de drepturi și libertăți. În mod evident, livrarea supravegheată nu va fi compatibilă cu urmărirea penală a oricărei infracțiuni, însă, în cazul unor infracțiuni mai puțin grave, credem că oricum procurorul nu va putea să justifice subsidiaritatea măsurii în fața judecătorului de drepturi și libertăți atunci când se va proceda la confirmarea măsurii.

Pentru autorizarea temporară a reținerii, predării și percheziționării corespondenței, vor trebui respectate condițiile generale despre care am discutat anterior, dar și condiții specifice, similare autorizării măsurilor de supraveghere tehnică pentru o durată de maximum 48 de ore (art. 141 C.pr.pen.). Astfel, pe lângă caracterul urgent, art. 147 alin. (4) C.pr.pen. adaugă drept condiții: *„întârzierea substanțială a cercetărilor, pierderea, alterarea sau distrugerea probelor ori ar pune în pericol siguranța victimei sau a altor persoane*".

În privința întârzierii substanțiale a cercetărilor, considerăm că legiuitorul a impus o condiție care nu se justifică raportat la durata relativ scurtă de timp în care se poate obține

[1] *Gh. Mateuț*, Observații critice privind noua reglementare a supravegherii tehnice într-o prezentare comparativă, în Caiete de Drept Penal nr. 3/2015, p. 31.

[2] *Ibidem*, p. 32.

un mandat de la judecătorul de drepturi și libertăți, astfel simplul motiv că cercetarea ar fi întârziată cu o zi sau două nu considerăm că poate constitui temei suficient.

În cazul pierderii, alterării sau distrugerii probelor, suntem de părere că măsura de cercetare ar putea fi *in abstracto* justificată, însă avem dubii cu privire la caracterul ei subsidiar, în condițiile în care se presupune că procurorul are cunoștință despre o trimitere poștală anume și dorește să o obțină.

Cea de-a treia situație prevăzută de lege este atunci când obținerea întârziată a mandatului de supraveghere tehnică ar pune în pericol siguranța victimei sau a altor persoane. Singura situație pe care ne-o putem imagina că s-ar justifica ar fi dacă trimiterea poștală ar conține ceva vătămător pentru persoana care o primește și s-ar impune oprirea punerii în pericol a vieții victimei. În condițiile acestea, credem că este mai facil ca organele de urmărire penală să procedeze la anunțarea victimei, și pentru asigurarea siguranței sale, prin alte mijloace, decât să folosească o metodă atât de ineficientă din punctul de vedere al rapidității aplicării sale. Legiuitorul nu a adaptat condițiile la specificul măsurii, procedând la copierea dispozițiilor art. 141 C.pr.pen. Ipotetic vorbind, pentru ca procurorul să autorizeze măsura, va trebui să cunoască mai multe elemente: că trimiterea poștală există, că reprezintă un pericol pentru viața victimei sau a altei persoane și să cunoască (cel puțin generic) cine ar putea fi destinatarul trimiterii. În aceste condiții, ar fi aplicabile condițiile privind autorizarea livrării supravegheate prevăzute de art. 151 alin. (2) C.pr.pen.

Autorizarea de către procuror a reținerii, predării și percheziționării trimiterilor poștale se dispune prin ordonanță, aceasta trebuind să conțină toate elementele prevăzute de art. 140 alin. (5) C.pr.pen., adică să aibă un conținut identic cu mențiunile obligatorii din mandatul și încheierea care se emit, în procedura obișnuită, de judecătorul de drepturi și libertăți.

Conform art. 141 alin. (3) C.pr.pen., procurorul are obligația ca, în termen de cel mult 24 de ore de la expirarea măsurii, să sesizeze judecătorul de drepturi și libertăți competent în vederea confirmării măsurii, înaintând un proces-verbal de redare rezumativă a activităților de supraveghere tehnică efectuate și dosarul cauzei. Cu această ocazia, procurorul poate să ceară dispunerea în continuarea a măsurii de cercetare în condițiile art. 140 C.pr.pen., putând, de altfel, formula această cerere și separat.

Judecătorul de drepturi și libertăți, fiind sesizat de procuror în vederea conformării măsurii de cercetare, are posibilitatea de a *infirma* sau *confirma* supravegherea tehnică efectuată în baza autorizației emise de procuror.

În situația în care judecătorul de drepturi și libertăți va constata că au fost încălcate dispozițiile art. 147 alin. (4) C.pr.pen. privind autorizarea de către procuror a reținerii, predării și percheziționării corespondenței, acesta va infirma măsura și va dispune distrugerea probelor obținute. Față de această încheiere, procurorul nu poate exercita nicio cale de atac, fiind obligat să procedeze la distrugerea probelor obținute, consemnând operațiunea într-un proces-verbal. Cu toate acestea, nu va însemna distrugerea trimiterii poștale, ci va conduce la restituirea acestora la destinatar.

În cazul în care judecătorul de drepturi și libertăți va aprecia că autorizarea măsurilor de supraveghere tehnică dispusă de procuror s-a făcut în conformitate cu prevederile art. 147 alin. (4) C.pr.pen., va proceda la *confirmarea măsurii* prin încheiere.

Capitolul VII
Punerea în executare a reținerii, predării și percheziționării trimiterilor poștale

Spre deosebire de măsurile de supraveghere tehnică, reținerea, predarea și percheziționarea trimiterilor poștale va presupune concursul unui furnizor de servicii poștale în vederea executării unei componente a măsurii, urmând ca organele de urmărire penală să procedeze la descoperirea conținutului corespondenței.

După ce judecătorul de drepturi și libertăți se pronunță asupra încuviințării măsurii și emite mandatul de reținere, predare și percheziționare a trimiterilor poștale, procurorul va proceda la transmiterea acestui mandat către fiecare furnizor de servicii poștale utilizat de suspect, inculpat sau altă persoană supusă măsurii. Nu va fi necesar să emită o ordonanță privind punerea în executare a măsurii, fiind suficientă transmiterea mandatului și indicarea modalității în care se va face predarea către procuror a corespondenței.

Potrivit art. 147 alin. (5) C.pr.pen., „*unitățile poștale sau de transport și orice alte persoane fizice sau juridice care efectuează activități de transport sau transfer de informații sunt obligate să rețină și să predea procurorului scrisorile, trimiterile poștale ori obiectele la care se face referire în mandatul dispus de judecător sau în autorizația emisă de procuror*". Această dispoziție legală se coroborează cu art. 4 alin. (2) din O.U.G. nr. 13/2013 privind serviciile poștale, în care se arată că „*reținerea, deschiderea sau divulgarea conținutului trimiterilor poștale este permisă numai în condițiile și cu procedura prevăzute de lege*".

Măsura de cercetare va presupune trei etape, care sunt prevăzute în denumirea marginală a art. 147 C.pr.pen.: **reținerea**, **predarea** și **percheziționarea**.

Prin „reținere" vom înțelege acea procedură prin care furnizorul de servicii poștale sau persoana fizică ori juridică ordonată să aplice mandatul judecătorului de drepturi și libertăți va opri toată corespondența trimisă sau destinată unei anumite persoane indicate în mandat sau a corespondenței dintre anumite persoane, potrivit dispozițiilor concrete cuprinse în mandat. Operațiunea se va desfășura oriunde ar fi surprinsă corespondența, în funcție de momentul încunoștințării venite din partea procurorului prin transmiterea mandatului.

Prin „predare" înțelegem operațiunea prin care furnizorul de servicii poștale sau persoana fizică ori juridică obligată să rețină corespondența unei persoane transmite posesia asupra acesteia către procuror. Chiar dacă art. 147 alin. (5) C.pr.pen. menționează că toate trimiterile poștale se vor preda procurorului, credem că acestea pot fi predate oricărui organ de urmărire penală prin intermediul unei ordonanțe de delegare din partea procurorului. Față de importanța redusă a acestei operațiuni, suntem de părere că legiuitorul ar fi trebui să folosească noțiunea de „organ de urmărire penală". Deși Codul nu prevede, se va impune ca efectuarea predării să fie consemnată într-un proces-verbal care să fie întocmit în dublu exemplar și care să detalieze fiecare trimitere poștală remisă, în caz contrar apreciind că probele obținute vor trebui să fie excluse ca fiind obținute în mod nelegal.

În cadrul procedurii de cameră preliminară, este necesar ca judecătorul de cameră preliminară să poată determina proveniența probelor în procesul penal, mai ales în cazul în care acestea au un caracter strâns legat de viața privată a unei persoane – corespondență, interceptări telefonice etc. –, în caz contrar trebuind să fie excluse, deoarece nu se poate certifica proveniența

lor. Ceea ce remarcăm este că, în cazul în care există dubii cu privire la proveniența unui mijloc de probă, incumbă procurorului să dovedească legalitatea obținerii probei în fața judecătorului de cameră preliminară. De aceea, considerăm că redactarea unui proces-verbal de predare a trimiterilor poștale este obligatorie, în caz contrar neputându-se demonstra cum au fost obținute trimiterile poștale și momentul în care au fost obținute, prin raportare la momentul emiterii mandatului de reținere, predare și percheziționare a trimiterilor poștale.

Prin „percheziționare" vom înțelege acel act desfășurat de organul de urmărire penală, prin care se deschide trimiterea poștală obținută și se evidențiază conținutul acesteia, urmând a se folosi conținutul acesteia ca mijloc de probă în procesul penal.

Codul de procedură penală nu ne conferă nicio sugestie privind modalitatea de realizare a percheziționării corespondenței, motiv pentru care se impun a fi adaptate regulile tactice privind efectuarea unei percheziții.

Percheziționarea se va realiza ținându-se seama de necesitatea obținerii cât mai multor probe din analiza fiecărei trimiteri în parte. Mai înainte de deschiderea propriu-zisă a corespondenței, organul de urmărire penală trebuie să descrie fiecare trimitere în parte, să consemneze dimensiunile, greutatea acestora, să noteze particularități aparte (mâzgălituri, semne distincte, pete de substanțe, mirosuri etc.) și să consemneze toate aceste aspecte într-un proces-verbal. Totodată, considerăm că se impune ca organul judiciar să fotografieze trimiterile poștale mai înainte de deschiderea lor, pentru a nu se contesta că trimiterea poștală a fost deschisă mai înainte de o altă persoană. În funcție de posibilitățile organului de urmărire penală, activitatea se poate și filma, înregistrarea depunându-se pe suport optic la dosarul cauzei.

Plicul sau cutia în care se află trimiterea poștală poate furniza probe dincolo de conținutul trimiterii. De pildă, în cazul unei scrisori, se obișnuiește ca rubricile expeditorului și ale destinatarului să fie scrise de mână, plicul putând servi la identificarea persoanei expeditorului, în cazul în care acesta va contesta ulterior transmiterea scrisorii. Este lesne de înțeles că, în cazul săvârșirii unei infracțiuni de amenințare prin intermediul unor scrisori, o persoană va încerca să își ascundă identitatea și să transmită amenințările sub un pseudonim prin folosirea unei scrisori neînregistrate, prin simpla francare a ei cu un timbru și inserarea într-o cutie poștală.

Deschiderea recipientului în care se află corespondența sau obiectele trimise trebuie să se facă într-o modalitate cât mai puțin distructivă, pentru a nu fi afectat conținutul acestuia și pentru a se conserva urmele care se regăsesc pe acesta.

În cuprinsul procesului-verbal care se impune a fi încheiat pentru consemnarea activităților de percheziție se va menționa, de asemenea, unde și cum s-a realizat deschiderea plicului sau a coletului și cu ce instrument s-a făcut.

Imediat după deschiderea trimiterii poștale, se va inventaria conținutul acesteia și se va consemna în procesul-verbal, realizându-se și fotografii cu toate înscrisurile sau obiectele găsite. Toate acestea vor fi verificate pentru urme sau alte semne distinctive.

Cu această ocazie, trebuie să subliniem că este necesar ca organul de urmărire penală să evalueze relevanța conținutului trimiterii poștale, în situația în care aceasta nu are legătură cu cauza, procedându-se la omiterea fotografierii conținutului, pentru a se proteja secretul corespondenței.

După ce s-a procedat la percheziționarea trimiterilor, acestea vor fi depuse la dosarul cauzei sau la camera de corpuri delicte în funcție de natura lor și de dimensiune. Sub aspectul naturii probelor care pot rezulta din folosirea măsurii de cercetare a reținerii, predării și percheziționării trimiterilor poștale, acestea pot fi înscrisurile și mijloacele materiale de probă.

În cazul în care din conținutul trimiterilor rezultă că acestea nu au legătură cu cauza, potrivit art. 147 alin. (6) C.pr.pen., acestea se vor restitui destinatarului. Deși nu se menționează, restituirea acestora se va face prin intermediul furnizorului de servicii poștale sau a persoanei fizice ori juridice care trebuie să realizeze transportul lor, pentru a nu ridica suspiciuni, în urma cărora să fie divulgate activitățile organelor de urmărire penală.

Odată cu încetarea duratei pentru care a fost încuviințată măsura de cercetare, procurorului îi va reveni obligația a de a încunoștința fiecare subiect al mandatului cu privire la măsura care a fost luată. În conformitate cu art. 147 alin. (7) C.pr.pen., în termen de cel mult 10 zile de la efectuarea măsurii de cercetare, procurorul va realiza această informare în scris, indicând persoanelor că au dreptul de a cunoaște activitățile desfășurate și, implicit, corespondența care le-a fost percheziționată, după caz.

Dată fiind natura trimiterilor poștale, pentru percheziționarea corespondenței, este necesar ca măsura de cercetare să fie încuviințată numai pentru una dintre persoanele implicate – expeditor, destinatar sau față de un terț, procurorul neavând nicio obligație de a informa asupra măsurii cealaltă persoană. Apreciem că textul de la art. 147 alin. (7) C.pr.pen. nu asigură o protecție suficientă drepturilor persoanei care nu a fost subiectul unui mandat emis de judecătorul de drepturi și libertăți, *de lege ferenda*, impunându-se informarea tuturor persoanelor care au fost afectate de măsură, chiar dacă nu au fost subiectul mandatului de reținere, predare și percheziționare a corespondenței.

Raportând art. 147 alin. (8) C.pr.pen. la art. 145 alin. (4) C.pr.pen., procurorul va putea să amâne motivat efectuarea informării persoanei numai în situația în care aceasta ar duce la perturbarea sau periclitarea bunei desfășurări a urmăririi penale în cauză. Această amânare are o durată maximă expusă de art. 145 alin. (5) C.pr.pen., respectiv până la terminarea urmăririi penale sau până la clasarea cauzei.

Capitolul VIII
Reținerea, predarea și percheziționarea trimiterilor poștale ale unui avocat

O problemă particulară în punerea în executare a măsurii de cercetare este interdicția de a o aplica corespondenței ori trimiterilor poștale dintre suspect, inculpat sau orice altă persoană vizată de măsură și avocatul acestora. Potrivit art. 147 alin. (2) C.pr.pen., este interzisă aplicarea măsurii asupra acestui tip de corespondență, cu excepția situației în care avocatul săvârșește sau pregătește săvârșirea unei infracțiuni dintre cele prevăzute la art. 139 alin. (2) C.pr.pen.

Mai înainte de a analiza aplicabilitatea acestei interdicții, trebuie să relevăm ce a înțeles legiuitorul prin calitatea de avocat în cadrul dispozițiilor art. 147 alin. (2) C.pr.pen. Potrivit art. 88 alin. (1) C.pr.pen., „*avocatul asistă sau reprezintă, în procesul penal, părțile ori subiecții procesuali principali, în condițiile legii*". O asemenea prevedere nu va fi completă, deoarece art. 147 C.pr.pen. permite aplicarea măsurii de cercetare și „altor persoane", care nu au nicio calitate în procesul penal, astfel că nu își pot angaja un avocat în cauza penală respectivă. Credem că, prin interdicția inserată în art. 147 alin. (2) C.pr.pen., prin „avocat al suspectului, inculpatului sau al unei alte persoane" vom înțelege avocatul care realizează asistarea sau reprezentarea persoanei în orice cauză pe care ar avea-o aceasta, nu numai procesul penal în cadrul căruia se dispune reținerea, predarea și percheziționarea corespondenței.

Aparent, prevederea din Codul de procedură penală pare clară, însă legiuitorul nu detaliază când ar trebui aceasta să fie avută în vedere: la momentul încuviințării măsurii sau la momentul punerii sale în aplicare. Răspunsul la o astfel de dilemă este că această prevedere este aplicabilă în ambele situații.

Dacă procurorul va dori să urmărească trimiterile poștale primite sau transmise de suspect, inculpat sau o altă persoană cu avocatul său, s-ar impune ca, față de avocat, să existe deja începută urmărirea penală pentru una dintre infracțiunile prevăzute la art. 139 alin. (2) C.pr.pen.[1] și ca acea infracțiune să aibă legătură cu cauza în care se dispune măsura de cercetare. Ca atare, avocatul va deveni una dintre persoanele față de care se ia măsura și se va impune ca judecătorul de drepturi și libertăți din cadrul instanței competente să se pronunțe asupra măsurii. Dacă procurorul formulează propunerea de încuviințare a măsurii fără să indice judecătorului de drepturi și libertăți că se efectuează o urmărire penală *in rem* față de o faptă imputată unui avocat, atunci nu se va putea proceda la percheziționarea trimiterilor poștale cu acel avocat.

[1] Potrivit art. 139 alin. (2) C.pr.pen.: „Supravegherea tehnică se poate dispune în cazul infracțiunilor contra securității naționale prevăzute de Codul penal și de legi speciale, precum și în cazul infracțiunilor de trafic de droguri, de efectuare de operațiuni ilegale cu precursori sau cu alte produse susceptibile de a avea efecte psihoactive, infracțiunilor privind nerespectarea regimului armelor, munițiilor, materialelor nucleare, al materiilor explozive și al precursorilor de explozivi restricționați, de trafic și exploatarea persoanelor vulnerabile, acte de terorism, de spălare a banilor, de falsificare de monede, timbre sau de alte valori, de falsificare de instrumente de plată electronică, în cazul infracțiunilor care se săvârșesc prin sisteme informatice sau mijloace de comunicare electronică, contra patrimoniului, de șantaj, de viol, de lipsire de libertate în mod ilegal, de evaziune fiscală, în cazul infracțiunilor de corupție și al infracțiunilor asimilate infracțiunilor de corupție, infracțiunilor împotriva intereselor financiare ale Uniunii Europene ori în cazul altor infracțiuni pentru care legea prevede pedeapsa închisorii de 5 ani sau mai mare".

O altă situație este atunci când, ulterior încuviințării măsurii, se descoperă probe cu privire la infracțiunea care se pregătește a fi săvârșită de avocat sau care a fost săvârșită de acesta. În această situație, apreciem că nu se poate trece la reținerea, predarea și percheziționarea corespondenței dintre avocat și persoana față de care s-a luat măsura, fiind necesară reautorizarea măsurii față de avocat. Această concluzie rezultă din interpretarea sistematică a art. 147 C.pr. pen., întrucât interdicția privind aplicarea măsurii asupra avocatului este inserată mai înainte de dispozițiile procedurale privind încuviințarea măsurii, fapt care conduce la necesitatea autorizării măsurii în mod distinct față de avocat. Cu alte cuvinte, competența funcțională de încuviințare a măsurii rămâne întotdeauna a judecătorului de drepturi și libertăți, chiar și dacă mandatul emis de către acesta ar fi unul suficient de cuprinzător pentru a include și corespondența cu un avocat, deoarece impune o nouă evaluare a condițiilor de autorizare, în special, prin raportare la art. 139 alin. (2) C.pr.pen., condiție care nu este prevăzută în cazul reținerii, predării și percheziționării trimiterilor poștale ale suspectului, inculpatului sau altor persoane.

În situația în care, în cursul punerii în executare a măsurii, procurorul descoperă că s-au reținut și predat trimiteri poștale trimise sau primite de suspect, inculpat sau altă persoană față de care s-a luat măsura și avocatul său, nu va avea dreptul să procedeze la percheziționarea acestora. O atare situație poate fi generată din eroarea furnizorului de servicii poștale sau din eroarea persoanei care transmite corespondența și care nu a indicat calitatea de avocat a destinatarului sau expeditorului.

Prima situație nu prezintă probleme deosebite, procurorul trebuind să restituie destinatarului corespondența nedeschisă, analog situației prevăzute la art. 147 alin. (6) C.pr.pen. Cu toate acestea, credem că se va impune o oarecare prudență din partea organului de urmărire penală, întrucât simpla declinare a unei calități de avocat nu trebuie să fie suficientă pentru a înlătura de sub măsură o anumită trimitere poștală. Această calitate va trebui să fie verificată prin accesarea tabloului avocaților și, în cazul în care persoana nu are calitatea de avocat, se va impune percheziționarea corespondenței. Dacă totuși organul de urmărire penală va deschide corespondența arătată, va putea fi tras la răspundere penală pentru săvârșirea infracțiunii de violarea secretului corespondenței, prevăzută de art. 302 alin. (3) C.pen.

În cea de-a doua situație, apreciem că se va impune percheziționarea trimiterii poștale pentru a se stabili conținutul său, până în momentul în care organul de urmărire penală va constata că reprezintă o trimitere poștală desfășurată cu un avocat, moment în care va trebui să se desisteze. Nu va fi culpabil organul de urmărire penală care realizează acest act, decât dacă va proceda la folosirea trimiterii poștale ca probă în procesul penal. În condițiile în care organul de urmărire penală a procedat la percheziționarea oricărei trimiteri poștale destinate sau trimise de un avocat, el va fi obligat să o restituie, de îndată, destinatarului, în conformitate cu art. 147 alin. (6) C.pr.pen. Mai mult decât atât, fiindcă a fost încălcat și secretul profesional dintre client și avocat[1], se impune încunoștințarea avocatului cu privire la măsura de cercetare, în conformitate cu art. 147 alin. (7) C.pr.pen., chiar dacă avocatul nu era un subiect al mandatului dat de judecătorul de drepturi și libertăți. Această lacună legislativă o putem regăsi și în cazul supravegherii tehnice, procurorul fiind obligat să încunoștințeze numai persoanele care au fost menționate în cadrul mandatului de supraveghere tehnică, nu și persoanele cu

[1] Potrivit art. 34 alin. (3) din Legea nr. 51/1995 privind organizarea și exercitarea profesiei de avocat, „nu vor putea fi ascultate și înregistrate, cu niciun fel de mijloace tehnice, convorbirile telefonice ale avocatului și nici nu va putea fi interceptată și înregistrată corespondența sa cu caracter profesional, decât în condițiile și cu procedura prevăzute de lege".

care aceasta a luat legătura. Considerăm că, atât în cazul supravegherii tehnice, cât și în cazul reținerii, predării și percheziționării trimiterilor poștale, avocatul va trebui să fie încunoștințat întotdeauna, întrucât aceste metode speciale de supraveghere sau cercetare aplicate asupra sa în mod indirect pot constituit un temei pentru contestarea caracterului echitabil al procesului penal.

Percheziționarea trimiterilor poștale ale unui avocat poate reprezenta prilejul pentru ca organele de urmărire penală să afle despre strategia avocatului în apărarea clientului său, putând periclita exercitarea unei apărări efective. Legiuitorul nu a prevăzut o procedură specială pentru încunoștințarea avocatului în situația descrisă mai sus, existând posibilitatea ca încunoștințarea acestuia să fie amânată în conformitate cu art. 145 alin. (4) lit. a) C.pr.pen., singurul temei posibil fiind o eventuală „*perturbare sau periclitare a bunei desfășurări a urmăririi penale în cauză*". Suntem ferm convinși că o asemenea situație nu poate reprezenta un impediment pentru desfășurarea urmăririi penale atât timp cât avocatului i se asigură inclusiv dreptul de a consulta dosarul cauzei. A crede altfel este a admite că un avocat ar trebui să se aștepte ca toate acțiunile sale să fie cunoscute prin intermediul metodelor speciale de supraveghere sau cercetare, chiar și indirect, printr-un mandat emis pe numele clientului său, fapt care ar pune sub semnul întrebării posibilitatea exercitării în mod neîngrădit a profesiei.

Capitolul IX
Concluzii

Reținerea, predarea și percheziționarea trimiterilor poștale reprezintă o formă particulară de percheziție, neînțeleasă în mod deplin de legiuitorul român.

Reglementarea acestei măsuri poate fi îmbunătățită prin accentuarea rolului judecătorului de drepturi și libertăți în procesul de detaliere a activităților încuviințate și, în special, asupra subiecților față de care se va lua măsura. Considerăm că este necesar ca legiuitorul să impună restricții, deoarece nu este admisibilă percheziționarea întregii corespondențe trimise sau primite de o persoană, mai ales în condițiile în care Codul nu prevede obligativitatea unei calități procesuale sau măcar ca persoana să fie bănuită că ar fi comis o faptă.

Totodată, asemenea supravegherii tehnice, legiuitorul trebuie să adopte măsuri pentru garantarea încunoștințării tuturor persoanelor afectate de măsură, nu numai a subiecților cuprinși în mandatul emis de judecătorul de drepturi și libertăți, precum și încunoștințarea, de îndată și fără posibilitate de amânare, a avocatului, în cazul în care s-a procedat, în mod neintenționat, la percheziționarea trimiterilor sale.

Titlul XII
Utilizarea investigatorilor sub acoperire și a colaboratorilor[1]

Capitolul I
Aspecte generale

Metoda folosirii unei persoane sub identitate conspirativă pentru descoperirea săvârșirii unei infracțiuni și tragerea la răspundere penală a făptuitorilor nu este o metodă de cercetare descoperită recent, ci reprezintă una dintre cele mai vechi metode, folosite încă din antichitate sub diferite forme. Prin specificul ei, metoda este aptă atât pentru a realiza activități judiciare, cât și pentru realizarea spionajului sau asigurarea stabilității politice. Din punct de vedere istoric, unul dintre primii „investigatori sub acoperire" poate fi considerat Iuda Iscarioteanul, care, fiind motivat de bani, strânge date și informații pentru autoritățile vremii. În epoca contemporană, situația nu s-a modificat decât sub aspectul gradului de specializare a metodelor folosite pentru infiltrare și a mijloacelor de probă care pot deriva din activitatea investigatorilor sub acoperire și a colaboratorilor. Deseori, un agent sub acoperire își va folosi puterea de convingere, fie prin afirmații, fie prin aluzii, uneori și cu privire la desfășurarea de către acesta a unor fapte ilicite, cu scopul de a dobândi încrederea persoanei vizate de măsură pentru a se infiltra sau pentru a obține date sau informații[2].

Printre elementele de noutate aduse de Codul de procedură penală[3] este reglementarea unitară a măsurii de cercetare a utilizării investigatorilor sub acoperire și a colaboratorilor. Anterior noii legi procesuale penale, această metodă de cercetare a fost prevăzută pentru prima dată în cuprinsul Legii nr. 143/2000 privind prevenirea și combaterea traficului și consumului ilicit de droguri[4], în care se arăta că vor putea fi folosiți investigatori sub acoperire în faza actelor premergătoare, pentru ca, ulterior, prin Legea nr. 281/2003 privind modificarea și completarea Codului de procedură penală și a unor legi speciale[5], să fie reglementată instituția și în cuprinsul Codului de procedură penală anterior, prin art. 221[1] și următoarele[6].

Numai prin Codul de procedură penală în vigoare s-a stabilit o identitate de sine stătătoare a măsurii de cercetare. Aceasta face parte din categoria **metodelor speciale de supraveghere sau cercetare**, definite de art. 138 C.pr.pen. Definiția legală a măsurii este dată în art. 138 alin. (10) C.pr.pen., în care se arată că: *„prin «utilizarea investigatorilor sub acoperire și a colaboratorilor» se înțelege folosirea unei persoane cu o altă identitate decât cea reală în scopul obținerii de date și informații cu privire la săvârșirea unei infracțiuni"*.

---

[1] Materialul prezentului titlu a constituit primul referat științific din cadrul studiilor doctorale și a fost publicat în Revista Penalmente Relevant nr. 2/2016, sub denumirea „Unele aspecte privind folosirea investigatorilor sub acoperire și a colaboratorilor", fiind modificat și actualizat în prezenta lucrare.

[2] *R.W. Shuy*, Deceptive ambiguity by Police and Prosecutors, Oxford University Press, New York, 2017, p. 124.

[3] Legea nr. 135 din 1 iulie 2010 privind Codul de procedură penală, republicată (publicată în M. Of. nr. 486 din 15 iulie 2010 și republicată în M. Of. nr. 418 din 2 iunie 2016).

[4] Publicată în M. Of. nr. 362 din 3 august 2000.

[5] Publicată în M. Of. nr. 468 din 1 iulie 2003.

[6] *G.-C. Zaharia*, Traficul de persoane, Ed. C.H. Beck, București, 2012, pp. 183-184.

În actuala reglementare, măsura este considerată o metodă specială de cercetare, și nu o metodă specială de supraveghere tehnică, raportat la faptul că nu este aptă să producă în mod direct probe în procesul penal și că autorizarea acesteia se face prin ordonanța procurorului. În același timp, Codul arată că măsurile prevăzute de art. 138 C.pr.pen care constituie **metode speciale de supraveghere tehnică** sunt numai cele cuprinse de art. 138 alin. (1) lit. a)-e)[1], celelalte metode reprezentând **metode speciale de cercetare**. O rațiune pentru divizarea metodelor speciale de supraveghere sau cercetare a fost arătată ca fiind, în aparență, timpul în care acestea se realizează. Metodele de supraveghere tehnică presupun ca organul de urmărire penală să primească informațiile chiar în timp ce se desfășoară activitățile, însă, în cazul metodelor speciale de cercetare, informațiile sunt primite după ce activitățile au avut loc[2]. Aceasta nu este decât o premisă eronată a Codului, deoarece realitatea ne arată că, în special, utilizarea investigatorilor sub acoperire și a colaboratorilor poate produce informații în timp real.

S-a susținut în mod întemeiat că nu este justificată alegerea legiuitorului de a separa în două metodele speciale de supraveghere sau cercetare, deoarece fiecare dintre acestea prezintă un grad ridicat de interferare cu drepturile fundamentale ale omului[3]. O altă alegere nejustificată a legiuitorului o constituie lipsa unei proceduri speciale unice de autorizare, aplicabile în cazul tuturor metodelor speciale, fiind contrară scopului creării instituției judecătorului de drepturi și libertăți, înființată pentru a garanta respectarea drepturilor și libertăților persoanei în cadrul unui proces penal[4].

Un neajuns al Codului de procedură penală îl reprezintă lipsa unei corelații legale între metodele speciale de cercetare care se întrepătrund. Distincțiile legislative dintre utilizarea investigatorilor sub acoperire și a colaboratorilor, participarea autorizată la anumite activități și livrarea supravegheată sunt create artificial. În realitate, toate aceste metode speciale de cercetare se bazează pe ideea desfășurării unei activități specifice de către un agent al statului (lucrător de poliție sau particular colaborator), care furnizează informații în cadrul urmăririi penale sau acționează ghidat de organele de urmărire penală în mediul în care își desfășoară activitatea persoanele bănuite de săvârșirea unor infracțiuni. Fie din considerente legislative, fie din considerente practice, aceste măsuri nu pot fi imaginate ca fiind complet distincte. Bunăoară, livrarea supravegheată presupune supravegherea continuă a transportului, activitate care ar impune o monitorizare digitală, astfel că o persoană va trebui să monteze pe transport un dispozitiv de localizare. În același sens, substituirea bunurilor transportate nu va fi lesne realizată de organe ale statului acționând în mod deschis fără a pune în pericol desfășurarea livrării supravegheate, fiind preferabilă utilizarea unor colaboratori – căpitani de nave maritime, responsabili de depozite etc.

O situație aparte este cea a participării autorizate la anumite activități, metodă specială greu de înțeles în afara contextului furnizat de utilizarea investigatorilor sub acoperire și a colaboratorilor. Ținând seama și de persoanele care pot realiza o astfel de activitate, prin raportare la art. 150 alin. (3) C.pr.pen., va fi necesară o ordonanță de utilizare a investigatorilor

[1] Sunt incluse în cadrul supravegherii tehnice următoarele măsuri: interceptarea comunicațiilor ori a oricărui tip de comunicare la distanță; accesul la un sistem informatic; supravegherea video, audio sau prin fotografiere; localizarea sau urmărirea prin mijloace tehnice; obținerea datelor privind tranzacțiile financiare ale unei persoane.

[2] *C.M. Chiriță*, în N. Volonciu, A.S. Uzlău (coord.), Noul Cod, 2014, p. 304.

[3] *Gh. Mateuț*, Observații critice privind noua reglementare a supravegherii tehnice într-o prezentare comparativă, în Caiete de Drept Penal nr. 3/2015, p. 13.

[4] *Ibidem*.

sub acoperire și a colaboratorilor, ceea ce va părea excesivă în practică, deoarece, și pentru investigatori sau colaboratori, procurorul stabilește activitățile care vor fi realizate, una dintre acestea putând fi chiar participarea autorizată la anumite activități.

Din punct de vedere legislativ, era preferabil ca participarea autorizată la anumite activități și livrarea supravegheată să fie reunite cu utilizarea investigatorilor sub acoperire și a colaboratorilor, iar particularitățile privind activitățile desfășurate să fie delimitate prin ordonanța procurorului.

În prezenta parte a lucrării, ne-am propus să abordăm principalele probleme incidente în cazul utilizării investigatorilor sub acoperire și a colaboratorilor, axându-ne atât pe elementele procesuale penale care reies din dispozițiile Codului de procedură penală, cât și pe practica folosirii acestei măsuri și evidențierea neajunsurilor actualei reglementări, care pot fi mai greu sesizate la o simplă lecturare a textului de lege. Ceea ce reglementează Codul de procedură penală în cuprinsul art. 148 considerăm că poate fi numai un cadru legal incomplet, la acesta trebuind să fie adăugate reguli tactice concrete pentru corecta punere în executare a măsurii și, mai apoi, corecta apreciere a probelor ce vor deriva din aceasta.

Capitolul II
Condițiile legale pentru autorizarea utilizării investigatorilor sub acoperire și a colaboratorilor

Utilizarea investigatorilor sub acoperire și a colaboratorilor, asemenea celorlalte metode speciale de supraveghere sau cercetare, presupune imixtiunea în libera exercitare a drepturilor și libertăților persoanei vizate, motiv pentru care se impune restrângerea folosirii acestora numai în situații prevăzute expres de lege și garantarea respectării proporționalității între interesul public și interesul persoanei.

Organul competent să dispună asupra autorizării utilizării investigatorilor sub acoperire și a colaboratorilor este *procurorul,* potrivit art. 148 C.pr.pen. Deoarece măsura este una de cercetare, și nu de supraveghere, nu este necesară încuviințarea măsurii de către judecătorul de drepturi și libertăți, considerându-se că restrângerea drepturilor fundamentale ale persoanei nu este într-o asemenea măsură încât să implice concursul judecătorului. Cu toate că aprecierea oportunității folosirii măsurii trebuie să aparțină procurorului, în condițiile în care urmărirea penală se desfășoară sub conducerea acestuia, *de lege ferenda*, se impune ca acesta să propună judecătorului de drepturi și libertăți încuviințarea măsurii.

Cu toate acestea, utilizarea investigatorilor sub acoperire și a colaboratorilor poate fi autorizată numai atunci când sunt îndeplinite mai multe condiții cumulative, prevăzute în cuprinsul art. 148 C.pr.pen. Mai înainte de orice condiție prevăzută expres de lege, este necesar *să fi fost începută urmărirea penală* cu privire la o faptă prevăzută de legea penală. Această condiție reiese din faptul că începerea urmăririi penale este actul procesual care creează întreg cadrul pentru desfășurarea activităților de urmărire penală, inclusiv administrarea probelor, dar și obținerea datelor și informațiilor prin intermediul unor metode de cercetare.

Cu toate acestea, prima condiție prevăzută de art. 148 alin. (1) C.pr.pen. este cea a existenței unei *suspiciuni rezonabile cu privire la pregătirea sau săvârșirea unei infracțiuni* dintre cele prevăzute în mod expres la lit. a) a articolului antemenționat. Din formularea textului de lege, observăm că este posibilă folosirea investigatorilor sub acoperire și a colaboratorilor și într-o anchetă *proactivă*, având ca scop prevenirea săvârșirii unor infracțiuni grave[1]. Cu această ocazie, reamintim că, în cazul infracțiunilor contra securității naționale, sunt incriminate și actele preparatorii, conform dispozițiilor art. 412 alin. (2) C.pen., care le asimilează tentativei. Într-o atare situație, nu vom vorbi despre o anchetă proactivă, din moment ce faptele deja întrunesc elementele constitutive ale unei fapte penale prevăzute de lege, însă se va urmări împiedicarea consumării faptei care se pregătește[2].

O trăsătură comună cu celelalte metode speciale de supraveghere sau cercetare este că utilizarea investigatorilor sub acoperire și a colaboratorilor poate fi incidentă numai în cursul urmăririi penale, nu și în celelalte faze ale procesului penal.

Metoda specială de cercetare poate fi incidentă numai în măsura în care infracțiunea cercetată este una dintre cele prevăzute în cuprinsul art. 148 alin. (1) lit. a) C.pr.pen., în care se arată că aceasta poate fi utilizată în caz de: „*infracțiuni contra securității naționale prevăzute*

[1] *C. Olaru*, op. cit., p. 43.

[2] *D.C-tin Mâță*, Securitatea națională. Concept. Reglementare. Mijloace de ocrotire, Ed. Hamangiu, București, 2016, p. 394.

de Codul penal și de alte legi speciale, precum și în cazul infracțiunilor de trafic de droguri, de efectuare de operațiuni ilegale cu precursori sau cu alte produse susceptibile de a avea efecte psihoactive, infracțiunilor privind nerespectarea regimului armelor, munițiilor, materialelor nucleare, al materiilor explozive și al precursorilor de explozivi restricționați, trafic și exploatarea persoanelor vulnerabile, acte de terorism sau asimilate acestora, de finanțare a terorismului, spălare a banilor, falsificare de monede, timbre sau de alte valori, falsificare de instrumente de plată electronică, în cazul infracțiunilor care se săvârșesc prin sisteme informatice sau mijloace de comunicare electronică, șantaj, lipsire de libertate în mod ilegal, evaziune fiscală, în cazul infracțiunilor de corupție, al infracțiunilor asimilate infracțiunilor de corupție, al infracțiunilor împotriva intereselor financiare ale Uniunii Europene".

Această listă evidențiază infracțiunile considerate ca prezentând cel mai înalt grad de risc pentru orânduirea socială contemporană, însă legiuitorul a inclus și un criteriu subsidiar privitor la pedeapsă, pentru a include orice infracțiune care ar fi de o anumită gravitate în sfera celor care pot justifica, sub aspectul gravității, autorizarea măsurii. Prin teza ultimă a art. 148 alin. (1) lit. a) C.pr.pen., utilizarea investigatorilor sub acoperire și a colaboratorilor se poate autoriza și „*în cazul altor infracțiuni pentru care legea prevede pedeapsa închisorii de 7 ani sau mai mare*". Raportându-ne la condiția subsidiară prevăzută în cazul supravegherii tehnice, observăm că legiuitorul a considerat că utilizarea investigatorilor sub acoperire și a colaboratorilor trebuie să fie restricționată „*la fapte de mai mare gravitate decât cele pentru care se poate dispune supravegherea tehnică*".

În mod corect s-a arătat în doctrină faptul că, și în situația în care actele preparatorii ale unor infracțiuni nu sunt pedepsite, însă fapta scop va îndeplini condițiile pentru a se dispune o măsură specială de supraveghere sau cercetare, se va avea în vedere infracțiunea scop[1] sub aspectul gravității.

Spre deosebire de supravegherea tehnică, utilizarea investigatorilor sub acoperire și a colaboratorilor se poate autoriza și în situația în care „*există o suspiciune rezonabilă că o persoană este implicată în activități infracționale ce au legătură cu infracțiunile enumerate la art. 148 alin. (1) lit. a) C.pr.pen.*", o situație distinctă față de cele arătate deja și care pune probleme privind claritatea textului de lege, deoarece nu sunt determinate activitățile infracționale care ar putea atrage posibilitatea folosirii măsurii speciale de cercetare. Neajunsul unei asemenea formulări este că nu obligă procurorul să detalieze care sunt activitățile infracționale proprii de care persoana este suspectată, fiind reglementat un caz subsidiar în care se poate autoriza măsura într-un mod care lasă loc arbitrariului.

O sursă a confuziei textului de lege o constituie noțiunea de „implicare în activități infracționale", o formulare improprie, în condițiile în care desfășurarea unei activități infracționale este sinonimă cu săvârșirea unei infracțiuni. În plus față de această constatare, observăm că nu se definește ce înseamnă o activitate infracțională care are legătură cu infracțiunile menționate mai sus. Într-un sens larg, putem accepta că va constitui o asemenea activitate infracțională săvârșirea oricărei infracțiuni în legătură cu cele menționate de textul de lege, însă considerăm că o asemenea abordare ar constitui o interpretare mult prea extinsă, ceea ce ar da prilej folosirii investigatorilor sub acoperire ori a colaboratorilor în orice cauză penală. Într-un sens mai restrâns, prin „activități infracționale în legătură cu infracțiunile prevăzute de Cod" putem

[1] *C.M. Chiriță*, în N. Volonciu, A.S. Uzlău (coord.), Noul Cod, 2014, p. 311.

înțelege *infracțiunile conexe*, în unele sisteme, considerate forme de participație subsecventă[1], privite de legiuitorul român ca infracțiuni *sui generis*, prin incriminarea infracțiunilor de tăinuire și favorizarea făptuitorului. *De lege ferenda*, se impune folosirea expresiei „există o suspiciune rezonabilă că o persoană a săvârșit o infracțiune pentru a sprijini săvârșirea infracțiunilor prevăzute" în art. 148 alin. (1) lit. a) C.pr.pen.

Cea de-a doua condiție care se impune a fi îndeplinită este cea privitoare la *proporționalitatea măsurii cu restrângerea drepturilor și libertăților fundamentale*. Această condiție este prevăzută de art. 148 alin. (1) lit. b) C.pr.pen. și se impune a fi analizată de procuror prin prisma criteriilor prevăzute de textul de lege: *particularitățile cauzei, importanța informațiilor ori a probelor ce urmează a fi obținute sau gravitatea infracțiunii*.

Proporționalitatea trebuie privită atât raportat la măsura în întregime, cât și cu privire la preferința legală a folosirii unui investigator sub acoperire față de folosirea unui colaborator. Nu se va putea accepta folosirea metodei speciale de cercetare după bunul plac al procurorului, fiind impusă numai dacă va fi proporțională prin raportare la infracțiunile ce fac obiectul urmăririi penale[2]. În același timp, măsura de cercetare nu va putea fi considerată ca fiind proporțională, în condițiile în care un procedeu probatoriu comun ar fi suficient pentru stabilirea stării de fapt. În același timp, potrivit reglementării în vigoare, proporționalitatea utilizării metodelor speciale de supraveghere sau cercetare va fi analizată *in concreto*, de către organele judiciare, prin raportare la obiectivul urmărit prin folosirea acestora. Această abordare a fost corect criticată în doctrină ca fiind incapabilă de a asigura un just echilibru între exigențele de interes general și salvgardarea drepturilor și libertăților fundamentale[3].

O situație specială o reprezintă *subsidiaritatea măsurii de cercetare* față de supravegherea tehnică. În doctrină s-a arătat că metoda de cercetare ar avea un caracter subsidiar față de supravegherea tehnică[4], considerându-se că, în măsura în care probele ar putea fi obținute prin supraveghere tehnică, nu va putea fi autorizată utilizarea investigatorilor sub acoperire. Nu putem fi de acord cu această afirmație din mai multe motive: utilizarea investigatorilor sub acoperire este o metodă specială de cercetare aparte față de procedeele probatorii, astfel că, în urma folosirii acesteia, nu vor rezulta probe, ci numai date și informații[5]. Totodată, ambele metode speciale pot fi folosite în același timp, așa cum rezultă și din prevederile art. 148 alin. (3) C.pr.pen., iar utilizarea investigatorilor și colaboratorilor se poate dispune nu numai când o altă măsură nu este posibilă, ci și atunci când ar presupune dificultăți deosebite ce ar prejudicia ancheta.

Prin „particularitățile cauzei" vom înțelege acele împrejurări specifice unei anumite cauze penale care vor impune utilizarea măsurii de cercetare pentru soluționarea cauzei, deoarece un altfel de mijloc nu ar fi propice pentru a stabili starea de fapt. De exemplu, în cazul infracțiunii de constituire a unui grup infracțional organizat, prevăzută de art. 367 C.pen., măsura poate

[1] *Tr. Pop*, Drept penal comparat. Partea generală, vol. II, Institutul de Arte Grafice „Ardealul", Cluj, 1923, pp. 801-803.

[2] CCR, Dec. nr. 778 din 17 noiembrie 2015 (M. Of. nr. 111 din 12 februarie 2016) (decizie de respingere).

[3] *Gh. Mateuț*, Observații critice privind noua reglementare a supravegherii tehnice într-o prezentare comparativă, în Caiete de Drept Penal nr. 3/2015, p. 23.

[4] *M. Bulancea*, în M. Udroiu (coord.), Codul de procedură penală, 2015, p. 449.

[5] Conform art. 148 alin. (5) C.pr.pen., „investigatorul sub acoperire culege date și informații în baza ordonanței emise potrivit alin. (1)-(3), pe care le pune în totalitate la dispoziția procurorului care efectuează sau supraveghează urmărirea penală, întocmind un proces-verbal". Aceasta nu înseamnă că nu vor putea fi obținute probe derivate, precum declarațiile investigatorilor sub acoperire, ale celor cu identitate reală și ale colaboratorilor.

fi necesară raportat la particularitățile cauzei, constând în modul de operare şi modul de interacționare al membrilor grupului, care ar evita să se întâlnească în locuri publice sau să aibă vreo interacțiune ce ar putea fi observată de terțe persoane. Într-o asemenea situație, este posibil ca administrarea probelor să nu poată fi făcută prin audierea persoanelor ca urmare a relațiilor strânse dintre acestea. O situație de speță[1] poate consta în constituirea unui grup infracțional organizat pe criterii etnice (toți participanții fiind de origine vietnameză), astfel că însuși elementul care îi unește (etnia) face dificilă interacțiunea lor cu alte persoane și descoperirea hotărârii infracționale și a infracțiunilor program, impunându-se folosirea supravegherii prin video, audio sau prin fotografiere, precum și utilizarea investigatorilor sub acoperire în mod concomitent, pentru identificarea unor persoane de legătură ale grupării și pentru stabilirea ierarhiei în cadrul grupului.

Prin „importanța informațiilor ori a probelor ce urmează a fi obținute" înțelegem contribuția pe care o pot avea informațiile sau probele obținute pentru stabilirea împrejurărilor esențiale ale cauzei. Ca atare, considerăm că proporționalitatea trebuie stabilită raportat la utilitatea probei ce urmează a fi obținută în mod derivat pe baza datelor și informațiilor obținute de investigatorul sub acoperire și în funcție de împrejurarea concretă care se urmărește a se dovedi.

„Gravitatea infracțiunii" presupune, în opinia noastră, o analiză a pericolului social concret pe care îl presupune săvârșirea infracțiunii care face obiectul urmăririi penale. Deși gravitatea unei infracțiuni se manifestă în limitele de pedeapsă prevăzute de lege, ca pericol social abstract[2], considerăm că acest criteriu a fost avut în vedere de legiuitor în privința măsurii de cercetare prevăzute de art. 148 alin. (1) C.pr.pen. Astfel, se va impune analizarea proporționalității sub aspectul pericolului social concret care justifică utilizarea investigatorilor sub acoperire și a colaboratorilor.

A treia condiție impusă de Codul de procedură penală pentru dispunerea supravegherii tehnice este *necesitatea* utilizării metodei menționate anterior, în vederea obținerii informațiilor sau probei. Această condiție este prevăzută în cuprinsul art. 148 alin. (1) lit. c) C.pr.pen. și limitează folosirea investigatorilor sub acoperire și a colaboratorilor la cazurile în care *„probele sau localizarea și identificarea făptuitorului, suspectului ori inculpatului nu ar putea fi obținute în alt mod sau obținerea lor ar presupune dificultăți deosebite ce ar prejudicia ancheta ori există un pericol pentru siguranța persoanelor sau a unor bunuri de valoare"*.

Există două situații prevăzute de lege în care se poate considera ca fiind necesară utilizarea investigatorilor sub acoperire și a colaboratorilor: *i)* imposibilitatea (absolută sau relativă) obținerii probelor localizării ori identității făptuitorului prin alt mod; *ii)* existența unui pericol pentru siguranța persoanei sau a unor bunuri de valoare.

În prima situație, necesitatea utilizării investigatorilor sub acoperire și a colaboratorilor este determinată de imposibilitatea obținerii datelor și informațiilor în orice alt mod, adică prin utilizarea unui procedeu probatoriu ori a altei măsuri de cercetare (imposibilitate absolută), or, obținerea probei prin utilizarea unui alt mijloc de probă ar aduce serioase impedimente anchetei (imposibilitate relativă). Prin această prevedere, legiuitorul subliniază faptul că, în cursul urmăririi penale, este obligatorie folosirea altor mijloace mai puțin intruzive dacă ele sunt apte să conducă la aceleași rezultate[3]. Considerăm că simpla celeritate a desfășurării

[1] C. Ap. Timișoara, dec. pen. nr. 205/A din data de 23 octombrie 2013, pronunțată în dosar nr. 5502/108/2013, nepublicată.

[2] *M. Basarab,* op. cit., p. 140.

[3] *M. Udroiu, O. Predescu*, Protecția europeană, 2008, p. 829.

procesului penal nu poate justifica apelarea la măsuri speciale de supraveghere sau cercetare drept o soluție, sensul dorit de legiuitor fiind cel de a se apela la aceste mijloace în situația în care îngreunarea ar proveni mai ales din perspectiva posibilității obținerii unei probe în condiții dificile, printr-un efort deosebit al organelor de urmărire penală.

Textul de lege al celei de-a treia condiții este asemănător celui utilizat în cazul supravegherii tehnice, cu diferența că, alături de obținerea unor probe ca urmare a folosirii investigatorilor sub acoperire sau a colaboratorilor, măsura de cercetare poate fi folosită și pentru localizarea și identificarea făptuitorului. Această diferență relevă natura sa de măsură de cercetare, și nu de procedeu probatoriu, deoarece identitatea făptuitorului și localizarea sa nu constituie obiect al probațiunii, ci reprezintă doar informații cu privire la o persoană. Prin „identificarea făptuitorului" considerăm că legiuitorul a avut în vedere situația în care există deja probe cu privire la săvârșirea unei infracțiuni, dar și date care să restrângă identificarea la un anumit grup. Rolul investigatorului sub acoperire și al colaboratorului ar consta în descoperirea persoanelor ori a probelor care pot furniza probe în dovedirea săvârșirii de către o persoană a unei infracțiuni.

Cea de-a doua situație prevede utilizarea investigatorilor sub acoperire și a colaboratorilor în cazul în care există un *pericol pentru siguranța persoanelor sau pentru unele bunuri de valoare*. Necesitatea este dată de însești valorile sociale ce ar urma să fie lezate de infracțiunea care se urmărește a fi săvârșită. În această situație vom fi numai în cazul unei anchete proactive, în care se urmărește prevenirea săvârșirii unei infracțiuni, nu și a strângerii de probe privind o infracțiune deja săvârșită. Acest lucru reiese din însești valorile sociale determinate generic (siguranța persoanei incluzând viața, integritatea fizică a persoanei și libertatea persoanei), față de care nu poate exista *un pericol*, în măsura în care infracțiunile respective sunt deja consumate.

Capitolul III
Procedura de autorizare a utilizării investigatorilor sub acoperire și a colaboratorilor

Măsura de cercetare a utilizării investigatorilor sub acoperire şi a colaboratorilor este una dintre metodele speciale de supraveghere sau cercetare pe care legiuitorul a lăsat-o la decizia procurorului pentru a fi utilizată în cursul urmăririi penale. Așa cum am arătat deja, există o lipsă de coeziune în cadrul metodelor speciale de supraveghere sau cercetare cu privire la criteriul care determină organul competent să le dispună, neexistând o reglementare coerentă, în special cu privire la metodele de cercetare prevăzute de art. 138 alin. (1) lit. f)-j) C.pr.pen., în care se alternează între autorizarea de către judecătorul de drepturi şi libertăți şi autorizarea de către procuror[1]. Deoarece utilizarea investigatorilor sub acoperire este o metodă de cercetare care interferează în mod semnificativ cu normala exercitare a drepturilor fundamentale ale persoanei, s-a considerat în mod justificat că se impune ca autorizarea să fie de competența judecătorului de drepturi şi libertăți[2], iar toate măsurile de supraveghere sau cercetare care poartă această restrângere a drepturilor persoanei să aibă o *procedură specială unică de autorizare*, care să pună în valoare judecătorul de drepturi şi libertăți[3]. Prin transferarea competenței de autorizare către judecătorul de drepturi şi libertăți considerăm că nu s-ar aduce atingere în vreun mod celerității desfășurării urmăririi penale, având în vedere că scopul creării acestei instituții este existența unui organ care să fie în permanență la dispoziția organelor de urmărire pentru judecarea cererilor în domeniul administrării probelor, a măsurilor preventive, asigurătorii şi de siguranță provizorii.

De lege lata, procurorul este cel care dispune asupra autorizării utilizării investigatorilor sub acoperire şi a colaboratorilor pentru o perioadă de maximum 60 de zile atunci când constată că sunt îndeplinite condițiile prevăzute de lege şi măsura este oportună din punct de vedere tactic. Ca măsură de cercetare, considerăm că oportunitatea va juca un rol important, deoarece alegerea momentului tactic pentru realizarea unor acte de procedură este esențială pentru desfășurarea cu succes a urmăririi penale, fiind necesar ca procurorul să aibă în vedere întregul său plan de urmărire penală şi să se raporteze şi la celelalte măsuri de cercetare sau procedee probatorii.

În conformitate cu prevederile art. 148 alin. (2) C.pr.pen., autorizarea se va dispune de către procuror *din oficiu* sau *la cererea organului de cercetare penală*, în toate cazurile, procurorul emițând o ordonanță în acest sens. Considerăm că legiuitorul a folosit impropriu expresia „la cererea organului de cercetare penală", în condițiile în care organul de urmărire penală nu este un subiect procesual principal ori parte în procesul penal pentru ca, în baza acestor calități, să aibă dreptul de a formula *cereri*. Procurorul şi organul de cercetare penală sunt în mod egal organe de urmărire penală, or, terminologia de cerere este aplicabilă în cazul în care s-ar adresa către un organ de o altă natură (de pildă, judecător de drepturi şi libertăți). Mai mult, nu putem vorbi despre o aprobare a unei cereri în condițiile în care urmărirea penală

[1] *C.M. Chiriță*, în N. Volonciu, A.S. Uzlău, Noul Cod, 2014, pp. 335-336.

[2] *Gh. Mateuț*, Observații critice privind noua reglementare a supravegherii tehnice într-o prezentare comparativă, în Caiete de Drept Penal nr. 3/2015, p. 13.

[3] *Ibidem*.

se exercită, în principal, de către procuror, astfel că acesta nu își poate decât *asuma* poziția organului de cercetare penală. *De lege ferenda*, se impune înlocuirea expresiei de „cerere a organului de cercetare penală" cu expresia „propunerea organului de cercetare penală", în acest sens menținându-se coerența Codului în privința relației dintre procuror și organele de cercetare penală. În cazul în care organul de cercetare va propune folosirea investigatorilor sub acoperire ori a colaboratorilor, se va impune întocmirea unui referat.

O problemă aparte, neabordată de Codul de procedură penală, este posibilitatea utilizării mai multor investigatori sub acoperire ori a mai multor colaboratori sau, în același timp, și a investigatorilor sub acoperire și a colaboratorilor. Observăm că nu există nicio dispoziție legală care să interzică folosirea mai multor persoane în cadrul acestei măsuri de cercetare, situație în care ordonanța procurorului se va putea referi la unul sau la mai mulți investigatori sau colaboratori ori procurorul va putea emite ordonanțe succesive, în funcție de necesități. O situație specială o constituie folosirea împreună a investigatorilor sub acoperire și a colaboratorilor concomitent sau succesiv. Într-o interpretare a dispozițiilor art. 148 alin. (10) C.pr.pen., prin care se arată că se poate dispune folosirea colaboratorilor atunci când „*folosirea investigatorului sub acoperire nu este suficientă*", putem considera că se poate dispune atât folosirea investigatorilor, cât și a colaboratorilor. În mod evident, va trebui respectată o condiție ce ține de subsidiaritatea folosirii colaboratorilor: autorizarea pentru activități diferite a investigatorului și a colaboratorului.

În privința duratei măsurii, subliniem faptul că durata maximă a măsurii va fi calculată de la prima autorizare a unui investigator ori colaborator, și nu pentru fiecare agent în parte. Emiterea unor ordonanțe succesive va fi legală în condițiile în care, așa cum vom vedea mai jos, ordonanța procurorului va trebui să justifice pentru fiecare investigator sau colaborator în parte folosirea sa, prin raportare și la activitățile concrete pe care le va realiza. Cu alte cuvinte, investigatorul și colaboratorul *sunt autorizați în mod limitat pentru anumite activități*.

Potrivit art. 148 alin. (9) C.pr.pen., „*durata totală a măsurii în aceeași cauză și cu privire la aceeași persoană nu poate depăși un an*". Cu toate acestea, semnalăm o problemă deosebit de gravă în reglementarea actuală a măsurii de cercetare, în condițiile în care există o excepție de la această regulă, prin care, în cazul anumitor infracțiuni, măsura poate fi prelungită pe un termen nedeterminat. Infracțiunile pentru care nu există un termen maxim de utilizare a măsurii sunt cele contra vieții, securității naționale, infracțiunilor de trafic de droguri, trafic de arme, trafic de persoane, acte de terorism, spălare a banilor și infracțiunile contra intereselor financiare ale Uniunii Europene. Deși lista pare a indica infracțiuni deosebit de grave, trebuie să avem în vedere că măsura de cercetare se poate dispune și dacă există suspiciunea privind implicarea unei persoane în activități infracționale în legătură cu aceste infracțiuni, situație în care se va extinde în mod nepermis și durata maximă a măsurii. În doctrină s-a arătat că, în lipsa unor prevederi exprese, măsura va putea fi folosită de procuror până la terminarea urmăririi penale, cu respectarea prevederilor privind prelungirea din 60 în 60 de zile a măsurii[1]. O astfel de constatare nu ajută, ci numai subliniază lipsa de logică a legiuitorului, în condițiile în care procurorului i-ar fi permisă folosirea măsurii până când ar reuși să obțină suficiente probe pentru a dovedi săvârșirea unei infracțiuni. Nu putem fi de acord cu această lacună legislativă, deoarece lasă loc abuzurilor din partea organelor de urmărire penală. În plus, lipsa unei durate maxime reprezintă o necorelare cu dispozițiile privind supravegherea tehnică, în care durata maximă a măsurii este de 120 de zile, potrivit art. 144 alin. (3) C.pr.pen.,

[1] *C.M. Chiriță*, în N. Volonciu, A.S. Uzlău (coord.), Noul Cod, 2014, p. 338.

indiferent de fapta care face obiectul urmăririi penale. *De lege ferenda*, se impune ca această excepție de la regula duratei maxime de un an să fie înlăturată, deoarece aduce o gravă atingere drepturilor fundamentale ale persoanei, în special dreptului la viață privată, prevăzut de art. 26 din Constituție.

O instituție care nu a fost prevăzută expres de legiuitor este *încetarea măsurii utilizării investigatorilor sub acoperire și a colaboratorilor*, spre deosebire de supravegherea tehnică, în care se reglementează distinct posibilitatea ca procurorul să dispună încetarea măsurii în cazul în care temeiurile care au justificat-o nu mai există. Pentru mai buna apărare a drepturilor persoanei vizate de această măsură de cercetare, se impune ca legiuitorul să introducă, pe cale de analogie, o prevedere similară cu cea incidentă în cazul supravegherii tehnice, care să retragă mandatul investigatorului sub acoperire și a colaboratorului de a-și continua activitatea până la expirarea măsurii.

Potrivit art. 148 alin. (2) lit. a)-c) C.pr.pen., în cuprinsul ordonanței procurorului se vor regăsi în mod obligatoriu următoarele elemente: *indicarea activităților pe care investigatorul sub acoperire sau colaboratorul este autorizat să le desfășoare*, *perioada pentru care s-a autorizat măsura* și *identitatea atribuită investigatorului sub acoperire sau colaboratorului*.

Cel mai important element din cuprinsul ordonanței procurorului îl constituie *indicarea activităților pe care investigatorul sub acoperire sau colaboratorul este autorizat să le desfășoare*, deoarece, față de această dispoziție, se va analiza, în principal, dacă agentul era autorizat să efectueze anumite acțiuni. Ordonanța reprezintă mandatul investigatorului sub acoperire și a colaboratorului[1], astfel că trebuie descrise cât mai detaliat acțiunile pe care aceștia pot să le întreprindă și pentru care sunt protejați de orice răspundere penală sau civilă. Verificarea respectării limitelor mandatului se va face în procedura camerei preliminare de către judecătorul de cameră preliminară, care, în situația depășirii mandatului de către investigatorul sub acoperire sau colaborator, va putea constata nulitatea actelor efectuate de acesta și va putea dispune excluderea probelor obținute în baza excesului de mandat. În situația în care proba care derivă din activitățile sale este însăși declarația investigatorului ori a colaboratorului, se va impune excluderea în integralitate a acesteia. Codul de procedură penală nu cunoaște sancțiunea nulității parțiale a unui act, ci doar a nulității totale a acestuia, astfel că nu se vor putea exclude numai părți ale declarației viciate. În măsura în care s-ar constata această nelegalitate, nu se va mai putea proceda la audierea în fața instanței a investigatorului sau colaboratorului cu privire la aspectele aflate în afara activităților pentru care a fost autorizat, deoarece și această declarație ar deveni nelegală.

În situația în care se constată o depășire a autorizării, considerăm că se va putea atrage răspunderea penală sau civilă a investigatorului sub acoperire sau a colaboratorului pentru acțiunile întreprinse, dacă acestea au lezat în vreun mod drepturile fundamentale ale persoanei care a fost suspusă măsurii de cercetare. Dacă o răspundere penală rămâne iluzorie în condițiile în care nu se va putea divulga identitatea reală a agentului, considerăm că *se va putea atrage răspunderea civilă delictuală a statului român pentru acțiunile ilicite ale investigatorului sub acoperire sau ale colaboratorului*.

În toate cazurile, activitatea investigatorilor sub acoperire și a colaboratorilor trebuie să se desfășoare în așa fel încât să nu ducă la provocarea săvârșirii de infracțiuni, în condițiile în care este nelegală determinarea unei persoane să săvârșească o infracțiune pentru a obține o probă. S-a arătat că rațiunea acestei interdicții constă în aceea că statul nu poate, prin agenții

[1] *Ibidem*.

săi, inclusiv un colaborator, să își depășească obligația de a aplica legea prin instigarea unei persoane să săvârșească o infracțiune pe care altfel nu ar fi comis-o[1]. Aceeași interdicție va fi incidentă și în situația în care se va autoriza concomitent și măsura participării autorizate la anumite activități. În dreptul francez, în situația în care se descoperă că proba s-a obținut prin provocare, sancțiunea incidentă va fi nulitatea absolută[2], o soluție superioară celei găsite de legiuitorul român în cuprinsul art. 101 C.pr.pen. Cu toate acestea, s-a arătat în jurisprudența națională că folosirea investigatorului sub acoperire pentru prinderea în flagrant a unei persoane pentru trafic de droguri nu constituie o încălcare a principiului loialității probei, în sensul dispozițiilor art. 68 alin. (2) C.pr.pen. anterior, dacă făptuitorul a luat hotărârea de a comite și a comis în mod repetat acțiuni specifice traficului de droguri înainte de a fi utilizat un investigator sub acoperire[3]. Pentru a diferenția o acțiune specifică măsurii utilizării investigatorilor sub acoperire și a colaboratorilor, putem apela la următorul exemplu: va constitui o activitate specifică măsurii de cercetare prezentarea ca un potențial cumpărător de droguri, afișarea unor sume de bani de către investigator către vânzătorul de droguri (*flash-roll*), în scopul simulării unei cumpărări[4]. În schimb, efectiva cumpărare de droguri de către un investigator sau colaborator va trebui să fie autorizată ca participare autorizată la anumite activități.

Cu privire la natura activităților pe care procurorul le va autoriza în cuprinsul ordonanței sale, nu va putea fi inclusă folosirea unor procedee probatorii, în special a unor măsuri de supraveghere tehnică. Singurele măsuri de supraveghere tehnică care pot fi utilizate de investigatorii sub acoperire și colaboratori sunt cele prevăzute de art. 138 alin. (1) lit. c) C.pr.pen., numai dacă se emite de către judecătorul de drepturi și libertăți un mandat de supraveghere tehnică pentru acestea. În consecință, orice alte măsuri de supraveghere tehnică nu vor putea fi puse în executare de către agenți și nici nu se va putea proceda la efectuarea unor procedee probatorii prin intermediul acestora, orice încălcare a acestei limitări ducând la nelegalitatea probei administrate.

În legătură cu activitățile pe care investigatorii și colaboratorii sunt autorizați să le întreprindă, considerăm că în cuprinsul ordonanței trebuie să se facă precizarea înscrisurilor ori obiectelor pe care organele judiciare le pun la dispoziția acestora. Motivul este că folosirea acestora trebuie să fie autorizată de către procuror, pentru a nu constitui o infracțiune. De pildă, va fi necesar ca investigatorul sub acoperire ori colaboratorul cu o altă identitate să primească acte de identitate ori alte înscrisuri care să certifice identitatea sa conspirativă, or, folosirea unor asemenea acte ar constitui infracțiune, atât pentru aceștia, cât și pentru organul de urmărire penală[5]. Prin dispozițiile art. 148 alin. (7) C.pr.pen. se introduce o *cauză justificativă*, menită a da o coerență legislației penale și de a pune la adăpost de orice posibilă acuzație penală folosirea unor obiecte de către investigator sau colaborator. În doctrină[6] s-a susținut că aceasta ar reprezenta o cauză de nepedepsire, opinie cu care nu putem fi de acord, pentru motivele pe care le vom arăta într-o altă secțiune[7].

---

[1] *M. Udroiu, R. Slăvoiu, O. Predescu*, Tehnici speciale, 2009, p. 165.

[2] *I.-C. Pașca*, Criminalitatea organizată în perspectiva legislațiilor europene, Ed. Universul Juridic, București, 2015, p. 129.

[3] ICCJ, s. pen., dec. nr. 5269 din 6 noiembrie 2007, pe *www.scj.ro*

[4] *C. Olaru*, op. cit., p. 55.

[5] Infracțiuni de fals, precum falsul privind identitatea (art. 327 C.pen.), uzul de fals (art. 323 C.pen.), falsul material în înscrisuri oficiale (art. 320 C.pen.).

[6] *C.M. Chiriță*, în N. Volonciu, A.S. Uzlău (coord.), Noul Cod, 2014, p. 339.

[7] *V. infra*, Titlul XII, Capitolul IV.3.

Un alt exemplu care poate fi imaginat este furnizarea unei arme ori muniții interzise[1] investigatorului sub acoperire ori colaboratorului, ceea ce ar putea contraveni regimului armelor și munițiilor stabilit prin Legea nr. 295/2004 privind regimul armelor și munițiilor, republicată[2], în măsura în care folosirea acestora nu va cădea sub incidența participării autorizate la anumite activități. Desigur, în situația în care necesitatea folosirii unor înscrisuri sau obiecte survine emiterii ordonanței de autorizare, considerăm că se va putea dispune ulterior încuviințarea folosirii acestora printr-o ordonanță a procurorului.

În jurisprudență s-a apreciat că desfășurarea activităților autorizate de procuror în afara unei arii teritoriale stabilite de acesta prin ordonanța de autorizare nu va afecta legalitatea măsurii, întrucât prin aceasta s-ar adăuga la lege o mențiune care nu este prevăzută de Codul de procedură penală[3]. Nu considerăm că soluția judiciară este una corectă, întrucât chiar dacă legiuitorul nu stabilește o mențiune privind aria geografică în care investigatorul sau colaboratorul este autorizat să acționeze, aceasta va face parte dintre activitățile care îi sunt autorizate, astfel că locația desfășurării intră în înțelesul art. 148 alin. (2) lit. a) C.pr.pen.[4]. Astfel, depășirea oricărei mențiuni din cuprinsul actului de autorizare, inclusiv aria geografică de desfășurare a activităților, va atrage nelegalitatea acestora.

Prin „perioada pentru care s-a autorizat măsura" înțelegem intervalul de timp determinat în mod absolut pentru care s-a autorizat măsura, cu indicarea datei și orei de la care curge și la care expiră. Așa cum prevede și art. 148 alin. (1) C.pr.pen., măsura se poate dispune pentru o perioadă de maximum 60 de zile. La determinarea perioadei optime pentru care se va autoriza măsura, procurorul va trebui să aibă în vedere elemente, precum complexitatea cauzei, mărimea grupului infracțional, durata necesară pentru infiltrarea investigatorului[5], or, în cazul unui colaborator, a relațiilor pe care le are acesta în cadrul grupului infracțional vizat. În situația în care procurorul constată că durata măsurii este insuficientă pentru atingerea scopului pentru care aceasta a fost autorizată și dacă există motive temeinice, va proceda potrivit art. 148 alin. (9) C.pr.pen. și va prelungi măsura.

Referitor la *identitatea atribuită investigatorului sub acoperire* ori *colaboratorului*, după caz, procurorul va dispune ca persoana în cauză să fie cunoscută sub o denumire generică, inventată de organul de urmărire penală și i se vor atribui la acel moment date de stare civilă care să corespundă cu noua identitate. În cuprinsul ordonanței nu vor putea fi folosite numele reale ale investigatorilor sub acoperire ori ale colaboratorilor cu altă identitate, ele rămânând secrete și neputând fi divulgate, potrivit art. 149 alin. (1) C.pr.pen. În situația în care colaboratorul se va folosi de identitatea sa reală, atunci este obligatorie menționarea sa expresă în cuprinsul ordonanței procurorului, cu indicarea numelui și prenumelui acestuia, precum și a datelor sale

[1] Potrivit art. 2 pct. II.1 din Legea nr. 295/2004 privind regimul armelor și al munițiilor, republicată, prin „arme și muniții interzise" înțelegem „armele și munițiile prevăzute în categoria A din anexă, a căror procurare, deținere, port și folosire sunt interzise persoanelor fizice și juridice, cu excepția (...) instituțiilor publice care au competențe în domeniul apărării, ordinii publice și securității naționale, a unităților aflate în subordonarea sau coordonarea acestora, înființate prin acte normative, (...) precum și a companiilor naționale și societăților reglementate de Legea nr. 31/1990, republicată, cu modificările și completările ulterioare, constituite prin acte normative în vederea producerii acestui tip de armament și muniție".

[2] Legea nr. 295 din 28 iunie 2004 (publicată în M. Of. nr. 583 din 30 iunie 2004 și republicată în M. Of. nr. 425 din 10 iunie 2014).

[3] C. Ap. București, s. a II-a pen., dec. pen. nr. 340 din 23 iunie 2015.

[4] În același sens, *C. Moisă*, op. cit., p. 149.

[5] *V. infra*, Titlul XII, Capitolul IV.1.

de identificare. Totodată, la momentul la care se autorizează măsura, este necesar a se menționa că se vor emite înscrisuri în dovedirea identității, cu nominalizarea acestora în ordonanță.

Alături de cele trei elemente care trebuie incluse, în cuprinsul ordonanței vor mai fi menționate și elementele comune oricărei ordonanțe, prevăzute de Cod la art. 286 alin. (2). Astfel, ordonanța va mai cuprinde: *i)* denumirea parchetului și data emiterii; *ii)* numele, prenumele și calitatea de procuror a emitentului; *iii)* fapta care face obiectul urmăririi penale, încadrarea juridică a acesteia; *iv)* date referitoare la persoana suspectului sau inculpatului (după caz). Elementele prevăzute la art. 286 alin. (2) lit. d) C.pr.pen., respectiv obiectul actului sau măsurii procesuale, precum și motivele de fapt și de drept ale acestora, se regăsesc în mod implicit în cele trei condiții speciale prevăzute în cazul autorizării folosirii investigatorilor sub acoperire și a colaboratorilor.

Capitolul IV
Obținerea probelor în procesul penal prin intermediul investigatorilor sub acoperire și a colaboratorilor

Așa cum am arătat în secțiunile anterioare, utilizarea investigatorilor sub acoperire și a colaboratorilor nu este un procedeu probatoriu, ci o metodă de cercetare, astfel că finalitatea nu constă în obținerea unor probe. Cu toate acestea, legiuitorul a prevăzut că din activitatea desfășurată de investigatori ori colaboratori pot rezulta, în mod derivat și indirect, mijloace de probe, prin mai multe procedee probatorii. Codul de procedură penală face referire expresă la două procedee probatorii: audierea investigatorului sub acoperire și a colaboratorului[1] și supravegherea video, audio sau prin fotografiere[2].

În condițiile în care investigatorii sub acoperire pot fi ofițeri de poliție judiciară, se impune a se lămuri dacă această calitate le poate conferi capacitatea de a participa la administrarea altor probe în cursul procesului penal decât cele arătate mai sus. În ceea ce ne privește, considerăm că, odată atribuită calitatea de investigator sub acoperire, această persoană nu mai are capacitatea de a fi și organ de urmărire penală sau de a strânge probe. Din punctul de vedere al formalităților de efectuare a oricărui act de urmărire penală, orice procedeu probatoriu prin care se obține un mijloc de probă trebuie să consemneze *numele și calitatea* organului de urmărire penală, ceea ce nu poate fi cazul în situația în care avem de-a face cu un investigator sub acoperire, care nu își va putea declina adevărata identitate în actele pe care le încheie. Un alt argument pentru care investigatorul sub acoperire nu va putea proceda la strângerea de probe îl constituie faptul că acțiunile sale au caracter ascuns, or, principiul legalității impune ca întreg procesul penal să se desfășoare cu respectarea legii, fiind necesară transparență în desfășurarea actelor de urmărire penală, pentru a se verifica fiecare act. De exemplu, în măsura în care un investigator sub acoperire ar proceda la strângerea de probe constând în înscrisuri, prin sustragerea acestora de la făptuitorii față de care s-a dispus măsura de cercetare, va fi pusă la îndoială legalitatea obținerii acelor înscrisuri, în condițiile în care acestea nu sunt obținute printr-un procedeu probatoriu (percheziție, ridicarea de obiecte, înscrisuri sau date informatice etc.) și în baza unui act procesual al procurorului, impunându-se excluderea acestora ca fiind obținute în mod nelegal, deoarece lipsește actul procesual prin care se dispune administrarea acestor probe. Într-o asemenea situație, investigatorul sub acoperire poate descoperi existența unor înscrisuri, poate informa de îndată procurorul, iar acesta din urmă să dispună în consecință prin ordonanță asupra administrării probei.

În concluzie, singurele probe care vor putea proveni ca urmare a activităților investigatorului sub acoperire sau ale colaboratorului vor fi înregistrările audio și video, fotografiile, la care se vor alătura declarațiile acestora.

---

[1] Potrivit art. 148 alin. (8) C.pr.pen., „investigatorii sub acoperire pot fi audiați ca martori în procesul penal în aceleași condiții ca și martorii amenințați".

[2] Potrivit art. 148 alin. (3) C.pr.pen., „în cazul în care procurorul apreciază că este necesar ca investigatorul sub acoperire să poată folosi dispozitive tehnice pentru a obține fotografii sau înregistrări audio și video, sesizează judecătorul de drepturi și libertăți în vederea emiterii mandatului de supraveghere tehnică. Dispozițiile art. 141 se aplică în mod corespunzător".

Secțiunea 1. Încuviințarea folosirii dispozitivelor tehnice pentru a obține fotografii sau înregistrări audio și video

În mod excepțional, Codul de procedură penală a prevăzut că investigatorii sub acoperire și colaboratorii pot fi împuterniciți să folosească dispozitive tehnice pentru realizarea unor fotografii ori înregistrări audio și video, ceea ce echivalează cu o contribuție în administrarea probelor în cursul procesului penal. Potrivit art. 148 alin. (3) C.pr.pen., obținerea acestor probe este condiționată de obținerea mandatului de supraveghere tehnică ori de autorizarea temporară a procurorului în acest sens. În opinia noastră, această formă de supraveghere tehnică va avea un caracter *specializat* și *restrâns*.

Prin „specializat", ne referim la faptul că supravegherea tehnică va fi realizată în contextul folosirii investigatorilor sub acoperire și a colaboratorilor, cu sprijinul acestora. Nu vom fi într-o asemenea situație atunci când se va pune în executare un mandat de supraveghere tehnică prin organe de poliție care se folosesc de o altă identitate pentru a instala tehnica de supraveghere audiovideo, deoarece este de natura implementării supravegherii tehnice în această situație declinarea, la nevoie, a unei identități fictive pentru a nu fi descoperită măsura. În cazul folosirii investigatorilor sub acoperire, supravegherea tehnică specializată va constitui o activitate complementară misiunii investigatorului sub acoperire. Un alt argument pentru caracterul specializat al măsurii este punerea în executare a măsurii numai de către investigatorul sub acoperire sau colaborator, nu și de celelalte organe menționate în cuprinsul art. 142 C.pr.pen.

Prin caracterul „restrâns" al măsurii, înțelegem limitarea măsurilor de supraveghere tehnică la cele prevăzute de art. 138 alin. (1) lit. c) C.pr.pen., la care se face referire expres prin art. 148 alin. (3) C.pr.pen., nefiind posibilă încuviințarea altor măsuri. În același timp, menționăm că nu se poate proceda la folosirea investigatorilor sub acoperire ori a colaboratorilor pentru realizarea oricărui alt procedeu probatoriu, singura excepție fiind fotografierea și realizarea de înregistrări audio și video. Prin aceasta s-a urmărit a se evita desfășurarea unei urmăriri penale numai prin mijlocirea investigatorilor sub acoperire, chiar și cu privire la metodele speciale de supraveghere sau cercetare.

Observăm că această instituție completează o măsură de cercetare – utilizarea investigatorilor sub acoperire și a colaboratorilor – cu metoda specială a supravegherii tehnice. Consecința acestui fapt este că orice probă obținută în urma supravegherii tehnice despre care facem vorbire se va afla într-o relație strânsă cu măsura de cercetare, derivând din aceasta. Pentru acest motiv, credem că înregistrările și fotografiile obținute de investigatorii sub acoperire și colaboratori vor fi *probe derivate* din operațiunea sub acoperire. Ca atare, la analizarea legalității administrării probelor în camera preliminară, se va impune constatarea legalității atât a ordonanței procurorului prin care s-a dispus autorizarea folosirii investigatorilor sub acoperire și a colaboratorilor, cât și a încheierii judecătorului de drepturi și libertăți prin care s-a încuviințat supravegherea tehnică, nelegalitatea unuia dintre cele două acte ducând la excluderea ca nelegală a probelor. Această situație este atipică, deoarece regula presupune excluderea probelor numai în situația în care s-a procedat la constatarea nulității actului de procedură prin care s-a dispus administrarea acelei probe[1], situație aplicabilă numai încheierii judecătorului de drepturi și libertăți la o primă vedere. Cu toate acestea, deoarece

[1] CCR, Dec. nr. 383 din 27 mai 2015, par. 21; Dec. nr. 51 din 16 februarie 2016, par. 32.

supravegherea tehnică se realizează în contextul folosirii investigatorilor sub acoperire, această măsură de cercetare creează cadrul care generează posibilitatea obținerii probelor, astfel că, în cazul constatării nulității ordonanței procurorului prin care s-a dispus autorizarea utilizării investigatorilor sub acoperire și a colaboratorilor, vor fi incidente dispozițiile art. 280 alin. (2) C.pr.pen., potrivit cărora actele îndeplinite ulterior actului nul sunt, la rândul lor, lovite de nulitate, atunci când există o legătură directă între acestea și actul declarat nul. Or, în situația prezentată, această legătură directă există, deoarece premisa emiterii încheierii prin care se încuviințează supravegherea tehnică o constituie existența unei *ordonanțe legale de autorizare a utilizării investigatorilor sub acoperire și a colaboratorilor*. Consecința constatării nulității acestei ordonanțe va atrage nulitatea încheierii judecătorului de drepturi și libertăți și va impune excluderea probelor obținute.

a) Încuviințarea măsurilor de supraveghere tehnică de către judecătorul de drepturi și libertăți;

Pentru încuviințarea măsurilor de supraveghere tehnică ce pot fi puse în executare de investigatorii sub acoperire și de colaboratori, procurorul trebuie să procedeze potrivit art. 148 alin. (3) C.pr.pen. și să sesizeze judecătorul de drepturi și libertăți cu o cerere în care să arate că solicită o supraveghere tehnică restrânsă. Considerăm că, față de natura specială a acestui tip de supraveghere tehnică, nu se va putea proceda la folosirea unui mandat de supraveghere tehnică obținut anterior, având în vedere că persoanele care vor pune în executare acest mandat nu vor avea în cauză calitățile cerute de lege[1]. Mai mult, textul de lege obligă procurorul să formuleze o nouă cerere pentru obținerea acestei supravegheri tehnice.

Judecarea cererii procurorului are loc în aceeași zi cu formularea ei, în camera de consiliu, fără citarea părților și cu prezența obligatorie a procurorului. Soluțiile pe care le poate pronunța judecătorul de drepturi și libertăți sunt fie respingerea cererii, fie admiterea ei.

Respingerea cererii se va dispune conform art. 140 alin. (6) C.pr.pen., atunci când judecătorul de drepturi și libertăți va respinge în totalitate cererea procurorului, fie ca inadmisibilă, fie ca nefondată. Considerăm că inadmisibilitatea cererii va fi atrasă în cazul care nu sunt respectate dispozițiile prevăzute de art. 139 alin. (2) C.pr.pen. privind infracțiunile în cazul cărora se poate dispune supravegherea tehnică. Un element aparte este soluția impusă de legiuitor atunci când cererea procurorului este adresată unui organ necompetent, contrar dispozițiilor art. 140 alin. (1) C.pr.pen. Astfel, în măsura în care procurorul va formula o cerere de încuviințare a supravegherii tehnice la un alt judecător de drepturi și libertăți decât cel competent, atunci cererea sa se va respinge ca inadmisibilă și nu se va proceda la o declinare de competență în sensul art. 50 C.pr.pen. O altă situație care va atrage respingerea ca inadmisibilă a cererii procurorului va fi formularea unei cereri de încuviințare identice cu o altă cerere precedentă ce a fost respinsă, în contradicție cu dispozițiile art. 140 alin. (8) C.pr.pen.

În cazul oricăreia dintre soluțiile adoptate de către judecătorul de drepturi și libertăți, aceasta nu va putea fi supusă niciunei căi de atac, însă procurorul va fi îndreptățit să formuleze o nouă cerere de încuviințare în cazul respingerii, dacă vor fi îndeplinite cerințele prevăzute de art. 140 alin. (8) C.pr.pen. Formularea unei a doua cereri de încuviințare a supravegherii tehnice va putea fi făcută numai în măsura în care au apărut sau s-au descoperit fapte sau

[1] Cu toate că investigatorul sub acoperire este un organ de poliție judiciară, el nu este un organ de cercetare penală în cauză, astfel că nu are calitatea cerută de art. 142 alin. (1) C.pr.pen. Investigatorul sub acoperire este un lucrător operativ din cadrul poliției judiciare, calitate diferită de lucrător specializat din cadrul poliției. Aceștia din urmă sunt specialiști în ramuri ale criminalisticii, informaticieni etc.

împrejurări noi, necunoscute la momentul soluționării cererii anterioare. Considerăm că această condiție nu trebuie să fie considerată una formală, ea trebuind să fie verificată în mod temeinic de către judecătorul de drepturi și libertăți, raportat la starea de fapt descrisă în cuprinsul primei cereri de încuviințare. Astfel, nu va putea constitui *descoperirea unei fapte noi* simpla schimbare a încadrării juridice, deoarece, în această situație, starea de fapt rămâne aceeași, doar semnificația sa juridică este schimbată.

Pentru ca faptele și împrejurările noi să poată justifica formularea unei noi cereri de încuviințare, este necesar ca acestea să nu fi fost cunoscute de judecătorul de drepturi și libertăți la soluționarea primei cereri de încuviințare. Semnificația acestei prevederi este bazată pe faptul că, dacă faptele sau împrejurările erau cunoscute de către judecătorul de drepturi și libertăți la momentul în care a respins prima cerere de încuviințare, acesta le-a avut în vedere atunci când a dispus respingerea cererii.

În cazul admiterii supravegherii tehnice, judecătorul de drepturi și libertăți este îndreptățit să încuviințeze numai măsura de supraveghere tehnică prevăzută de art. 138 alin. (1) lit. c) C.pr.pen. Admiterea cererii se face prin încheierea judecătorului de drepturi și libertăți, care va proceda la emiterea imediată a mandatului de supraveghere tehnică, întocmind în mod obligatoriu o minută. Măsura poate fi dispusă pentru o perioadă maximă de 30 de zile, însă, conform art. 144 C.pr.pen., poate fi prelungită, fiecare prelungire neputând depăși 30 de zile. Totodată, conform art. 144 alin. (3) C.pr.pen., durata totală a măsurilor de supraveghere tehnică cu privire la aceeași persoană nu poate depăși 6 luni, cu excepția supravegherii video, audio sau prin fotografiere *în spații private*, care nu poate depăși 120 de zile.

Așa cum am arătat deja, supravegherea tehnică prin intermediul investigatorului sub acoperire și a colaboratorului are un caracter *special*, ceea ce introduce problema duratei maxime pentru care se va putea dispune măsura. Deoarece măsurile de supraveghere tehnică aduc atingere gravă drepturilor fundamentale ale persoanei, nu se poate ca acestea să se desfășoare pentru o perioadă nelimitată în timp. Ca atare, deoarece dispozițiile art. 148 alin. (3) C.pr.pen. fac trimitere la instituția supravegherii tehnice, fără a preciza vreo limită temporală, suntem de părere că supravegherea prin fotografiere și înregistrarea audio și video realizată în aceste condiții va trebui socotită în termenul maxim de 6 luni, cu excepția situației în care se realizează în spații private.

După admiterea cererii procurorului de întrebuințare a metodelor de supraveghere tehnică, judecătorul de drepturi și libertăți emite, conform art. 140 alin. (5) C.pr.pen., *mandatul de supraveghere tehnică*, acesta trebuind să cuprindă mai multe elemente prevăzute expres de Cod. Aceste elemente sunt cele care trebuie cuprinse și în încheierea de admitere a cererii, motiv pentru care le vom aborda unitar.

Elementele comune care nu pun probleme deosebite sunt cele privind *denumirea instanței*, *data, ora și locul emiterii*, *numele, prenumele* și *calitatea persoanei care a dat încheierea și a emis mandatul*, *semnătura judecătorului și ștampila instanței*. Considerăm că nu era necesar ca mențiunea privind locul emiterii mandatului de supraveghere tehnică să mai fie prevăzută expres de către legiuitor, deoarece, fiind vorba de un judecător de drepturi și libertăți, se subînțelege faptul că acesta își va desfășura activitatea numai la sediul instanței, iar judecarea cererii se face în *cameră de consiliu*, cu prezența procurorului, nefiind permisă emiterea mandatului de supraveghere tehnică decât în același timp cu soluționarea cererii procurorului. În schimb, ora emiterii mandatului de supraveghere tehnică, alături de dată, prezintă semnificație deosebită, deoarece de la acel moment curge obligativitatea procurorului de a pune în executare mandatul

de supraveghere tehnică. Un alt element comun care nu ridică probleme este perioada pentru care se dispun măsurile de supraveghere tehnică, aceasta putând fi de maximum 30 de zile.

Alături de acestea, în cuprinsul art. 140 alin. (5) lit. e) teza a II-a C.pr.pen., legiuitorul a prevăzut că este obligatorie menționarea *scopului* pentru care s-a încuviințat măsura. Scopul este un element important în cazul acestei supravegheri tehnice limitate și specializate, deoarece trebuie să facă referire la posibilitatea utilizării mandatului numai prin intermediul investigatorului sub acoperire ori a colaboratorului.

Un alt element care trebuie să se regăsească în cuprinsul mandatului de supraveghere tehnică este numele persoanei supuse măsurii de supraveghere tehnică, dacă acesta este cunoscut. Între această persoană și persoana față de care s-a dispus utilizarea măsurii de cercetare a utilizării investigatorilor sub acoperire și a colaboratorilor trebuie să existe identitate.

O situație aparte o constituie *supravegherea video, audio sau prin fotografiere în spații private*, prin care se permite organelor de urmărire penală să pătrundă în spații private pentru a activa sau dezactiva mijloacele tehnice ce urmează a fi folosite pentru executarea măsurii de supraveghere tehnică. În opinia noastră, considerăm că va putea fi pusă în aplicare și de către investigatorul sub acoperire ori de către colaborator, în măsura în care procurorul va solicita acest lucru, judecătorul de drepturi și libertăți fiind obligat să prevadă în mod expres încuviințarea supravegherii tehnice în spații private.

În cuprinsul art. 148 alin. (3) teza finală C.pr.pen. regăsim posibilitatea ca procurorul să autorizeze temporar măsuri de supraveghere tehnică care să fie puse în executare prin intermediul persoanelor care realizează măsura de cercetare.

Nu va fi necesară o autorizare din partea organelor judiciare dacă o înregistrare ambientală este realizată de colaborator mai înainte de a dobândi această calitate prin ordonanța procurorului, în această situație fiind incidente dispozițiile art. 139 alin. (3) C.pr.pen.[1].

b) Încetarea măsurilor de supraveghere tehnică;

Pentru garantarea drepturilor persoanei vizate de mandatul de supraveghere tehnică, Codul de procedură penală a introdus instituția încetării supravegherii tehnice mai înainte de expirarea mandatului emis de judecătorul de drepturi și libertăți. Aceasta este aplicabilă și în situația în care măsura se dispune în contextul utilizării investigatorilor sub acoperire și a colaboratorilor. Instituția constituie o excepție de la regula simetriei, prin aceea că un alt organ decât cel emitent se pronunță asupra încetării supravegherii tehnice. Acest lucru este firesc raportat la faptul că, după momentul emiterii mandatului de supraveghere tehnică, judecătorul de drepturi și libertăți nu exercită supravegherea și controlul punerii în executare a supravegherii tehnice. Acest rol îi este atribuit procurorului, care, conform art. 142 alin. (4) C.pr.pen., este garantul dreptului la viață privată al persoanei față de care s-a dispus supravegherea tehnică.

De îndată ce nu mai există temeiuri care să justifice folosirea metodelor de supraveghere tehnică încuviințate, procurorul este obligat să dispună încetarea măsurii, informând de îndată judecătorul care a emis mandatul. Prin expresia „temeiurile încetează să existe", legiuitorul indică faptul că nu mai există motivele care au justificat inițial măsura[2]. În concret, există o multitudine de cazuri în care temeiurile pot înceta; deseori, din datele care sunt strânse până la acel moment, se dovedește că o anumită persoană nu are cunoștință despre săvârșirea ori pregătirea săvârșirii infracțiunii care face obiectul cauzei.

[1] *V.-I. Pușcașu, C. Ghigheci*, op. cit., p. 366.
[2] *Gr.Gr. Theodoru*, op. cit., p. 340.

O altă situație în care procurorul va fi obligat să dispună încetarea măsurii de supraveghere tehnică este atunci când se depășește un anumit moment operativ, la care temeiurile care au justificat măsura încetează să mai existe. Cel mai bun exemplu în acest sens este momentul la care încetează folosirea investigatorilor sub acoperire ori a colaboratorilor, având în vedere că măsura de supraveghere se realizează întotdeauna prin intermediul acestora.

Odată ce procurorul dispune încetarea măsurii, acesta este obligat să încunoștințeze judecătorul de drepturi și libertăți care a emis mandatul de supraveghere tehnică cu privire la încetarea măsurii. S-a arătat în literatura de specialitate că, în măsura în care nu se dispune încetarea mandatului de supraveghere tehnică în condițiile mai sus arătate, iar, în urma continuării supravegherii tehnice, sunt găsite noi informații, proba obținută va fi legal obținută[1]. Considerăm că opinia este corectă, deoarece, în lipsa ordonanței procurorului prin care acesta dispune încetarea supravegherii tehnice, măsurile de supraveghere tehnică sunt întrebuințate în mod legal, fiind de competența procurorului de a se pronunța asupra încetării existenței temeiurilor care au justificat acest procedeu probatoriu.

Datele rezultate din operațiunile de supraveghere tehnică pot să nu fie utile cauzei penale în care sunt strânse, din perspectiva procurorului, caz în care ele vor fi folosite în alte cauze, conform art. 142 alin. (5) C.pr.pen., ori vor fi arhivate, conform art. 142 alin. (6) C.pr.pen., la sediul parchetului, în locuri speciale, cu asigurarea confidențialității. Termenul de păstrare a acestor date este de un an de zile de la momentul la care rămâne definitivă soluția definitivă dată în cauză, după care vor fi distruse de procuror.

c) Autorizarea măsurilor de supraveghere tehnică de către procuror;

În mod excepțional și cu controlul ulterior al judecătorului de drepturi și libertăți, Codul de procedură penală permite procurorului să autorizeze temporar, pentru o perioadă care nu poate depăși 48 de ore, folosirea mijloacelor de supraveghere tehnică, această posibilitate fiind extinsă și în cazul în care supravegherea tehnică va fi pusă în executare de către un investigator sub acoperire, în cadrul operațiunii desfășurate de acesta.

Această procedură este una excepțională, putând fi utilizată de procuror numai atunci când sunt întrunite condițiile stricte ale art. 141 C.pr.pen., măsura fundamentându-se pe urgența efectuării supravegherii tehnice. Urgența impune procurorului să procedeze direct la autorizarea supravegherii tehnice ca urmare a faptului că nu există timpul necesar pentru parcurgerea procedurii ordinare în fața judecătorului de drepturi și libertăți. Aceste situații pot fi, de cele mai multe ori, prevăzute în practică în condițiile existenței unui investigator sub acoperire sau a unui colaborator infiltrat în cadrul grupului infracțional țintă. Chiar și în situația luării unei decizii de moment de către membrii grupului, considerăm că ar reflecta o lipsă de tactică a procurorului să nu fi cerut deja și obținut un mandat de supraveghere tehnică cu privire la activitatea pentru care a dispus folosirea investigatorilor sub acoperire ori a colaboratorilor. De exemplu, în situația în care se fac cercetări cu privire la persoane suspectate de săvârșirea unor infracțiuni de trafic cu substanțe interzise, este previzibil faptul că se vor lua decizii în timp real pentru a diminua posibilitatea descoperirii persoanelor. Din punct de vedere logistic, investigatorul sub acoperire și colaboratorul trebuie dotați cu *tehnică operativă numai după autorizarea măsurilor de supraveghere*, anterior acestui moment ei nefiind autorizați să dețină asupra lor acest tip de echipamente, cu excepțiile cotidiene (telefoane mobile, aparate foto etc.).

[1] *C.M. Chiriță*, în N. Volonciu, A.S. Uzlău (coord.), Noul Cod, 2014, p. 323.

În doctrina recentă s-a arătat că, deși instituția autorizării unor măsuri de supraveghere tehnică de către procuror a rămas neschimbată, ca urmare a modificării fundamentale a procesului penal, dispozițiile art. 141 C.pr.pen. sunt neconstituționale raportat la art. 21 alin. (3) din Constituție, având în vedere că „*procurorul nu prezintă garanții suficiente de independență și imparțialitate pentru luarea unor măsuri prin care se aduce atingere gravă drepturilor și libertăților persoanei*"[1]. În același timp, se arată, în mod corect, că instituția judecătorului de drepturi și libertăți a fost creată pentru a soluționa probleme urgente[2], inclusiv dispunerea întrebuințării metodelor speciale de supraveghere, iar dispozițiile art. 141 C.pr.pen. dă prerogative identice procurorului, contrar principiului separării funcțiilor judiciare în procesul penal. Specificul autorizării de către procuror a supravegherii tehnice este urgența, or, noul Cod de procedură penală a creat deja un organ care să soluționeze chestiunile urgente care țin de restrângerea drepturilor și libertăților fundamentale ale persoanei: judecătorul de drepturi și libertăți. *De lege ferenda*, considerăm că se impune abrogarea completă a posibilității autorizării de către procuror a oricăror măsuri de supraveghere tehnică.

Condițiile care trebuie întrunite sunt cele specifice și procedurii de emitere a mandatului de supraveghere tehnică, art. 141 alin. (1) lit. b) C.pr.pen. făcând trimitere la condițiile prevăzute de art. 139 alin. (1) și (2) C.pr.pen.[3]. Alături de aceste condiții, se mai impune ca autorizarea să fie dispună numai în măsura în care „*există urgență, iar obținerea mandatului de supraveghere tehnică în condițiile art. 140 C.pr.pen. ar conduce la o întârziere substanțială a cercetărilor, la pierderea, alterarea sau distrugerea probelor ori ar pune în pericol siguranța persoanei vătămate, a martorului sau membrilor familiilor acestora*". În privința întârzierii substanțiale a cercetărilor, considerăm că legiuitorul a impus o condiție care nu se justifică, raportat la durata relativ scurtă de timp în care se poate obține un mandat de supraveghere tehnică, astfel simplul motiv că cercetarea ar fi întârziată cu o zi sau două nu considerăm că poate constitui motiv suficient pentru autorizarea supravegherii tehnice decât în cazuri excepționale. Trebuie avut în vedere că organele de urmărire penală cunosc, în principiu, în timp real, activitățile infracționale desfășurate de grupul infracțional vizat prin folosirea investigatorilor sub acoperire, astfel va exista întotdeauna posibilitatea audierii investigatorului cu privire la aceste împrejurări. În același sens, în cazul pierderii, alterării sau distrugerii probelor, considerăm că acuzarea se va putea prevala de declarația investigatorului.

Cea de-a treia situație prevăzută de lege este atunci când obținerea întârziată a mandatului de supraveghere tehnică ar pune în pericol siguranța persoanei vătămate, a martorului sau membrilor familiilor acestora. O atare situație impune cât mai rapida folosire a supravegherii tehnice pentru a preîntâmpina săvârșirea unei infracțiuni împotriva acestor persoane. Cu toate acestea, raportat la măsurile de supraveghere care pot fi întrebuințate de investigator, observăm că ele nu sunt de natura oferirii unor date care să preîntâmpine asemenea situații. În concret, filmarea ori fotografierea unor violențe exercitate asupra unei persoane nu contribuie la salvarea acesteia, ci numai la dovedirea existenței violențelor. Într-o asemenea situație, în funcție de posibilități, investigatorul sub acoperire (nu și colaboratorul) va putea să ia măsurile necesare pentru salvarea persoanei.

[1] *Gh. Mateuț*, Observații critice privind noua reglementare a supravegherii tehnice într-o prezentare comparativă, în Caiete de Drept Penal nr. 3/2015, p. 31.

[2] *Ibidem*, p. 32.

[3] *V. supra*, Titlul XII, Capitolul II.1.

Autorizarea de către procuror a folosirii măsurilor de supraveghere tehnică se dispune prin ordonanță, aceasta trebuind să conțină toate elementele prevăzute de art. 140 alin. (5) C.pr.pen., adică să aibă un conținut identic cu mențiunile obligatorii din mandatul de supraveghere tehnică și încheierea care se emit, în procedura obișnuită, de judecătorul de drepturi și libertăți.

Conform art. 141 alin. (3) C.pr.pen., procurorul are obligația ca, în termen de cel mult 24 de ore de la expirarea măsurii, să sesizeze judecătorul de drepturi și libertăți competent în vederea *confirmării măsurii*, înaintând un proces-verbal de redare rezumativă a activităților de supraveghere tehnică efectuate de investigator și dosarul cauzei. Cu această ocazie, procurorul poate să ceară dispunerea în continuarea supravegherii tehnice în condițiile art. 140 C.pr.pen., putând, de altfel, formula această cerere și separat.

Judecătorul de drepturi și libertăți, fiind sesizat de procuror în vederea confirmării supravegherii tehnice, are posibilitatea de a *infirma* sau *confirma* supravegherea tehnică efectuată în baza autorizației emise de procuror.

În situația în care judecătorul de drepturi și libertăți va constata că au fost încălcate dispozițiile art. 141 alin. (1) C.pr.pen. privind autorizarea de către procuror a supravegherii tehnice, acesta va infirma măsura și va dispune distrugerea probelor obținute. Față de această încheiere, procurorul nu poate exercita nicio cale de atac, fiind obligat să procedeze la distrugerea probelor obținute, consemnând operațiunea într-un proces-verbal. În doctrină s-a exprimat o îngrijorare justificată privind informațiile obținute în urma unei supravegheri tehnice infirmate de către judecătorul de drepturi și libertăți și care ar putea duce la obținerea de probe prin alte procedee[1].

În cazul în care judecătorul de drepturi și libertăți va aprecia că autorizarea măsurilor de supraveghere tehnică dispusă de procuror s-a făcut în conformitate cu prevederile art. 141 alin. (1) C.pr.pen., va proceda la *confirmarea măsurii* prin încheiere. Considerăm că numai din acest moment probele obținute de procuror vor putea fi folosite în procesul penal. Cu toate că judecătorul de drepturi și libertăți constată legalitatea autorizării, el *nu se va pronunța asupra legalității probei*, acesta fiind atributul judecătorului de cameră preliminară. Ca atare, legalitatea probei va putea fi contestată de către părți în procedura de cameră preliminară, încheierea de confirmare a măsurii neavând autoritate de lucru judecat asupra legalității probei.

d) Punerea în executare și consemnarea măsurilor de supraveghere tehnică.

Indiferent de modul în care sunt dispuse măsurile de supraveghere tehnică, punerea în executare a lor se va face de către investigatorul sub acoperire ori de colaboratorul desemnat prin ordonanța procurorului de autorizare a folosirii investigatorilor sub acoperire și a colaboratorilor. Aceasta constituie o derogare de la regula exprimată în cuprinsul art. 141 alin. (1) C.pr.pen., în care se arată că procurorul pune în executare mandatul de supraveghere tehnică ori poate dispune ca acesta să fie pus în executare de către un organ de cercetare penală. Deși investigatorul sub acoperire este un lucrător din poliția judiciară, el nu va avea calitatea de organ de cercetare penală în această situație.

În condițiile în care Codul de procedură penală nu reglementează distinct punerea în executare a acestui mandat de supraveghere tehnică specializat, considerăm că vor fi aplicabile dispozițiile de drept comun, cuprinse în art. 142 C.pr.pen., evident adaptate la realitățile acestei forme de supraveghere tehnică specializată și restrânsă. Astfel, procurorul va fi obligat

[1] *Gh. Mateuț*, Observații critice privind noua reglementare a supravegherii tehnice într-o prezentare comparativă, în Caiete de Drept Penal nr. 3/2015, pp. 33-34.

să dispună prin ordonanță ca mandatul de supraveghere să fie pus în executare de către investigatorii sub acoperire sau colaboratorii pentru care a obținut mandat, nominalizându-i după numele conspirativ sau real, după caz. Ulterior emiterii acestei ordonanțe, investigatorii și colaboratorii vor fi dotați cu tehnica operativă necesară pentru realizarea fotografiilor sau a supravegherii audio și video și vor fi instruiți cu privire la modul lor de folosire.

După realizarea operațiunilor specifice acestei măsuri de supraveghere în cursul activităților desfășurate de investigatorul sub acoperire ori de colaborator, aceștia vor preda suporții pe care se află informațiile obținute, urmând ca activitățile lor să fie consemnate într-un proces-verbal. Acest proces-verbal poate servi ca punct de debut în întrebările care să îi fie adresate de părți investigatorului sau colaboratorului în cursul unei eventuale audieri a sa, însă servesc și ca mijloc de verificare a legalității măsurii, prin raportare la activitățile autorizate prin ordonanța procurorului și încheierea judecătorului de drepturi și libertăți.

Secțiunea a 2-a. Audierea investigatorilor sub acoperire și a colaboratorilor

Cea mai importantă, dar și cea mai controversată probă care derivă din activitățile investigatorului sub acoperire și ale colaboratorului o reprezintă declarațiile acestora în cursul procesului penal. Importanța acestei probe este dată de împrejurarea obținerii unei mărturii directe de la aceste persoane prin care să se detalieze aspectele pe care le-au putut surprinde prin propriile simțuri, asemenea martorilor. Cu toate acestea, nu trebuie să uităm faptul că aceste persoane nu sunt martori, ci sunt agenți ai statului (în cazul investigatorilor sub acoperire) ori persoane cu un anumit interes (colaboratorii), ceea ce pune la îndoială obiectivitatea relatărilor pe care le pot face organelor judiciare.

Așa cum am arătat la începutul acestui articol, folosirea investigatorilor sub acoperire și a colaboratorilor va produce date și informații în procesul penal, fiind necesar a se întrebuința alte procedee probatorii pentru obținerea probelor, unul dintre acestea fiind audierea lor. Alături de necesitatea audierii pentru obținerea probelor, procedeul probatoriu servește și ca garanție pentru respectarea dreptului la apărare al inculpatului[1].

Codul de procedură penală conține anumite dispoziții privind modul în care sunt audiate aceste persoane și care este valoarea probantă a declarațiilor acestora, avându-se în vedere necesitatea protejării caracterului secret al identității lor, dar și împiedicarea pronunțării unei soluții defavorabile inculpatului fundamentată numai pe aceste probe.

Calitatea investigatorilor sub acoperire și a colaboratorilor din procesul penal este una distinctă, însă, în privința audierii acestora, situația lor este asimilată martorilor. Potrivit art. 148 alin. (8) C.pr.pen., investigatorii sub acoperire și colaboratorii pot fi audiați ca martori în procesul penal, iar, în situația în care sunt audiați, ei vor fi audiați în aceleași condiții ca martorii amenințați. Fiind asimilați martorilor amenințați, investigatorii sub acoperire și colaboratorii vor beneficia de măsurile de protecție prevăzute de lege[2] și vor fi audiați în condiții speciale, pentru a li se asigura, în primul rând, anonimatul și, în al doilea rând, siguranța față

[1] Prin Hotărârea din 22 noiembrie 2005, în cauza *Taal c. Estonia*, Curtea Europeană a Drepturilor Omului a constatat încălcarea art. 6 Conv.EDO, ca urmare a imposibilității inculpatului de a examina martorii anonimi în stadiile procesului penal.

[2] *V. infra*, Titlul XII, Capitolul VI.

de orice încercare de a le zădărnici audierea, de a le fi influențată declarația ori de a fi victimele unei răzbunări pentru ajutorul acordat justiției.

Persoanele care pot fi audiate, potrivit dispozițiilor speciale prevăzute de art. 129 C.pr.pen. privind audierea martorilor amenințați, sunt *investigatorii sub acoperire* și *colaboratorii atât cu identitate reală, cât și cu identitate atribuită*.

În cazul primei categorii, motivarea dată pentru audierea acestora în condiții speciale este nevoia de a proteja persoanele de o răzbunare ulterioară, precum și de a le garanta siguranța față de operațiuni similare, care vor fi desfășurate ulterior în cariera acestora de polițiști. Așa cum vom arăta într-o secțiune ulterioară[1], investigatorii sub acoperire trebuie să aibă o identitate atribuită, care să nu îi lege de activitatea lor din viața reală. Situația colaboratorilor este identică celei a investigatorilor sub acoperire, cu deosebirea că nu va conta dacă aceștia s-au folosit în timpul activității lor de identitatea reală sau de o identitate atribuită. Motivul pentru audierea acestora în aceleași condiții ca martorii amenințați este dat de faptul că ei pot fi ținta unei răzbunări sau identitatea lor reală trebuie să rămână necunoscută participanților la procesul penal.

Audierea investigatorului sub acoperire poate avea loc numai în cursul urmăririi penale și în cursul judecății, conform dispozițiilor art. 129 C.pr.pen., care nu fac trimitere la nicio dispoziție legală care să permită audierea acestuia în cursul procedurii în camera preliminară, ceea ce constituie un neajuns, din perspectiva posibilității de a administra probe, cu privire la legalitatea obținerii probelor în cursul urmăririi penale. În jurisprudența Curții Constituționale[2] s-a arătat necesitatea *investigării elementelor de fapt care au stat la baza obținerii anumitor probe*, deoarece acestea au o relevanță directă și implicită asupra legalității probei, astfel că se va impune administrarea de probe în procedura camerei preliminare, în cazul în care se invocă aspecte ce țin de nelegalitate ori neloialitate[3]. O situație concretă în care s-ar impune o audiere în cameră preliminară este pentru a se determina elementele care au motivat colaboratorul să coopereze cu organele de urmărire penală, în condițiile în care ar exista suspiciuni privind ilegalitatea unor beneficii cu care acesta ar fi fost avantajat, de pildă, o soluție de clasare pentru fapte ce nu au legătură cu cauza ori reținerea unei încadrări mai ușoare pentru asemenea fapte. Dacă, în alte sisteme, aceste beneficii sunt considerate legale, în sistemul român nu se prevede o atare posibilitate pentru procuror, fiind necesar a se verifica dacă colaboratorul nu a primit promisiuni de asemenea natură de la procuror pentru a-l determina să coopereze. *De lege ferenda*, se impune introducerea obligativității semnării unui acord între procuror și investigatorul sub acoperire, în care să fie cuprinse și beneficiile pe care ar urma să le primească colaboratorul, constituind atât o garanție cu privire la legalitatea administrării măsurii de cercetare, dar și a probelor ce derivă din aceasta, cât și o obligație pentru sistemul judiciar de a reține în favoarea colaboratorului toate cauzele de nepedepsire ori de atenuare a pedepsei care ar fi incidente. În același timp, ca urmare a Deciziei Curții Constituționale nr. 641/2014, considerăm că va fi posibilă audierea investigatorului sub acoperire și a colaboratorului în faza de cameră preliminară, impunându-se modificarea Codului de procedură penală în acest sens.

Audierea investigatorului sub acoperire și a colaboratorului nu se poate face în prezența fizică a acestora, fiind necesară folosirea mijloacelor tehnice de transmitere audiovideo pentru a se putea comunica cu investigatorul sub acoperire sau colaboratorul, fiind obligatorie

[1] *V. infra*, Titlul XII, Capitolul V.1.

[2] CCR, Dec. nr. 641 din 11 noiembrie 2014, par. 60 (M. Of. nr. 887 din 5 decembrie 2014).

[3] *I. Kuglay*, în M. Udroiu (coord.), Codul de procedură penală, 2017, p. 903.

distorsionarea vocii și a imaginii acestuia. Instanțele judecătorești dispun de tehnica necesară pentru a realiza acest lucru: televizoare, camere video, rețea de microfoane, aparatură de distorsionare a vocii și imaginii și de transmitere a acesteia[1]. Comunicarea va avea loc în timp real.

Cu toate că nu va exista un contact direct între participanții la procesul penal și investigatorul ori colaboratorul audiat, judecătorul va putea percepe în mod nemijlocit reacțiile martorului și va putea cunoaște adevărata lor identitate, putându-și forma o poziție asupra credibilității acestuia[2].

Deși dispozițiile art. 126 alin. (1) lit. d) C.pr.pen. și art. 127 lit. d) C.pr.pen. arată că nu se poate proceda la audierea în prezența investigatorului sub acoperire ori a colaboratorului, va trebui evitată, pe cât posibil, aflarea identității reale a acestora prin incidente la locul în care se realizează audierea. Având în vedere dotarea deficitară a unor unități de parchet, audierile de acest fel se realizează în cadrul instanțelor, care sunt dotate cu tehnica necesară, astfel că persoanele implicate în procedură se pot afla în aceeași clădire, existând posibilitatea de a se întâlni pe culoarele instanței. Ca atare, vor trebui luate măsuri, precum: aducerea investigatorului sub acoperire ori a colaboratorului înaintea orei fixate; folosirea unor culoare separate de acces; deghizarea persoanei pe drumul către sala în care va fi audiată[3]; folosirea unei alte locații pentru transmiterea comunicațiilor etc.

Din interpretarea dispozițiilor art. 129 alin. (3) teza a II-a C.pr.pen., reiese că nu se poate proceda la adresarea de întrebări care să conducă la identificarea persoanei audiate prin această procedură. Din aceasta rezultă două consecințe: *i)* verificarea identității înainte de audiere și *ii)* respingerea oricăror întrebări care ar putea conduce la identificarea persoanei.

Așa cum se prevede în cazul oricărei audieri, există o etapă preliminară care constă în lămurirea identității persoanelor care urmează a fi audiate prin verificarea cărții de identitate ori a pașaportului, urmată de înscrierea acestor date în cuprinsul declarației. Această verificare se realizează, potrivit art. 119 C.pr.pen., prin adresarea de întrebări, cu excepția situației în care sunt dispuse măsuri de protecție a martorului, situație în care se va verifica identitatea reală numai de către organul judiciar, iar aceasta nu va fi consemnată în declarație, fiind înlocuită de identitatea conspirativă. În concret, mai înainte de audiere, procurorul care va realiza audierea în cursul urmăririi penale sau judecătorul de drepturi și libertăți, după caz, și instanța, în cursul judecății, vor proceda la verificarea identității persoanei în mod nemijlocit, într-o locație separată de locul în care se va comunica cu persoana. În mod evident, organele judiciare vor trebui să ia cunoștință de identitatea reală a investigatorului sub acoperire ori a colaboratorului, situație care nu contravine legii, fiind prevăzută această posibilitate în cuprinsul art. 149 alin. (2) C.pr.pen.

Un aspect neclar în legislație, reclamat și de doctrină[4], îl reprezintă situația în care investigatorul sub acoperire sau colaboratorul este audiat într-un alt loc decât sediul organului de urmărire penală sau sediul instanței, situație în care se pune problema organului competent

[1] A se vedea și *D. Lupașcu, M. Mareș*, Considerații referitoare la protecția martorilor și procesul echitabil, în Dreptul nr. 11/2017, p. 112.

[2] CEDO, cauza *Windisch c. Austria*, Hotărârea din 27 septembrie 1990, §29, pe *hudoc.echr.coe.int*. În această cauză, Curtea a reținut că reprezintă o încălcare a art. 6 par. 1 și 3 Conv.EDO neasigurarea audierii nemijlocite a martorului acuzării, în condițiile păstrării anonimatului acestuia, iar imposibilitatea cunoașterii nici de către instanță a identității martorilor o împiedică să poată evalua în mod corect credibilitatea acestora.

[3] De pildă, investigatorul, în funcție de constituția sa, va putea fi deghizat în uniforma lucrătorilor mascați care însoțesc, de regulă, persoanele aduse din detenție în fața instanței.

[4] *T.-V. Gheorghe*, în N. Volonciu, A.S. Uzlău (coord.), Noul Cod, 2014, pp. 290-291.

să verifice identitatea sa. Potrivit art. 129 alin. (5) C.pr.pen., se arată că va semna atât organul de urmărire penală, cât și *procurorul care a fost prezent la audierea martorului* (corelativ, și a investigatorilor), ceea ce pare a fi o neconcordanță, în condițiile în care procurorul este și el un organ de urmărire penală. În realitate, legiuitorul a vrut să indice obligativitatea ca un procuror să participe la audierea investigatorului și colaboratorului prin prezența sa fizică în aceeași încăpere, verificând identitatea acestuia, fără a realiza însăși audierea. Dacă situația este de înțeles în cazul urmăririi penale, nu există nicio dispoziție legală care să rezolve o situație similară în cazul procedurii în fața instanței. Prin dispozițiile art. 129 alin. (6) C.pr.pen. se arată că declarația martorului se semnează de președintele completului de judecată, fără a se specifica dacă acesta, în toate cazurile, va verifica identitatea persoanei. Până la o completare a acestei reglementări, suntem de părere că singura modalitate legală de audiere a investigatorilor sub acoperire și a colaboratorilor (și, implicit, a martorilor amenințați) va fi audierea la sediul instanței ori prin asigurarea prezenței unui judecător la locul unde se află persoana audiată, urmând ca acesta să semneze declarația, alături de președintele completului.

Ulterior acestei etape, în cursul audierii, se va proceda la următoarea etapă obligatorie: prestarea jurământului de către investigatorul sub acoperire și de către colaborator, aceasta fiind îndeplinită prin intermediul sistemului de videoconferință instalat. Practic, acesta va fi debutul procedurii la care vor putea asista părțile în cursul judecății ori avocații subiecților procesuali și ai părților în cursul urmăririi penale.

Deoarece identitatea acestor persoane trebuie să rămână secretă, organele judiciare vor respinge orice întrebare care poate conduce la identificarea persoanei audiate, pentru a preîntâmpina orice răzbunare împotriva sa ori a familiei sale. Pentru a reuși acest lucru, este esențial ca organul judiciar să studieze materialul cauzei[1] înaintea audierii persoanei, în vederea cunoașterii tuturor împrejurărilor în care a putut fi implicată. De pildă, în situația în care la o întâlnire a fost prezent un număr redus de persoane, printre care și investigatorul sub acoperire sau colaboratorul, în cazul în care se confirmă de către cel audiat că a fost prezent, inculpatul ar putea deduce identitatea acestuia.

Modalitatea consemnării declarației investigatorului sub acoperire și a colaboratorului prezintă anumite particularități față de modalitatea obișnuită de consemnare a declarațiilor. În realitate, vom avea parte de *două declarații*, una care va fi păstrată la dosarul cauzei și una care va fi păstrată în condiții de confidențialitate. Această situație reiese din coroborarea dispozițiilor art. 129 alin. (4) C.pr.pen. cu cele din alin. (5) al aceluiași articol. Pe de o parte, se arată că declarația se înregistrează prin mijloace tehnice audio și video și se redă integral în formă scrisă, iar, pe de altă parte, se arată că declarația martorului, *transcrisă*, va fi semnată *și de acesta* și va fi păstrată în dosarul depus la parchet/instanță într-un loc special, în condiții de confidențialitate. În concret, indiferent de faza procesuală, organul judiciar care realizează audierea va consemna în scris declarația investigatorului sau a colaboratorului și o va semna de față cu celelalte părți, subiecți procesuali ori avocați și, ulterior acestui moment, va realiza o transcriere a acestei declarații pe care o va da persoanei audiate spre semnare. Deși, în mod corect, s-a punctat că semnătura unei persoane poate duce la identificarea acesteia de către ceilalți participanți la procesul penal[2], suntem de părere că, raportându-ne la condițiile de confidențialitate în care declarația se păstrează, la cunoașterea identității persoanei de către

[1] *S. Alămoreanu*, Elemente de criminalistică, Ed. Alma Mater, Sibiu, 2000, p. 178; *Em. Stancu*, op. cit., p. 420.

[2] *T.-V. Gheorghe*, în N. Volonciu, A.S. Uzlău (coord.), Noul Cod, 2014, p. 291.

judecător sau procuror, precum și a faptului că actele procesuale din care rezultă identitatea investigatorului sub acoperire ori a colaboratorului sunt depozitate în același dosar, se va impune ca declarația confidențială să includă *datele reale ale persoanei audiate*.

În ceea ce privește înregistrarea video și audio a declarației investigatorului sub acoperire și a colaboratorului, apreciem că rațiunea acesteia este de a conferi un suport autentic în care să fie consemnate în mod fidel cuvintele persoanei. Este de înțeles împrejurarea păstrării în condiții de confidențialitate a înregistrărilor realizate în timpul audierii persoanelor arătate în cursul urmăririi penale și judecății, cu mențiunea că aceste înregistrări atrag caracterul confidențial, deoarece conțin video și audio nedistorsionate, putând duce la identificarea persoanei. Acest lucru înseamnă că reglementarea a fost gândită pentru sisteme care prelucrează imaginile și sunetele captate și, în același timp, le transmit distorsionate în timp real și le înregistrează în mod neprelucrat pe un suport.

Suportul pe care se află înregistrarea audio și video a declarației investigatorului sub acoperire ori a colaboratorului se va păstra sigilat, cu sigiliul instanței sau al parchetului, fie în cadrul parchetului, fie în cadrul instanței, în funcție de faza procesului penal. Potrivit art. 129 alin. (7) C.pr.pen., în situația sesizării instanței, suporții optici pe care se află înregistrările vor fi transmiși instanței de judecată, împreună cu dosarul cauzei, și vor fi ținuți în aceleași condiții de confidențialitate.

În privința legalității audierii investigatorilor sub acoperire și a colaboratorilor, atât în cursul urmăririi penale, cât și în faza de judecată, suntem de părere că această probă va depinde de caracterul legal al măsurii de cercetare. În situația în care, în cursul procedurii de cameră preliminară, se va constata că utilizarea investigatorilor sub acoperire și a colaboratorilor s-a făcut cu încălcarea legii, chiar și din prisma realizării unor activități care nu au fost autorizate expres de procuror, considerăm că nelegalitatea se va răsfrânge și asupra declarațiilor ce vor fi date în cursul urmăririi penale. Mai mult, deoarece textul art. 102 alin. (4) C.pr.pen. privind probele derivate nu se referă la probele derivate obținute în aceeași fază procesuală, considerăm că nu vor putea fi avute în vedere nici declarațiile investigatorului sau colaboratorului din fața instanței cu privire la împrejurările aflate prin depășirea mandatului. Desigur, în măsura în care se va constata nulitatea ordonanței procurorului prin care s-a autorizat utilizarea investigatorilor sub acoperire și a colaboratorilor, orice probă care derivă din această activitate, inclusiv declarațiile date în fața instanței, vor trebui să fie excluse. În opinia noastră, într-o asemenea situație, s-ar impune ca o cerere de audiere a investigatorului sub acoperire ori a colaboratorului să fie respinsă de instanță, fiind incident cazul prevăzut de art. 100 alin. (4) lit. f) C.pr.pen., anume că „*administrarea probei este contrară legii*".

Valoarea probantă a declarațiilor investigatorilor sub acoperire și a colaboratorilor este una limitată, ea neputând fi niciodată considerată o probă determinantă în cazul unei soluții de condamnare, de renunțare la aplicarea pedepsei ori de amânare a aplicării pedepsei. Aceasta reprezintă consecința necesității păstrării anonimatului acestor persoane, punându-se în balanță interesul inculpatului de a putea audia în mod nemijlocit un martor al acuzării și pentru a-i pune la îndoială credibilitatea. În jurisprudența Curții Europene a Drepturilor Omului s-a reținut că lipsirea inculpatului de posibilitatea de a pune la îndoială declarațiile unui investigator sub acoperire, de a-i pune întrebări și de a putea obține o confruntare în fața instanței constituie o încălcare a art. 6 par. 3 din Convenția de la Budapesta[1]. Interesul legitim al statului de a păstra anonimitatea unui investigator sub acoperire nu îl absolvă de obligația

[1] CEDO, cauza *Ludi c. Elveția*, Hotărârea din 15 iunie 1992, §47-48.

de a asigura audierea acestuia de către instanță, în condiții în care să îi fie păstrată identitatea reală. Această atingere adusă dreptului la un proces echitabil există într-o măsură mai mică în situațiile în care declarațiile investigatorului ori colaboratorului joacă un rol redus într-o soluție de condamnare, standardul impus de Curtea Europeană a Drepturilor Omului fiind în sensul obligativității asigurării posibilității adresării de întrebări de către apărare numai în situațiile în care o asemenea declarație joacă un rol principal în acuzare[1].

În jurisprudența sa recentă, în analiza caracterului echitabil al unui proces în care martorii anonimi sunt audiați, Curtea analizează dacă există motive pentru a păstra confidențială identitatea martorului, precum și dacă declarația acestuia a fost exclusivă sau determinantă pentru pronunțarea unei soluții de condamnare. În cazul în care o condamnare se întemeiază în mod exclusiv sau determinant pe declarația unui martor anonim, Curtea trebuie să constate că au existat în cauză garanții procesuale solide, care să permită o evaluare echitabilă și justă a gradului de fiabilitate a declarației respective[2]. În sistemul român, apreciem că este favorabilă dispoziția categorică din cuprinsul art. 103 alin. (3) C.pr.pen. privind imposibilitatea reținerii ca probă determinantă declarația unui investigator sub acoperire sau colaborator.

Secțiunea a 3-a. Participarea autorizată la anumite activități

Participarea autorizată la anumite activități este o metodă specială de cercetare prevăzută de legiuitor, în principal, pentru a completa activitatea desfășurată prin utilizarea investigatorilor sub acoperire și a colaboratorilor. Spre deosebire de cea din urmă măsură, în concepția legiuitorului, finalitatea participării autorizate la anumite activități constă în obținerea unor mijloace de probă cu privire la săvârșirea unei infracțiuni, deși considerăm că obținerea probelor în baza acestei măsuri se va restrânge la probele derivate din aceasta, precum audierea persoanei autorizate să participe la aceste activități. Întrucât am dedicat acestei metode speciale de cercetare o secțiune distinctă în lucrarea de față[3], în prezenta parte vom trata succint legătura dintre această metodă specială de cercetare și utilizarea investigatorilor sub acoperire și a colaboratorilor și vom detalia probele care se obțin în procesul penal prin folosirea metodei speciale.

Legătura dintre cele două măsuri este una deosebit de strânsă, în condițiile în care, pentru a se obține infiltrarea unui investigator sub acoperire ori a unui colaborator în cadrul unui grup infracțional organizat, acesta va trebui să adere formal la grup și să participe la activitățile ilicite ale acestuia pentru a i se da credibilitate, dar și pentru a cunoaște mai bine modul în care infractorii operează. În doctrină au fost emise păreri din care rezultă că metoda specială de cercetare nu ar trebui să fie una autonomă, ci să fie considerată o activitate din cadrul măsurii utilizării investigatorilor sub acoperire și a colaboratorilor, întrucât nu se poate concepe ca un organ de cercetare penală sau un investigator cu identitate reală să poată fi folosit[4]. Deși

[1] CEDO, cauza *Krasniki c. Cehia*, Hotărârea din 28 februarie 2006, §78-79; în același sens, și cauza *Kök c. Turcia*, Hotărârea din 19 octombrie 2006; cauza *Visser c. Olanda*, Hotărârea din 14 februarie 2002; cauza *Van Mechelen ș.a. c. Olanda*, Hotărârea din 23 aprilie 1997, §50-55; cauza *Asch c. Austria*, Hotărârea din 26 aprilie 1991, §27; cauza *Delta c. Franța*, Hotărârea din 19 decembrie 1990, §36, pe *hudoc.echr.coe.int*

[2] CEDO, cauza *Pesukic c. Elveția*, Hotărârea din 6 decembrie 2012, §45, pe *hudoc.echr.coe.int*; a se vedea și *M. Udroiu*, Procedură penală. Partea generală. Sinteze și grile, ed. a 3-a, Ed. C.H. Beck, București, 2016, pp. 344-345.

[3] *V. infra*, Titlul XIII.

[4] *Gh. Mateuț*, Procedură penală, 2019, pp. 729-730; în același sens, *M. Bulancea, R. Slăvoiu*, în M. Udroiu (coord.), Codul de procedură penală, 2017, p. 731.

legea prevede această posibilitate și recunoaște caracterul autonom al metodei speciale de cercetare, este greu de imaginat o situație în care ar fi preferabil ca un organ de cercetare penală să dorească să se expună unor riscuri nejustificate. Mai mult, imediat după realizarea activității autorizate, apreciem că organul de cercetare penală va deveni incompatibil în respectiva cauză, astfel că este de preferat ca legiuitorul să înlăture din textul legal posibilitatea ca un organ de cercetare penală să realizeze activitățile autorizate. Cu toate acestea, suntem de părere că metoda specială de cercetare trebuie să își păstreze caracterul autonom, pentru că, față de utilizarea investigatorilor sub acoperire, reprezintă o ingerință suplimentară în viața privată a unei persoane, motiv care impune un control mai strict asupra folosirii ei.

Definiția metodei speciale de cercetare se regăsește în cuprinsul art. 138 alin. (11) C.pr.pen., în care se arată că, prin „participarea autorizată la anumite activități", se va înțelege: „*comiterea unei fapte similare laturii obiective a unei infracțiuni de corupție, efectuarea de tranzacții, operațiuni sau orice fel de înțelegeri privind un bun sau privind o persoană despre care se bănuiește că ar fi dispărută, că este victima traficului de persoane ori a unei răpiri, efectuarea de operațiuni privind droguri, precum și prestarea unui serviciu, desfășurate cu autorizarea organului judiciar competent, în scopul obținerii de mijloace de probă*". Cu alte cuvinte, măsura de cercetare constă în săvârșirea unor fapte prevăzute de legea penală, cu autorizarea prealabilă a procurorului, în vederea obținerii de mijloace de probe.

Menirea folosirii participării autorizate la anumite activități este de a permite unui agent al statului să observe și să interacționeze cu participanții la săvârșirea unei infracțiuni într-un mod pasiv ori, cel mult, complicitar, în vederea obținerii unor probe.

În cazul infracțiunilor privind traficul de droguri, legiuitorul a fost mult mai clar, permițând orice operațiune cu privire la aceste infracțiuni. Considerăm că această măsură de cercetare își regăsește cel mai bine utilitatea în cazul infracțiunilor de acest fel, deoarece folosirea unui colaborator, alături de autorizarea unor operațiuni, precum vânzarea de droguri sau deținerea acestora, îi va crește posibilitatea de a se integra în grupul infracțional.

Pentru *autorizarea măsurii participării autorizate* la anumite activități, procurorul va emite o ordonanță similară celei pe care o va emite în cazul utilizării investigatorilor sub acoperire și a colaboratorilor, aceasta conținând: *indicarea activităților autorizate*, *perioada pentru care s-a autorizat măsura* și *persoana care desfășoară activitățile*.

Finalitatea acestei măsuri de cercetare constă într-un proces-verbal încheiat de procuror, potrivit art. 150 alin. (5) C.pr.pen., în care vor fi consemnate: „*datele la care măsura a început și s-a încheiat, date cu privire la persoanele care au desfășurat activitățile autorizate, descrierea dispozitivelor tehnice utilizate în cazul în care s-a autorizat de către judecătorul de drepturi și libertăți, folosirea mijloacelor tehnice de supraveghere, identitatea persoanelor cu privire la care a fost pusă în aplicare măsura*".

Spre deosebire de procesul-verbal prevăzut în cazul folosirii investigatorilor sub acoperire și a colaboratorilor, valoarea probatorie va fi diferită, având în vedere caracterul expres al reglementării în cazul art. 148 alin. (5) C.pr.pen., în care se arată că procesul-verbal va conține datele și informațiile obținute, și nu probe privind faptele urmărite. Cu toate acestea, observăm că, în cazul participării autorizate la anumite activități, procesul-verbal întocmit potrivit dispozițiilor art. 150 alin. (5) C.pr.pen. nu conține mențiuni cu privire la activitățile care s-au realizat. Ca atare, considerăm că, în cuprinsul art. 138 alin. (11) C.pr.pen., legiuitorul precizează că această măsură se va utiliza în scopul obținerii de probe, din moment ce, prin ea

însăși, nu duce la obținerea niciunei probe[1]. Este inexplicabil de ce, în cazul măsurii participării autorizate la anumite activități, nu se detaliază în concret fiecare activitate care a fost realizată, în această situație apreciem că acest proces-verbal nu va putea fi considerat un mijloc de probă care să rezulte direct din folosirea măsurii de cercetare, deoarece nu conține elemente privitoare la faptele care fac obiectul urmăririi penale.

Însuși procesul-verbal menționat va proba numai desfășurarea participării autorizate la anumite activități, actul fiind necesar pentru a semnala finalizarea măsurii[2]. În mod evident, metoda specială de cercetare este utilă, iar probele care derivă din aceasta, în special declarațiile persoanei autorizate, pot avea o valoare deosebită, dar acest lucru nu schimbă caracterul *derivat* și *facultativ*[3] al acestora.

În privința audierii ca martor a persoanei care a realizat activitățile autorizate, au existat mai multe opinii, unele susținând obligativitatea audierii persoanei care a desfășurat activitățile[4], stabilindu-i-se calitatea de martor, altele susținând că textul de lege nu impune o astfel de obligație[5]. Strict formal, cea de-a doua opinie este validă, întrucât corespunde cu caracterul facultativ al audierii persoanei, astfel cum acesta este enunțat de art. 150 alin. (6) C.pr.pen. Cu toate acestea, credem că prima opinie este cea corectă, întrucât legiuitorul a greșit în reglementarea caracterului facultativ al audierii; constituind probă în procesul penal o atare declarație, nu se poate ca organele de urmărire penală să nu procedeze la audierea persoanei care a realizat activitățile autorizate. Expunem această opinie și din două considerente proprii: *caracterul subsidiar al folosirii supravegherii tehnice, caracterul de procedeu probatoriu al metodei speciale de cercetare* și *necesitatea audierii persoanei în vederea stabilirii caracterului loial al măsurii*.

În primul rând, conform art. 150 alin. (5) C.pr.pen., metodele speciale de supraveghere tehnică vor putea fi folosite numai dacă au fost încuviințate de judecătorul de drepturi și libertăți, aceasta constituind o situație apreciată de legiuitor ca excepțională. Ca atare, în lipsa unor asemenea tehnici speciale, nu se va putea dovedi săvârșirea infracțiunii decât prin audierea persoanei care a realizat activitatea autorizată. Bunăoară, este util să fie folosite astfel de metode, mai ales supravegherea video și audio la momentul realizării flagrantului, dar, în cazul în care activitatea autorizată se realizează pentru infiltrarea unui grup infracțional, poate fi periculos pentru investigatorul sub acoperire să realizeze o astfel de supraveghere (de pildă, prin atașarea asupra acestei persoane a unor dispozitive de înregistrare) sau să fie imposibil de realizat (obiectivul unde s-ar putea realiza supravegherea tehnică este păzit de membrii grupării vizate).

În al doilea rând, potrivit însăși definiției „participării autorizate la anumite activități", cuprinsă în art. 138 alin. (11) C.pr.pen., scopul metodei speciale este *obținerea de mijloace de probă* (corectă ar fi fost expresia „obținerea de probe" – n.n.). Ca atare, ținând seama de conținutul procesului-verbal cuprins la art. 150 alin. (5) C.pr.pen. și al caracterului subsidiar al supravegherii tehnice care poate fi dispuse în cauză, nu se poate identifica niciun alt procedeu

[1] În același sens, *Gh. Mateuț*, Procedură penală, 2019, p. 731; în sens contrar, a se vedea *M. Udroiu*, Procedură penală, vol. I, 2019, p. 615.

[2] Sub acest aspect, trebuie semnalată existența unei simetrii în procedeele probatorii care presupun o autorizare prealabilă – existența unui act de autorizare și a unui act de finalizare a activității autorizate, situația fiind comună și procedeelor probatorii obișnuite (de pildă, procesul-verbal de percheziție domiciliară).

[3] În condițiile în care, în cuprinsul art. 150 alin. (6) C.pr.pen., se precizează că persoana autorizată va fi audiată numai dacă organul judiciar apreciază că audierea este necesară.

[4] *Gh. Mateuț*, Procedură penală, 2019, p. 731.

[5] *M. Udroiu*, Procedură penală, vol. I, 2019, p. 615.

probatoriu decât audierea în calitate de martor a persoanei care a realizat participarea autorizată la anumite activități.

În al treilea rând, trebuie să avem în vedere că participarea autorizată la anumite activități este un subiect deosebit de delicat, ridicând deseori probleme din perspectiva garantării dreptului la un proces echitabil, existând riscul ca persoana care participă autorizat la anumite activități să determine persoana să comită o infracțiune. Fiind o problemă de existență a unei infracțiuni provocate, cu atât mai mult va trebui să fie audiată persoana care a pus în executare metoda specială de cercetare, pentru a se putea proba caracterul loial sau neloial al măsurii, ceea ce, în situația acestei metode speciale de cercetare, apreciem că este obligatoriu.

În mod similar măsurii utilizării investigatorilor sub acoperire și a colaboratorilor, mijloacele de probă care vor rezulta din măsura de cercetare sunt numai cele derivate, în sensul că persoanele care realizează activitățile autorizate vor putea fi audiate în cursul procesului penal în calitate de martori, aplicându-se regulile specifice în situația audierii martorilor amenințați[1], în același timp putând fi utilizate, concomitent, măsuri de supraveghere tehnică.

[1] A se vedea *supra*, Titlul XII, Capitolul IV.2.

Capitolul V
Activitățile specifice investigatorilor sub acoperire și colaboratorilor

Secțiunea 1. Investigatorul sub acoperire, colaboratorul și informatorul – noțiuni, distincții și activitate specifică

Alături de problemele de drept procesual penal care țin de autorizarea măsurii de cercetare, un element deosebit de important, cu consecințe asupra legalității și loialității probelor obținute prin mijlocirea oferită de utilizarea măsurii, îl constituie persoanele care realizează o operațiune sub acoperire ori furnizează date cu privire la săvârșirea unei infracțiuni.

Codul de procedură penală operează cu mai mulți termeni în raport de calitatea pe care persoanele care realizează activitățile autorizate o au. Aceștia pot fi **investigatori** sau **colaboratori**. Alături de aceștia, considerăm că mai există încă o categorie de persoane care furnizează date și informații în cursul procesului penal, **informatorii**, care nu beneficiază de o reglementare individuală în Cod.

§1. Investigatorul sub acoperire

Spre deosebire de colaboratori sau de informatori, investigatorii sub acoperire primesc o definiție legală în cuprinsul art. 148 alin. (4) C.pr.pen., aceștia fiind „*lucrători operativi din cadrul poliției judiciare*". Cu alte cuvinte, un investigator sub acoperire va face parte, în mod obligatoriu, din Poliția Română ca organ de poliție judiciară, ca un criteriu minim, însă nu se poate socoti că orice astfel de polițist va putea fi folosit ca investigator sub acoperire. Pentru realizarea activităților specifice, este necesară o pregătire specială prin care agenții și ofițerii de poliție să aibă deprinderile necesare pentru a se infiltra într-o organizație criminală[1].

Excepția de la regula enunțată mai sus o constituie folosirea ca investigatori sub acoperire a lucrătorilor operativi din cadrul organelor de stat care desfășoară activități de informații în vederea asigurării securității naționale. Potrivit legii, următoarele instituții au atribuții în domeniul securității naționale: Serviciul Român de Informații[2]; Serviciul de Informații Externe[3]; Ministerul Afacerilor Interne, prin Direcția Generală de Informații și Protecție Internă; Direcția Generală Anticorupție și Direcția Generală de Combatere a Criminalității Organizate[4]; Ministerul Apărării

[1] *C. Olaru*, op. cit., p. 47.

[2] Potrivit art. 1 din Legea nr. 14 din 24 februarie 1992 privind organizarea și funcționarea Serviciului Român de Informații (M. Of. nr. 33 din 3 martie 1992): „Serviciul Român de Informații este serviciul organizat de stat specializat în domeniul informațiilor privitoare la siguranța națională a României, parte componentă a sistemului național de apărare, activitatea sa fiind organizată și coordonată de Consiliul Suprem de Apărare a Țării".

[3] Potrivit art. 1 din Legea nr. 1 din 6 ianuarie 1998 privind organizarea și funcționarea Serviciului de Informații Externe (republicată în M. Of. nr. 511 din 18 octombrie 2010): „Serviciul de Informații Externe este organul de stat specializat în domeniul informațiilor externe privind siguranța națională și apărarea României și a intereselor sale".

[4] Potrivit art. 3 lit. b) pct. 2 și 16, precum și art. 10 alin. (3) din O.U.G. nr. 30 din 25 aprilie 2007 privind organizarea și funcționarea Ministerului Internelor și Reformei Administrative (M. Of. nr. 309 din 9 mai 2007).

Naționale, prin Direcția Generală de Informații a Apărării[1]; Serviciul de Protecție și Pază[2]. Acești lucrători operativi nu vor putea fi utilizați ca investigatori sub acoperire în toate cauzele, ci numai în cele în care sunt cercetate infracțiuni contra securității naționale și infracțiuni de terorism. Prin „infracțiuni contra securității naționale" vom înțelege infracțiunile prevăzute de art. 394-410 C.pen., iar infracțiunile de terorism sunt cele prevăzute de art. 32-38 din Legea nr. 535/2004 privind prevenirea și combaterea terorismului[3].

Investigatorul sub acoperire este acea persoană căreia i se atribuie o identitate fictivă, prin atribuirea unor date de stare civilă nereale, în vederea prezentării sale în fața persoanelor care urmează a fi cercetate, sub o identitate conspirativă. Datele care i se atribuie constau într-un nume nou, domiciliu nou, starea civilă, furnizându-i-se înscrisuri care să certifice această identitate (carte de identitate, pașaport, permis de conducere etc.), în plus față de acestea trebuind să se construiască o identitate nouă a investigatorului care să fie credibilă. Asemenea lucrătorilor operativi din cadrul serviciilor de informații, nu este suficient ca investigatorului să i se atribuie date de stare civilă noi, ci el trebuie să privească *o altă identitate*, ceea ce înseamnă că trebuie să i se creeze o biografie falsă pe care acesta trebuie să și-o însușească: locul nașterii, numele părinților, dacă aceștia sunt sau nu în viață, localitățile unde a trăit până în acel moment, religia, locul unde și-a desfășurat studiile, ce profesie are, care au fost ocupațiile sale trecute, ce hobby-uri are etc. În plus, considerăm că se impune crearea unor elemente conexe, precum o identitate electronică: cont de Facebook, adresă de poștă electronică etc., deoarece, în societatea actuală, lipsa unor asemenea elemente atrage suspiciuni, mai ales dacă investigatorul sub acoperire are vârsta sub 30 de ani. Practic, prin identitatea fictivă, se impune crearea unui statut profesional fictiv, anume al investigatorului sub acoperire, nu numai o simplă identitate nereală, fiind absurd să i se dea doar un nume fictiv, dar să fie cunoscut ca fiind polițist[4].

Scopul utilizării unei identități fictive este dublu: îngreunarea identificării investigatorului ca un lucrător al poliției și protejarea investigatorului de răzbunări pentru activitatea sa. Pentru aceste motive, nu se poate admite folosirea aceleiași identități conspirative în cazul unor procese penale diferite, impunându-se atribuirea de noi identități pentru investigatori. Totodată, ar fi o lipsă de prevedere gravă din partea organelor de urmărire penală folosirea aceluiași investigator sub acoperire în două procese penale care se desfășoară concomitent, deoarece ar implica folosirea a două identități conspirative, alături de înscrisuri care să certifice aceste două identități.

Este lesne de înțeles că orice grupare infracțională ori chiar un infractor singur vor încerca să se ferească de a fi descoperiți de către organele de urmărire penală, motiv pentru care vor pune la îndoială identitatea și motivația unei persoane nou intrate în cercul lor de cunoștințe. Cel mai simplu mod de a afla dacă o persoană are legături cu un organ judiciar este de a se

[1] Potrivit art. 13 alin. (2) din Legea nr. 346 din 28 iulie 2006 (M. Of. nr. 654 din 28 iulie 2006): „Personalul Direcției generale de informații a apărării își desfășoară activitatea deschis sau acoperit, în raport cu nevoile de realizare a securității naționale în domeniul militar. Pentru culegerea de informații în teatrele de operații și pentru lupta împotriva terorismului, Direcția generală de informații a apărării poate avea în subordine structuri combatante".

[2] Potrivit art. 1 alin. (1) din Legea nr. 191 din 19 octombrie 1998 (M. Of. nr. 402 din 22 octombrie 1998): „Serviciul de Protecție și Pază este organ de stat cu atribuții în domeniul siguranței naționale, specializat în asigurarea protecției demnitarilor români, a demnitarilor străini pe timpul șederii lor în România, a familiilor acestora, în limitele competențelor legale, precum și în asigurarea pazei sediilor de lucru și a reședințelor acestora, potrivit hotărârilor Consiliului Suprem de Apărare a Țării".

[3] Publicată în M. Of. nr. 1161 din 8 decembrie 2004.

[4] CCR, Dec. nr. 323 din 9 mai 2017 (M. Of. nr. 640 din 4 august 2017).

folosi de numele acesteia și de a întreba alte persoane cu legături în Poliția Română despre ocupația reală a investigatorului. O metodă mai simplă este căutarea acelei persoane pe rețele de socializare sau chiar pe internet pentru a afla anumite informații. De pildă, în condițiile în care rezultatele la admiterea în cadrul Academiei de Poliție „Alexandru Ioan Cuza" sunt publice, este ușor ca un infractor cu minime cunoștințe să afle dacă persoana cu care are legătură a absolvit studiile acestei instituții și, ca atare, este polițist. Deconspirarea calității reale de investigator poate avea consecințe grave pentru acesta[1], în primul rând, și mai apoi pentru desfășurarea cercetărilor ca urmare a înștiințării infractorilor cu privire la desfășurarea unei urmăriri penale împotriva acestora.

În funcție de durata pentru care un ofițer stă sub acoperire, doctrina[2] arată că se pot stabili patru categorii: operațiuni sub acoperire de scurtă durată, operațiuni sub acoperire de durată medie, operațiuni de lungă durată și operațiuni sub acoperire adâncă (*deep undercover*).

Operațiunile sub acoperire de scurtă durată, denumite și „operațiuni sub acoperire ocazionale", sunt acelea care pot fi realizate cu sau fără atribuirea unei identități fictive, nu implică modificarea aspectului fizic al investigatorului sub acoperire ori a obiceiurilor acestuia și nu implică un contact direct cu făptuitorii sau potențialii făptuitori. Această categorie de operațiuni nu vor putea intra sub incidența dispozițiilor art. 148 C.pr.pen., ele constituind, în realitate, forme de supraveghere tehnică ori măsuri speciale de cercetare. De exemplu, un ofițer de poliție judiciară primește sarcina să realizeze o înregistrare audiovideo a întâlnirii dintre mai multe persoane ce are loc într-o grădină de vară, fără a-și asuma o activitate fictivă, folosindu-se de tehnică operativă. Un alt exemplu de operațiune de scurtă durată este cumpărarea unor substanțe interzise într-o singură ocazie, situație în care va fi incidentă măsura de cercetare a participării autorizate la anumite activități, prevăzută de art. 150 C.pr.pen. În vederea probării acestei activități, alți lucrători de poliție vor realiza supravegherea video a persoanelor înainte de a se întâlni.

Operațiunile sub acoperire de durată medie se caracterizează prin asumarea unei identități fictive, care poate sau nu să presupună schimbarea aspectului fizic al investigatorului sub acoperire. O asemenea operațiune va privi un număr limitat de interacțiuni directe cu făptuitori sau potențiali făptuitori.

Operațiunile sub acoperire de lungă durată implică asumarea de către investigatorul sub acoperire a unei identități fictive, cu schimbări semnificative în aspectul fizic și obiceiurile personale[3], în scopul de a se întâlni cu făptuitori sau potențiali făptuitori în vederea derulării operațiunii pentru o perioadă mai mare de 6 luni. În același timp, acest tip de operațiune presupune contact direct și frecvent cu aceiași făptuitori sau potențiali făptuitori în locații particulare pe o perioadă extinsă de timp. Este important a se nota că, în asemenea operațiuni, investigatorul își menține independența față de grupul țintă.

Operațiunile sub acoperire adâncă presupun adoptarea de către investigatorul sub acoperire a unei identități fictive cu semnificative schimbări de aspect fizic și de obiceiuri personale, cu scopul de a se infiltra într-un grup infracțional organizat. Investigatorul sub acoperire va lucra

[1] În funcție de persoanele urmărite penal, un investigator a cărui calitate este aflată poate fi inclusiv omorât.

[2] *D.G. Fitzgerald*, Informants, Cooperating Witnesses, and Undercover Investigations. A Practical Guide to Law, Policy and Procedure, Second Edition, CRC Press, Boca Raton, Florida, 2015, pp. 371-372.

[3] Prin aceasta înțelegem schimbări, precum modificarea stilului de păr, creșterea unei bărbi, tatuarea, schimbarea tipului de haine purtate, dar și modificarea obiceiurilor unei persoane: frecventarea unor locuri noi, lipsa de interacțiune cu familia reală ori cu organele de urmărire penală, schimbarea domiciliului, adoptarea sau renunțarea la unele vicii etc.

într-o locație particulară ori într-o societate comercială deținută de grupul infracțional organizat și va avea în mod regulat și continuu contact direct cu făptuitori sau potențiali făptuitori.

§2. Colaboratorul

Colaboratorul este acea persoană care nu face parte dintre organele judiciare și care acționează sub coordonarea acestora pentru obținerea de date și informații[1]. Utilizarea colaboratorilor are caracter subsidiar, în sensul că nu se va putea autoriza utilizarea lor decât în situațiile în care, potrivit art. 148 alin. (10) C.pr.pen., folosirea investigatorului sub acoperire nu este suficientă pentru obținerea datelor ori informațiilor ori nu este posibilă. Din aceste dispoziții s-a dedus în doctrină că folosirea colaboratorilor ar avea un caracter excepțional[2], iar folosirea investigatorilor sub acoperire ar constitui regula atunci când se dispune măsura. În contrast cu doctrina autohtonă, literatura de specialitate străină relevă că folosirea lucrătorilor de poliție ca investigatori sub acoperire reprezintă excepția și că majoritatea operațiunilor presupun folosirea unui colaborator sau informator[3].

S-a considerat în mod eronat în doctrină că investigatorul sub acoperire va fi ajutat de un colaborator[4], în realitate nefiind necesară decât autorizarea colaboratorului care va acționa singur, păstrând legătura cu organele de urmărire penală prin lucrători de poliție. Nu este exclus ca ordonanța procurorului să presupună autorizarea atât a unui investigator sub acoperire, cât și a unui colaborator, însă pentru activități diferite. Nu vom fi de acord nici cu opinia că, pentru a fi utilizat un colaborator, va trebui să existe și un investigator sub acoperire autorizat[5].

Colaboratorii sunt, de regulă, infractori care au fost identificați de organele de urmărire penală și sunt determinați să își ofere sprijinul prin diferite metode. Nu este exclusă posibilitatea ca o persoană care nu a comis fapte prevăzute de legea penală să devină un colaborator al organelor de urmărire penală, însă realitatea ne învață că o persoană care nu este cointeresată în vreun mod (financiar, reținerea unei cauze de nepedepsire ori a unei cauze de reducere a pedepsei) nu își va pune în primejdie viața pentru a ajuta organele de urmărire penală, ea putând fi, în cel mai bun caz, un informator[6] anonim și ocazional ori un denunțător.

În practică, trebuie avute în vedere și considerente tactice în luarea deciziei folosirii unui colaborator în locul investigatorului sub acoperire, în special raportându-ne la factorul timp. Pentru eficiența unei acțiuni conspirative, este necesar ca investigatorul sub acoperire sau colaboratorul să se infiltreze în cadrul unei grupări, adică să ia legătură cu membrii grupului, să câștige încrederea acestora și, mai apoi, să acționeze în interesul grupului, dobândind în acest timp datele și informațiile necesare identificării membrilor grupului, a structurii organizaționale, precum și a descoperirii modului de operare și a faptelor comise de aceștia. Avantajul folosirii unui colaborator constă în faptul că acesta este, de cele mai multe ori, infiltrat în gruparea criminală vizată și nu trebuie să își dovedească loialitatea față de grup pentru a afla date și informații. Ca atare, colaboratorului nu i se va atribui o altă identitate în majoritatea

[1] *M. Bulancea*, în M. Udroiu (coord.), Codul de procedură penală, 2017, p. 449.

[2] *D. Grădinaru*, Investigarea infracțiunilor contra intereselor financiare ale UE, Ed. C.H. Beck, București, 2016, pp. 213-214.

[3] *D.G. Fitzgerald*, op. cit., p. 70; *R. Valdemar*, Cultivating Effective Gang Informants, în Police Magazine din 5 decembrie 2012, pe *www.policemag.com*

[4] *I.-C. Pașca*, op. cit., p. 119.

[5] *C. Olaru*, op. cit., p. 62.

[6] *V. infra*, Titlul XII, Capitolul V.2.

cazurilor, ci își va asuma propria sa identitate şi va continua activitățile sale în cadrul grupului pentru perioada de timp pentru care se continuă utilizarea în calitate de colaborator. Cu toate acestea, prevederile art. 148 alin. (10) C.pr.pen. nu exclud posibilitatea ca unui colaborator să i se atribuie o nouă identitate, situație pe care o considerăm excepțională şi care ridică reale probleme cu privire la legalitatea procedeului, procurorul trebuind să motiveze temeinic, mai ales într-o asemenea situație, necesitatea folosirii colaboratorului în locul unui investigator sub acoperire.

Deși prevederile Codului de procedură penală consideră că folosirea colaboratorilor se poate justifica numai în cazuri excepționale, preferându-se folosirea investigatorilor sub acoperire, realitatea este complet diferită. Ceea ce determină folosirea unui colaborator în locul unui investigator sub acoperire sunt situațiile concrete din teren, precum natura structurilor infracționale, modalitatea de organizare şi relațiile stabilite între membrii grupului[1].

Această metodă specială de cercetare este folosită mai ales în situațiile în care infracțiunile se săvârşesc ca urmare a existenței unui grup infracțional ori, cel puțin, există legături între mai multe persoane într-un lanț de aprovizionare (de pildă, în cazul infracțiunilor privind traficul şi consumul ilicit de droguri), fapt ce impune unui investigator sub acoperire obligativitatea infiltrării sale în acest grup. Din acest punct de vedere, trebuie să fie avută în vedere necesitatea realizării unor acțiuni care s-ar circumscrie săvârşirii unei infracțiuni, fiind necesară autorizarea unei participări autorizate la anumite activități, ceea ce ar putea contraveni interesului general al societății. De pildă, în cazul infiltrării unui investigator sub acoperire într-o rețea de traficanți de droguri, este necesar ca investigatorul să comită acte reprobabile, precum comercializarea unor substanțe interzise. Cu toate că fapta sa nu va constitui o infracțiune (fiind incidentă o variantă specializată a cauzei justificative a îndeplinirii unei obligații[2]), nu trebuie ignorat că fapta va avea urmări pe plan social – va încuraja consumul de droguri, ceea ce este contrar scopului pe care îl au organele judiciare – de a preveni săvârşirea de noi infracțiuni. În cazul folosirii unui colaborator, se vor utiliza serviciile unei persoane care a desfăşurat deja activități ilicite pentru care va fi trasă la răspundere penală ori, cel puțin, nu va fi sancționată ca urmare a unei cauze de nepedepsire, creându-se premisele pentru reeducarea acesteia[3]. Un alt argument priveşte durata maximă a măsurii, care, potrivit art. 148 alin. (10) C.pr.pen., este de un an, cu derogare în cazul unor anumite infracțiuni, situație în care infiltrarea unui investigator sub acoperire poate fi anevoioasă şi poate dura mai mult decât este permis prin lege a se folosi măsura.

Considerăm că minusurile utilizării unui colaborator în locul unui investigator sub acoperire pot fi soluționate prin măsuri legislative, precum obligarea procurorului de a prezenta, în detaliu, *care au fost avantajele de care a beneficiat colaboratorul* în urma activităților pe care le-a prestat. *De lege ferenda*, similar procedurii acordului de recunoaştere, se impune ca procurorul să propună în scris colaboratorului anumite beneficii legale (de pildă, reținerea unei cauze de nepedepsire, în măsura în care sunt îndeplinite şi celelalte condiții legale), iar acesta din urmă să semneze că este de acord să devină colaborator în schimbul acestor beneficii. Existența unui asemenea *acord de colaborare* este esențială pentru corecta exercitare a dreptului la apărare al suspectului sau inculpatului prin cunoaşterea motivelor pentru care

[1] *C.M. Chiriță*, în N. Volonciu, A.S. Uzlău (coord.), Noul Cod, 2014, p. 336.

[2] *Fl. Streteanu*, op. cit., p. 543.

[3] Ar fi greşit, din punct de vedere tactic, ca activitățile ulterioare ale unei asemenea persoane să nu fie cercetate în scop preventiv de către organele de poliție, aspect cunoscut şi de colaborator, care va fi îndemnat ca pe viitor să adopte un comportament conform cu normele sociale.

persoana a colaborat și constituie un fundament pe baza căruia instanța poate evalua probele care derivă din activitatea colaboratorului ori a declarației acestuia.

Remarcăm că, în practică, se întâlnește frecvent noțiunea de „martor denunțător" pentru a desemna o persoană care denunță săvârșirea unei infracțiuni pentru ca, mai apoi, să fie audiată în calitate de martor. În mod evident, terminologia uzitată este incorectă, în condițiile în care denunțătorul este acea persoană care formulează un act de sesizare a organelor de urmărire penală și nu are nicio calitate în procesul penal. În schimb, martorul este un subiect procesual secundar și este titularul unor drepturi și obligații, cuprinse în art. 117-118 și 120 C.pr.pen.

O versiune controversată a acestui martor denunțător este denunțătorul colaborator, adică acea persoană care, ulterior formulării unui denunț, realizează acțiuni în vederea obținerii de probe împotriva unei persoane, cu sprijinul organelor de urmărire penală. Deoarece declarația unui denunțător, audiat în calitate de martor, nu poate fundamenta o acuzație de natură penală, organele de urmărire penală se folosesc de aceste persoane pentru obținerea de probe prin realizarea unor înregistrări audiovideo sau audio, fără a declara vreun moment că persoanele au calitatea de colaboratori. În concret, se poate proceda la organizarea unor întâlniri între denunțătorul colaborator și persoana cercetată, în condițiile în care se plasează asupra denunțătorului colaborator tehnică operativă de supraveghere[1], ori se poate proceda și la înregistrarea de tehnică în casa denunțătorului colaborator în perioada în care acesta se afla în arest la domiciliu, deci cunoștea și își dădea acordul instalării dispozitivelor[2]. Astfel de tactici de cercetare sunt neloiale, în condițiile în care se neagă existența unei înțelegeri de colaborare între denunțător și procuror în vederea evitării dispozițiilor art. 103 alin. (3) C.pr.pen., care arată că o hotărâre de condamnare, renunțarea la aplicarea pedepsei ori amânarea aplicării pedepsei nu se poate fundamenta în mod determinant pe declarațiile investigatorilor, ale colaboratorilor ori ale martorilor protejați. Problemele privind loialitatea probei incidente sunt: cointeresarea colaboratorului în producerea unor probe *pro causa* pentru acuzare și audierea denunțătorului colaborator în calitate de martor, declarația sa putând fi apreciată de judecător ca probă determinantă în alegerea soluției.

Prima problemă de loialitate constă în caracterul cointeresat și ascuns al acțiunilor martorului colaborator, care beneficiază de o cauză de nepedepsire ori de reducere a pedepsei, în cazul în care denunță săvârșirea unei infracțiuni și, mai apoi, ajută la tragerea la răspundere penală a persoanei. Deși acțiunea de a denunța fapte de natură penală este cea care atrage, de cele mai multe ori, cauza de nepedepsire (de pildă, în cazul infracțiunii de dare de mită), reținerea acesteia rămâne la latitudinea procurorului, astfel că, până la soluționarea cauzei penale privind denunțătorul, acesta nu are o certitudine că va beneficia de ea. Așa cum prevede și art. 101 alin. (1) C.pr.pen., este considerată o probă neloială acea probă obținută prin constrângere și promisiuni ori îndemnuri făcute asupra denunțătorului colaborator, ceea ce pune sub semnul întrebării loialitatea tuturor probelor obținute prin mijlocirea acestuia, deoarece, spre deosebire de un investigator sub acoperire, colaboratorul va avea un interes personal concret să determine celelalte persoane cu care interacționează fie să comită o infracțiune, fie să recunoască comiterea unei infracțiuni trecute ori să extragă informații care să poată fi folosite împotriva persoanei cercetate. *De lege ferenda*, se impune ca, la momentul

[1] De regulă, se folosește tehnică audio, nu audiovideo, iar înregistrările se clasifică drept înregistrări ambientale, cu scopul de a se susține că denunțătorul colaborator nu a avut nicio implicare.

[2] C. Ap. Oradea, încheierea nr. 28 din 29 martie 2016 a judecătorului de cameră preliminară, pronunțată în dosar nr. 84/35/2016, nepublicată.

formulării unui denunț, să se încheie un acord cu procurorul, prin care să se rețină cauza de nepedepsire ori de reducere a pedepsei, indiferent de contribuția ulterioară a denunțătorului, or, dacă această contribuție este incidentă, procurorul va trebui să procedeze la autorizarea denunțătorului în calitate de colaborator.

Cea de-a doua problemă de loialitate se referă la eludarea dispozițiilor legale privind audierea investigatorilor, colaboratorilor și martorilor protejați, care obligă instanța să nu își întemeieze hotărârea în mod determinant pe probele care rezultă din audierea acestor categorii de persoane. Dacă în cazul unui colaborator obișnuit, aceasta nu reprezintă o problemă, fiind necesar a se verifica existența la dosarul cauzei a unei ordonanțe de autorizare a acestuia, în cazul unui denunțător colaborator, acest lucru este mai dificil, deoarece instanța nu are suficiente date pentru a reconsidera persoana drept colaborator. Mai mult, la momentul audierii sale în fața instanței, etapa camerei preliminare este deja parcursă, astfel că nu se poate proceda la excluderea unor declarații date de denunțătorul colaborator în cursul urmăririi penale ori a probelor produse prin mijlocirea sa. Pentru a determina existența unei colaborări fără autorizare, instanța va trebui să analizeze următoarele aspecte: dacă denunțătorul colaborator a avut vreun beneficiu în urma activității sale (prin raportare la existența altor dosare penale în care să aibă calitatea de inculpat, reținerea unor cauze de nepedepsire etc.), dacă acte de urmărire penală, în special măsuri de supraveghere tehnică, s-au realizat în prezența denunțătorului colaborator și, mai apoi, dacă, în urma vizionării suporților optici ai acestuia, se poate identifica amplasarea tehnicii operative pe persoana colaboratorului[1], dacă înregistrările s-au desfășurat în locații private ale denunțătorului colaborator, dacă în cuprinsul discuțiilor dintre colaborator și alte persoane s-a urmărit obținerea unor confesiuni ori s-a instigat la obținerea unor formulări compromițătoare etc.

Cu toate acestea, dacă instanța are suficiente indicii că denunțătorul a realizat acte la îndemnul procurorului și a acționat ca un colaborator, considerăm că se impune înlăturarea lor odată cu soluționarea fondului cauzei, potrivit art. 403 alin. (1) lit. c) C.pr.pen. În privința remediului privind audierea în calitate de martor a denunțătorului colaborator, considerăm că instanța va trebui să aprecieze declarația acestuia ca fiind una interesată, iar, potrivit art. 103 alin. (3) C.pr.pen., o soluție de condamnare, renunțare la aplicarea pedepsei ori amânare a aplicării pedepsei nu se va putea fundamenta în mod determinant pe aceasta.

§3. Informatorul

Deși în cuprinsul art. 148 C.pr.pen. se menționează numai două calități, investigator și colaborator, observăm că textul art. 149 C.pr.pen. face referire și la o a treia categorie de persoane: *informatorul*. Această din urmă calitate este menționată strict cu privire la măsurile de protecție de care pot beneficia investigatorii sub acoperire și colaboratorii, fără a fi menționați în legătură cu efectuarea unor activități sub autorizarea procurorului.

Doctrina română nu face nicio referire la noțiunea de „informator" și semnificația acesteia pentru procesul penal, o omisiune care nu a trecut de legiuitor însă. Raportându-ne la doctrina americană, observăm că se face o distincție între mai multe tipuri de persoane care pot participa în anchete care implică obținerea unor informații din interiorul unui grup țintă, informatorul

[1] De exemplu, în cazul unei înregistrări audiovideo, va fi evidentă situația descrisă din cauză că imaginile se vor deplasa deodată cu denunțătorul colaborator și nu îi vor putea surprinde fizicul. În cazul înregistrărilor audio, va trebui să se urmărească foșnetul hainelor, precum și volumul dialogului dintre persoanele înregistrate, vocea colaboratorului fiind la un volum mai ridicat datorită apropierii față de microfon.

fiind considerat acea persoană care își va păstra în toate cazurile anonimitatea, nu va putea fi audiat în calitate de martor și va furniza organului de urmărire penală *date sau informații cu privire la săvârșirea unei infracțiuni*[1].

În ceea ce ne privește, considerăm că, în sistemul român, informatorul poate fi definit ca acea persoană care cunoaște date sau informații cu privire la săvârșirea unei infracțiuni ori cu privire la împrejurări legate de aceasta, utile pentru soluționarea cauzei și care își păstrează întotdeauna anonimitatea.

Informatorii sunt, de regulă, persoane cu probleme de natură penală (infractori) ori persoane din cercul unor persoane suspectate de săvârșirea unor infracțiuni, care furnizează la cerere informații cu privire la alte persoane ori cu privire la fapte. Colaborarea lor cu organele de urmărire penală nu este continuă cu privire la un anumit caz și nu trebuie confundați cu colaboratorii, în condițiile în care informatorul nu este împuternicit de procuror să culeagă date și informații conform art. 148 alin. (5) C.pr.pen., ci el furnizează date și informații pe care le cunoaște ca urmare a interacțiunilor sale cotidiene (uneori simple zvonuri). În măsura în care unei asemenea persoane i se va cere să culeagă date despre o persoană ori despre o anumită faptă, considerăm că informatorul va deveni un colaborator.

În sistemul american, în special[2], fiecare agenție a Departamentului de Justiție (F.B.I., A.T.F., D.E.A.) urmează o politică agresivă de recrutare a informatorilor și a colaboratorilor în vederea desfășurării activităților curente. Ca urmare a diferențelor existente în modul de operare a celor trei agenții amintite, dar și a diferenței dintre legislația statală și cea federală, termenul de „informator" poate desemna mai multe realități faptice, putându-se referi inclusiv la persoane care nu au legătură cu activități infracționale, la persoane care nu sunt recrutate, dar își oferă direct serviciile ca informatori, la cetățeni obișnuiți (*good citizens*) sau la persoane care divulgă informații din cadrul unei organizații (*whistleblowers*). Realitatea este că, pentru acest sistem, informatorii și colaboratorii sunt esențiali pentru soluționarea unor cauze care implică activități de grup ori privesc comercializarea unor bunuri interzise (substanțe interzise, arme etc.), însă sunt extinse și asupra unor cazuri de corupție. Informatorii, asemenea colaboratorilor, sunt recrutați de către organele de poliție și își mențin caracterul conspirativ pe o perioadă nedeterminată, cu anumite excepții. Procedura de recrutare și verificare a informatorilor și colaboratorilor este stabilită prin regulile interne, adeseori secrete, ale fiecărei agenții[3].

În lipsa unei reglementări exprese a informatorilor în legislația română, considerăm că aceștia nu pot fi folosiți de către organele de urmărire penală pentru strângerea unor probe și nici chiar pentru realizarea operațiunilor la care se referă art. 148 C.pr.pen., decât în măsura în care devin colaboratori. În același timp, informatorul poate fi audiat în calitate de martor în cursul procesului penal, în măsura în care acceptă să facă acest lucru, iar acest lucru nu dăunează din punct de vedere tactic urmăririi penale, sau folosirea sa în alte cauze subsecvente. Este eronat a crede că organele de poliție și organele de urmărire penală nu dispun de legături în lumea interlopă, polițiștii având deseori legături cu persoane implicate în acțiuni ilegale, dar care pot cunoaște amănunte despre săvârșirea unor alte infracțiuni. Cu ocazia efectuării unor acte de urmărire penală ori chiar și a unor acte de menținere a ordinii publice, polițiștii intră în legătură cu aceste persoane, pe care le audiază în mod informal despre problemele din

[1] F.B.I., Manual of Investigative Operations and Guidelines (MIOG), art. 137-3.

[2] *D.G. Fitzgerald*, op. cit., p. 29.

[3] De exemplu, în cazul F.B.I., documentul se numește „Manual of Investigative Operations and Guidelines", în vol. III, secțiunea 137 fiind dezbătute problemele privind informatorii și colaboratorii.

zona în care locuiesc sau despre persoane care ar fi săvârșit anumite fapte. În urma acestor demersuri pot rezulta zvonuri sau chiar informații despre locul unde s-ar afla o anumită persoană ori date despre obiecte văzute asupra unei anumite persoane (și provenite dintr-un furt), activitățile economice ale unei persoane (amanetarea unor bijuterii) etc., pe baza cărora organele de urmărire penală pot proceda la realizarea unor acte de urmărire penală care să ducă la soluționarea cauzei. De pildă, un informator încunoștințează un organ de urmărire penală că urmează să aibă loc un transport de droguri și indică elemente care să ajute la identificarea autovehiculului și, folosindu-se de această informație, poliția organizează un filtru în urma căruia se constată infracțiunea flagrantă. Importanța informatorilor este deosebită în lupta contra infracționalității cotidiene, inclusiv în cazul infracțiunilor de furt, unde persoane de aceeași etnie care locuiesc în construcții improvizate pot constitui informatori ai poliției, uneori pentru beneficii mărunte (sume modice de bani, alimente etc.), și pot da detalii cu privire la persoane care au obținut în ultima vreme bunuri.

Secțiunea a 2-a. Recrutarea și motivarea colaboratorilor și informatorilor

În situația folosirii colaboratorilor în cursul aplicării măsurii prevăzute de art. 148 C.pr.pen., dar și în activitățile obișnuite ale organelor de urmărire penală, în cadrul cărora se folosesc date și informații furnizate de informatori, trebuie exercitată o grijă deosebită asupra încrederii de care poate beneficia o astfel de persoană, care se răsfrânge în special asupra credibilității probelor ori informațiilor oferite de aceștia. O atare problemă nu o regăsim în situația investigatorului sub acoperire, în privința acestuia neexistând niciun dubiu că este un agent al statului, de cele mai multe ori, un ofițer de poliție judiciară, ca atare este interesat de dovedirea existenței unei fapte de natură penală și de a contribui la construirea probatoriului în sprijinul acuzării. În schimb, în situația colaboratorului și a informatorului, există tendința de a-l confunda cu un martor obișnuit, care nu ar avea niciun interes să nu spună adevărul în cauză și nu ar fi determinat de vreun beneficiu să realizeze activitățile cerute. Or, o astfel de abordare este fundamental greșită, deoarece atât informatorul, cât și colaboratorul sunt *persoane care au un interes privat în cauză*, ele furnizându-și serviciile în schimbul unui beneficiu patrimonial (bani – retribuție pentru informațiile furnizate), al unor avantaje nepatrimoniale (reținerea unei circumstanțe atenuante, a unei cauze de nepedepsire etc.) sau a unor beneficii de natură morală (siguranță, îndeplinirea îndatoririlor civice etc.).

În această parte a lucrării, vom aborda problema modului în care sunt *recrutați în slujba organelor de urmărire penală colaboratorii și informatorii*, pentru ca, mai apoi, să analizăm care sunt *principalele motive pentru care o persoană ar dori să activeze drept colaborator sau informator*.

§1. Recrutarea colaboratorilor și informatorilor

Un element deosebit de important este *modul în care sunt recrutați colaboratorii*, în condițiile în care aceștia nu au legături instituționale cu organele judiciare și modul în care aceștia sunt *motivați pentru a colabora*.

Prin „recrutare" înțelegem procedeul inițial de abordare a persoanei, care se dorește a fi folosită drept colaborator sau informator de către organele de urmărire penală, prin prezentarea unor avantaje care să o motiveze pentru a coopera. Nu orice persoană poate fi utilă soluționării unei cauze penale în calitatea de informator sau colaborator și astfel este necesar să existe o

selecție prealabilă pentru a se recruta persoane care să nu pună în primejdie aflarea adevărului ori persoanele care realizează urmărirea penală. Din păcate, sistemul judiciar român nu a creat un set de reguli pentru a ajuta în această problemă, lăsând la latitudinea și îndemânarea organului de urmărire penală acest demers.

În schimb, organe de urmărire penală din alte state au pus la punct ghiduri concrete[1] și recomandări la nivelul cel mai înalt[2] în privința modului în care se recrutează informatorii și colaboratorii, punând accent pe problema loialității lor după recrutare, a posibilității furnizării de informații și a posibilității de a lucra împotriva organelor de urmărire penală.

Potrivit celui mai recent Manual de investigații al Federal Bureau of Investigations, se arată că următoarele criterii trebuie avute în vedere la determinarea aptitudinii unei persoane de a fi folosită ca informator sau colaborator:

a. dacă persoana pare să fie într-o poziție care să îi permită să furnizeze informații cu privire la încălcări ale legii și care intră în competența de investigare a F.B.I.;

b. dacă persoana este dispusă să ofere în mod liber informații către F.B.I.;

c. dacă persoana pare să fie comandată de alții pentru a obține informații din interiorul F.B.I.;

d. dacă există elemente în trecutul persoanei de natură a o face inaptă pentru a fi folosită ca informator;

e. dacă natura obiectului urmăririi penale și dacă importanța informațiilor care pot fi obținute de F.B.I. depășește ca importanță gravitatea oricărui comportament infracțional trecut sau prezent de care informatorul este bănuit;

f. dacă motivele invocate de informatorul care se oferă în mod voluntar să furnizeze informații sunt raționale, reale și oneste;

g. dacă informațiile care pot fi furnizate de informator pot fi obținute într-un mod mai rapid și mai eficient de la alte surse sau prin măsuri mai puțin intruzive;

h. dacă informatorul este de nădejde și demn de încredere și dacă există un mijloc adecvat prin care se poate verifica credibilitatea sa;

i. dacă persoana pare să fie de acord să se conformeze pe viitor metodologiei F.B.I. și a Attorney General cu privire la operațiunea desfășurată;

j. dacă F.B.I. va fi apt să monitorizeze și să controleze în mod adecvat activitățile informatorului;

k. dacă folosirea informatorului ca măsură de cercetare va constitui o intruziune asupra unor comunicări privilegiate[3] ori asupra dreptului persoanei la liberă asociere ori liberă exprimare a ideilor;

l. dacă folosirea unui informator poate compromite o cercetare în curs sau, ulterior trimiterii în judecată, ar impune reprezentantului Guvernului[4] să solicite restituirea cauzei[5].

---

[1] F.B.I., Manual of Investigative Operations and Guidelines, desecretizat la nivelul anului 1998, Secțiunea 137, pe *vault.fbi.gov*

[2] Office of the Inspector General of the U.S.A., The Federal Bureau of Investigation's Compliance with the Attorney General's Investigative Guidelines, Capitolul III. The Attorney General's Guidelines Regarding the Use of Confidential Informants, pe *oig.justice.gov*

[3] Sensul de *privileged communications* este un termen specific dreptului american, el putând fi echivalat cu acele informații pe care o persoană le furnizează unei alte persoane, între acestea existând obligația păstrării secretului (profesional), de pildă, discuții purtate cu un medic, un avocat, un psiholog. Pentru o explicație asupra privilegiilor în general, a se vedea *www.law.harvard.edu*

[4] Procurorul.

[5] În engleză, *dismissal of the case*, o instituție ce nu se aseamănă cu restituirea cauzei care poate avea loc în camera preliminară, putând avea și efect peremptoriu asupra întregii acțiuni penale.

Toate regulile metodologice expuse mai sus sunt gândite pentru a constitui un ghid atât pentru procurori, cât și pentru organele de cercetare penală, în determinarea aptitudinii unei persoane de a servi la aflarea adevărului în calitate de informator sau colaborator, avându-se în vedere și caracterul subsidiar al acestei măsuri.

În opinia noastră, deși nu se impune legiferarea unor asemenea criterii, considerăm că procurorul va trebui să aibă în vedere câteva dintre condițiile arătate mai sus, pentru a determina dacă se impune utilizarea unei persoane drept colaborator:

- persoana poate afla informații noi despre pregătirea sau săvârșirea unei infracțiuni care să ducă la aflarea adevărului;
- persoana își declină motivația reală pentru a colabora cu organele de urmărire penală și aceasta poate fi verificată;
- persoana s-a asociat într-un mod superficial, întâmplător, ori a fost forțată să adere la grupul infracțional;
- persoana a avut sau nu antecedente de natură penală și care au fost acestea;
- dacă persoana pare dispusă să respecte indicațiile primite de la organele de urmărire penală;
- dacă persoana a fost condamnată pentru săvârșirea infracțiunii de mărturie mincinoasă;
- dacă persoana urmărește aflarea unor informații de la organele de urmărire penală pentru folosul membrilor unui grup infracțional organizat;
- dacă folosirea persoanei o poate pune în pericol grav ori poate pune în pericol grav o altă persoană ori poate periclita aflarea adevărului în cauză.

Alături de criteriile propuse mai sus, procurorul va trebui să aibă în vedere și condițiile generale pentru dispunerea măsurii utilizării investigatorilor sub acoperire și a colaboratorilor.

În ceea ce privește modalitatea concretă de recrutare a viitorului colaborator sau informator, se impune ca, mai întâi, potențialul candidat să fie descoperit și, mai apoi, să fie convins să sprijine organele de urmărire penală prin oferirea unui beneficiu de către procuror.

Descoperirea potențialului colaborator sau informator se poate face prin reținerea persoanei, în măsura în care există suspiciunea săvârșirii unei infracțiuni. Cu această ocazie, dacă sunt date că această persoană ar face parte dintr-un grup infracțional organizat sau ar avea cunoștință despre persoane care activează într-un asemenea grup, se impune adoptarea unei atitudini în funcție de nivelul de pregătire și caracteristicile psihologice ale persoanei: o atitudine frontală, directă și agresivă a organului de urmărire penală, alături de o prezentare detaliată a consecințelor unei condamnări pentru faptele de care este acuzat, pot convinge o persoană influențabilă să vrea să activeze în calitate de colaborator. În doctrina americană se arată că momentul propice este înainte ca persoana să fie asistată de un avocat[1].

O altă ipostază în care o persoană poate fi abordată este dacă este chemată să dea o declarație în calitate de martor și se descoperă că are cunoștință despre anumite activități infracționale.

În ambele situații, colaboratorul va fi o persoană care este suspectată de săvârșirea unei infracțiuni, ea urmărind, prin colaborarea cu organele de urmărire penală, să obțină un beneficiu care îi și poate fi oferit în măsura în care este legal. În niciun caz nu se poate admite folosirea de promisiuni ori prezentarea unor informații false pentru a atrage o persoană spre a deveni colaborator. În același timp, nu i se poate promite reținerea unei cauze de atenuare neprevăzute de lege sau a unor beneficii nelegale (de pildă, dispunerea unei soluții de clasare în mod nelegal) în vederea obținerii colaborării sale.

[1] *D.G. Fitzgerald*, op. cit., p. 75.

Cel mai des întâlnit caz de colaborator este cel al consumatorilor de droguri, care sunt reținuți de organele de urmărire penală și asupra lor se găsesc cantități mici de substanțe interzise. Motivând aceste persoane prin apelare la anumite cauze de reducere a pedepsei ori de nepedepsire, procurorul poate reuși să le determine să ajute în mod concret strângerea de probe. Odată determinată să colaboreze, persoana este instruită să ia legătura cu traficanți și, mai apoi, să cumpere cantități de droguri cu banii furnizați de organele de poliție (evident, cu autorizarea prealabilă a participării autorizate la anumite activități), în timp ce este supravegheată de alte organe de urmărire penală, obținându-se probe cu privire la cumpărarea de droguri de la o anumită persoană.

O altă modalitate prin care se poate reuși recrutarea unei persoane este prin folosirea stării sale emoționale în dezavantajul său, prin invocarea posibilității de a fi încadrată într-un program de protecție a martorilor. Dacă o persoană care se dorește a fi recrutată acuză amenințări și o stare de temere, în măsura în care este reală, recrutarea se poate face contra promisiunii că va fi inclusă într-un program de protecție. Avantajul folosirii acestei metode este că permite oricând procurorului să îl constrângă pe colaborator să fie fidel cauzei, în caz contrar putând înceta programul său de protecție, la cererea procurorului.

După un prim contact cu potențialul colaborator sau informator, se impune ca acesta să fie supravegheat o perioadă de timp înainte de a fi folosit pentru prima dată de organele de urmărire penală. Deși nu suntem adepții ideii unor colaboratori de carieră, este esențială evaluarea încrederii ce poate fi garantată de aceste persoane. Problema nu este așa de gravă în cazul informatorilor, care furnizează date organelor de urmărire penală într-un mod neoficial.

Încrederea pe care organele de urmărire penală o pot avea în persoana recrutată drept colaborator afectează cel mai mult veridicitatea informațiilor date. Ca în orice alt domeniu al vieții, încrederea trebuie câștigată, iar organul de urmărire penală trebuie să își testeze colaboratorul și informatorul înainte să îi trimită spre a realiza activități importante sau care pot dăuna urmăririi penale, dacă sunt realizate greșit. Câștigarea încrederii în colaborator sau informator va fi treptată, dar va trebui să fie consemnată în cazul fiecărei persoane, de-a lungul timpului. În metodologia adoptată de F.B.I., perioada inițială în care colaboratorul este verificat și testat este de 120 de zile (SI – *suitability and pertinence inquiry*) și poate fi prelungită până la 240 de zile, moment până la care trebuie să se determine că individul este de încredere și este apt să fie folosit într-o cauză penală, iar, în măsura în care după acest termen maxim nu se poate stabili acest lucru, el nu va fi folosit[1]. În timpul perioadei de probă, persoana trebuie să fie supusă unei investigații amănunțite cu privire la persoana sa, pentru a se determina dacă există elemente din care să rezulte că este inapt. De exemplu, se descoperă că are o relație amoroasă cu o femeie din grupul infracțional organizat și aceasta este în relație de rudenie cu un lider al grupării, se descoperă că este consumator de droguri, iar urmărirea penală privește fapte de altă natură etc. Într-o asemenea procedură, considerăm că sunt oportune măsuri de supraveghere tehnică exercitate asupra viitorului colaborator, însă, la acest moment, legea nu permite acest lucru.

[1] Art. 137-3.1 alin. (1) din F.B.I., Manual of Investigative Operations and Guidelines: „The SI will be conducted for a period not to exceed 120 days. An extension of the initial 120 day period may be authorized by the SAC. (...) If an individual cannot be certified within 240 days from intitiation of the SI, he/she should be closed".

§2. Motivarea colaboratorilor și informatorilor

Problema motivării colaboratorilor și chiar a informatorilor este deosebit de importantă pentru aflarea adevărului, atât din perspectiva organelor de urmărire penală, cât și a avocatului suspectului sau inculpatului, existând posibilitatea ca probele, datele sau informațiile obținute prin folosirea colaboratorilor și a informatorilor să fie viciate de însșiși factorii care îi determină să ajute organele de urmărire penală.

Legiuitorul nu a reușit să creeze un mecanism procedural care să permită în mod eficient verificarea motivației care stă la baza acceptării de un colaborator sau informator să ajute organele de urmărire penală, prezumându-se că aceste motive ar fi unele licite. În prezent, singura cale în care se poate afla motivația aceasta este prin intermediul audierii colaboratorului, însă ne exprimăm rezerve cu privire la eficiența acestei soluții prin raportare la posibilitatea instanței de a cenzura orice întrebare care ar putea duce la divulgarea identității persoanei, iar motivația, în unele situații, ar putea fi considerată de un judecător excesiv de precaut ca putând contribui în acest sens.

Este important ca motivele care stau în spatele ajutorului conferit de colaboratori și informatori să fie cunoscute de instanță, pentru a se evita soluții care sunt departe de adevărul absolut și sunt determinate de declarațiile mincinoase ale unui colaborator interesat de obținerea unui beneficiu ca urmare a ajutării acuzării. Deși Codul de procedură penală arată că soluția instanței nu se poate baza în mod determinant pe declarațiile investigatorului sub acoperire ori ale colaboratorului, nimic nu împiedică instanța să coroboreze o probă viciată cu alte probe indirecte și să ajungă la o soluție de condamnare. Situația a fost subliniată în doctrină, arătându-se că, în măsura în care există mai multe probe indirecte în acuzare, iar ansamblul probator conduce în mod univoc la stabilirea faptei, persoana va putea fi găsită vinovată[1].

Din perspectiva procurorului, se impune ca motivarea colaboratorului să cântărească mult în aprecierea credibilității lui, acesta trebuind să știe în orice moment ce a determinat acea persoană să ajute organele de urmărire penală, pentru a putea menține persoana de partea organelor de urmărire penală[2] și a se evita, în special, obținerea de informații asupra anchetei de către persoanele față de care s-a dispus măsura de cercetare (situația unui colaborator – **agent dublu**). Nu trebuie uitat că un colaborator și un informator au acces la informații cunoscute numai de către organele de urmărire penală, iar acestea pot fi esențiale pentru buna desfășurare a unei cauze. Un exemplu care poate fi imaginat este autorizarea mai multor colaboratori, dintre care unul este un așa-zis agent dublu, infiltrat în cadrul organelor de urmărire penală pentru a descoperi identitatea altor colaboratori sau informatori[3].

În privința rolului avocatului în audierea unui colaborator în cursul procesului penal, dezvoltarea unei strategii de apărare efective impune aflarea motivelor care au determinat colaboratorul spre a se verifica loialitatea obținerii probelor derivate din măsura de cercetare. Atunci când întreaga urmărire penală s-a desfășurat cu ajutorul unui colaborator (denunț formulat de acesta, furnizarea mai multor declarații, înregistrarea ambientală a convorbirilor din cadrul domiciliului acestuia, purtarea tehnicii operative la întâlniri cu alte persoane etc.), chiar și unul ascuns sub denumirea generică de „denunțător", strategia apărării va fi afectată în mod determinat de modul în care se va reuși aflarea motivației acestui colaborator.

[1] *I. Neagu*, op. cit., pp. 441-442.
[2] *D.G. Fitzgerald*, op. cit., p. 45.
[3] *Ibidem*, pp. 54-55.

Soluția pe care o propunem este ca, în cursul urmăririi penale, să se încheie, mai înainte de emiterea ordonanței de autorizare a utilizării colaboratorilor, un acord de colaborare între procuror și viitorul colaborator, în care să se evidențieze care sunt beneficiile oferite colaboratorului în schimbul serviciilor sale pentru buna înfăptuire a justiției. Considerăm că termenul de „serviciu" este cel mai adecvat termen, deoarece, așa cum vom vedea, motivarea unui colaborator se poate face inclusiv prin contraprestații bănești din partea autorităților.

Principalele motive care determină persoanele să ajute organele de urmărire penală în calitate de colaboratori sau informatori sunt: banii, frica, răzbunarea, amenințările primite de la făptuitori, tratament special în timpul stării de deținere, ego-ul, amenințări cu deportarea, remușcări sau îndatorirea cetățenească[1]. Alături de aceste motivații surprinse în doctrină, considerăm că, în sistemul român, cel mai des motiv de colaborare îl constituie *reținerea unei cauze de nepedepsire sau de reducere a pedepsei.*

2.1. Reținerea unei cauze de nepedepsire sau a unei cauze de reducere a pedepsei

Un motiv important pentru oferirea sprijinului către organele de urmărire penală îl constituie posibilitatea reținerii unor cauze legale de nepedepsire sau de reducere a limitelor de pedeapsă pentru colaboratorii care ajută în mod determinant, prin activitatea lor, tragerea la răspundere penală a unor persoane. Aceste dispoziții nu se vor aplica investigatorilor care, fiind lucrători ai Poliției Române, sunt incompatibili cu însăși ideea de a avea un trecut infracțional ori să fie implicați în activități infracționale.

Pentru a se reține o cauză de reducere sau de nepedepsire, legea stipulează, în funcție de fiecare cauză în parte, necesitatea realizării unor activități care să ajute la prinderea și tragerea la răspundere penală a unor infractori sau numai a unor participanți la infracțiune. Uneori, poate fi suficientă și sesizarea organelor de urmărire penală prin denunț pentru a se reține o cauză de nepedepsire sau de reducere a pedepsei, dar, în asemenea situații, procurorul va prefera să continue folosirea acelei persoane pentru strângerea de probe, aceasta fiind situația în care un colaborator va fi considerat în practică un așa-zis „martor denunțător", un termen impropriu prin însăși natura sa.

Motivarea colaboratorilor prin intermediul acestor cauze legale este un demers relativ simplu pentru procuror, deoarece constă în prezentarea unor dispoziții legale ce ar atrage beneficii pentru viitorul colaborator, care ar fi promise verbal. Neajunsul unei asemenea abordări, cauzate mai ales de lipsa reglementării unui mod de a obliga procurorul să își onoreze promisiunea, constă în subordonarea colaboratorului până în momentul încetării măsurii de cercetare autorizate. Colaboratorul va cunoaște că prestația sa va fi evaluată de procuror, fiind posibil ca acesta să realizeze în mod voluntar activități care nu i-au fost solicitate, pentru a-și spori utilitatea. O asemenea situație o poate constitui determinarea săvârșirii unei infracțiuni de către gruparea infracțională, ceea ce nu este permis unui colaborator chiar și în situația în care se folosește măsura participării autorizate la anumite activități. De pildă, colaboratorul care activează în cadrul unei urmăriri penale care are ca obiect fapte de corupție, va înmâna unui politician un plic mat, în care ar pretinde că se află documente, în acesta fiind, în realitate, bani, organizându-se în același timp un flagrant. În mod evident, dacă un colaborator va avea o atitudine de asemenea natură, se vor strânge mai lesne probe (de pildă, prin supravegherea tehnică a membrilor unui grup infracțional), însă probele vor avea un caracter neloial prin raportare la dispozițiile art. 101 alin. (3) C.pr.pen.

[1] *Ibidem*, p. 45.

Promisiunea reținerii unei cauze legale de nepedepsire sau reducere a pedepsei este întotdeauna condiționată de eficiența și de calitatea serviciilor prestate de colaborator, iar siguranța acordării acestora o poate avea numai în momentul terminării urmăririi penale față de acesta printr-o soluție de clasare, trimitere în judecată ori de renunțare la urmărirea penală.

Dintr-o altă perspectivă, trebuie avute în vedere și efectele pozitive ale activității colaboratorului cu privire la demersurile pe care le face, chiar și încurajat de beneficiul nepedepsirii ori reducerii limitelor de pedeapsă, către reeducarea sa. În mod real, o persoană care activează în calitate de colaborator și, în măsura în care nu a avut antecedente penale într-un număr ridicat, va înțelege mai bine consecințele faptelor sale, mai ales în condițiile în care activitatea să îi poată pune în pericol viața, servind drept o experiență de viață pe care nu va dori să o repete.

Cauzele de nepedepsire ori de reducere a pedepsei se pot stabili numai prin lege, ele fiind prevăzute în cuprinsul Codului penal sau a legislației penale speciale. În cele ce urmează vom face succinte precizări cu privire la cele mai importante cauze de nepedepsire sau reducere a pedepsei.

Codul penal reglementează, în cazul infracțiunilor de corupție, două situații în care persoana care a săvârșit o faptă de corupție activă nu va fi pedepsită în cazul în care va formula un denunț cu privire la propria sa faptă de corupție, mai înainte ca organul de urmărire penală să fi fost sesizat cu privire la această faptă. Cu alte cuvinte, este recompensată acea persoană care, ulterior săvârșirii unei fapte, denunță această activitate, ducând la descoperirea faptei de către organul de urmărire penală și contribuind, în acest mod, la tragerea la răspundere penală a autorului celeilalte infracțiuni bilaterale. Această cauză de nepedepsire este incidentă în cazul infracțiunilor de dare de mită și cumpărare de influență, fiind reglementată prin art. 290 alin. (3) C.pen., respectiv art. 292 alin. (2) C.pen.

Tot în cazul infracțiunilor de corupție poate fi incidentă o cauză de reducere a limitelor de pedeapsă, cuprinsă în dispozițiile art. 19 din O.U.G. nr. 43/2002 privind Direcția Națională Anticorupție, republicată[1]. Această cauză de reducere a limitelor de pedeapsă va fi incidentă în cazul în care o persoană a săvârșit o faptă care intră în competența D.N.A., iar în timpul urmăririi penale, *denunță* și *facilitează* identificarea și tragerea la răspundere penală a altor persoane care au săvârșit astfel de infracțiuni. Incidența acestei cauze este limitată doar la faptele care pot face obiectul unei urmăriri penale realizate de D.N.A.[2]. Nu va fi suficientă denunțarea unor infracțiuni care intră în competența D.N.A., ci se va impune ca persoana să ajute organele de urmărire penală în tragerea la răspundere penală a acestora, implicând o contribuție fie în calitate de martor, fie în calitate de colaborator. Din modul în care este reglementată cauza de reducere a pedepsei, se observă că procurorul va avea o largă apreciere cu privire la caracterul determinant al *facilitării* tragerii la răspundere penală a altor persoane. În cazul în care se va reține această cauză de reducere a pedepsei, beneficiul va consta în reducerea la jumătate a limitelor pedepsei prevăzute de lege pentru fapta săvârșită și care intră în competența D.N.A.

În cazul infracțiunii de constituirea unui grup infracțional organizat, reglementată de art. 367 C.pen., se prevede o cauză de nepedepsire și o cauză de reducere a pedepsei. Cauza de nepedepsire de la art. 367 alin. (4) C.pen. presupune ca un membru al grupului să denunțe existența acestuia către organul de urmărire penală mai „*înainte ca acesta să fi fost descoperit* și *mai înainte ca acesta să fi început săvârșirea infracțiunilor care intră în scopul grupului*". Cauza de nepedepsire nu are aptitudinea de a motiva un colaborator raportat la faptul că acesta trebuie

[1] O.U.G. nr. 43 din 4 aprilie 2002 (M. Of. nr. 244 din 11 aprilie 2002).

[2] Competența D.N.A. este stabilită prin dispozițiile art. 13 din O.U.G. nr. 43/2002.

numai să denunțe existența grupului, astfel că nu va mai fi motivat să își continue activitatea în cadrul acestuia în această calitate. În schimb, este mai lesne de motivat un colaborator prin promisiunea reținerii cauzei de reducere a pedepsei prevăzută de art. 367 alin. (5) C.pen. Se vor reduce la jumătate limitele speciale ale pedepsei infracțiunii dacă o persoană, care este membru al grupului și a săvârșit una dintre faptele scop, *înlesnește aflarea adevărului și tragerea la răspundere penală* a unuia sau mai multor membri ai unui grup infracțional organizat.

Asemănător situației infracțiunilor a căror cercetare este dată în competența D.N.A., și în cazul infracțiunilor pentru care este competentă D.I.I.C.O.T., este reglementată o cauză de reducere a pedepsei. În cuprinsul art. 18 din Legea nr. 508 din 17 noiembrie 2004[1] se arată că persoana care a comis o infracțiune atribuită în competența D.I.I.C.O.T., iar în cursul urmăririi penale, denunță și facilitează identificarea și tragerea la răspundere penală a altor *participanți* la săvârșirea infracțiunii, beneficiază de reducerea la jumătate a limitelor pedepsei prevăzute de lege. Spre deosebire de cauza de reducere a pedepsei reglementate prin art. 19 din O.U.G. nr. 43/2002, aplicabilitatea este restrânsă numai la infracțiunea de care este acuzată persoana, ca urmare a folosirii termenului de „participanți".

O altă cauză de reducere a pedepsei este prevăzută de art. 411 C.pen. în cazul săvârșirii unei infracțiuni contra securității naționale, prin care persoana care a săvârșit o asemenea faptă va beneficia de reducerea limitelor speciale ale pedepsei la jumătate dacă, în cursul urmăririi penale, va înlesni aflarea adevărului și tragerea la răspundere penală a autorului sau a participanților la acea faptă.

Un domeniu în care sunt des întâlnite situații de utilizare a colaboratorilor este cel al prevenirii și combaterii traficului și consumului ilicit de droguri. În cazul infracțiunilor incriminate prin Legea nr. 143 din 26 iulie 2000 privind prevenirea și combaterea traficului și consumului ilicit de droguri, republicată[2], va fi aplicabilă o cauză de nepedepsire ori o cauză de reducere a pedepsei.

În cazul săvârșirii infracțiunilor prevăzute de art. 2-9 din Legea nr. 143/2000, infractorul va beneficia de impunitate dacă, mai înainte de a fi începută urmărirea penală, denunță participarea sa la comiterea infracțiunii, contribuind astfel la identificarea și tragerea la răspundere penală a autorului sau a celorlalți participanți. În mod asemănător infracțiunilor de corupție la care am făcut referire mai sus, cauza de nepedepsire presupune denunțarea propriei fapte și nu are în vedere ca făptuitorul să contribuie în plus la tragerea la răspundere penală a celorlalte persoane care au participat la săvârșirea infracțiunii. În realitate, reținerea acestei cauze de nepedepsire va presupune ca viitorul colaborator să probeze implicarea altor persoane în fapta proprie, de regulă, prin dovedirea caracterului continuat al infracțiunii, prin relevarea actelor de executare subsecvente denunțării. Condiția aplicării acestei cauze de nepedepsire este inexistența unei sesizări penale cu privire la fapta proprie a viitorului colaborator. În situația în care există deja o sesizare cu privire la fapta sa, se va putea aplica o cauză de reducere a pedepsei, care, potrivit art. 15 din Legea nr. 143/2000, republicată, va atrage reducerea cu o jumătate a limitelor de pedeapsă prevăzute de lege pentru infracțiunile în legătură cu droguri săvârșite. Pentru a beneficia de această cauză de reducere a pedepsei, este necesar ca persoana să denunțe și să

[1] Legea nr. 508 din 17 noiembrie 2004 privind înființarea, organizarea și funcționarea în cadrul Ministerului Public a Direcției de Investigare a Infracțiunilor de Criminalitate Organizată și Terorism (republicată în M. Of. nr. 98 din 7 februarie 2014).

[2] Legea nr. 143 din 26 iulie 2000 privind prevenirea și combaterea traficului și consumului ilicit de droguri, republicată (publicată în M. Of. nr. 362 din 3 august 2000 și republicată în M. Of. nr. 163 din 6 martie 2014).

faciliteze tragerea la răspundere penală a altor persoane care au săvârșit infracțiuni (inclusiv alte infracțiuni) legate de droguri.

Legea nr. 682/2002 privind protecția martorilor, republicată[1], include o cauză legală de reducere a pedepsei în cuprinsul art. 19, aplicabilă martorilor „*în sensul dispozițiilor legii speciale*". Astfel, potrivit art. 2 lit. a) din lege, nu va fi necesar ca persoana să aibă calitatea de martor în cursul procesului penal, ci doar cea de martor în sensul legii, dispozițiile legale răsfrângându-se și în beneficiul colaboratorilor și informatorilor. Pentru a opera, este necesar ca martorul să denunțe și să faciliteze tragerea la răspundere penală a altor persoane care au săvârșit infracțiuni de aceeași natură ca a sa. În privința fazei procesului penal în care martorul poate acționa în vederea beneficierii de cauza de reducere a pedepsei, textul de lege arată că denunțarea și facilitarea tragerii la răspundere penală poate interveni înainte de sesizarea organelor de urmărire penală, în cursul urmăririi penale sau în timpul judecății. Fazele procesuale se vor referi la cercetarea și judecarea faptelor martorului, și nu ale persoanelor față de care se formulează denunțul. Cauza legală de reducere a pedepsei are un caracter mai larg decât cele arătate anterior, fiind aplicabilă persoanelor care au săvârșit o infracțiune gravă. Cu toate că textul de lege prevede condiția că infracțiunea săvârșită trebuie să fie una gravă, Curtea Constituțională a apreciat că această prevedere este neconstituțională, fiind discriminatorie, deoarece nu ar permite aplicarea cauzei de reducere a pedepsei în cazul în care martorul nu a săvârșit o infracțiune gravă[2].

2.2. Banii ca motivație a colaboratorilor și informatorilor

Fiind des întâlnită în cazul colaboratorilor și informatorilor folosiți de organele de urmărire penală din S.U.A., această motivație nu este larg răspândită în sistemul român, având în vedere că nu există un cadru legal care să permită plata colaboratorilor și a informatorilor, cu o singură excepție.

În legislație se poate întâlni un singur caz în care sunt alocate fonduri din bugetul de stat care ar putea fi folosite pentru plata colaboratorilor și informatorilor, însă el este limitat la cauzele instrumentate de D.I.I.C.O.T. Conform art. 1 alin. (6) din Legea nr. 508/2004 privind înființarea, organizarea și funcționarea în cadrul Ministerului Public a Direcției de Investigare a Infracțiunilor de Criminalitate Organizată și Terorism, abrogată în prezent: „*Anual se constituie un depozit în valoare* ***de 1.000.000 lei*** *pentru acțiuni privind organizarea și constatarea infracțiunilor flagrante sau* ***ocazionate de folosirea investigatorilor sub acoperire, a informatorilor ori colaboratorilor acestora****, la dispoziția procurorului-șef al Direcției de Investigare a Infracțiunilor de Criminalitate Organizată și Terorism, iar modul său de gestionare și de utilizare se va stabili prin ordin al procurorului-șef al acestei direcții*" (s.n.). Prin „cheltuieli ocazionate de folosirea investigatorilor sub acoperire, a informatorilor și colaboratorilor" vom înțelege, în special, cheltuieli pe care le suportă Ministerul Public pentru a conferi credibilitate acestora în fața membrilor grupurilor pe care le infiltrează ori pentru a se asigura sprijinul logistic în desfășurarea măsurilor de cercetare (închirierea unui imobil pentru a servi drept domiciliu pentru colaborator). Un exemplu concret constă în participarea la anumite activități prin care un colaborator achiziționează o cantitate de droguri de la o persoană, folosindu-se de banii primiți de la ofițerul de legătură în vederea realizării acestei tranzacții.

[1] Republicată în M. Of. nr. 288 din 18 aprilie 2014.

[2] CCR, Dec. nr. 67 din 26 februarie 2015 (M. Of. nr. 185 din 18 martie 2015).

Alături de aceste utilizări, textul de lege permite plata din aceste fonduri a colaboratorilor și informatorilor cu titlu de retribuție pentru serviciile prestate în sprijinul organelor de urmărire penală, având în vedere că puține persoane ar fi dispuse să se pună în primejdie, fără a fi asigurate că vor primi o remunerație substanțială[1]. Problema reală nu este plata unor sume de bani, ci condiționarea primirii sumelor de bani de obținerea unor rezultate[2], precum confiscarea unor cantități de droguri, tragerea la răspundere penală a anumitor persoane, descoperirea săvârșirii unor noi infracțiuni etc. În condițiile în care organele de urmărire penală ar recunoaște motivația colaboratorului ca fiind una patrimonială și ar specifica-o, această împrejurare ar contribui la stabilirea valorii probante a declarației acestuia. De exemplu, dacă sumele de bani oferite erau semnificative și condiționate de obținerea unor rezultate, este pus în discuție caracterul real al celor declarate, deoarece colaboratorul are un interes patrimonial în sancționarea unui inculpat, în special dacă sumele de bani nu sunt plătite decât după soluționarea cauzei.

Informatorii și colaboratorii, dacă sunt plătiți în funcție de rezultatele pe care le obțin și dacă aceste rezultate se cuantifică în numărul de persoane arestate ori trimise în judecată, pot deveni cel mai repede subordonați ai organelor de urmărire penală. Ei devin „colaboratori de serviciu" (situație similară denunțătorului de serviciu) și vor fi interesați financiar să contribuie la soluționarea cât mai multor cauze.

În opinia noastră, informatorii și colaboratorii sunt esențiali pentru cercetarea anumitor infracțiuni, astfel că se impune ca aceștia să fie recompensați într-un mod legal pentru serviciile lor. Referitor la informatori, este obligatoriu ca aceștia să fie plătiți în mod regulat, dar numai în măsura în care informațiile oferite de-a lungul timpului au fost reale și au contribuit la soluționarea unor cauze.

2.3. Frica

Un motiv substanțial pentru ca o persoană cu un trecut infracțional sau care întreprinde activități de natură infracțională să devină un colaborator sau informator este frica pe care o resimte față de mai multe situații ori persoane. Starea aceasta o poate determina să renunțe la legăturile avute anterior cu membrii unui grup infracțional și, pentru a-și căuta siguranța, să ajute organele de urmărire penală la cercetarea acestora.

Frica poate avea mai multe cauze[3]:

- frica de a fi arestat;
- frica de a fi condamnat la o pedeapsă privativă de libertate;
- frica de stigmatul social ce decurge din arestarea sau condamnarea unei persoane;
- frica de răzbunări din partea altor făptuitori;
- frica separării de familie;
- frica arestării unui membru de familie.

Aceste motive pot contribui semnificativ și la recrutarea persoanei, în condițiile în care cea mai mare parte dintre situațiile arătate mai sus poate fi evitată prin includerea persoanei

[1] U.S. Court of Appeals, Fifth Circuit, cauza *United States of America c. Cervantes-Pacheco,* 826 F.2d 310, dec. din 21 august 1987, par. 29, pe *openjurist.org*

[2] U.S. Court of Appeals, Eleventh Circuit, cauza *United States c. Edenfield*, 995 F.2d 197, dec. din 14 iulie 1993, par. 3, pe *www.leagle.com*

[3] *Gr.D. Lee,* Drug Informants: Motives, Methods, and Management, în FBI Law Enforcement Bulletin, 1 septembrie 1993, pe *www.thefreelibrary.com*

într-un program de protecție a martorilor, potrivit Legii nr. 682/2002, republicată. O persoană care contribuie în baza acestui motiv va trebui crezută mai degrabă decât o persoană care va avea un interes patrimonial, însă nu va putea fi privită ca un martor obiectiv, având în vedere că însăși o traumă psihologică a determinat-o să colaboreze cu organele de urmărire penală.

2.4. Răzbunarea

Alături de frică, un alt motiv psihologic care determină un informator sau colaborator să acționeze în sprijinul organelor de urmărire penală este răzbunarea față de o persoană din cadrul grupului infracțional care face obiectul unei urmăriri penale. O atare motivație o poate avea și persoana care face parte dintr-o grupare infracțională rivală, iar furnizarea unor informații către organele de urmărire penală este determinată de dorința ca membrii acelui grup să fie trași la răspundere penală, nu din motive altruiste, ci pentru ca grupul al cărui membru este să culeagă beneficiile din eliminarea unui rival. O astfel de situație poate fi întâlnită în cazul infracțiunilor prevăzute de Legea nr. 143/2000 privind combaterea traficului și consumului ilicit de droguri, republicată.

Dorința de răzbunare poate fi generată și de rivalități la locul de muncă ori de despărțirea de un partener sentimental, de nemulțumirile unui angajat sau chiar de către un creditor nemulțumit de neplata creanțelor sale (de pildă, în cazul unor infracțiuni de evaziune fiscală).

2.5. Remușcările ca factor motivant

Un motiv real ori aparent pentru ca o persoană să devină un colaborator sau informator al organelor de urmărire penală îl poate reprezenta o stare emoțională cauzată de remușcări față de faptele de natură penală comise în trecut. Acest motiv poate fi unul aparent și poate ascunde, de fapt, dorința unei persoane de a beneficia de o cauză de reducere a pedepsei și de un tratament sancționator atenuat[1] (mai ales în privința individualizării executării pedepsei).

Alte persoane sunt sincere în abordare și văd în colaborarea cu organele de urmărire penală o modalitate de a începe o viață nouă și de a se îndrepta ca persoană. Nu este exclus ca un individ să invoce motive spirituale sau religioase pentru schimbarea de atitudine.

În orice situație, va fi obligatoriu ca organul judiciar să afle motivația reală a persoanei, pentru a nu permite, în realitate, o răzbunare împotriva unor persoane cercetate penal și nici reținerea unor cauze de atenuare pentru oferirea unor informații sau chiar declarații care să conțină elemente închipuite de către colaborator sau informator.

2.6. Altruismul

Un motiv care poate fi invocat de către un colaborator sau informator este altruismul, adică grija pe care o poartă față de o persoană anume care acționează în cadrul unui grup infracțional organizat și pe care o dorește protejată. De pildă, un colaborator va fi determinat de altruism dacă va dori să își protejeze o rudă de un comportament distructiv, precum dependența de droguri, prin ajutarea organelor de urmărire penală să tragă la răspundere penală persoanele care îi furnizează aceste substanțe. În atare situații, considerăm că se impune o evaluare atentă a motivației, deoarece este posibil să existe și alte motive incidente de natură mai puțin nobilă.

[1] *D.G. Fitzgerald*, op. cit., p. 52.

2.7. Colaboratorii și informatorii motivați de ego-ul personal

În această categorie intră persoane care sunt determinate să activeze în calitate de informatori sau colaboratori datorită particularităților psihice și a unor țeluri ale vieții pe care nu și le-au putut îndeplini. De regulă, aceste persoane pot fi profesioniști în domeniul lor, precum piloți, antreprenori, foști militari activi și alte asemenea persoane[1].

O situație similară poate apărea în cazul persoanelor care și-au dorit să activeze în domeniul ordinii publice, dar nu au fost admiși din diverse cauze la examenele de admitere în profesii, precum cea de magistrat sau polițist. În alte cazuri, colaboratorii și informatorii consideră că își pot trăi visele neîmplinite, văzând în activitatea lor o aventură, ei fiind denumiți de organele de urmărire penală din S.U.A. drept persoane suferinde de „sindromul James Bond"[2].

2.8. Colaboratorii și informatorii motivați de simțul civic

Cea mai puțin credibilă categorie de colaboratori și informatori o reprezintă cei care invocă în fața unui organ judiciar că doresc să ajute organele de urmărire penală, întrucât au în vedere binele societății. Deși este un deziderat ca fiecare cetățean să gândească în acest mod, în realitate, o atare motivație trebuie privită cu foarte multă circumspecție, deoarece ascunde un alt adevăr: colaboratorul sau informatorul are motive reale pe care nu dorește să le dezvăluie. Persoanele care sunt dispuse să își pună viața în primejdie doar pentru binele societății și fără niciun beneficiu ulterior sunt rarități. În vederea aflării dacă o astfel de persoană este într-adevăr motivată de simțul civic, se impune în mod obligatoriu verificarea antecedentelor penale ale acestei persoane.

[1] *Ibidem*, p. 56.
[2] *Ibidem*, p. 53.

Capitolul VI
Măsurile de protecție a investigatorilor sub acoperire, a colaboratorilor și informatorilor

Activitatea investigatorilor sub acoperire și a colaboratorilor nu poate fi concepută fără a li se asigura protecția față de potențiale răzbunări pentru ajutorul dat justiției. Spre a li se asigura siguranța și pentru a-i motiva să realizeze operațiunile specifice, acestor persoane li se asigură o protecție legală prevăzută în cuprinsul dispozițiilor Codului de procedură penală și în legislația specială.

Regimul aplicării măsurilor de protecție se regăsește în cuprinsul art. 149 C.pr.pen., în care se detaliază două categorii de măsuri: *protejarea identității conspirative* și *aplicarea facultativă a măsurilor specifice de protecție a martorilor*. La acestea vom adăuga și măsurile de protecție ce se vor aplica în mod obligatoriu în situația audierii investigatorului sub acoperire și a colaboratorului[1].

Cea mai importantă măsură de protecție este interdicția absolută de a se dezvălui identitatea investigatorilor sub acoperire și a colaboratorilor de către persoanele care au ajuns să cunoască aceste împrejurări ca urmare a atribuțiilor lor de serviciu. Măsura de cercetare implică un cerc restrâns de persoane care cunosc identitatea reală a acestora, ele fiind procurorul și ofițerul de poliție care păstrează legătura cu investigatorul sub acoperire sau colaboratorul. În cazul procurorului, situația se explică, deoarece acesta este cel care dispune autorizarea măsurii, astfel că este necesar ca acesta să cunoască atât identitatea reală, cât și identitatea conspirativă. Mai mult, dispozițiile art. 149 alin. (2) C.pr.pen. sunt incidente și în cazul procurorului care participă la audierea investigatorului sub acoperire prin folosirea mijloacelor de comunicare la distanță cu distorsionarea vocii și imaginii.

Deoarece apropierea investigatorului sau a colaboratorului de sediul organelor de poliție sau de sediul parchetului ar atrage suspiciuni și ar periclita operațiunea, comunicarea cu organele de urmărire penală se va realiza prin intermediul unui ofițer de poliție de legătură, care va prelua datele și informațiile obținute și îi va transmite instrucțiuni și noi însărcinări ori îi va furniza tehnica operativă pentru realizarea supravegherii tehnice.

Alături de persoanele arătate mai sus, este permisă cunoașterea identității de către judecătorul de drepturi și libertăți, de către judecătorul de cameră preliminară și de către instanța de judecată. Cu toate că le este permisă cunoașterea identității reale, suntem de părere că nu se va impune ca aceste organe să procedeze la aflarea acesteia decât în măsura în care există temeiuri care să impună în cursul unei proceduri aceste verificări.

Informațiile privind identitatea adevărată a investigatorilor și colaboratorilor sunt secrete de serviciu și sunt protejate împotriva dezvăluirii lor prin intermediul incriminării unei asemenea acțiuni în cuprinsul art. 304 C.pen., unde este prevăzută o formă agravată, în ipoteza în care, ca urmare a divulgării identității reale, s-a comis o infracțiune împotriva investigatorului sub acoperire, a martorului protejat sau a persoanei incluse în programul de protecție a martorilor[2]. Observăm că, în cazul formei agravate, nu se consideră că infracțiunea

[1] *V. infra*, Titlul XII, Capitolul IV.2.

[2] Potrivit art. 304 C.pen., constituie infracțiune:

„(1) Divulgarea, fără drept, a unor informații secrete de serviciu sau care nu sunt destinate publicității, de către cel care le cunoaște datorită atribuțiilor de serviciu, dacă prin aceasta sunt afectate interesele sau activitatea unei persoane, se pedepsește cu închisoare de la 3 luni la 3 ani sau cu amendă. (...)

de divulgarea informațiilor secrete de serviciu ar avea un caracter mai grav în situația în care s-a săvârșit o infracțiune împotriva unui *colaborator*, fiind o evidentă lacună a legiuitorului, care se impune a fi completată prin modificarea dispozițiilor art. 304 alin. (3) C.pen.

Alături de protejarea identității reale a investigatorilor și colaboratorilor, Codul de procedură penală prevede posibilitatea ca aceștia, membrii familiilor acestora și alte persoane supuse amenințărilor să beneficieze de măsurile de protecție a martorilor prevăzute de lege. Aceste măsuri de protecție au caracter facultativ, deoarece, de regulă, însăși păstrarea secretului identității reale este suficientă pentru a preveni orice acțiune infracțională de răzbunare sau intimidare. Din păcate, considerăm că se va impune cu precădere utilizarea acestor măsuri de protecție în situația în care se procedează la folosirea unui colaborator cu identitate reală, situație în care persoanele cercetate vor cunoaște identitatea celui care a ajutat organele de urmărire penală.

În sfera persoanelor care pot beneficia de măsuri de protecție sunt incluse, în primul rând, înseși persoanele care au legătură cu cercetarea cauzei: investigatorii sub acoperire, colaboratorii și informatorii, protejarea lor fiind necesară în vederea prevenirii potențialelor răzbunări cauzate de ajutorul adus justiției, pentru a se preveni împiedicarea obținerii declarației lor or pentru a asigura continuarea carierei lor profesionale (în cazul investigatorilor).

Ar fi fost insuficient a se asigura măsuri de protecție acestor persoane dacă nu vor fi protejate persoanele apropiate lor de acte infracționale îndreptate împotriva acestora. În condițiile în care un investigator sau colaborator ar beneficia de o măsură de protecție, persoanele vizate de cercetare și care ar reuși să afle identitatea adevărată a acestora ar putea exercita acte de răzbunare împotriva unor persoane apropiate ori acte de intimidare în vederea păstrării tăcerii cu privire la aspectele descoperite. Este mai periculos un asemenea tip de comportament, deoarece se îndreaptă împotriva unor persoane care nu au contribuit în niciun mod la desfășurarea procesului penal, fiind victime colaterale.

Potrivit art. 149 alin. (3) C.pr.pen., pot beneficia de măsurile de protecție și *membrii de familie* ai investigatorului sub acoperire, colaboratorului ori informatorului, precum și *alte persoane supuse intimidărilor sau actelor de violență în legătură cu activitatea de cercetare desfășurată*. Reglementarea măsurilor de protecție de care aceste persoane pot beneficia nu se regăsește în cuprinsul Codului de procedură, ci în Legea nr. 682/2002 privind protecția martorilor, republicată[1].

Prin „membrii de familie" vom înțelege acele persoane considerate ca atare de legislația specială privind protecția martorilor[2], și nu persoanele care fac parte din membrii de familie, în conformitate cu dispozițiile Codului penal[3]. Considerăm că se impunea, pentru evitarea

(3) Dacă, urmare a faptei prevăzute în alin. (1) și alin. (2) s-a săvârșit o infracțiune împotriva investigatorului sub acoperire, a martorului protejat sau a persoanei incluse în Programul de protecție a martorilor, pedeapsa este închisoarea de la 2 la 7 ani, iar dacă s-a comis cu intenție o infracțiune contra vieții, pedeapsa este închisoarea de la 5 la 12 ani".

[1] Legea nr. 682 din 19 decembrie 2002 privind protecția martorilor (republicată în M. Of. nr. 288 din 18 aprilie 2014).

[2] Potrivit art. 2 lit. d) din Legea nr. 682/2002, republicată: „membrii de familie ai martorului protejat sunt soțul sau soția, părinții și copiii acestuia".

[3] Potrivit alin. (1) al art. 177 C.pen., „Prin «membru de familie» se înțelege:

a) ascendenții și descendenții, frații și surorile, copiii acestora, precum și persoanele devenite prin adopție, potrivit legii, astfel de rude;

b) soțul;

c) persoanele care au stabilit relații asemănătoare acelora dintre soți sau dintre părinți și copii, în cazul în care conviețuiesc".

oricărei confuzii, lărgirea sensului noțiunii de „membru de familie" în legislația specială, în condițiile în care scopul întregii reglementări este acoperirea unui număr cât mai mare de situații care se pot regăsi în practică. Această necorelare este dăunătoare, deoarece, din perspectiva Codului penal, fratele și sora sunt membri de familie, însă, din perspectiva Legii privind protecția martorilor, aceștia au calitatea de *persoane apropiate martorilor protejați*.

În același timp, în cuprinsul Codului de procedură penală, legiuitorul a extins posibilitatea de protejare către un număr nedeterminat de persoane prin includerea unei categorii reziduale, denumită „alte persoane supuse amenințărilor, intimidărilor sau actelor de violență". Deoarece relațiile de familie și, în general, relațiile interumane prezintă un grad mare de complexitate, s-a dorit evitarea oricărei posibilități reale de a se realiza intimidări ori răzbunări indirecte împotriva persoanelor care și-au dat concursul pentru buna înfăptuire a justiției. Aceasta nu explică de ce în cuprinsul Codului de procedură penală se vorbește despre categoria arătată, iar în legislația specială se folosește noțiunea de „persoane apropiate martorului protejat"[1].

În categoria arătată vor intra acele persoane cu care investigatorul, colaboratorul sau informatorul are o relație apropiată și care este supusă amenințărilor, intimidărilor sau actelor de violență. Spre deosebire de situația membrilor de familie, față de care este necesară existența unei suspiciuni că se vor exercita acte de intimidare, amenințare sau răzbunare, în cazul altor persoane, este necesară existența unui singur act concret care să indice că au fost exercitate asemenea acte și că vor continua în viitor. Formularea folosită de legiuitor intră în contradicție cu cea din Legea nr. 682/2002, republicată, în care se arată în mod expres faptul că persoana care beneficiază de măsurile de protecție trebuie să se afle într-o *stare de pericol*. Prin „stare de pericol", legea definește situația în care se află martorul (inclusiv investigatorul sub acoperire și colaboratorul), membrii familiei sale ori persoane apropiate acestuia, a căror viață, integritate corporală sau libertate este amenințată, ca urmare a datelor și informațiilor furnizate ori pe care a fost de acord să le furnizeze organelor judiciare sau a declarațiilor sale.

Pentru realizarea activităților necesare protejării persoanelor arătate mai sus, precum și a celor care au calitatea de martor protejat, potrivit Legii nr. 682/2002, republicată, în cadrul Ministerului Afacerilor Interne și în subordinea Inspectoratului General al Poliției Române s-a creat Oficiul Național pentru Protecția Martorilor. Prin această instituție sunt desfășurate toate programele individuale de protecție a martorilor.

Pentru ca un investigator, colaborator, informator ori membrii familiei sale, precum orice persoană apropiată acestuia să beneficieze de un program de protecție, este necesar să aibă calitatea prevăzută de Legea nr. 682/2002, republicată, să se afle într-o stare de pericol și să existe o propunere în acest sens din partea organelor abilitate. În cursul urmăririi penale, organul de cercetare penală poate solicita procurorului includerea unei persoane în Program, în cursul procedurii în camera preliminară și în timpul judecății, procurorul putând formula o cerere de acest fel în fața judecătorului de cameră preliminară, respectiv instanței. Prin ordonanță sau, după caz, încheiere, organele mai sus menționate se vor pronunța în termen de 5 zile cu privire la propunerea de includere în Programul de protecție a martorilor, iar, în caz de admitere, actul emis se va transmite O.N.P.M. Ulterior, O.N.P.M. va încheia în scris un protocol de protecție cu fiecare persoană care beneficiază de măsuri de protecție, numai la momentul semnării considerându-se că o persoană face parte din Program.

[1] Potrivit art. 2 lit. e) din Legea nr. 682/2002, republicată, „persoana apropiată martorului protejat este persoana de care respectivul martor este legat prin puternice legături afective".

În cuprinsul Protocolului de protecție sunt incluse obligațiile părților, între care cele mai importante sunt cele ale O.N.P.M. În schimbul protecției, martorul protejat are anumite obligații, iar neîndeplinirea acestora va duce la încetarea protecției de care beneficiază. Așa cum am arătat într-o secțiune precedentă, includerea în Programul de protecție a martorilor constituie o modalitate de a asigura cooperarea persoanei protejate, în condițiile în care frica de eventuale răzbunări din partea persoanelor împotriva cărora operează o determină să ajute organele de urmărire penală. Mai mult, cooperarea continuă a acestora în cursul urmăririi penale este asigurată de posibilitatea procurorului de a sista Programul de protecție prin ordonanță[1].

Potrivit art. 11 din Legea nr. 682/2002, republicată, principalele obligații ale martorilor protejați constau în: furnizarea de informații și date cu caracter determinant în aflarea adevărului, respectarea măsurilor stabilite în schema de sprijin a protocolului, abținerea de la orice activitate care i-ar putea pune în pericol sau care ar putea periclita punerea în aplicare a Programului, evitarea contactului cu persoane cunoscute sau cu persoane din medii infracționale, informarea imediată a O.N.P.M. cu privire la orice schimbare în viața personală și în activitățile pe care le desfășoară ori dacă a intrat în contact involuntar cu o persoană cunoscută sau care face parte din medii infracționale.

În schimb, pentru a proteja persoana, O.N.P.M. poate lua mai multe *măsuri de protecție* sau *măsuri de asistență*. Cu toate că dispozițiile art. 149 alin. (3) C.pr.pen. vorbesc numai de măsuri de protecție, considerăm că legiuitorul a vrut să asigure persoanelor amintite și măsurile de asistență de care pot beneficia martorii protejați în baza Legii nr. 682/2002, republicată.

Măsurile de protecție de care pot beneficia martorii protejați sunt:

a) protecția datelor de identitate a martorului protejat;

b) protecția declarației acestuia (potrivit modalității specifice de audiere[2]);

c) ascultarea martorului protejat de către organele judiciare, sub o altă identitate decât cea reală sau prin modalități speciale de distorsionare a imaginii și a vocii;

d) protecția martorului aflat în stare de reținere, arestare preventivă sau în executarea unei pedepse privative de libertate, în colaborare cu organele care administrează locurile de deținere;

e) măsuri sporite de siguranță la domiciliu, precum și de protejare a deplasării martorului la și de la organele judiciare;

f) schimbarea domiciliului;

g) schimbarea identității;

h) schimbarea înfățișării.

Așa cum rezultă din dispozițiile legale, se pune accentul pe asigurarea elementelor de bază care definesc o persoană în societate, în principal identitatea, înfățișarea și domiciliul, toate acestea putând fi cunoscute, chiar și fragmentat, de către persoane interesate de acțiuni împotriva martorului protejat. Alături de acestea, există și măsuri accesorii care tind să îmbunătățească siguranța persoanei, precum condițiile de siguranță la domiciliu – asigurarea mai bună a punctelor de acces, instalarea unui sistem de alarmă, de supraveghere video etc., ori să asigure anonimitatea persoanei în deplasările la organele judiciare – folosirea unor mașini cu geamuri fumurii, deplasarea într-o mașină conspirativă, utilizarea unor intrări interzise publicului, aducerea persoanei la sediu la ore târzii din noapte etc. Măsurile de protecție

[1] Potrivit art. 17 alin. (2) din Legea nr. 682/2002, republicată, „încetarea programului se dispune de procuror prin ordonanță sau de către instanță prin încheiere".

[2] *V. infra*, Titlul XII, Capitolul IV.2.

enumerate se vor acorda în funcție de particularitățile fiecărei situații, ele putând fi cumulate pe durata Programului de protecție. În realizarea Programului, persoana protejată va ține legătura cu O.N.P.M. în mod conspirativ, printr-o persoană de legătură anume desemnată, iar, în situațiile în care aceasta consideră că persoana de legătură a fost deconspirată, va exista întotdeauna o altă persoană nominalizată în Protocolul de protecție pe care o va putea contacta în locul aceleia. Sub nicio formă persoana protejată nu trebuie să aibă contact direct sau să se prezinte la sediul O.N.P.M.

Pe lângă măsurile de protecție, persoana protejată va putea să beneficieze și de anumite *măsuri de asistență*, ce vor putea fi prevăzute în schema de sprijin a Programului de protecție:

a) reinserția în alt mediu social;

b) schimbarea sau asigurarea locului de muncă;

c) asigurarea unui venit până la găsirea unui loc de muncă.

Aceste măsuri nu contribuie la protejarea efectivă a persoanei, dar îi asigură posibilitatea realizării unor sume de bani pentru a-și asigura traiul, posibilitatea de a avea interacțiuni cu alte persoane din societate, străine de persoanele cu care a luat contact până la acel moment. Până la finalizarea Programului de protecție, scopul acestuia este să realizeze o dispariție din societate a persoanei și reintegrarea sa în mod conspirativ într-un alt mediu, necunoscut pentru persoanele care ar putea să o pună în pericol.

O chestiune importantă o constituie termenul în care se poate desfășura un Program de protecție și care sunt situațiile în care acesta poate înceta. Legea specială nu indică un termen maxim pentru care o persoană poate să beneficieze de măsurile de protecție, ele fiind impuse de starea de pericol în care se află persoana și vor dura până ce această stare de pericol încetează.

În cuprinsul legii sunt indicate mai multe situații în care programul încetează:

a) la cererea martorului protejat, exprimată în formă scrisă și transmisă către O.N.P.M.;

b) dacă în cursul procesului penal martorul protejat depune mărturie mincinoasă;

c) dacă martorul protejat comite cu intenție o infracțiune;

d) dacă sunt probe sau indicii temeinice că, ulterior includerii în Program, martorul protejat a aderat la un grup sau organizație criminală;

e) dacă martorul protejat nu respectă obligațiile asumate prin semnarea Protocolului de protecție sau dacă a comunicat date false cu privire la orice aspect al situației sale;

f) dacă viața, integritatea corporală sau libertatea martorului protejat nu mai este amenințată;

g) dacă martorul protejat decedează.

Organul competent să se pronunțe asupra încetării măsurilor de protecție este procurorul, în cursul urmăririi penale, sau instanța, în cursul judecății. Observăm că art. 17 alin. (2) din Legea 682/2002, republicată, nu include posibilitatea încetării programului în procedura camerei preliminare, având în vedere că această fază a procesului penal nu ar trebui să dureze mai mult de 60 de zile. În practică, în condițiile în care faza procesuală în discuție poate dura peste un an, în funcție de complexitatea cauzei, se impune completarea textului de lege, dându-se posibilitatea judecătorului de cameră preliminară să dispună încetarea Programului.

Cea mai mare parte dintre situațiile în care Programul încetează nu necesită explicații suplimentare, însă ne vom referi succint la încetarea Programului, în cazul în care persoana aderă la un grup infracțional sau nu se mai află într-o stare de pericol. În contextul în care toate situațiile de încetare în cursul urmăririi penale sunt la latitudinea procurorului, suntem de părere că cele două situații amintite îi pot permite acestuia să se folosească de ele ca mijloc de motivare (sau constrângere) a activității prestate de colaborator sau informator.

Situația aderării la un grup sau la o organizație criminală este deficitară în cazul colaboratorului, care, prin natura sa, poate fi parte a unei organizații criminale, astfel că Programul de protecție va înceta numai dacă procurorul va constata că activitatea colaboratorului se desfășoară contrar intereselor administrării justiției, urmărindu-se protejarea grupului infracțional. Acest temei motivează colaboratorul să realizeze operațiunile sale într-o relație de deplină subordonare față de organul de urmărire penală, știind că siguranța sa și a familiei sale depinde de convingerea procurorului că acesta urmărește în continuare interesele justiției.

Cel de-al doilea caz de încetare a Programului, care prezintă probleme, este reprezentat de dispariția stării de pericol pentru viața, integritatea corporală sau libertatea colaboratorului, care se va aprecia de procuror, în cursul urmăririi penale, și de instanță, în cursul judecății. Un temei cert pentru dispariția unei asemenea stări de pericol îl poate reprezenta condamnarea definitivă a persoanelor care au făcut obiectul procesului penal în care investigatorul sau colaboratorul a acționat. În afara acestei situații, trebuie să existe indicii că identitatea persoanei nu este cunoscută de persoanele care fac obiectul procesului penal și că aceasta deja a fost audiată în cauză. Suntem de părere că măsurile de protecție menționate trebuie menținute în perioada în care se întrebuințează măsura specială de cercetare a utilizării investigatorilor sub acoperire și a colaboratorilor. Totodată, pentru buna înfăptuire a justiției, este necesar ca măsura să fie menținută și după, până în momentul în care persoana va fi audiată de organele de urmărire penală, putându-se obține probe derivate din măsura de cercetare folosită.

Capitolul VII
Concluzii

Utilizarea investigatorilor sub acoperire și a colaboratorilor constituie o măsură de cercetare care încă se află într-un stadiu incipient de dezvoltare și de reglementare în sistemul judiciar român. Cu toate că reprezintă o gravă ingerință în viața persoanei vizate de măsură, folosirea ei constituie o necesitate în cazul cercetării unor infracțiuni, precum cele de terorism, de trafic și consum ilicit de droguri și chiar a infracțiunilor de corupție.

Reglementarea măsurii de cercetare poate fi îmbunătățită prin revizuirea modalității de autorizare a acesteia, în sensul trecerii competenței în sarcina judecătorului de drepturi și libertăți, precum și reglementarea unui acord de colaborare pentru persoanele care urmează a fi folosite drept colaboratori. Un asemenea acord ar reprezenta o garanție pentru un proces echitabil, oferind atât apărării, cât și instanței posibilitatea cercetării credibilității colaboratorului prin raportare la motivarea avută de acesta – reținerea unei cauze de nepedepsire, de reducere a pedepsei, oferirea unei remunerații etc. Pentru serviciile prestate de colaboratori, se impune ca aceștia să poată fi plătiți în vederea motivării cât mai multor persoane să colaboreze cu organele de urmărire penală.

Totodată, se impune realizarea unui suport legislativ care să permită organelor de cercetare penală să își dezvolte în mod licit o rețea de informatori, plătiți regulat, pentru a beneficia de date și informații cu privire la orice infracțiune, fără a fi necesară autorizarea unei măsuri speciale de cercetare.

Existența acestei măsuri de cercetare este impusă de necesitatea prevenirii și pedepsirii infracțiunilor grave săvârșite în cadrul grupurilor infracționale. Ca atare, trebuie acceptată ideea existenței acesteia, a importanței datelor și informațiilor pe care le poate furniza și înțelegerea că puterea ei nu stă doar în probarea existenței unei infracțiuni, ci și în ajutorul pe care îl conferă în destructurarea unor grupuri infracționale și în prevenirea săvârșirii de noi infracțiuni.

Titlul XIII
Participarea autorizată la anumite activități

Capitolul I
Aspecte generale

Secțiunea 1. Utilitatea reglementării metodei speciale de cercetare a participării autorizate la anumite activități

Participarea autorizată la anumite activități este o metodă specială de cercetare prevăzută de legiuitor pentru a completa activitatea desfășurată prin utilizarea investigatorilor sub acoperire și a colaboratorilor. Spre deosebire de cea din urmă măsură, în concepția legiuitorului, finalitatea declarată a participării autorizate la anumite activități constă în obținerea unor mijloace de probă cu privire la săvârșirea unei infracțiuni, deși considerăm că obținerea probelor în baza acestei măsuri se va restrânge doar la probele derivate din aceasta, precum audierea persoanei autorizate să participe la aceste activități sau cele rezultate în urma administrării unor metode speciale de supraveghere. Puterea conferită procurorului de a autoriza o astfel de metodă specială de cercetare este deosebit de mare, întrucât implică mai mult decât utilizarea unui investigator sub acoperire sau a unui colaborator, presupunând chiar desfășurarea unei fapte prevăzute de legea penală cu acordul și sprijinul organelor de urmărire penală.

Legătura dintre utilizarea investigatorilor sub acoperire și a colaboratorilor și participarea autorizată la anumite activități este una deosebit de strânsă, în condițiile în care, pentru a se obține infiltrarea unui investigator sub acoperire ori a unui colaborator în cadrul unui grup infracțional organizat, acesta va trebui să creeze aparența aderării la grup și să participe la activitățile ilicite ale acestuia pentru a i se da credibilitate, dar și pentru a cunoaște mai bine modul în care infractorii operează și pentru a putea identifica structura și membrii organizației. Alături de cele două metode speciale de cercetare, amintim și livrarea supravegheată care se va putea folosi concomitent cu cele două măsuri[1].

Denumirea aleasă de legiuitor pentru măsură este criptică, deoarece nu evocă în mod suficient de clar ceea ce înseamnă această metodă de cercetare. Definiția acesteia se regăsește în cuprinsul art. 138 alin. (11) C.pr.pen., în care se arată că prin «participarea autorizată la anumite activități» se va înțelege: „*comiterea unei fapte similare laturii obiective a unei infracțiuni de corupție, efectuarea de tranzacții, operațiuni sau orice fel de înțelegeri privind un bun sau privind o persoană despre care se bănuiește că ar fi dispărută, că este victima traficului de persoane ori a unei răpiri, efectuarea de operațiuni privind droguri, precum și prestarea unui serviciu, desfășurate cu autorizarea organului judiciar competent, în scopul obținerii de mijloace de probă*".

[1] De exemplu, ulterior autorizării folosirii unui investigator sub acoperire, se va autoriza participarea autorizată la anumite activități pentru a permite acestuia să se integreze în grupul infracțional bănuit de trafic de droguri, mai târziu acesta aflând informații cu privire la intrarea în țară a unui transport cu droguri, informațiile obținute putând sta la baza realizării livrării supravegheate.

Cu alte cuvinte, măsura de cercetare constă în săvârșirea unor fapte prevăzute de legea penală, cu autorizarea prealabilă a procurorului, în vederea obținerii de mijloace de probe.

Definiția dată de legiuitor o apreciem ca fiind imprecisă, deoarece expresia „comiterea unei fapte similare laturii obiective a unei infracțiuni de corupție" nu este corectă și poate duce la confuzii. Latura obiectivă a unei infracțiuni constituie o parte a tipicității faptei incriminate, cu alte cuvinte, latura obiectivă este un criteriu în funcție de care se determină dacă o faptă este prevăzută de legea penală (prima trăsătură esențială a infracțiunii). A spune că „sunt autorizate fapte similare laturii obiective a unei infracțiuni" semnifică a admite autorizarea unor fapte care nu vor îndeplini niciodată condiții de tipicitate, deoarece fapta comisă este doar similară, astfel că nu va intra în sfera de aplicare a legii penale. Conform acestei interpretări, existența unei măsuri de cercetare de acest fel s-ar suprapune cu cea a utilizării investigatorilor sub acoperire și a colaboratorilor. De fapt, autorizarea va viza exact o faptă care va întruni elementele constitutive ale unei infracțiuni de corupție, în condițiile în care acest tip de infracțiuni sunt uneori bilaterale, astfel că nu se poate concepe (decât în situația constrângerii venite din partea persoanei mituite) că celălalt participant nu va comite o faptă prevăzută de legea penală. Prevederea în discuție se impune a fi modificată, în condițiile în care răspunderea penală a persoanei autorizate este înlăturată ca urmare a existenței unei cauze justificative, și nu a lipsei de tipicitate a faptei.

Menirea folosirii participării autorizate la anumite activități este de a permite unui agent al statului să observe și să interacționeze cu participanții la săvârșirea unei infracțiuni într-un mod pasiv ori, cel mult, complicitar, în vederea obținerii unor probe. În nicio situație nu se va putea accepta ca fiind legală determinarea unei persoane de a săvârși o infracțiune[1], aceasta constituind o infracțiune provocată de către un agent al statului[2]. Cu toate acestea, persoana autorizată va putea să acționeze în vederea organizării unui flagrant în care să se surprindă fapta urmărită, astfel să se limiteze la o activitate pasivă.

În situația participării autorizate la anumite activități, constând în „*operațiuni sau orice fel de înțelegeri privind un bun sau privind o persoană despre care se bănuiește că ar fi dispărută, că este victima traficului de persoane ori a unei răpiri*", considerăm că legiuitorul a fost neclar în formularea expresiei „operațiuni sau orice fel de înțelegeri privind un bun", întrucât nu se poate determina suficient de clar tipul de infracțiune care ar putea face obiectul măsurii. Totuși, dacă vom compara aceste dispoziții legale cu cele cuprinse în art. 150 alin. (1) lit. a) C.pr.pen., această metodă specială ar putea fi aplicată, în funcție de circumstanțele concrete, atunci când deținerea sau comercializarea bunurilor este reglementată strict de lege, precum în cazul armelor și muniților, materialelor nucleare și explozive, inclusiv precursorilor acestora, falsificării de monedă, timbre sau alte valori (de pildă, se autorizează cumpărarea unor dispozitive pentru falsificare).

În situația în care operațiunile sau înțelegerile privesc o persoană, vom putea folosi metoda în cazul unei infracțiuni de trafic de persoane[3] sau de lipsire de libertate. În ceea ce privește infracțiunea de trafic de persoane, persoana care participă autorizat va putea să „negocieze" o

[1] *M. Bulancea*, în M. Udroiu (coord.), Codul de procedură penală, 2017, p. 454; *Gh. Mateuț*, Procedură penală, 2019, pp. 731-732.

[2] *V. infra*, Titlul XIII, Capitolul V.

[3] Deși textul legal se referă la traficul de persoane, credem că nu va fi incident numai în cazul infracțiunii cu aceeași denumire prevăzută de art. 210 C.pen., ci și în cazul infracțiunii de trafic de minori, prevăzută de art. 211 C.pen.

transferare a persoanei de la infractor către aceasta contra unei sume de bani, în lipsa autorizării metodei speciale, fapta constituind infracțiune[1].

În cazul infracțiunilor privind traficul de droguri, legiuitorul a fost mult mai clar, permițând *orice operațiune* cu privire la aceste substanțe. Considerăm că această măsură de cercetare își regăsește cel mai bine utilitatea în cazul infracțiunilor de acest fel, deoarece folosirea unui investigator sub acoperire, alături de autorizarea unor operațiuni, precum vânzarea de droguri sau deținerea acestora, îi va crește posibilitatea de a se integra în grupul infracțional. Mai mult, în privința acestor tip de fapte, nu este eficient să se urmărească doar prinderea membrilor inferiori ai organizației, ci descoperirea modului în care substanțele interzise ajung în țară ori locul unde sunt produse, sens în care se va putea întrebuința și metoda specială de cercetare a livrării supravegheate. În cazul cercetării unor asemenea infracțiuni, se va impune ca investigatorul să fie integrat într-o operațiune pe termen lung (*deep undercover*), adică mai mult de 6 luni, pentru a se descoperi date și informații suficiente pentru prinderea persoanelor.

Prestarea unui serviciu constituie o altă variantă a participării autorizate la anumite activități, constând în realizarea unui serviciu licit în vederea obținerii de informații. De exemplu, s-a considerat ca fiind un altfel de serviciu un amanet condus în mod ascuns de către organele de poliție și folosit pentru depistarea și tragerea la răspundere penală a unor persoane care au comis furturi[2].

Secțiunea a 2-a. Participarea autorizată la anumite activități sub imperiul Codului de procedură penală anterior și a legislației speciale

Înainte de intrarea în vigoare a Codului de procedură penală, legislația procesuală penală nu conținea dispoziții privind participarea autorizată la anumite activități în afara legislației speciale penale, în care această măsură era prevăzută ca o parte a utilizării investigatorilor sub acoperire.

Prin Legea nr. 78/2000 pentru prevenirea, descoperirea și sancționarea faptelor de corupție[3], în forma anterioară intrării în vigoare a Codului de procedură penală, se prevedea că, în cadrul folosirii metodei de investigație a utilizării investigatorilor sub acoperire, putea fi realizată o procedură similară cu participarea autorizată la anumite activități.

Astfel, conform art. 26[1] alin. (6) din Legea nr. 78/2000[4], „*investigatorii sub acoperire sau investigatorii cu identitate reală pot fi autorizați să promită, să ofere sau, după caz, să dea bani ori alte foloase unui funcționar, în condițiile prevăzute la art. 254, 256 sau 257 din Codul penal*". Cu alte cuvinte, legea permitea autorizarea realizării elementului constitutiv al infracțiunilor de luare de mită, primirea de foloase necuvenite și trafic de influență de către o persoană prin intermediul unui investigator sub acoperire, care realiza latura obiectivă a infracțiunii corespondente. Ipoteza avută în vedere la acel moment este preluată în cuprinsul dispozițiilor

[1] *C. Villacampa, K. Flórez*, Human Trafficking for criminal exploitation and participation in armed conflicts: the Colombian case, în Crime, Law and Social Change 69, 421-445 (2018), p. 429.

[2] EWCA, cauza *Regina c. Palmer, Gyamfi, Cooke*, Dec. din 7 august 2014, [2014] EWCA Crim 1681, pe *www.bailii.org*

[3] Legea nr. 78 din 8 mai 2000 pentru prevenirea, descoperirea și sancționarea faptelor de corupție (M. Of. nr. 219 din 18 mai 2000).

[4] Art. 26[1] a fost introdus de pct. 3 al articolului unic din O.U.G. nr. 124 din 6 septembrie 2005 (M. Of. nr. 842 din 19 septembrie 2005), fiind însă abrogat prin art. 41 pct. 3 din Titlul II din Legea nr. 255/2013.

art. 138 alin. (11) C.pr.pen., în care se arată că persoana autorizată să participe la anumite activități va comite o faptă similară laturii obiective a unei infracțiuni de corupție. Din punctul de vedere al clarității textului, legea veche era mai clară sub aspectul acțiunilor vizate, fără ca legiuitorul să fi fost nevoit să recurgă la eufemisme privind fapte similare cu latura obiectivă, putând să fi enumerat acțiunile pe care le putea realiza persoana care participa la anumite activități. Menționăm că, față de legislația actuală, era posibil numai ca un investigator să fie autorizat, nu și un colaborator, ca în cazul legii actuale. De altfel, instituția colaboratorului era cunoscută în cazul altor legislații penale speciale, după cum vom vedea în continuare.

O altă lege specială în care era prevăzută posibilitatea ca investigatorii să poată fi autorizați să pună în executare metoda specială de cercetare similară celei pe care o analizăm era Legea nr. 143/2000 privind prevenirea și combaterea traficului și consumului ilicit de droguri[1], în care se prevedea, la art. 22 alin. (1), că: „*polițiștii din formațiunile de specialitate, care acționează ca investigatori acoperiți, precum și colaboratorii acestora pot procura droguri, substanțe chimice, esențiale și precursori, cu autorizarea prealabilă a procurorului, în vederea descoperirii activităților infracționale și a identificării persoanelor implicate în astfel de activități*". În textul legal citat, putem observa că s-a avut în vedere numai procurarea drogurilor, nu și vânzarea acestora către alte persoane, cum este posibil potrivit Codului de procedură penală în vigoare. Astfel, era restrânsă folosirea metodei speciale de cercetare numai la acea activitate care nu presupunea distribuirea de substanțe narcotice către eventuali consumatori. Această situație reflectă un aspect deosebit de important din punctul de vedere al necesității unui control de proporționalitate a măsurii din partea procurorului, întrucât procurarea de substanțe interzise nu va pune în pericol sănătatea publică, restrângând numai dreptul la viață privată al persoanei față de care se ia măsura, întrucât substanțele vor fi confiscate de îndată. Cumpărarea de droguri de la o persoană bănuită anterior că este implicată în traficul de droguri este forma de participare autorizată la anumite activități întâlnită de cele mai multe ori, fiind și situația în care s-a ridicat cel mai des problema unei infracțiuni provocate. Cu toate acestea, infiltrarea unui investigator sub acoperire într-o organizație preocupată cu traficul de droguri poate ridica dificultăți care să impună ca investigatorul să realizeze și alte activități decât procurarea, sens în care Codul de procedură penală în vigoare permite desfășurarea mai multor operațiuni[2].

Similar legii procesuale penale în vigoare, sub imperiul Legii nr. 143/2000, se puteau autoriza atât investigatorii, cât și colaboratorii pentru procurarea substanțelor amintite în art. 22 din lege. Distinct față de legislația actuală stă valoarea probantă a actelor încheiate de investigatori și colaboratori în realizarea activităților arătate mai sus, conform art. 22 alin. (2) din Legea nr. 143/2000: „*actele încheiate de polițiștii și colaboratorii acestora, prevăzuți la alin. (1), pot constitui mijloace de probă*", ceea ce înseamnă că, în urma folosirii metodei speciale de cercetare, ar fi rezultat mijloace de probă.

Ceea ce nu se menționa expres în cuprinsul celor două legi la care am făcut referire este că operațiunile autorizate nu vor constitui infracțiuni, fiind subînțeles că, operațiunea fiind autorizată de procuror în vederea strângerii de probe, va avea un caracter licit.

[1] Legea nr. 143 din 26 iulie 2000 privind prevenirea și combaterea traficului și consumului ilicit de droguri (M. Of. nr. 362 din 3 august 2000).

[2] *C. Olaru*, op. cit., p. 97.

Secțiunea a 3-a. Participarea autorizată la anumite activități de la momentul adoptării Codului de procedură penală până la forma în vigoare

Chiar dacă sub imperiul legislației procesuale penale anterioare și a legislației speciale, procesul penal român cunoștea metoda specială de cercetare a participării autorizate la anumite activități în cadrul utilizării investigatorilor sub acoperire, prin Codul de procedură penală, metoda a fost separată de aceasta din urmă, creându-se o metodă autonomă, asemenea cum este ea reglementată în prezent.

La momentul adoptării Codului de procedură penală, metoda specială de cercetare era prevăzută de art. 138 alin. (1) lit. i) C.pr.pen., fiind denumită „constatarea unei infracțiuni de corupție sau a încheierii unei convenții". Deși denumirea actuală a metodei speciale de cercetare nu este foarte inspirată, ea este totuși superioară celei avute în vedere la momentul adoptării Codului de procedură penală, unde metoda specială părea să nu aibă legătură cu tehnicile speciale, ci mai degrabă cu o eventuală infracțiune flagrantă sau cu operațiuni ce țin de probațiune în dreptul civil. Nici în privința definițiilor, legiuitorul nu era mai inspirat, întrucât prevedea două alineate distincte prin care definea cele două ipoteze, conducând la ideea că poate ar exista două metode speciale de cercetare.

Conform art. 138 alin. (10) C.pr.pen., în forma adoptată de Parlament, „*constatarea unei infracțiuni de corupție se poate realiza și prin acțiunea sau inacțiunea ce este similară unei infracțiuni de corupție, îndeplinită în scopul strângerii de probe în cadrul procesului penal*". Nu credem că era înțelept ca un procedeu probatoriu să conțină expresia de „constatare a unei infracțiuni", întrucât aceasta este similară cu terminologia folosită în cazul modurilor de sesizare a organelor de urmărire penală.

Potrivit art. 138 alin. (11) C.pr.pen., în forma adoptată de Parlament, „*constatarea încheierii unei convenții se poate realiza și prin cumpărarea sau orice altă operațiune privind un obiect ce poate constitui mijloc de probă de la o persoană suspectată de comiterea unei infracțiuni, prestarea unui serviciu pentru persoana suspectată de comiterea unei infracțiuni ori cumpărarea sau orice altă operațiune privind o persoană care se bănuiește că ar fi dispărută, că este victima traficului de persoane sau a unei răpiri*". În privința acestei definiții, legiuitorul a fost mai clar, întrucât intuiește operațiuni care se realizează curent în cazul investigării traficului de droguri, fără a indica expres că se referă la acestea. Definiția cu privire la celelalte elemente este similară cu cea din forma în vigoare, cu unele modificări care nu schimbă esența sa.

În ceea ce privește condițiile legale și procedura de autorizare a măsurii, acestea nu diferă în mod semnificativ de forma în vigoare, cu excepția unor situații pe care le vom expune în continuare.

Pentru început, la momentul adoptării Codului de procedură penală, în cazul tehnicii speciale de cercetare a *constatării unei infracțiuni de corupție sau a încheierii unei convenții*, nu era clar care organ judiciar avea competența să dispună asupra autorizării măsurii, întrucât dispozițiile art. 150 C.pr.pen. erau contradictorii. Pe de o parte, în cuprinsul art. 150 alin. (1) C.pr.pen. rezulta că judecătorul de drepturi și libertăți poate dispune asupra măsurii, la propunerea procurorului. Pe de altă parte, în cuprinsul art. 150 alin. (2) C.pr.pen. se arăta că măsura se dispune de procuror, din oficiu sau la propunerea organelor de cercetare penală. Este evident că exista o scăpare a legiuitorului în această privință, misterul fiind în ce sens a fost scăparea? Astfel cum vom arăta în prezenta lucrare, față de gravitatea ingerinței aduse vieții private a persoanei, precum și dreptului la siguranță al persoanei, *de lege ferenda*, se impune ca

măsura să fie autorizată de judecătorul de drepturi și libertăți, pentru a limita cazurile în care să poată fi folosită și a se stabili foarte clar activitățile care pot fi realizate.

În ceea ce privește infracțiunile față de care era necesară existența unei suspiciuni rezonabile privind pregătirea sau săvârșirea lor, forma adoptată de Parlament a art. 150 alin. (1) lit. a) C.pr.pen. era diferită față de forma care a intrat în vigoare la 1 februarie 2014, prin aceea că nu erau menționate și *infracțiunile asimilate infracțiunilor de corupție și infracțiunile împotriva intereselor financiare ale Uniunii Europene*, mențiunea privind acestea fiind introdusă prin legea de punere în aplicare. Ca atare, forma inițială a textului legal era: „*există o suspiciune rezonabilă cu privire la pregătirea sau săvârșirea unei infracțiuni de trafic de droguri, trafic de arme, trafic de persoane, acte de terorism, spălare a banilor, falsificare de monede sau alte valori, șantaj, lipsire de libertate, evaziune fiscală, în cazul infracțiunilor de corupție sau în cazul unor alte infracțiuni pentru care legea prevede pedeapsa închisorii de 7 ani sau mai mare ori dacă există o suspiciune rezonabilă că o persoană este implicată în activități infracționale care au legătură cu infracțiunile enumerate mai sus*".

O altă distincție față de forma în vigoare este cea cuprinsă în art. 150 alin. (3) C.pr.pen., în care se arăta că: „*activitatea persoanei care participă la constatarea unei infracțiuni de corupție sau de încheiere a unei convenții nu constituie* ***provocare****, contravenție sau infracțiune*" (s.n.). Menționarea cuvântului „provocare" constituia o gravă încălcare a garanțiilor privind echitabilitatea procesului penal, întrucât legiuitorul stabilea *ab initio* că, în cazul acestei metode speciale de cercetare, nu va putea fi reținută provocarea ca temei de înlăturare a probei obținute în mod neloial prin raportare la art. 101 alin. (3) C.pr.pen. Or, tocmai această metodă specială de cercetare este cea mai propice în a conduce la discuții privind existența sau nu a unei provocări din partea organelor de urmărire penală. Mai mult, nu putem afirma că scopul legiuitorului ar fi fost unul corect, întrucât menirea întregului alineat este de a preveni persoana care pune în executare metoda specială de cercetare de a suferi vreo consecință penală sau contravențională, nu ca proba obținută să fie ferită de orice critici privind legalitatea sau loialitatea ei.

În afara celor menționate mai sus, metoda specială de cercetare, cunoscută în prezent ca „participarea autorizată la anumite activități", nu a suferit modificări majore față de forma inițială adoptată de Parlament, cu excepția celei suferite prin O.U.G. nr. 18/2016. Prin acest din urmă act legislativ, a fost modificat art. 150 alin. (1) lit. a) C.pr.pen., în care au fost menționate suplimentar mai multe infracțiuni, iar unele dintre cele anterioare au fost redenumite, forma actuală a textului legal fiind: „*există o suspiciune rezonabilă cu privire la pregătirea sau săvârșirea unei infracțiuni de trafic de droguri, de efectuare de operațiuni ilegale cu precursori sau cu alte produse susceptibile de a avea efecte psihoactive, infracțiuni privind nerespectarea regimului armelor, munițiilor, materialelor nucleare, al materiilor explozive și al precursorilor de explozivi restricționați, trafic și exploatarea persoanelor vulnerabile, acte de terorism sau asimilate acestora, de finanțare a terorismului, spălare a banilor, falsificare de monede, timbre sau de alte valori, unei infracțiuni care se săvârșește prin sisteme informatice sau mijloace de comunicare electronică, șantaj, lipsire de libertate în mod ilegal, evaziune fiscală, în cazul infracțiunilor de corupție, al infracțiunilor asimilate infracțiunilor de corupție și al infracțiunilor împotriva intereselor financiare ale Uniunii Europene sau în cazul altor infracțiuni pentru care legea prevede pedeapsa închisorii de 7 ani sau mai mare ori dacă există o suspiciune rezonabilă că o persoană este implicată în activități infracționale care au legătură, potrivit art. 43, cu infracțiunile enumerate mai sus*".

Capitolul II
Condițiile legale pentru autorizarea metodei speciale de cercetare

Participarea autorizată la anumite activități, asemenea celorlalte metode speciale de supraveghere sau cercetare, presupune imixtiunea în libera exercitare a drepturilor și libertăților persoanei vizate, motiv pentru care se impune restrângerea folosirii acesteia numai în situații prevăzute expres de lege, precum și garantarea respectării proporționalității între interesul public și interesul persoanei.

Organul competent să dispună asupra autorizării utilizării investigatorilor sub acoperire și a colaboratorilor este *procurorul*, potrivit art. 150 C.pr.pen. Deoarece măsura este una de cercetare, și nu de supraveghere, nu este necesară încuviințarea măsurii de către judecătorul de drepturi și libertăți, considerându-se că restrângerea drepturilor fundamentale ale persoanei nu este într-o asemenea măsură încât să implice concursul judecătorului. Cu toate că aprecierea oportunității folosirii măsurii trebuie să aparțină procurorului, în condițiile în care urmărirea penală se desfășoară sub conducerea acestuia, *de lege ferenda*, se impune ca acesta să propună judecătorului de drepturi și libertăți încuviințarea măsurii, mai ales că legiuitorul a prevăzut condiții legale mai stricte pentru întrebuințarea acestui procedeu probatoriu. Considerăm că nu este justificat ca un mandat de supraveghere tehnică să poată fi emis doar de judecătorul de drepturi și libertăți (cu excepția autorizării provizorii de către procuror) și o măsură care este socotită de legiuitor mai intruzivă [în acest sens este criteriul gravității faptei urmărite, prevăzut de art. 150 alin. (1) lit. a) C.pr.pen.] să poată fi dispusă prin ordonanța procurorului. Astfel, cum am arătat și în cazul metodei speciale a utilizării investigatorilor sub acoperire și a colaboratorilor, se impune modificarea legii în sensul autorizării acesteia de către judecătorul de drepturi și libertăți, la propunerea procurorului.

O trăsătură comună cu celelalte metode speciale de supraveghere sau cercetare este că utilizarea investigatorilor sub acoperire și a colaboratorilor poate fi incidentă numai în cursul urmăririi penale, nu și în celelalte faze ale procesului penal. Mai întâi de toate, este necesar ca, pentru autorizarea măsurii, să fie începută urmărirea penală, întrucât Codul de procedură penală nu mai prevede faza actelor premergătoare.

Condițiile care trebuie să fie îndeplinite în cazul măsurii participării la anumite activități sunt similare cu cele care trebuie îndeplinite în cazul utilizării investigatorilor sub acoperire și a colaboratorilor și sunt prevăzute de art. 150 alin. (1) C.pr.pen., constând în: *gravitatea infracțiunii care face obiectul urmăririi penale*, *proporționalitatea măsurii* și *necesitatea măsurii*. În privința ultimelor două condiții, legiuitorul a folosit aceeași formulare ca în cazul autorizării folosirii investigatorilor sub acoperire și a colaboratorilor. În schimb, în cazul condiției privind gravitatea infracțiunii pentru care se poate dispune măsura, observăm că există câteva diferențe referitoare la măsura participării la anumite activități, sfera infracțiunilor fiind mai redusă.

În privința primei condiții legale, conform art. 150 alin. (1) lit. a) C.pr.pen., pentru autorizarea metodei speciale de cercetare, este necesar să existe: „*o suspiciune rezonabilă cu privire la pregătirea sau săvârșirea unei infracțiuni de trafic de droguri, de efectuare de operațiuni ilegale cu precursori sau cu alte produse susceptibile de a avea efecte psihoactive, infracțiuni privind nerespectarea regimului armelor, munițiilor, materialelor nucleare, al materiilor explozive și al precursorilor de explozivi restricționați, trafic și exploatarea persoanelor vulnerabile, acte*

de terorism sau asimilate acestora, de finanțare a terorismului, spălare a banilor, falsificare de monede, timbre sau de alte valori, unei infracțiuni care se săvârșește prin sisteme informatice sau mijloace de comunicare electronică, șantaj, lipsire de libertate în mod ilegal, evaziune fiscală, în cazul infracțiunilor de corupție, al infracțiunilor asimilate infracțiunilor de corupție și al infracțiunilor împotriva intereselor financiare ale Uniunii Europene sau în cazul altor infracțiuni pentru care legea prevede pedeapsa închisorii de 7 ani sau mai mare ori dacă există o suspiciune rezonabilă că o persoană este implicată în activități infracționale care au legătură, potrivit art. 43, cu infracțiunile enumerate mai sus".

Față de metodele speciale de supraveghere și chiar și față de unele metode speciale de cercetare, observăm că legiuitorul a limitat cu mai multă înțelepciune posibilitatea organelor de urmărire penală de a întrebuința participarea autorizată la anumite activități, ținând cont de ingerința deosebit de mare adusă vieții private a unei persoane.

Comparând textele care reglementează această condiție în cazul ambelor măsuri, observăm că, în ceea ce privește participarea autorizată la anumite activități, nu se prevede în mod expres folosirea măsurii în situația *infracțiunilor contra securității naționale prevăzute de Codul penal și de alte legi speciale*. Aparent, nu s-ar putea dispune măsura în acest caz, dar, pe de altă parte, condiția subsidiară a săvârșirii unei infracțiuni pedepsite cu închisoarea de 7 ani sau mai mare ar permite folosirea ei în majoritatea infracțiunilor contra securității naționale. Cu toate acestea, considerăm că legiuitorul a arătat o doză de înțelepciune în această situație, deoarece infracțiunile contra securității naționale constituie, în opinia noastră, faptele care aduc cea mai gravă atingere societății având în vedere amploarea consecințelor pe care le pot produce și realizarea participării autorizate la anumite activități poate, prin ea însăși, să constituie o atingere adusă securității naționale[1]. Astfel, potrivit art. 1 al Legii nr. 51/1991 privind siguranța națională a României, republicată[2], „*prin «siguranța națională a României» se înțelege starea de legalitate, de echilibru și de stabilitate socială, economică și politică necesară existenței și dezvoltării statului național român, ca stat suveran, unitar, independent și indivizibil, menținerii ordinii de drept, precum și climatului de exercitare neîngrădită a drepturilor, libertăților și îndatoririlor fundamentale ale cetățenilor, potrivit principiilor și normelor democratice statornicite prin Constituție*". Totodată, a participa la asemenea infracțiuni contravine scopului procesului penal – cel de a preveni săvârșirea de noi infracțiuni și de a trage la răspunderea penală persoane care comit astfel de fapte.

O altă diferență constituie includerea unei referiri la art. 43 C.pr.pen. în cazul subsidiar al existenței unei *suspiciuni rezonabile că o persoană este implicată în activități infracționale care au legătură, potrivit art. 43, cu infracțiunile* enumerate la art. 150 alin. (1) lit. a) C.pr.pen. Prin referirea la instituția „reunirii cauzelor" nu credem că legiuitorul a elucidat în vreun fel problema similară măsurii utilizării investigatorilor sub acoperire și a colaboratorilor, deoarece, în conformitate cu art. 43 alin. (2) lit. c) C.pr.pen., reunirea cauzelor se dispune *când între două sau mai multe infracțiuni există legătură*. Cu alte cuvinte, legiuitorul își dublează teza, în condițiile în care atât art. 43 C.pr.pen., cât și art. 150 alin. (1) lit. a) C.pr.pen. vorbesc despre existența unei legături între infracțiuni. Criteriul este unul interesant, considerându-l a fi unul legal, întrucât gravitatea infracțiunilor amintite face necesară extinderea activității organelor de urmărire și față de persoane sau fapte care au o legătură cu infracțiunile prevăzute

[1] *M. Bulancea, R. Slăvoiu*, în M. Udroiu (coord.), Codul de procedură penală, 2017, pp. 730-731.

[2] Legea nr. 51 din 29 iulie 1991 privind siguranța națională a României, publicată în M. Of. nr. 163 din 7 august 1991 și republicată în M. Of. nr. 190 din 18 martie 2014.

de art. 150 alin. (1) C.pr.pen.[1]. Ceea ce va trebui să se aibă în vedere este această legătură care se bazează pe elemente obiective, și nu este doar o presupunere a organelor de urmărire penală, caz în care vom putea vorbi despre o infracțiune provocată, ceea ce nu poate fi acceptat în procesul penal[2].

În privința *proporționalității măsurii*, ca a doua condiție legală, deși formularea este identică celei utilizate în cazul autorizării folosirii investigatorilor sub acoperire și a colaboratorilor[3], apreciem că proporționalitatea se va raporta și la elemente adiționale, în situația acestei măsuri. La momentul autorizării măsurii, procurorul va trebui să compare gravitatea faptelor autorizate cu cele care fac obiectul urmăririi penale. Măsura nu va respecta condiția de proporționalitate în cazul în care faptele autorizate sunt de *gravitate mai mare* decât faptele care fac obiectul procesului penal. Nu se poate admite decât în mod excepțional ca o persoană să fie autorizată să săvârșească fapte de natură penală și numai atunci când ordinea publică ar fi mai grav afectată dacă nu s-ar proceda la autorizarea măsurii.

În același timp, măsura de cercetare nu va putea fi considerată ca fiind proporțională, în condițiile în care un procedeu probatoriu comun ar fi suficient pentru stabilirea stării de fapt, fără a fi necesară realizarea unei investigații secrete. În același timp, potrivit reglementării în vigoare, proporționalitatea utilizării metodelor speciale de supraveghere sau cercetare va fi analizată *in concreto* de către organele judiciare, prin raportare la obiectivul urmărit prin folosirea acestora. Pentru a se determina caracterul proporțional al măsurii, vor fi avute în vedere *particularitățile cauzei*, *importanța informațiilor care ar putea fi obținute* și *gravitatea infracțiunii*.

Prin „particularitățile cauzei" vom înțelege acele împrejurări specifice unei anumite cauze penale care vor impune utilizarea măsurii de cercetare pentru soluționarea cauzei, deoarece un altfel de mijloc nu ar fi propice pentru a stabili starea de fapt. De exemplu, în cazul infracțiunilor privind operațiunile ilicite cu substanțe aflate sub control național (Legea nr. 143/2000, republicată), poate fi esențială, pentru integrarea unui investigator sub acoperire, dovedirea că este dispus să realizeze operațiuni cu droguri față de unii consumatori, sens în care aceasta reprezintă o particularitate (des întâlnită) a respectivei cauze.

Prin „importanța informațiilor ori a probelor ce urmează a fi obținute" înțelegem contribuția pe care o pot avea informațiile sau probele obținute pentru stabilirea împrejurărilor esențiale ale cauzei. Întrucât am arătat deja că, prin participarea autorizată la anumite activități, proba va putea reieși din audierea ca martor a persoanei autorizate să pună în executare măsura sau din mijloace de supraveghere tehnice, considerăm că proporționalitatea trebuie stabilită raportat la utilitatea probei ce urmează a fi obținută în mod derivat pe baza datelor și informațiilor ce ar putea fi descoperite. Este lesne de imaginat că, dacă se organizează un flagrant la momentul realizării participării autorizate la anumite activități, se va putea dovedi infracțiunea care face obiectul urmăririi penale, dar se vor putea descoperi și reține persoanele vizate de măsură.

---

[1] În această privință, trebuie să avem în vedere inclusiv Hotărârea Tele2 a Curții de Justiție a Uniunii Europene, în care se arată că, pentru a aplica unele tehnici speciale care creează ingerințe deosebite vieții private, este necesar ca faptele cercetate sau persoanele vizate să fie în legătură obiectivă cu săvârșirea unor infracțiuni grave – CJUE, cauzele reunite C-203/15 și C-698/15, *Tele2 Sverige AB, Secretary of State for the Home Department și alții*, Hotărârea din 21 decembrie 2016, §115 și §119.

[2] Conform art. 101 alin. (3) C.pr.pen., „este interzis organelor judiciare penale sau a altor persoane care acționează pentru acestea să provoace o persoană să săvârșească ori să continue săvârșirea unei fapte penale, în scopul obținerii unei probe".

[3] *V. supra*, Titlul XII, Capitolul II.1.

A treia condiție impusă de Codul de procedură penală pentru dispunerea supravegherii tehnice este *necesitatea (subsidiaritatea)* pentru obținerea informațiilor sau probei. Această condiție este prevăzută în cuprinsul art. 150 alin. (1) lit. c) C.pr.pen. și limitează folosirea participării autorizate la anumite activități la cazurile în care „*probele sau localizarea și identificarea făptuitorului, suspectului sau inculpatului nu ar putea fi obținute în alt mod sau obținerea lor ar presupune dificultăți deosebite ce ar prejudicia ancheta ori există un pericol pentru siguranța persoanelor sau a unor bunuri de valoare*". Ținând seama de particularitățile acestei metode speciale de cercetare și de asemănarea acesteia cu utilizarea investigatorilor sub acoperire și a colaboratorilor, apreciem că se va evalua condiția necesității administrării probei prin această metodă specială de cercetare în același mod, sens în care facem trimitere la explicațiile date anterior în prezenta lucrare[1].

[1] *Ibidem*.

Capitolul III
Procedura autorizării participării autorizate la anumite activități

Metoda specială de cercetare, putând fi întrebuințată numai în cursul urmăririi penale și vizând fapte și împrejurări numai pentru viitor, poate fi dispusă de procuror atât din oficiu, cât și la propunerea organelor de cercetare penală.

Pentru *autorizarea măsurii participării autorizate* la anumite activități, conform art. 150 alin. (2) C.pr.pen., procurorul va emite o ordonanță similară celei pe care o va emite în cazul utilizării investigatorilor sub acoperire și a colaboratorilor, aceasta conținând: *indicarea activităților autorizate*, *perioada pentru care s-a autorizat măsura* și *persoana care desfășoară activitățile*.

Prin „indicarea activităților autorizate" procurorul trebuie să arate în cuprinsul ordonanței acțiunile pe care persoana autorizată le poate realiza, într-un mod în care să poată fi determinată activitatea de natură infracțională care urmează a fi realizată. Spre deosebire de măsura utilizării investigatorilor sub acoperire și a colaboratorilor, activitățile autorizate vor fi diferite prin aceea că, în cazul celei din urmă metode speciale, ele nu vor putea întruni elementele laturii obiective ale unei infracțiuni[1]. Aceasta reprezintă o diferență fundamentală între cele două măsuri, fiind obligatoriu ca procurorul să indice în mod expres că faptele ar putea întruni elementele constitutive ale unei infracțiuni. Din punctul de vedere al clarității ordonanței, ca o condiție a legalității acesteia, va fi necesar ca procurorul să prevadă cât mai detaliat activitățile autorizate, în opinia noastră, impunându-se indicarea concretă a faptelor de natură penală care pot fi realizate de persoana autorizată, prin raportare la textul de lege care incriminează aceste fapte ori prin detalierea precisă a acțiunilor prin raportare la elementele constitutive ale unei infracțiuni, chiar și fără indicarea textului normei de incriminare. Neindicarea faptelor ori indicarea generică a posibilității realizării laturii obiective a unor infracțiuni nu îndreptățește persoana autorizată să realizeze măsura. În situația în care investigatorul sub acoperire sau colaboratorul (ori organul de cercetare penală) vor depăși conținutul activităților autorizate, ei nu vor mai fi protejați de răspundere penală ca efect al ordonanței procurorului și vor putea fi trași la răspundere penală pentru săvârșirea unei infracțiuni, în afară de cazul existenței unei alte cauze justificative sau de neimputabilitate incidente în cauză[2].

În ceea ce privește activitățile care pot fi autorizate, procurorul nu are o deplină libertate, fiind limitat de acele fapte pentru care nu poate exista o autorizare a legii, ca urmare a gravei încălcări a drepturilor fundamentale ale unei persoane sau grava afectare a ordinii de drept. O atare limitare nu este arătată în cuprinsul Codului de procedură penală, o lacună deosebit de gravă a legiuitorului care se impune a fi remediată. În doctrină[3] s-a arătat cu privire la cauzele justificative că nu poate exista o îndeplinire a unei obligații impuse de lege în situațiile în care anumite valori sociale ar duce la concluzia că, în mod vădit, activitățile autorizate sunt incompatibile cu respectarea drepturilor fundamentale ale persoanei. De exemplu, nu se va putea autoriza participarea la uciderea intenționată a unei persoane, la torturarea acesteia sau la exercitarea unui tratament degradant, deoarece această măsură ar contraveni flagrant dispozițiilor art. 22 alin. (1) și (2) din Constituție.

---

[1] *M. Bulancea, R. Slăvoiu*, în M. Udroiu (coord.), Codul de procedură penală, 2017, p. 731.

[2] *Ibidem*.

[3] *Fl. Streteanu*, op. cit., pp. 543-545.

Toate activitățile detaliate de procuror în cuprinsul ordonanței de autorizare care vor cădea sub incidența dispozițiilor art. 150 alin. (4) C.pr.pen. nu constituie infracțiuni sau contravenții, fiind incidentă o cauză justificativă legală ce exclude posibilitatea tragerii la răspundere penală. În măsura în care se vor realiza activități care excedează mandatul existent ca urmare a autorizării procurorului, persoana va răspunde pentru faptele sale din punct de vedere penal, contravențional sau civil[1].

Un alt element obligatoriu în cuprinsul ordonanței procurorului îl reprezintă durata pentru care se va lua măsura, aceasta putând fi de maximum 60 de zile, cu posibilitatea prelungirii măsurii de către procuror, fiecare prelungire neputând depăși o durată de 60 de zile. Dată fiind natura activităților autorizate prin această metodă specială de cercetare, procurorul va trebui la fiecare prelungire să pună în balanță ambele elemente ale interesului public: prevenirea săvârșirii de noi infracțiuni, lezată în mod concret prin măsura dispusă, și descoperirea și tragerea la răspundere penală a persoanelor care săvârșesc infracțiuni. Pe măsură ce se acordă noi prelungiri, considerăm că ingerința în viața privată va deveni una din ce în ce mai mare, presupunând existența unor temeiuri noi care să justifice prelungirea măsurii.

Trebuie avut în vedere și efectul pe care participarea autorizată la anumite activități îl are asupra ordinii publice, întrucât realizarea unor asemenea activități nu poate fi permisă dacă ar pune în pericol această valoare socială. Trebuie să avem în vedere că, alături de viața privată, unul dintre drepturile fundamentale ale unui cetățean este dreptul la siguranță, prevăzut de art. 23 alin. (1) din Constituție și art. 5 Conv.EDO. Or, în măsura în care organele de urmărire penală autorizează săvârșirea unor fapte prevăzute de legea penală și apoi prelungesc măsura pentru o perioadă de timp, se poate afirma că dreptul la securitate al celorlalte persoane va fi restrâns, fiind necesar a se găsi un echilibru între interesul legitim urmărit și drepturile care pot fi restrânse. Nu va fi permis ca, prin prelungirea metodei speciale de cercetare, să se ajungă la consecințe mai grave decât cele care s-ar fi produs în cazul în care metoda nu ar fi fost întrebuințată.

Limitele temporale maxime ale măsurii participării autorizate la anumite activități diferă față de măsura utilizării investigatorilor sub acoperire și a colaboratorilor prin aceea că are *o durată maximă pentru care poate fi dispusă, de un an*, de la care nu există nicio derogare legală în cazul anumitor infracțiuni, diferit de prevederea înscrisă, în situația utilizării investigatorilor sub acoperire și a colaboratorilor, în art. 148 alin. (9) C.pr.pen.[2]. Această abordare o apreciem ca fiind corectă, în condițiile în care este esențial ca în toate cazurile legiuitorul să prevadă un termen maxim, însă nu înțelegem de ce în această situație s-a inclus această durată maximă, în special în condițiile similarității textului legal cu cel de la utilizarea investigatorilor sub acoperire și a colaboratorilor.

Spre deosebire de metoda specială de cercetare a utilizării investigatorilor sub acoperire și a colaboratorilor, în cazul participării autorizate la anumite activități, cercul persoanelor care

[1] Trib. Suceava, s. pen., încheierea din 4 mai 2015, definitivă prin încheierea nr. 42 din 26 iunie 2015 a C. Ap. Suceava.

[2] Conform art. 148 alin. (9) C.pr.pen.: „Durata măsurii poate fi prelungită pentru motive temeinic justificate, în cazul în care sunt îndeplinite condițiile prevăzute la alin. (1), fiecare prelungire neputând depăși 60 de zile. Durata totală a măsurii, în aceeași cauză și cu privire la aceeași persoană, nu poate depăși un an, cu excepția infracțiunilor contra vieții, securității naționale, infracțiunilor de trafic de droguri, nerespectarea regimului armelor, munițiilor, materialelor nucleare, al materiilor explozive și al precursorilor de explozivi restricționați, trafic și exploatarea persoanelor vulnerabile, acte de terorism sau asimilate acestora, de finanțare a terorismului, spălare a banilor, precum și infracțiunilor împotriva intereselor financiare ale Uniunii Europene".

pot fi autorizate este mai larg. Potrivit art. 150 alin. (3) C.pr.pen., activitățile autorizate se pot desfășura de către un organ de cercetare penală, de către un investigator cu identitate reală sau sub acoperire și de către un colaborator. În cazul în care se va utiliza un organ de cercetare penală sau un investigator cu identitate reală, nu se va impune autorizarea măsurii prevăzute de art. 148 C.pr.pen. De pildă, nu va fi necesară folosirea unui investigator sub acoperire, ci va fi suficientă folosirea unui organ de cercetare penală în situația în care se va realiza un flagrant în care organul de cercetare penală va cumpăra de la făptuitor o cantitate de substanțe a căror deținere este interzisă de lege. Totuși, avem rezerve serioase că un organ de cercetare ar putea fi folosit, consecințele fiind nefavorabile în caz că îi este cunoscută calitatea de către infractori.

În schimb, în cazul în care se va folosi un investigator sub acoperire și un colaborator, se impune autorizarea și a utilizării investigatorilor și a colaboratorilor alături de participarea autorizată la anumite activități. În doctrină s-a arătat că măsurile ar putea fi autorizate prin aceeași ordonanță[1], opinie cu care suntem de acord, având în vedere faptul că o parte dintre activitățile autorizate de procuror pot cădea sub incidența dispozițiilor art. 150 C.pr.pen. Opinia este susținută și de practica instanțelor de judecată care s-au pronunțat asupra legalității acestei situații[2]. Aceasta nu va însemna ca procurorul să nu detalieze și să prevadă în mod expres autorizarea măsurii participării autorizate la anumite activități, neputând să se subînțeleagă acest lucru din cuprinsul ordonanței de autorizare a utilizării investigatorilor sub acoperire și a colaboratorilor. Considerăm greșită soluția instanței de a se considera implicit dispusă participarea autorizată la anumite activități atunci când se deleagă organele de cercetare penală să realizeze un flagrant alături de un colaborator, fără ca, față de colaborator, să se dispună măsura specială de cercetare amintită[3]. Dintr-o ordonanță de delegare nu se poate deduce implicit și autorizarea colaboratorului în sensul art. 150 C.pr.pen., lipsind și elementele obligatorii care trebuie să fie prevăzute în ordonanța procurorului de participare autorizată la anumite activități[4].

[1] *M. Bulancea*, în M. Udroiu (coord.), Codul de procedură penală, 2017, p. 453; *D. Grădinaru*, op. cit., p. 213.

[2] Trib. Mureș, s. pen., încheierea nr. 147 din 31 octombrie 2016.

[3] C. Ap. București, s. I pen., încheierea nr. 506 din 8 noiembrie 2016.

[4] *C. Moisă*, op. cit., p. 154.

Capitolul IV
Punerea în executare a participării autorizate la anumite activități

Spre deosebire de metodele de supraveghere tehnică, în cazul metodelor speciale de cercetare, nu va fi nevoie de o ordonanță separată de punere în executare, ținând seama de conținutul ordonanței prin care se dispune asupra măsurii. Față de împrejurările cauzei, este posibil să fie necesară întrebuințarea de metode speciale de supraveghere tehnică, precum supravegherea video, audio sau prin fotografiere, caz în care se va impune încuviințarea prealabilă a măsurii de către judecătorul de drepturi și libertăți sau autorizarea provizorie de către procuror. Ținând seama de faptul că participarea autorizată la anumite activități va completa utilizarea investigatorilor sub acoperire, un mandat emis anterior pentru investigator sau colaborator va fi valabil și pentru participarea autorizată la anumite activități. Cu această ocazie, reamintim faptul că pentru aceste două metode speciale de cercetare se include posibilitatea folosirii de către investigator sau colaborator a unor dispozitive tehnice, pentru a obține fotografii sau înregistrări audiovideo, dar numai cu încuviințarea prealabilă a judecătorului de drepturi și libertăți, sens în care mandatul va indica în mod expres că se autorizează ca investigatorul sau colaboratorul să le utilizeze. Deși nu pare o problemă de interes deosebit, este de observat că punerea în executare a supravegherii audio, video sau prin fotografiere se va face de investigatorul sub acoperire sau de colaborator, prin derogare de la dispozițiile art. 142 C.pr.pen. Dacă, în cazul investigatorilor sub acoperire, apreciem că ei pot fi asimilați lucrătorilor specializați din cadrul poliției (fiind lucrători operativi ai poliției), în cazul colaboratorilor, art. 142 alin. (1) C.pr.pen. nu ar permite punerea în executare a supravegherii de către aceștia, ei neavând competență funcțională, întrucât nu sunt organe de urmărire penală sau lucrători de poliție. Din acest punct de vedere, era necesar ca legiuitorul să prevadă distinct posibilitatea folosirii supravegherii video, audio sau prin fotografiere, ceea ce a și făcut în cazul măsurii utilizării investigatorilor sub acoperire și a colaboratorilor[1]. În cazul participării autorizate la anumite activități, incidența acestei situații este evidențiată prin art. 150 alin. (5) C.pr.pen., în care se menționează că în procesul-verbal de consemnare a punerii în executare va fi precizată „*descrierea dispozitivelor tehnice utilizate în cazul în care s-a autorizat de către judecătorul de drepturi și libertăți, folosirea mijloacelor tehnice de supraveghere*". În niciun caz situația nu trebuie confundată cu desfășurarea unei supravegheri tehnice în paralel cu metoda specială de cercetare, mențiunile anterioare fiind aplicabile numai atunci când investigatorul sub acoperire și colaboratorul se folosesc de astfel de dispozitive.

Pentru realizarea metodei speciale de cercetare, se poate impune ca persoana care pune în executare măsura să aibă nevoie de diverse *înscrisuri* sau *obiecte* pentru desfășurarea activității autorizate. Această posibilitate este prevăzută în cuprinsul art. 150 alin. (7) C.pr.pen. în mod similar cu dispozițiile art. 148 alin. (7) C.pr.pen. Înscrisurile pot consta în documente de identitate, înscrisuri contrafăcute în vederea folosirii lor etc., iar obiectele în sume de bani, substanțe interzise, arme etc. Persoana care pune la dispoziție sau folosește înscrisurile ori obiectele nu va săvârși o infracțiune prin desfășurarea acestor activități, în cazul în care acestea constituie infracțiuni.

[1] *M. Bulancea, R. Slăvoiu*, în M. Udroiu (coord.), Codul de procedură penală, 2017, p. 726.

Odată finalizată punerea în executare a acestei metode speciale de cercetare, procurorul va încheia un proces-verbal, potrivit art. 150 alin. (5) C.pr.pen., în care vor fi consemnate: *„datele la care măsura a început și s-a încheiat, date cu privire la persoanele care au desfășurat activitățile autorizate, descrierea dispozitivelor tehnice utilizate în cazul în care s-a autorizat de către judecătorul de drepturi și libertăți, folosirea mijloacelor tehnice de supraveghere, identitatea persoanelor cu privire la care a fost pusă în aplicare măsura*".

În situațiile în care măsura va fi pusă în executare de către un investigator sub acoperire sau de către un colaborator cu identitate atribuită, se va proceda la utilizarea numelui conspirativ folosit de acesta, și nu a numelui real.

Spre deosebire de procesul-verbal prevăzut în cazul folosirii investigatorilor sub acoperire și a colaboratorilor, valoarea probatorie va fi diferită având în vedere caracterul expres al reglementării în cazul art. 148 alin. (5) C.pr.pen., în care se arată că procesul-verbal va conține datele și informațiile obținute, și nu probe privind faptele urmărite. Cu toate acestea, observăm că, în cazul participării autorizate la anumite activități, procesul-verbal întocmit potrivit dispozițiilor 150 alin. (5) C.pr.pen. nu conține mențiuni cu privire la activitățile care s-au realizat. Ca atare, considerăm că, în cuprinsul art. 138 alin. (11) C.pr.pen., legiuitorul precizează în mod nejustificat că această măsură se va utiliza în scopul obținerii de probe, din moment ce, prin ea însăși, măsura nu duce la obținerea niciunei probe. În mod evident, ea este utilă, iar probele care derivă din aceasta, în special declarațiile persoanei autorizate, pot avea o valoare deosebită, dar acest lucru nu schimbă caracterul *derivat* și *facultativ*[1] al acestora.

În privința măsurii utilizării investigatorilor sub acoperire și a colaboratorilor, procesul-verbal este întocmit de *investigatorul sub acoperire ori de colaborator*, și nu de către procuror, ca în cazul măsurii participării autorizate la anumite activități, nefiind obligatorie detalierea activităților concrete realizate de către acesta, ci numai a datelor și informațiilor furnizate organelor de urmărire penală. În același timp, referitor la detalierea tuturor activităților acestor persoane, suntem de părere că o asemenea prevedere ar putea duce la identificarea acestora, ceea ce ar contraveni regulii prevăzute de art. 149 alin. (1) C.pr.pen., potrivit căreia identitatea investigatorilor sub acoperire și a colaboratorilor cu altă identitate nu poate fi dezvăluită. În schimb, este inexplicabil de ce, în cazul măsurii participării autorizate la anumite activități, nu se detaliază în concret fiecare activitate care a fost realizată, în această situație fiind de părere că acest proces-verbal nu va putea fi considerat un mijloc de probă care să rezulte direct din folosirea măsurii de cercetare, deoarece nu conține elemente privitoare la faptele care fac obiectul urmăririi penale.

În mod similar măsurii utilizării investigatorilor sub acoperire și a colaboratorilor, mijloacele de probă care vor rezulta din măsura de cercetare sunt numai cele derivate, în sensul că persoanele care realizează activitățile autorizate vor putea fi audiate în cursul procesului penal în calitate de martori, aplicându-se regulile specifice în situația audierii martorilor amenințați[2], în același timp putând fi utilizate, concomitent, măsuri de supraveghere tehnică.

[1] În condițiile în care în cuprinsul art. 150 alin. (6) C.pr.pen. se precizează că persoana autorizată va fi audiată numai dacă organul judiciar apreciază că audierea este necesară.

[2] *V. supra*, Titlul XII, Capitolul VI.

Capitolul V
Provocarea infracțiunii

Secțiunea 1. Considerații generale

O problemă comună atât în cazul utilizării investigatorilor sub acoperire și a colaboratorilor, cât și a participării autorizate la anumite activități este cea a evitării provocării unei persoane să comită o infracțiune la solicitarea organelor de urmărire penală[1]. Incidența acestei probleme este dată de caracterul secret al operațiunii, organele de urmărire penală simulând o participare la activitățile infracționale ale unor alte persoane, în vederea strângerii de probe[2].

Prin art. 101 alin. (3) C.pr.pen., legiuitorul a interzis expres provocarea infracțiunii, stabilind că „*este interzis organelor judiciare penale sau altor persoane care acționează pentru acestea să provoace o persoană să săvârșească ori să continue săvârșirea unei fapte penale, în scopul obținerii unei probe*". Această dispoziție legală trebuie să fie pusă în contextul în care orice investigație sub acoperire (utilizarea investigatorilor sub acoperire, participarea autorizată la anumite activități și livrarea supravegheată) prezintă necesitatea ca investigatorul sub acoperire să se infiltreze, câștigând încrederea persoanelor cu care intră în contact. Un atare comportament nu este unul greșit, dar poartă cu el riscul de provocare la săvârșirea unei infracțiuni atunci când investigatorul sub acoperire determină, prin convingere sau constrângere, o persoană să comită o infracțiune pe care altfel nu ar fi comis-o[3]. De altfel, este recunoscut faptul că o serie de infracțiuni nu pot fi cercetate în mod complet fără a apela la astfel de metode, precum cazurile de crimă organizată, terorism sau trafic de droguri[4].

Principial, problema infracțiunii provocate a fost întotdeauna între limitele statului de a cerceta săvârșirea unei infracțiuni, inclusiv prin metode care ar constitui, prin ele însele, infracțiuni și de a abuza de puterea sa într-un asemenea mod în care, în loc să prevină infracțiuni, creează criminalitate. S-a arătat că: „*dacă autoritățile statului, prin poliție sau prin informatori instigați de poliție, demarează o operațiune de a testa o persoană dacă ar comite o infracțiune într-o anumită situație, există o limită de la care acest demers devine o infracțiune creată de stat, iar pentru ca statul să creeze o infracțiune și apoi să tragă la răspundere penală o persoană constituie un teribil abuz de putere*"[5].

Acțiunea de provocare poate fi clasificată prin raportare la calitatea persoanei care realizează acțiunea față de acuzat în următoarele categorii: *i)* provocarea de către un agent al statului; *ii)* provocarea de către un privat cu interese comerciale și *iii)* provocarea realizată de un informator[6].

Provocarea de către un agent al statului are loc atunci când se realizează direct de către un investigator sub acoperire – lucrător operativ de poliție, care este angajat al statului și face

[1] *C. Olaru*, op. cit., p. 58.
[2] *N. Brady*, op. cit., p. 44.
[3] EWCA, cauza *Regina c. M.*, Dec. din 18 martie 2011, EWCA Crim 648, §18.
[4] *S. McKay*, Covert Policing, 2015, p. 270.
[5] *A. Ashworth, M. Redmayne*, The Criminal Process, 2014, p. 286.
[6] *C. Wells*, op. cit., p. 107.

parte din ramura executivă sau judiciară. Cu alte cuvinte, o astfel de provocare are loc prin persoanele care realizează investigațiile sub acoperire, fără ca acestea să fie implicate sau să fi fost implicate direct în alte activități infracționale. Aceasta este cea mai des întâlnită formă de provocare, fiind realizată de agenți ai poliției, cu autorizarea organelor judiciare competente.

Provocarea de către un privat cu interese comerciale a fost evidențiată în practică atunci când un particular – de regulă, un jurnalist – realizează în scop comercial, pentru publicația sa sau cea la care lucrează, operațiuni care ar putea fi clasificate ca investigații sub acoperire, obținând probe (de regulă, înregistrări) privind săvârșirea unor infracțiuni pe care, mai apoi, le pune la dispoziția organelor de urmărire penală. Acestea activități se realizează fără autorizarea, supravegherea sau aprobarea organelor de urmărire penală[1]. Într-o asemenea situație, nu vom putea vorbi de o infracțiune provocată, jurisprudența fiind constantă în acest sens, cu mențiunea că Curtea Europeană a Drepturilor Omului arată că, și în aceste situații, după caz, ar putea fi incidentă o încălcare a art. 6 Conv.EDO[2].

Provocarea de către un informator constă în acțiunea unei persoane care are legătură cu organele de poliție și, prin activitatea sa, sesizează pregătirea unei infracțiuni sau posibilitatea ca aceasta să fie comisă, contribuind efectiv la realizarea activităților sub acoperire[3]. Când discutăm de un informator, avem în vedere numai un informator care nu este autorizat în respectiva cauză și va avea calitatea despre care am făcut vorbire într-o secțiune precedentă[4]. Într-o cauză din Marea Britanie s-a constatat contribuția unui informator ca fiind o provocare în limitele legii (provocare la probă), atunci când a observat, pe ușa toaletei dintr-un tren, un mesaj al unei persoane care căuta fete între 8 și 13 ani pentru sex contra cost, lăsând un număr de telefon și cerând să fie contactat prin SMS sau telefonic. Informatorul a pretins că este o minoră și a intrat în conversații prin mesaje cu pedofilul, primind mesaje cu conținut sexual și invitații să se întâlnească, moment în care a sesizat organele de urmărire penală. Ulterior, poliția a realizat, printr-un investigator sub acoperire, o întâlnire cu pedofilul, acesta fiind arestat atunci când a ajuns la locația stabilită[5].

Doctrina engleză stabilește câțiva factori determinanți pentru constatarea existenței provocării: „*i) existența suspiciunii rezonabile privind existența unei activități infracționale ca un temei pentru acțiunea organelor de poliție (reprezentând un mecanism de control pentru verificarea bunei-credințe a poliției); ii) autorizarea legală și supravegherea acțiunii organelor de urmărire penală; iii) necesitatea și proporționalitatea măsurii folosite de poliție prin raportare la infracțiunea cercetată; iv) evidențierea conceptelor de «oportunitate neexcepțională» și «cauzație»; v) certificarea probelor obținute (convorbirile purtate, persoanele întâlnite etc.)*"[6].

Într-o altă abordare, doctrina arată că nu pot exista două cauze la fel, astfel că, pentru identificarea existenței unei provocări, trebuie să se răspundă la un set de întrebări, evident neexhaustive, prin care să se răspundă la aspecte esențiale, precum: este natura cazului una care să nu permită desfășurarea cercetărilor prin metode de cercetare obișnuite?; activitatea infracțională desfășurată are un caracter secret ori consensual (de pildă, acte sexuale cu un minor – n.n.) sau din alte motive este greu de descoperit?; există posibilitatea ca investigatorul să participe la săvârșirea infracțiunii și este posibilă determinarea unor limite peste care nu

[1] *Ibidem*, p. 115; CEDO, cauza *Shannon c. Marea Britanie*, Hotărârea din 6 aprilie 2004.
[2] CEDO, cauza *Shannon c. Marea Britanie*, Hotărârea din 6 aprilie 2004.
[3] *C. Wells*, op. cit., p. 117.
[4] *V. supra*, Titlul XII, Capitolul V.3.
[5] EWCA, cauza *Regina c. Ian Anthony Jones*, Dec. din 15 mai 2007, EWCA Crim 1118, pe *www.bailii.org*
[6] *D. Ormerod, D. Perry, P. Murphy (coord.)*, op. cit., p. 1419.

se poate trece, de la începutul cercetării?; acuzatului i se oferă o oportunitate neexcepțională de a săvârși infracțiunea? (ar fi comis infracțiunea și fără intervenția investigatorului sub acoperire?); a fost respectat principiul proporționalității prin raportare la nivelul de intruziune în viața privată?; există temeiuri suficiente pentru realizarea operațiunii sub acoperire și se fundamentează pe probe sau informații credibile?; investigatorii sub acoperire au acționat cu bună-credință?; au fost țintite persoane sau grupuri de persoane anume cu rea-credință?; este problema în cauză una cu caracter geografic sau într-o locație unde numai prin investigații sub acoperire se poate descoperi fapta? (de exemplu, în cartiere cu criminalitate organizată ridicată)[1].

În dreptul englez se arată că, deși săvârșirea unei infracțiuni provocate (*entrapment*) nu poate constitui o apărare pe fondul cauzei, în sensul de a putea influența existența și întrunirea elementelor constitutive ale infracțiunii, poate conduce la oprirea procedurii în fața instanței (*grant of stay* – regula) sau poate conduce la excluderea probelor obținute nelegal (ca excepție de la regulă)[2]. O atare abordare se bazează pe ideea că, deși persoanele acuzate sunt culpabile, decizia instanțelor de a opri procedura (chiar și permanent) sau de a exclude probe se bazează pe necesitatea respectării statului de drept (*rule of law*) și a păstrării integrității procesului penal, întrucât a judeca o persoană în asemenea circumstanțe ar constitui un afront la conștiința publică și o inechitate[3].

Pentru a nu fi considerată o infracțiune provocată, este necesar să se stabilească, asemenea jurisprudenței Curții Europene a Drepturilor Omului, că persoana cercetată avea intenția să săvârșească respectiva infracțiune sau o infracțiune de același fel[4]. Sub acest aspect, se face distincția între determinarea unei persoane să săvârșească o infracțiune și oferirea unei oportunități să încalce legea, iar dacă persoana în cauză profită de această oportunitate prezentată de organele de urmărire penală[5], atunci situația calificată ar fi cea de participare pasivă a organelor de urmărire penală, ceea ce nu va constitui provocare la infracțiune[6]. O atare situație a fost relevată în jurisprudența engleză atunci când organele de poliție au realizat o operațiune sub acoperire prin deschiderea unui amanet pentru care au creat, în cartierul în care se afla, reputația ca fiind ilegal, ocupându-se de vânzarea de bunuri furate, urmărind să descopere și să tragă la răspundere penală persoanele implicate în furturi și tâlhării din respectiva zonă, prin ademenirea lor în amanet, unde erau instalate camere de supraveghere, reușind să obțină condamnarea a 118 infractori[7]. Curtea de Apel a reținut în respectiva cauză că nu poate fi incidentă o provocare din partea poliției, întrucât niciunul dintre acuzați nu a fost obligat sau determinat să intre în amanet, investigatorii sub acoperire au fost controlați și li s-a amintit regulat că trebuie să se poarte într-un mod în care să nu instige persoanele, toată operațiunea fiind supravegheată și înregistrată, astfel că nimic din ceea ce au făcut investigatorii nu putea fi catalogat ca fiind nepotrivit[8].

---

[1] *S. McKay*, Covert Policing, 2015, pp. 271-272.

[2] *Ibidem*, p. 261; *D. Ormerod, D. Perry, P. Murphy (coord.)*, op. cit., p. 1419.

[3] *C. Wells*, op. cit., p. 105.

[4] UKHL, cauza *Regina c. Looseley*, UKHL 53, dec. din 25 octombrie 2001, §21, pe *www.bailii.org*

[5] *Ibidem*, §101.

[6] *J. Dworzecki, Š. Kočan*, Fighting Against Organized Crime With the Use of Agent Provocateur. The Experience of Slovak Republic. Outline of Issues, în Internal Security, vol. 10, no. 2/2018, p. 50.

[7] EWCA, cauza *Regina c. Palmer, Gyamfi, Cooke*, EWCA Crim 1861, Dec. din 7 august 2014.

[8] *Ibidem*, §79.

În general, pentru a exista provocare, este necesar ca investigatorul sub acoperire să realizeze o acțiune față de acuzat, constând într-o formă de persuasiune sau de constrângere, prin care să îl determine să săvârșească fapta[1]. Niciun act nu trebuie să aibă un anumit nivel, rezultatul putând fi obținut și prin cereri repetate, de pildă, s-a constatat o astfel de provocare când investigatorul sub acoperire a formulat cereri repetate unei persoane vulnerabile – dependentă de droguri – de a-i procura acestuia substanțe interzise și când, în final, persoana dependentă a achiesat, s-a organizat flagrantul și a fost trasă la răspundere penală[2]. În cazul în care nu există nicio constrângere sau nicio formă de persuasiune exercitată asupra acuzatului, nu se va putea reține incidența provocării la infracțiune[3].

Cele arătate mai sus definesc principalele caracteristici ale infracțiunii provocate și ale acțiunii de provocare ce vor constitui temei pentru excluderea probelor nelegal obținute, din perspectiva legii procesuale penale române. Astfel cum vom vedea în secțiunea următoare, majoritatea criteriilor de determinare a existenței provocării se vor reflecta din doctrină și jurisprudență în jurisprudența Curții Europene a Drepturilor Omului.

Secțiunea a 2-a. Condițiile de existență a provocării infracțiunii din perspectiva jurisprudenței Curții Europene a Drepturilor Omului

Jurisprudența Curții Europene a Drepturilor Omului este bogată în cazuistica privind problema provocării săvârșirii unei infracțiuni de către agenți ai statului, în vederea obținerii de probe în procesul penal. În esență, Curtea a subliniat ca principiu director ca agenții statului care desfășoară o anchetă proactivă să adopte o atitudine pasivă cu privire la infracțiunile pe care le constată, fără a li se permite să determine persoane să adopte un comportament infracțional.

Pentru existența infracțiunii provocate, este necesar ca acțiunea de provocare să fie desfășurată de organele de urmărire penală sau, în sens general, de un agent al statului care acționează în numele acestora (de pildă, un colaborator).

Întrucât problema provocării infracțiunii se află în strânsă legătură cu problema folosirii tehnicilor speciale de cercetare a unor infracțiuni, Curtea s-a pronunțat în sensul în care nu va constitui o încălcare a dreptului la un proces echitabil folosirea unor astfel de tehnici, însă acestea trebuie să fie limitate la scopul măsurii[4]. Acest scop trebuie să constea doar în dovedirea existenței infracțiunii, și nu determinarea unei persoane să comită o infracțiune pentru ca prin aceasta să fie dovedită însăși această infracțiune[5], indiferent de gravitatea faptei care face obiectul urmăririi penale sau de necesitatea de a asigura celeritatea în tragerea la răspundere penală a unei persoane[6]. În mod corect a constatat Curtea că, indiferent cât de grave sunt faptele, nu se poate justifica întrebuințarea provocării pentru apărarea interesului public, toate probele obținute trebuind să fie excluse[7].

---

[1] *D. Ormerod, D. Perry, P. Murphy (coord.)*, op. cit., p. 1420.

[2] *S. McKay*, Covert Policing, 2015, p. 270.

[3] *C. Wells*, op. cit., p. 106.

[4] CEDO, cauza *Ramanauskas c. Lituania*, Hotărârea din 5 februarie 2008, §51, pe *hudoc.echr.coe.int*

[5] *Ibidem*, §55; CEDO, cauza *Teixeira de Castro c. Portugalia*, Hotărârea din 9 iunie 1998, §38, pe *hudoc.echr.coe.int*

[6] *Ibidem*, §53; CEDO, cauza *Delcourt c. Belgia*, Hotărârea din 17 ianuarie 1970, §25, pe *hudoc.echr.coe.int*

[7] CEDO, cauza *Furcht c. Germania*, Hotărârea din 23 ianuarie 2015, §64.

În privința existenței unei provocări incompatibile cu art. 6 Conv.EDO, Curtea a stabilit anumite criterii pe baza cărora se va determina dacă a existat o provocare în săvârșirea unei infracțiuni, realizată de agenți sub acoperire ai statului.

În primul rând, este necesar să se dovedească faptul că persoana care a comis infracțiunea avea motive, inclinații sau hotărârea să comită respectivul tip de infracțiune, astfel ca fapta care face obiectul urmăririi penale să nu constituie doar o situație excepțională. Cu alte cuvinte, va fi interzisă provocarea realizată de agenți ai statului dacă persoana nu era bănuită în mod obiectiv de vreo activitate infracțională trecută sau avea o predispoziție în acest sens[1].

Între subcriteriile stabilirii lipsei unei suspiciuni obiective privind implicarea în activități infracționale, Curtea a amintit absența antecedentelor penale ale persoanei, faptul că nu s-a desfășurat anterior față de aceasta o urmărire penală, că nu era o persoană aflată în atenția poliției, că nu s-au găsit droguri la domiciliul acesteia și cantitatea de droguri aflată în posesia sa nu era mai mare decât cantitatea cerută de organele de poliție[2]. Într-o atare situație, s-a stabilit că acțiunile organelor de urmărire penală au depășit acțiunile care puteau fi autorizate (în cazul nostru, printr-o participare autorizată la anumite activități) și au procedat la instigarea unei persoane să comită infracțiunea. Toate aceste criterii trebuie să fie coroborate și trebuie să indice familiaritatea persoanei cu săvârșirea de infracțiuni.

Simplul fapt că o persoană are antecedente penale nu va fi suficient pentru a se considera că desfășoară în continuare activități ilicite atunci când nu este dovedită o predispoziție de a săvârși același tip de infracțiuni. Ca atare, nu s-a considerat a fi suficient ca dintre cei doi inculpați unul să fi avut antecedente penale legate de consumul ilicit de narcotice atunci când niciodată nu a existat vreo bănuială față de acesta că ar realiza și trafic de droguri[3]. Și în situația în care o persoană ar avea antecedente penale pentru același tip de infracțiune, este necesar ca organele de urmărire penală să fi cunoscut acest lucru la momentul realizării acțiunii de provocare[4], și nu să fi descoperit această împrejurare în cursul urmăririi penale.

Întrucât antecedentele penale reflectă numai existența unei fapte anterioare dovedite, ele nu vor fi la fel de relevante în a justifica o suspiciune față de o anumită persoană. În schimb, familiarizarea unei persoane cu modalitatea săvârșirii concrete a unei infracțiuni a fost considerată drept o dovadă a unei activități infracționale preexistente. Astfel de indicii constau în modalitatea de obținere a drogurilor (MDMA), a măsurilor de precauție luate de persoană pentru a evita primirea unor bani marcați de poliție (obligarea schimbării bancnotelor cu altele), remiterea prin interpuși a drogurilor către investigatorul sub acoperire și depunerea drogurilor într-o cutie poștală pentru a fi ridicate[5]. Din aceste împrejurări rezultă că persoana avea experiență în activitate, cunoscând riscurile evidente și a încercat să le evite, fapt care dovedește înclinația infracțională.

În cauzele de corupție va fi important ca organele de urmărire penală să fie încunoștințate de comiterea faptei într-una dintre formele sale – pretindere, de exemplu –, pentru a putea autoriza participarea autorizată la anumite activități și a surprinde în flagrant acțiunea de luare de mită. Curtea a stabilit că nu va exista o infracțiune provocată atunci când funcționarul a cerut, chiar și sub formă deghizată, o sumă de bani drept mită pentru ca, ulterior, la sesizarea

[1] CEDO, cauza *Bannikova c. Rusia*, Hotărârea din 4 februarie 2011, §38.

[2] CEDO, cauza *Teixeira de Castro c. Portugalia*, Hotărârea din 9 iunie 1998, §37-38.

[3] CEDO, cauza *Constantin și Stoian c. România*, Hotărârea din 29 decembrie 2009, §55, pe *hudoc.echr.coe.int*

[4] CEDO, cauza *Sepil c. Turcia*, Hotărârea din 12 februarie 2014, §34, pe *hudoc.echr.coe.int*

[5] CEDO, cauza *Virgil Dan Vasile c. România*, Hotărârea din 15 august 2018, §53, pe *hudoc.echr.coe.int*

persoanei de la care s-a pretins mita, să se realizeze un flagrant prin care funcționarul să primească suma de bani solicitată[1]. În același sens, Curtea a analizat atitudinea persoanei implicată în activități de corupție, în special privind posibilitatea ca persoana (care solicita un procentaj din proiectul de investiții) să poată să renunțe la activitatea infracțională în mai multe rânduri sau să încunoștințeze organele de urmărire penală că i se ofereau sume de bani de către investitorul străin[2].

În al doilea rând, în determinarea existenței unei infracțiuni provocate, va fi necesar să se stabilească dacă persoana a fost determinată să săvârșească infracțiunea. Cu alte cuvinte, va trebui să se verifice dacă inițiativa săvârșirii faptei a venit de la persoana vizată sau de la un agent al statului. Dacă inițiativa vine din partea persoanei urmărite penal, nu va avea importanță predispoziția sa la săvârșirea de infracțiuni. De pildă, o atare situație este dacă o persoană care nu era bănuită de comiterea de infracțiuni se oferă să vândă unui investigator sub acoperire o cantitate de droguri sau să ofere unui funcționar o sumă de bani[3]. Tot în acest sens, dacă o persoană contactează un colaborator al organelor de urmărire penală în vederea organizării unui transport de cocaină[4], ulterior colaboratorii participând la transportul ilicit, nu se va considera că a fost provocată în săvârșirea faptei, deoarece intenția inițială i-a aparținut[5]. În schimb, s-a stabilit că a existat o instigare din partea unui investigator sub acoperire atunci când, în lipsa elementelor arătate mai sus privind predispoziția către săvârșirea unei infracțiuni, investigatorul l-a sunat pe inculpat și i-a cerut să îi vândă o cantitate de droguri, astfel reținându-se provocarea la săvârșirea unei infracțiuni[6].

Tot din perspectiva inițiativei va trebui analizat și dacă provocarea realizată de agenții statului a presupus oferirea unei sume disproporționate de mari față de obiectele care făceau obiectul tranzacției. S-a considerat a fi un indiciu al existenței provocării atunci când agentul provocator a oferit și ulterior remis o sumă de 3.000 de euro pentru o cantitate de amfetamină, anterior obținând doar câteva mostre de substanță[7]. În cauza citată, decizia Curții s-a bazat și pe faptul că nu s-a putut dovedi în mod obiectiv că inculpatul avea o predispoziție pentru săvârșirea unor infracțiuni, în condițiile în care autoritățile statului au refuzat să pună la dispoziția Curții modul și criteriile în care au ajuns la concluzia implicării inculpatului în activități anterioare, pe motiv că ar afecta posibilitatea lor de a cerceta și alte fapte de trafic de droguri.

Instigarea la săvârșirea unei infracțiuni din partea investigatorilor sub acoperire poate căpăta și forme deosebit de perverse, prin apelul la compasiunea inculpatului și prin inducerea ideii că investigatorul suferă de sevraj și că s-ar putea sinucide dacă nu i se procură droguri[8].

În al treilea rând, în evaluarea existenței unei infracțiuni provocate, este necesar a se determina dacă gruparea infracțională a fost doar infiltrată de investigatorul sub acoperire sau că acesta a procedat la însăși instigarea desfășurării de activități ilicite. Dacă vom vorbi despre o acțiune de infiltrare și investigatorul realizează acte care vor fi autorizate de procuror prin

[1] CEDO, cauza *Gorgievski c. Macedonia*, Hotărârea din 10 decembrie 2009, §53, pe *hudoc.echr.coe.int*

[2] CEDO, cauza *Matanović c. Croația*, Hotărârea din 4 iulie 2017, §142-143, pe *hudoc.echr.coe.int*

[3] CEDO, cauza *Ramanauskas c. Lituania (nr. 2)*, Hotărârea din 20 mai 2018, §68, pe *hudoc.echr.coe.int*

[4] *D.-Șt. Paraschiv*, Pericolul creșterii traficului și consumului ilicit de stupefiante, în Acta Universitatis George Bacovia, vol. 5, nr. 1/2016, p. 3.

[5] CEDO, cauza *Sequeira c. Portugalia*, Hotărârea din 6 mai 2003, pe *hudoc.echr.coe.int*

[6] CEDO, cauza *Burak Hun c. Turcia*, Hotărârea din 15 martie 2010, §44, pe *hudoc.echr.coe.int*; în același sens, cauza *Sepil c. Turcia*, Hotărârea din 12 februarie 2014, §34.

[7] CEDO, cauza *Malininas c. Lituania*, Hotărârea din 1 octombrie 2010, §37, pe *hudoc.echr.coe.int*

[8] CEDO, cauza *Vanyan c. Rusia*, Hotărârea din 15 martie 2006, §11, pe *hudoc.echr.coe.int*

participarea autorizată la anumite activități, atunci probele derivate din activitățile desfășurate vor fi legal obținute. În Hotărârea *Milinienė c. Lituania*, Curtea a constatat că, într-o cauză de corupție în care inculpatul a lăsat să se înțeleagă că, pentru realizarea unui act (admiterea unei cereri de chemare în judecată), va fi nevoie să îi fie remise bunuri (o mașină nouă), persoana vătămată a formulat denunț, fiind mai apoi autorizată folosirea de tehnică de înregistrare asupra sa și sprijinind-o în demersurile sale în fața funcționarului corupt[1]. Prin această activitate, Curtea a constatat că organele de urmărire penală nu au avut o acțiune determinantă, ele alăturându-se acțiunii particularului desfășurată în legătură cu cea a inculpatului, ținându-se seama și de obligația organelor de urmărire penală de a da curs unei sesizări penale și de a combate efectul nociv al corupției judiciare.

În al patrulea rând, pentru a se determina existența sau nu a infracțiunii provocate, trebuie verificată existența unei autorizări din partea organelor de urmărire penală pentru realizarea participării autorizate la anumite activități. Aceasta nu va trebui să existe doar formal, impunându-se ca legiuitorul să stabilească, prin procedura de autorizare, reguli clare și previzibile pentru a fi autorizată o astfel de măsură. De pildă, legea română se ridică la acest standard în cazul operațiunilor privind drogurile, întrucât ele sunt amintite în cuprinsul art. 138 alin. (11) C.pr.pen., fiind previzibil pentru o persoană implicată în săvârșirea unei infracțiuni prevăzute de Legea nr. 143/2000, republicată, desfășurarea, de către organele de urmărire penală, a unor acțiuni ce vor fi încadrate ca participare autorizată la anumite activități. Cu toate acestea, este necesară autorizarea în prealabil a activităților desfășurate, neputându-se accepta ca acestea să se extindă asupra unei alte persoane decât cea avută în vedere inițial, fără a exista o autorizație distinctă[2]. În niciun caz nu vor putea fi folosite persoane în vederea organizării flagrantului, chiar și cele care au formulat plângere penală împotriva viitorului inculpat, în lipsa autorizării lor de către organul judiciar competent să desfășoare activități care se pot încadra ca tehnici speciale de cercetare. Într-o cauză judecată relativ recent[3], Curtea a stabilit că, deși o persoană a formulat o plângere penală împotriva unui funcționar public pentru săvârșirea unei infracțiuni de trafic de influență (sub forma pretinderii), organele de urmărire penală nu au obținut autorizarea instanței pentru folosirea persoanei care a făcut plângerea în calitate de colaborator, activitatea constituind o provocare la infracțiune.

În consecință, prin raportare la criteriile arătate mai sus și care rezultă din jurisprudența Curții Europene a Drepturilor Omului, se pot stabili limitele între care se poate realiza, în mod legal și în acord cu art. 6 Conv.EDO, metoda specială de participare autorizată la anumite activități, fără ca aceasta să constituie o provocare la săvârșirea de infracțiuni.

[1] CEDO, cauza *Milinienė c. Lituania*, Hotărârea din 24 septembrie 2008, §37-38, pe *hudoc.echr.coe.int*
[2] CEDO, cauza *Teixeira de Castro c. Portugalia*, Hotărârea din 9 iunie 1998, §38.
[3] CEDO, cauza *Tchokhonelidze c. Georgia*, Hotărârea din 28 septembrie 2018, §51, pe *hudoc.echr.coe.int*

Capitolul VI
Concluzii

Participarea autorizată la anumite activități reprezintă o metodă specială de cercetare introdusă prin Codul de procedură penală ca o metodă de investigație distinctă. Deși, legislativ, ar putea fi considerată o măsură specială autonomă, ea va face parte întotdeauna dintr-o urmărire penală în care se folosesc forme de investigație sub acoperire (prin investigatori, colaboratori, informatori), fiind de neconceput existența măsurii în afara unei asemenea situații. În loc să fi prevăzut o metodă specială distinctă, legiuitorul trebuia să condiționeze măsura de utilizarea investigatorilor sub acoperire și a colaboratorilor, sens în care apreciem ca fiind utilă necesitatea unei autorizări suplimentare în cazul în care un agent al statului trebuie să realizeze activități care ar avea caracter infracțional, pentru a se infiltra într-o organizație infracțională.

Deși Codul de procedură penală prevede posibilitatea autorizării unui organ de cercetare penală să realizeze participarea autorizată la anumite activități, în realitate, nu ar fi posibilă o atare situație, urmând a fi folosit un investigator sub acoperire dacă se dorește o acțiune din partea unui organ de poliție specializat, și nu a unui colaborator.

Cele arătate mai sus ne fac să concluzionăm că această metodă specială de cercetare reprezintă o formă mai invazivă decât utilizarea investigatorilor sub acoperire sau a colaboratorilor, ceea ce impune folosirea ei numai în cazuri în care este absolut necesară și numai dacă este proporțională cu restrângerea drepturilor fundamentale ale persoanei.

Întrucât presupune o activitate autorizată care ar îmbrăca forma unei fapte prevăzute de legea penală, este obligatoriu ca, prin activitatea sa, investigatorul sub acoperire sau colaboratorul să nu determine săvârșirea unei infracțiuni, ci trebuie să adopte numai o atitudine pasivă, cel mult să ofere persoanei cercetate doar o simplă oportunitate de a comite o infracțiune, fără a întreprinde nicio acțiune prin care să îl convingă să facă acest lucru.

Titlul XIV
Livrarea supravegheată

Capitolul I
Aspecte generale

Secțiunea 1. Utilitatea reglementării metodei speciale a livrării supravegheate

Metoda specială de cercetare a livrării supravegheate este un instrument investigativ prin care se permite ca un transport ilegal să intre, să tranziteze și să iasă de pe teritoriul unuia sau mai multor state, sub supravegherea autorităților competente, pentru a identifica toate componentele organizațiilor infracționale care există în statele de origine, tranzit sau destinație[1]. Aceasta diferă de metodele investigative clasice și de procedeele probatorii prin crearea posibilității descoperirii amplorii depline a infracționalității organizate. Dacă nu s-ar putea întrebuința o asemenea metodă de investigație, ar exista riscul ca obiectele transportate să fie descoperite și confiscate prematur și, astfel, să nu se poată proceda la identificarea liderilor unei grupări organizate sau destinatarilor finali ai transportului[2].

Față de celelalte metode speciale de supraveghere sau cercetare, trebuie să remarcăm caracterul strict specializat al măsurii de cercetare, apt să fie folosit numai în urmăriri penale care privesc transportul unor bunuri ilicite și reflectă un grad mare de complexitate. Caracterul său maxim de specializare este dat de regulile aparte stabilite în desfășurarea acesteia, dar și de caracterul său inerent transfrontalier și polițienesc, fiind mai degrabă o măsură polițienească decât una specifică urmăririi penale.

Originea livrării supravegheate constă în activitatea desfășurată de D.E.A.[3] față de exporturile de droguri din Europa de care au aflat prin alte metode de investigație, informând organele de urmărire penală din statele europene cu care S.U.A. întreținea relații amicale pentru a se permite transportul către acest din urmă stat[4]. Cu timpul, odată ce s-a aflat despre aceste operațiuni care se desfășurau la limita legalității, D.E.A. a asigurat organele de urmărire penală că persoanele care realizau transportul urmau să fie arestate și cercetate în țara de destinație și că drogurile urmau să fie confiscate și substituite în timpul transportului[5], procedându-se la „livrări curate”[6].

---

[1] *C. Olaru*, op. cit., p. 85.

[2] *I.M. De Lucas Martín, C.-E. Ștefan*, Livrările supravegheate transnaționale în contextul investigării traficului de droguri, Ed. Magic Print, București, 2016, p. 148, accesibil și online pe *www.mpublic.ro*

[3] U.S. Drug Enforcement Administration, agenție aflată în subordinea U.S. Department of Justice.

[4] *N. Boister*, An Introduction to Transnational Criminal Law, First Edition, Oxford University Press, Oxford, 2012, p. 168; *M. Ruiu, C. Dariciuc*, Metode și tehnici speciale de investigare a infracțiunilor de trafic de droguri, în Forum Criminalistic, vol. IX, nr. 1/2016, p. 31.

[5] *N. Boister*, op. cit., p. 168.

[6] Printr-o „livrare curată” vom înțelege o livrare controlată în care bunul suspect sau ilicit este sustras sau substituit la origine, pentru a diminua riscul pentru ordinea publică pe care îl presupune tehnica specială de investigare.

Noțiunea de „livrare supravegheată" a fost recunoscută internațional pentru prima dată prin Convenția ONU contra traficului ilicit de stupefiante și substanțe psihotrope din 1988[1], reflectând preocuparea internațională privind combaterea infracțiunilor grave, mai ales în domeniul traficului de droguri[2], domeniu în care își are aplicabilitatea cea mai largă această metodă specială de cercetare[3]. Necesitatea unei asemenea tehnici speciale este legată de faptul că un control național al traficului de droguri este imposibil de realizat dacă, la nivel internațional*: i)* statele nu controlează producția ilicită și traficul în teritoriile sale; *ii)* statele nu își coordonează eforturile pentru combaterea globală a fenomenului[4]. Ulterior, metoda specială a fost amintită ca metodă de investigație și în Convenția ONU împotriva criminalității transnaționale organizate din 2000[5], precum și în Convenția ONU împotriva corupției din 2003[6]. Este important a se menționa aceste trei convenții internaționale, întrucât, așa cum vom vedea în secțiunile următoare, până la adoptarea Codului de procedură penală, măsura putea fi aplicată numai în temeiul legislației speciale în domeniul combaterii traficului și consumului ilicit de droguri și combaterii criminalității organizate. Noțiunea de „livrare supravegheată" constituie o traducere a expresiei *controlled delivery* din limba engleză.

Metoda specială de cercetare va putea fi întrebuințată numai în cazul unui *transport de bunuri*, conform dispozițiilor art. 151 alin. (1) C.pr.pen., neputând fi utilizată în cazul în care se realizează un trafic de persoane. Acceptarea livrării supravegheate de persoane este problematică, întrucât activitatea desfășurată de organele de urmărire penală și organele care pun în aplicare măsura poate pune în pericol viața sau sănătatea persoanelor traficate, sens în care devine incidentă răspunderea statului ca urmare a omisiunii luării măsurilor pentru protejarea acestor persoane, în condițiile în care cunoșteau și monitorizau transportul. Din acest punct de vedere, livrarea supravegheată se va putea limita numai la bunuri (chiar și animale vii), dar nu va putea să privească vreodată persoane[7].

Nu vom putea să întrebuințăm metoda specială de cercetare în situațiile în care transportul de bunuri ar avea o aparență de legalitate sau ar presupune transportarea unor bunuri ușor identificabile prin modalitatea de amplasare în suportul de transport, decât în situația falsificării

[1] Conform art. 1 lit. k) din Convenția ONU contra traficului ilicit de stupefiante și substanțe psihotrope din 1988 (M. Of. nr. 341 din 30 decembrie 1992), „livrare supravegheată" se referă la „metodele care constau în permiterea trecerii prin teritoriul uneia sau mai multor țări a stupefiantelor sau substanțelor psihotrope, a substanțelor înscrise în tabelul I sau tabelul II, anexe la prezenta convenție, sau substanțelor care le sunt substituite, expediate în mod ilicit sau suspectate de aceasta, cu știința și sub controlul autorităților competente din țările indicate, în scopul identificării persoanelor implicate în comiterea infracțiunilor stabilite conform paragrafului 1 al art. 3 din convenție".

[2] *C. Fazey*, International Policy on Illicit Drug Trafficking: The formal and Informal Mechanisms, în Journal of Drug Issues, vol. 37, no. 4/2007, p. 760.

[3] *A.C. Moise*, Analysis of Offences Concerning Drug Trafficking in Romanian Legislation, în Law Review (Universul Juridic), vol. VIII, no. 2/2018, p. 215.

[4] *N. Boister*, op. cit., p. 50.

[5] Conform art. 2 lit. i) din Convenția ONU împotriva criminalității transnaționale organizate din 2000 (M. Of. nr. 813 din 8 noiembrie 2002), „livrarea supravegheată" se definește ca „metoda care constă în permiterea trecerii pe teritoriul unuia sau mai multor state a unor expedieri ilicite ori suspecte de a fi ilicite, cu știrea și sub controlul autorităților competente ale acestor state, în vederea anchetării unei infracțiuni și identificării persoanelor implicate în săvârșirea ei".

[6] Convenția ONU împotriva corupției din 2003 (M. Of. nr. 903 din 5 octombrie 2004) preia în cuprinsul art. 2 lit. i) aceeași definiție a metodei de investigare ca în cazul Convenției ONU împotriva criminalității transnaționale organizate.

[7] *A.M. Matyshova*, Covert Investigative Activities in Kazakhstan: Purpose, Occurring Conflicts and Ways of their Overcoming, în Journal of Advanced Research in Law and Economics, vol. VII, no. 3/2016, p. 557.

documentelor de proveniență (autoturisme sau utilaje furate). Metoda specială de cercetare va fi aptă să ajute investigațiile când bunurile transportate au fost ascunse sau disimulate în mijlocul de transport ori se realizează o livrare a unui bun fără ca acesta să fie însoțit (un colet[1], un container naval etc.).

Nu este exclus ca livrarea supravegheată să privească transportul realizat de o persoană prin bunurile aflate asupra sa, această situație fiind prevalentă atunci când persoana se deplasează cu bagaje sau prin disimularea existenței bunurilor în haine sau în cavitățile corporale.

Asupra modului de deplasare al transportului, livrarea supravegheată nu se poate considera că este o metodă specială de cercetare restrânsă la vreun mijloc de transport, ea putând fi întrebuințată în mod universal. Aeroporturile rămân cel mai important punct de intrare a drogurilor folosit de grupurile de criminalitate organizată, astfel că măsura va trebui să aibă în vedere și monitorizarea zborurilor suspectate că ar fi folosite pentru transportul de bunuri ilicite[2]. Nu trebuie uitat și faptul că, pentru transportul unor cantități mari de droguri, se vor folosi containere de transport marfă[3] sau metode mai exotice, precum narco-submarine[4], ori simple nave maritime închiriate[5]. Transportul feroviar va putea fi incident în cazul în care se folosește un tren de marfă pentru transportul unor bunuri voluminoase sau un container maritim preluat din port.

Cea mai complicată modalitate de realizare a livrării supravegheate va fi incidentă atunci când vom avea un transport rutier, întrucât, spre deosebire de celelalte mijloace de transport, acesta se va putea opri în orice moment, se va putea ascunde și astfel să conducă la eșecul operațiunii[6]. În cazul transportului maritim și aerian, aceste riscuri sunt mai puțin incidente, dar nu trebuie excluse, mai ales în cazul transporturilor maritime.

Livrarea supravegheată se va putea realiza atât pe teritoriul național, cât și pe teritoriul mai multor state prin care tranzitează transportul, putând fi demarată și pusă în aplicare începând cu statul de origine al transportului[7]. În situația unei livrări supravegheate cu caracter transfrontalier, activitățile desfășurate vor constitui o formă de cooperare internațională în materie penală, măsurile fiind aplicate de autoritățile judiciare (și/sau de poliție) din alte state[8]. Din această privință, includerea în Codul de procedură penală a livrării supravegheate va familiariza și organele de urmărire penală cu măsura, în cazul în care acestea vor trebui să

[1] Trib. Ilfov, s. pen., sent. nr. 33 din 4 februarie 2016, pe *portal.just.ro*

[2] *I.M. De Lucas Martín, C.-E. Ștefan*, op. cit., p. 25.

[3] Pentru combaterea acestui tip de transport, UNODC (Oficiul Națiunilor Unite pentru Droguri și Criminalitate) și WCO (Organizația Mondială a Vămilor) au demarat, în 2004, inițiativa comună denumită *Container Control Programme*, prin care s-a constituit o rețea de prevenire a traficului de bunuri în peste 50 de state și cu peste 100 de unități de control în porturi pentru a permite libera circulație între autorități a informațiilor privind containerele transportate. Rezultatele au fost semnificative, atât privind traficul de droguri, cât și de arme, alcool, țigări, obiecte contrafăcute etc. – *www.unodc.org*

[4] În special pentru transportul cocainei pe mare, sunt întrebuințate astfel de submarine, de regulă, construite ad-hoc de grupări de crimă organizată și folosite pentru transportul unor cantități mari de droguri. Un caz recent a fost descoperit în luna noiembrie 2019, când, în Spania, a fost depistat un submarin care transporta 3.000 de kg de cocaină cu destinația Marea Britanie; a se vedea Cocaine seized from "narco-submarine" in Spain was likely headed for UK, pe *www.theguardian.com*

[5] *J.S. Beittel*, Mexico: Organized Crime and Drug Trafficking Organizations, în Congressional Research Service Report, 2019, p. 5, pe *fas.org*

[6] Trib. Dolj, s. pen., sent. nr. 327 din 7 martie 2014, pe *portal.just.ro*

[7] *C. Olaru*, op. cit., p. 89.

[8] *Gh. Mateuț*, Procedură penală, 2019, p.732.

aplice această măsură la solicitarea unor alte state, în condițiile legii române pentru segmentul de tranzit pe teritoriul României.

Considerăm că reglementarea acestei metode speciale de cercetare a fost făcută doar pentru combaterea criminalității infracționale organizate, neputând fi aplicabilă unor infracțiuni care nu sunt comise în cadrul unui astfel de grup. În condițiile în care livrarea supravegheată poate fi incidentă numai în situația existenței unui transport de bunuri, va fi necesară implicarea mai multor persoane în întreaga operațiune – persoane care obțin bunurile transportate, persoane care se ocupă de încărcarea mărfurilor transportate, șoferii sau piloții folosiți pentru conducerea mijloacelor de transport folosite, dar și persoanele care se află la destinația transportului sau cele care vor asigura distribuția bunurilor odată ce ele au fost primite. Față de elementele constitutive ale infracțiunii de constituirea unui grup infracțional organizat prevăzută de art. 367 C.pen., regăsim în mod facil elemente din definiția „grupului infracțional organizat" – numărul minim de persoane (trei), constituirea pentru o anumită perioadă de timp, acțiunea coordonată și scopul comiterii uneia sau mai multor infracțiuni. Va fi deosebit de dificil să găsim infracțiuni de transport ilegal de bunuri la nivel transfrontalier fără ca acestea să fie realizate de un grup infracțional, într-o atare situație, fiind suficientă prinderea persoanei care transportă bunurile pentru dovedirea faptei și prinderea infractorilor[1].

În relevarea utilității metodei speciale de supraveghere, va trebui să avem în vedere și caracterul său subsidiar față de alte metode de investigație, nefiind necesar sau propice în cazul infracționalității de gravitate redusă. De pildă, nu va fi necesară o astfel de măsură în cazul unui transport ilegal de lemne tăiate ilegal din pădure, fiind suficientă depistarea persoanelor care au realizat tăierile și apoi transportul.

Secțiunea a 2-a. Livrarea supravegheată în legi speciale înainte de intrarea în vigoare a Codului de procedură penală

Anterior intrării în vigoare a Legii nr. 135/2010 privind Codul de procedură penală, tehnica specială de investigație a livrării supravegheate nu era cuprinsă în Codul de procedură penală din 1968, putând fi întrebuințată numai în cauze de gravitate ridicată și în condițiile legislației speciale. Autorizarea metodei speciale nu se putea face de către procurorul care supraveghea sau efectua urmărirea penală, ci numai de către procurorul desemnat de procurorul general al P.I.C.C.J.

Legislația actuală constituie un amestec format din prevederile diferite din legislația specială care au fost combinate de legiuitor pentru a rezulta o metodă specială de cercetare unitară. Cu toate acestea, astfel cum vom vedea în secțiunile următoare, vor exista unele reminiscențe ale formelor vechi, care nu mai sunt justificate în prezent.

Fiindcă metoda specială de cercetare a fost gândită inițial pentru combaterea traficului transfrontalier de narcotice, vom începe cu Legea nr. 143/2000 privind prevenirea și combaterea traficului și consumului ilicit de droguri în forma avută anterior intrării în vigoare a Codului de procedură penală.

Potrivit art. 1 lit. j) din Legea nr. 143/2000, prin „livrarea supravegheată" se înțelegea „*metoda folosită de instituțiile sau organele legal abilitate, cu autorizarea și sub controlul procurorului, care*

[1] *S. Ruggeri (coord.)*, Transnational Inquiries and the Protection of Fundamental Rights in Criminal Proceedings. A study in Memory of Vittorio Grevi and Giovanni Tranchina, Ed. Springer, Berlin, 2013, p. 85.

constă în permiterea trecerii sau circulației pe teritoriul țării de droguri ori precursori, suspecți de a fi expediați ilegal, sau de substanțe care au înlocuit drogurile ori precursorii, în scopul descoperirii activităților infracționale și al identificării persoanelor implicate în aceste activități". După cum putem observa, definiția conținea mai multe elemente care sunt prevăzute la acest moment în lege, precum: referirea la punerea în aplicare de către instituțiile sau organele legal abilitate (care controlează transportul, tranzitul frontierei etc.), controlul procurorului asupra măsurii, permiterea trecerii sau circulației pe teritoriul țării, dar și scopul descoperirii activităților infracționale și identificării persoanelor implicate în aceste activități.

În ceea ce privește procedura de autorizare a livrării supravegheate, aceasta era prevăzută într-un mod simplist prin art. 20 din Legea nr. 143/2000, în care se arăta că: „*Parchetul de pe lângă Curtea Supremă de Justiție poate autoriza, la solicitarea instituțiilor sau organelor legal abilitate, efectuarea de livrări supravegheate, cu sau fără substituirea totală a drogurilor ori a precursorilor*". Regăsim elemente din legislația curentă în textul legal citat, respectiv *necesitatea existenței unei solicitări din partea instituțiilor și organelor legal abilitate* (competente) și *posibilitatea substituirii totale a drogurilor și precursorilor*.

În privința existenței unei solicitări din partea instituțiilor sau organelor legal abilitate, textul arătat se referă la o sesizare din partea procurorului care efectuează urmărirea penală în vederea autorizării livrării supravegheate în cursul unei urmăriri penale desfășurate de organele de urmărire penală române sau la o cerere din partea organelor de urmărire penală dintr-un stat solicitant străin de a se autoriza livrarea supravegheată în România, în vederea sprijinirii urmăririi penale desfășurate de acestea. Fiind o tehnică specială de investigație a infracțiunilor privind traficul și consumul ilegal de droguri prevăzută atât de lege, cât și de tratatele internaționale, ea nu putea fi dispusă decât în contextul desfășurării unei urmăriri penale.

Posibilitatea substituirii parțiale sau integrale a bunurilor care fac obiectul livrării, prevăzută de art. 151 alin. (1) C.pr.pen., își are originea în mențiunea anterior prevăzută în cuprinsul art. 20 din Legea nr. 143/2000. Sub acest aspect, trebuie reținut că acțiunea de substituire are o importanță deosebită atunci când obiectele supuse transportului prezintă un pericol deosebit dacă sunt puse în circulație – droguri, precursori, arme, medicamente contrafăcute etc. De regulă, nu este necesar ca drogurile să fie păstrate în transport în integralitatea lor, date fiind riscurile inerente ale metodei speciale de cercetare, fiind preferabil ca o parte sau toată cantitatea să fie confiscată și substituită cu o substanță similară, pentru a nu fi sesizată lipsa drogurilor.

În Legea nr. 143/2000 se prevedea numai posibilitatea substituirii totale a drogurilor sau precursorilor, fără a fi menționată ipoteza substituirii parțiale. În interpretarea noastră, se putea realiza și o substituire parțială, sub acest aspect, textul Codului de procedură penală în vigoare cuprinde expres substituirea parțială a obiectelor transportate.

Continuând cu legislația specială în domeniul combaterii criminalității organizate, livrarea supravegheată era prevăzută și în cuprinsul Legii nr. 39/2003 privind prevenirea și combaterea criminalității organizate în forma aplicabilă dinainte de intrarea în vigoare a Codului de procedură penală. Deși legea nu conține o definiție a „livrării supravegheate", autorizarea metodei speciale de cercetare este reglementată mai bine.

Potrivit art. 16 alin. (1) din Legea nr. 39/2003, articol abrogat în prezent: „*Procurorul desemnat de procurorul general al Parchetului de pe lângă Curtea Supremă de Justiție poate autoriza, la solicitarea instituțiilor sau a organelor legal abilitate, efectuarea de livrări supravegheate, cu sau fără sustragerea sau substituirea totală ori parțială a bunurilor care fac obiectul livrării*".

În mod similar cu Legea nr. 143/2000, atributul de autorizare aparținea procurorului general al P.I.C.C.J., acesta desemnând un procuror (inclusiv putându-se desemna pe sine însuși) pentru autorizarea unor astfel de metode speciale de cercetare. Din nou, observăm că se face menţiunea că autorizarea se va da la *solicitarea instituţiilor sau a organelor legal abilitate*, sens în care facem trimitere la cele arătate mai sus. Față de Legea nr. 143/2000, în Legea nr. 39/2003, s-a prevăzut în mod expres că se poate realiza o substituire parțială a bunurilor care fac obiectul transportului supus livrării supravegheate. Observăm că în cuprinsul textului de lege arătat nu se face nicio trimitere la infracțiunile care trebuie să facă obiectul urmăririi penale pentru a fi autorizată o astfel de măsură, în opinia noastră, livrarea supravegheată putând fi aplicabilă numai în situația în care faptele erau între cele cuprinse în Legea nr. 39/2003.

În ceea ce privește conținutul ordonanței prin care se autoriza livrarea supravegheată, potrivit art. 16 alin. (2) din Legea nr. 39/2003, articol abrogat în prezent: „*livrarea supravegheată este autorizată prin ordonanță motivată care trebuie să cuprindă, pe lângă menţiunile prevăzute la art. 203 din Codul de procedură penală, următoarele: a) indiciile temeinice care justifică măsura și motivele pentru care măsura este necesară; b) detalii cu privire la bunurile care fac obiectul livrării supravegheate și, după caz, la bunurile care urmează a fi sustrase ori substituite, precum și la bunurile care urmează a le înlocui pe acestea; c) timpul și locul efectuării livrării sau, după caz, itinerarul ce urmează a fi parcurs în vederea efectuării livrării, dacă acestea sunt cunoscute; d) datele de identificare a persoanelor autorizate să supravegheze livrarea*". Comparând dispozițiile citate menționate, observăm că au fost preluate în integralitatea lor în cuprinsul art. 151 alin. (5) C.pr.pen., motiv pentru care facem trimitere la explicațiile care vor fi date privind procedura de autorizare a livrării supravegheate[1].

Un ultim aspect privind livrarea supravegheată reglementată prin Legea nr. 39/2003 era limitarea adusă aplicării măsurii în cazul în care ar fi putut afecta valori sociale importante. Potrivit art. 16 alin. (3) din Legea nr. 39/2003, articol abrogat în prezent: „*nu se poate autoriza efectuarea livrărilor supravegheate în cazul în care prin acestea s-ar pune în pericol siguranța națională, ordinea sau sănătatea publică*". O atare prevedere apreciem că era necesară și în cazul legislației actuale, fiind un filtru de proporționalitate cu privire la aceste valori. Este firesc că nu se pot accepta situații în care prin aducerea în țară a unor obiecte periculoase din străinătate să fie pusă în pericol siguranța statului sau ordinea publică, întrucât organele de urmărire penală sunt datoare să protejeze aceste valori superioare necesității descoperirii și prinderii tuturor persoanelor implicate. De pildă, nu s-ar fi putut concepe o livrare supravegheată care ar fi permis intrarea pe teritoriul țării a unei bombe, care putea fi detonată de persoana care o transporta, într-o asemenea situație, aceasta trebuind să fie neutralizată cât mai rapid.

Legislația specială penală nu mai includea alte situații în care să poată fi întrebuințată livrarea supravegheată, cu menţiunea că au existat și încă există menţiuni specifice privind punerea în aplicare a metodei speciale de cercetare, acestea urmând a fi tratate separat în prezenta lucrare.

În cazul ambelor legi speciale, observăm că lipsește orice dispoziție legală cu privire la caracterul justificat al acțiunilor care vor fi întreprinse de persoanele care pun în aplicare livrarea supravegheată, fapt care face superioară legea procesuală penală nouă, în care se prevede că punerea în aplicarea a livrării supravegheate nu constituie infracțiune.

Abrogarea tuturor metodelor speciale de cercetare din legislația specială era necesară pentru crearea unui cadru unitar pentru cercetarea infracțiunilor, astfel că legiuitorul a ales în mod

[1] *V. infra*, Titlul XIV, Capitolul IV.

inspirat ca diferitele dispoziții – chiar dacă aveau în vedere aceeași măsură – să fie abrogate. În același timp, s-a avut în vedere și necesitatea explicitării caracteristicilor și condițiilor pentru realizarea livrării supravegheate, inclusiv prin includerea unei cauze justificative exprese. Cu toate acestea, perspectiva istorică asupra reglementării măsurii ne arată că aceasta a fost gândită pentru prevenirea și combaterea unor infracțiuni grave, precum traficul de narcotice și infracțiunile de criminalitate organizată. Dincolo de gravitatea faptelor, complexitatea acestora poate fi una deosebită, impunând organelor de urmărire penală să folosească măsuri de supraveghere a transporturilor pentru descoperirea și prinderea întregii grupări implicate în săvârșirea de infracțiuni.

Secțiunea a 3-a. Livrarea supravegheată în Codul de procedură penală

Prin Legea nr. 135/2010 privind Codul de procedură penală s-a realizat unificarea măsurilor de investigație prevăzute fragmentat în legislația specială, prin introducerea unei metode speciale de cercetare unitare privind livrarea supravegheată. Între textele care reglementau metoda specială de cercetare în forma Codului de procedură penală adoptată de Parlament și textele care o reglementează nu există diferențe numeroase, ele urmând să fie analizate în secțiunea aceasta.

Mai întâi, trebuie să precizăm faptul că definiția legală a „livrării supravegheate" nu cunoaște modificări, păstrându-și aceleași caracteristici ca sub legislația anterioară și este în acord cu convențiile internaționale la care am făcut trimitere mai sus.

Conform art. 138 alin. (12) C.pr.pen., „*prin «livrare supravegheată» se înțelege tehnica de supraveghere și cercetare prin care se permit intrarea, circulația sau ieșirea de pe teritoriul țării a unor bunuri în privința cărora există o suspiciune cu privire la caracterul ilicit al deținerii sau obținerii acestora, sub supravegherea ori cu autorizarea autorităților competente, în scopul investigării unei infracțiuni sau al identificării persoanelor implicate în săvârșirea acesteia*".

Ca o primă critică adusă, legiuitorul se referă la livrarea supravegheată ca fiind o *tehnică*, și nu o *metodă*, astfel că există o necorelare apărută la momentul adoptării legii de punere în aplicare a Codului de procedură penală, prin care tehnicile speciale de supraveghere sau cercetare au fost redenumite „metode speciale de supraveghere sau cercetare". Nu există nicio consecință a acestei erori, de altfel, în opinia noastră, întreg capitolul studiat putea să își păstreze denumirea adoptată de Parlament inițial, expresia de „tehnici speciale" fiind întrebuințată anterior intrării în vigoare a Codului.

Metoda specială este considerată a fi *de supraveghere și cercetare*, fapt care constituie o eroare din partea legiuitorului, întrucât măsura este una de cercetare, și nu de supraveghere. Conform concepției legiuitorului, prin „metode speciale de supraveghere" vom înțelege numai supravegherea tehnică astfel cum ea este definită de art. 139 alin. (13) C.pr.pen. Deși există o componentă du supraveghere în livrarea supravegheată, același lucru poate fi spus despre toate metodele speciale de supraveghere sau cercetare.

Prin raportare la scopul prevăzut de legiuitor, cel al *investigării unei infracțiuni sau al identificării persoanelor implicate în săvârșirea acesteia*, rezultă caracterul de metodă de investigare a livrării supravegheate, aceasta neputând fi considerată un procedeu probatoriu, întrucât nu va conduce la obținerea directă de probe.

În ceea ce privește condițiile de autorizare și procedura de autorizare a măsurii, Codul de procedură penală împrumută prevederile cuprinse în legislația specială în vigoare înainte

de intrarea în vigoare a Codului de procedură penală, în special cele din Legea nr. 39/2003. Observăm că, în forma inițială a metodei speciale de cercetare, adoptată și, ulterior, intrată în vigoare până la adoptarea O.U.G. nr. 18/2016, nu exista nicio prevedere privind posibilitatea de a substitui, în tot sau în parte, obiectele traficate cu obiecte înlocuitoare, lipsind o prevedere pe care o avea livrarea supravegheată reglementată în Legea nr. 39/2003. Conform formei actuale a art. 151 alin. (1) C.pr.pen., „*livrarea supravegheată poate fi autorizată, prin ordonanță, de către procurorul care supraveghează sau efectuează urmărirea penală, la solicitarea instituțiilor sau organelor competente, cu sau fără sustragerea ori substituirea totală sau parțială a bunurilor care fac obiectul livrării*". Necesitatea includerii posibilității sustragerii și substituirii bunurilor era necesară pentru ca organele de urmărire penală să se asigure de înlăturarea pericolului pentru ordinea publică sau pentru persoanele vătămate (în cazul unor obiecte furate), pe care îl constituie deținerea bunurilor de către persoanele vizate de măsură[1]. Astfel, chiar și în situația în care livrarea supravegheată nu își va atinge obiectivele propuse prin planul procurorului, cel puțin bunurile transportate vor rămâne în custodia organelor de urmărire penală.

Potrivit formei inițiale a dispozițiilor art. 151 C.pr.pen. și până la adoptarea O.U.G. nr. 18/2016, livrarea supravegheată nu se putea dispune dacă avea în vedere transporturi de obiecte exclusiv pe teritoriul țării, trebuind ca întotdeauna măsura să aibă caracter transfrontalier, întrucât art. 151 alin. (3) C.pr.pen. prevedea, ca în prezent, necesitatea îndeplinirii unor condiții legale speciale cu privire la autoritățile din statele străine tranzitate. Având în vedere contextul în care a apărut la nivel internațional metoda specială de cercetare, era firesc ca aceasta să aibă un caracter preponderent internațional. Chiar și în prezent, apreciem că justificarea existenței reglementării livrării supravegheate naționale are o importanță redusă, absența ei putând fi compensată prin alte metode speciale de supraveghere sau cercetare.

O ultimă modificare legislativă a fost schimbarea condițiilor pe care trebuie să le îndeplinească ordonanța procurorului prin care se autorizează livrarea supravegheată, aceasta având loc tot ca urmare a adoptării O.U.G. nr. 18/2016. Conform art. 151 alin. (5) C.pr.pen., „*pentru fiecare livrare supravegheată procurorul emite câte o ordonanță, care trebuie să cuprindă, pe lângă mențiunile prevăzute la art. 286 alin. (2): a) numele suspectului sau inculpatului, dacă sunt cunoscute; b) motivele concrete care justifică măsura; c) indicarea bunurilor care fac obiectul livrării supravegheate și a dovezilor din care rezultă caracterul ilicit al acestora, a bunurilor care urmează a fi sustrase sau substituite, precum și a bunurilor care urmează a le înlocui pe acestea, după caz; d) timpul și locul efectuării livrării sau, după caz, itinerarul ce urmează a fi parcurs în vederea efectuării livrării, dacă acestea sunt cunoscute; e) modalitățile în care va fi efectuată supravegherea; f) datele de identificare a persoanelor autorizate să supravegheze livrarea*". Anterior, ordonanța de autorizare a procurorului trebuia să conțină, în plus față de mențiunile cuprinse la art. 286 alin. (2) C.pr.pen., „*numele suspectului sau inculpatului, dacă sunt cunoscute*, *dovezile din care rezultă caracterul ilicit al bunurilor ce urmează să între, să tranziteze sau să iasă de pe teritoriul țării* și *modalitățile în care va fi efectuată supravegherea*". Sub acest aspect, forma în vigoare anterior adoptării O.U.G. nr. 18/2016 constituia un regres față de legislația specială anterioară, în care erau prevăzute condiții suplimentare. Din fericire, legiuitorul delegat a observat acest neajuns și a completat legea prin preluarea mențiunilor speciale ce trebuiau cuprinse în ordonanța procurorului emisă potrivit art. 16 alin. (2) din Legea nr. 39/2003, în forma în vigoare anterioară datei de 1 februarie 2014.

[1] *C. Olaru*, op. cit., p. 89.

Capitolul II
Natura juridică a livrării supravegheate

Livrarea supravegheată constituie o tehnică specială de investigare a unor categorii de infracțiuni asociate, de regulă, cu traficul transfrontalier de bunuri sau substanțe interzise, fapte pentru care a și fost gândită măsura. Fiind înrudită cu utilizarea investigatorilor sub acoperire și a colaboratorilor, trebuie să apreciem dacă această măsură va avea ca finalitate obținerea unei probe sau doar va putea facilita obținerea de probe în procesul penal prin procedee probatorii derivate din aceasta. Cu alte cuvinte, se impune a se stabili dacă livrarea supravegheată constituie un procedeu probatoriu sau este doar o tehnică specială de investigații.

Din definiția „livrării supravegheate" conținută de art. 138 alin. (12) C.pr.pen. rezultă că scopul măsurii îl constituie „*investigarea unei infracțiuni sau identificarea persoanelor implicate în săvârșirea acesteia*". Spre deosebire de alte metode speciale de supraveghere sau cercetare, nu se indică că scopul îl constituie obținerea de mijloace de probă, fapt care ne conduce, cel puțin din definiția măsurii, la ideea că aceasta nu este aptă să furnizeze direct probe în procesul penal.

Nici din cuprinsul art. 151 C.pr.pen. nu rezultă că livrarea supravegheată ar constitui un procedeu probatoriu, întrucât nu se evidențiază niciun mijloc de probă care ar rezulta în urma punerii în executare a măsurii. Au existat opinii multiple cu privire la această problemă, o parte dintre autori susținând că procesul-verbal întocmit la finalizarea livrării supravegheate va constitui un mijloc de probă, alții susținând că acesta nu va putea constitui un mijloc de probă.

Prima opinie consideră că „*mijlocul de probă în care sunt consemnate atât datele obținute cu prilejul livrării supravegheate, cât și modul în care a fost pusă în executare măsura, este procesul-verbal întocmit de persoanele autorizate de procuror să ducă la îndeplinire măsura*"[1]. Neajunsul acestei opinii este că omite faptul că acest proces-verbal nu este întocmit de un organ de urmărire penală, ci de un organ al statului care pune în aplicare o măsură de cercetare. Mai mult, se omite faptul că procurorul este cel care stabilește, coordonează și controlează modul de aplicare, procesul-verbal fiind întocmit de organele care pun în aplicare măsura pentru a informa procurorul asupra modului de îndeplinire a sarcinilor, nu pentru ca acest proces-verbal să constituie un mijloc de probă. În același timp, trebuie să fie avută în vedere și împrejurarea că livrarea supravegheată va presupune participarea mai multor organe ale statului, ținând cont că livrarea supravegheată va implica trecerea bunurilor prin circumscripția teritorială a mai multor organe, fiecare trebuind să întocmească un astfel de proces-verbal. De pildă, până la trecerea frontierei de stat, livrarea supravegheată va putea fi pusă în aplicare de către organele de poliție, la frontieră, măsura fiind preluată pentru a fi pusă în aplicare de poliția de frontieră și autoritatea vamală care, la rândul lor, vor transfera această măsură către organele din statul străin. În ultimul rând, textul art. 151 alin. (8) C.pr.pen. se referă numai la activitățile desfășurate pe teritoriul României, nu și la activitățile din statul de origine, statul de tranzit, față de care nu există prevăzută o astfel de obligație.

A doua opinie apreciază că „*procesul-verbal nu constituie mijloc de probă. El va putea fi folosit însă de organul de urmărire penală în vederea obținerii probelor cu respectarea regulilor*

[1] *M. Bulancea, R. Slăvoiu*, în M. Udroiu (coord.), Codul de procedură penală, 2017, p. 734; în același sens, *C.M. Chiriță*, în N. Volonciu, A.S. Uzlău (coord.), Noul Cod, 2014, p. 344.

procedurale, în condițiile legii"[1]. Apreciem că această opinie este corectă și are în vedere atât rolul organelor de urmărire penală în administrarea probelor, cât și natura reală a metodei speciale de cercetare, aceea de a fi o tehnică specială de investigare prin care se creează oportunitatea administrării de probe și a obținerii de informații.

Livrarea supravegheată nu trebuie să fie înțeleasă ca fiind rezumată numai la activitățile cuprinse în art. 151 C.pr.pen., aceasta presupunând un complex de acțiuni cu finalitatea de a obține probe în procesul penal. Condiția ca transportul să fie supravegheat presupune ca procurorul să facă toate demersurile pentru autorizarea metodelor speciale de supraveghere tehnică în cauză pentru a se asigura de monitorizarea operațiunii. Ca atare, va fi importantă localizarea sau urmărirea prin mijloace tehnice a transportului [prin dispozitive amplasate pe mijlocul de transport, în sensul art. 138 alin. (7) C.pr.pen.], supravegherea video, audio sau prin fotografiere. Aceste metode speciale de supraveghere vor constitui procedee probatorii prin care organele de urmărire penală vor dovedi transportul ilicit, traseul urmărit, persoanele care au participat sau cu care s-a interacționat etc.

Finalitatea livrării supravegheate va trebui să o constituie organizarea flagrantului, care va asigura obținerea de probe și prinderea traficanților. Astfel, s-a reținut că „*operațiunile de prindere în flagrant implică prinderea traficanților de droguri la momentul efectuării tranzacțiilor, atunci când intră în posesia transporturilor de droguri, a sumelor de bani derivate din vânzarea drogurilor livrate într-o operațiune supravegheată, atunci când deschid coletele poștale într-o operațiune supravegheată etc.*"[2]. Cea mai importantă fază a livrării supravegheate va fi lăsată la latitudinea organelor de urmărire penală, în funcție de acțiunile – imprevizibile, de altfel – ale persoanelor care realizează transportul. Momentul la care se realizează flagrantul va fi influențat de informațiile obținute prin intermediul monitorizării transportului supus livrării supravegheate, procurorul trebuind să fie pregătit ca oricând să intervină, să sisteze măsura și să organizeze flagrantul. În cadrul acestei proceduri se vor putea obține probe privind existența obiectelor transportate, a persoanelor care sunt implicate și, în special, a destinatarului, putând fi obținute probe care pot conduce la tragerea la răspundere penală a mult mai multor persoane decât dacă transportul ar fi fost oprit la debutul călătoriei sale.

În concluzie, apreciem că metoda specială de cercetare a livrării supravegheate nu constituie un procedeu probatoriu, ci doar o tehnică de investigare prin care se realizează cadrul necesar administrării unor probe derivate din informațiile obținute prin supraveghere tehnică și prin organizarea flagrantului. Ca atare, metoda specială de cercetare va putea fi întrebuințată pentru a furniza *informații* organelor de urmărire penală care pot sta la baza administrării de probe, în condițiile legii.

[1] *Gh. Mateuț*, Procedură penală, 2019, p. 733.
[2] *I.M. De Lucas Martín, C.-E. Ștefan*, op. cit., pp. 175-176.

Capitolul III
Condițiile legale pentru autorizarea livrării supravegheate

Secțiunea 1. Condiții generale pentru autorizarea măsurii

Livrarea supravegheată diferă de celelalte metode speciale de supraveghere sau cercetare atât prin prisma condițiilor legale particulare ale acesteia, cât și prin includerea unor condiții speciale în cazul fiecăruia dintre cele două tipuri de livrare supravegheată.

O particularitate a livrării supravegheate o constituie prevederea cuprinsă în art. 151 alin. (1) C.pr.pen. privitoare la autorizarea măsurii *la solicitarea instituțiilor sau organelor competente*. O atare situație pare a condiționa ca procurorul să autorizeze măsura, în lipsa unei sesizări din partea unor anumite instituții sau organe din afara organelor de cercetare penală. Credem că textul prevăzut de legiuitor este imprecis, întrucât nu poate condiționa modul de desfășurare a urmăririi penale de voința unui alt organ. În plus, numai organul de cercetare penală poate face propuneri procurorului, întocmind referate în acest sens. Observăm că formularea este tributară dispozițiilor cuprinse anterior în Legea nr. 39/2003[1], unde se regăsea la art. 16 din lege, cu diferența că livrarea supravegheată era autorizată numai de procurorul anume desemnat de procurorul general al P.I.C.C.J. Privind din acest context, la momentul acela, expresia avea un alt înțeles, întrucât procurorul care efectua urmărirea penală sesiza procurorul desemnat de procurorul general al României ori acesta era sesizat de organele competente dintr-un stat străin în cadrul mecanismelor de cooperare internațională în materie penală pentru a pune în aplicare livrarea supravegheată dispusă de un stat străin.

Credem că, prin Codul de procedură penală, legiuitorul a dorit să indice cu totul altceva, respectiv că, pentru realizarea unei livrări supravegheate, *trebuie să existe informații cu privire la un transport ilicit de obiecte*, care vor proveni, de regulă, de la instituții sau organe – de poliție, de informații, de urmărire penală – dintr-un alt stat, de regulă, cel din care pornește transportul pe baza mecanismelor de cooperare internațională. Nu putem exclude nici situația în care din actele de urmărire penală efectuate în cauză rezultă probe că se pregătește un transport ilicit către țara noastră, sens în care procurorul se va pronunța pe baza actelor efectuate în cauză.

Apreciem că expresia „la solicitarea instituțiilor sau organelor competente" nu ar trebui să existe în Codul de procedură penală atunci când România este stat solicitat, caz în care va trebui să fie avute în vedere condițiile cuprinse de Legea nr. 302/2004, republicată[2]. În acest din urmă caz, dacă autoritățile române sunt solicitate de un stat străin, *autoritățile judiciare competente* (procurorul competent) vor autoriza livrarea supravegheată solicitată potrivit dispozițiilor legii române, respectiv a Codului de procedură penală, urmând ca livrarea supravegheată să se desfășoare (cel puțin pe teritoriul țării) potrivit legii române[3]. Astfel, în situația în care

[1] Legea nr. 39 din 21 ianuarie 2003 (M. Of. nr. 50 din 29 ianuarie 2003).

[2] Legea nr. 302 din 26 iunie 2004 privind cooperarea judiciară internațională în materie penală (republicată în M. Of. nr. 411 din 27 mai 2019).

[3] Conform art. 237 din Legea nr. 302/2004, republicată: „Livrări supravegheate

(1) Autoritățile judiciare române competente autorizează, la cerere, în condițiile prevăzute de legea română, livrări supravegheate, în cadrul unor proceduri penale privind infracțiuni care pot da loc la extrădare.

(2) Livrările supravegheate se derulează potrivit legii române.

România este stat solicitat, procurorul va trebui să dispună începerea urmăririi penale în cauză pentru a crea contextul procesual necesar, dispunând prin ordonanță autorizarea livrării supravegheate solicitate de autoritățile competente din statul străin și a punerii în aplicare a acesteia. Totodată, după caz, livrarea supravegheată va putea face obiectul unui ordin european de anchetă, conform art. 348 alin. (1) lit. b) din Legea nr. 302/2004, republicată.

Organul competent să dispună autorizarea livrării supravegheate va fi procurorul care supraveghează sau efectuează urmărirea penală, care va dispune prin ordonanță, atunci când sunt îndeplinite condițiile legale.

Pentru a se putea autoriza livrarea supravegheată, este necesar ca *urmărirea penală să fi fost începută în cauză pentru o faptă prevăzută de legea penală*. Nu va putea fi dispusă o astfel de măsură mai înainte de începerea urmăririi penale. Totodată, livrarea supravegheată nu se va putea dispune în cursul judecății, fiind o măsură specifică urmăririi penale.

Față de alte metode speciale de supraveghere sau cercetare, legiuitorul nu a limitat aplicarea măsurii în baza criteriului gravității infracțiunii, prevăzând două situații în care se poate dispune livrarea supravegheată, cuprinse în art. 151 alin. (2) C.pr.pen.

În prima situație, conform art. 151 alin. (2) lit. a) C.pr.pen., se va putea autoriza livrarea supravegheată „*dacă descoperirea sau arestarea persoanelor implicate în transportul ilegal de droguri, arme, obiecte furate, materiale explozive și precursori de explozivi restricționați, nucleare, alte materiale radioactive, sume de bani și alte obiecte care rezultă din activități ilicite ori obiecte utilizate în scopul comiterii de infracțiuni nu ar putea fi făcută în alt mod sau ar presupune dificultăți deosebite ce ar prejudicia ancheta ori un pericol pentru siguranța persoanelor sau a unor bunuri de valoare*".

Primul termen al condiției enunțate mai sus, „descoperire", conduce la scopul principal al livrării supravegheate, cel de a cunoaște în întregime membrii, structura și modul de operare al grupului infracțional cercetat, putându-se cunoaște întreaga rețea prin intermediul supravegherii acțiunilor întreprinse atât în timpul transportului, cât și a organizării flagrantului la locul de destinație.

În privința termenului de „arestare" folosit de legiuitor, apreciem că acesta este unul imprecis, întrucât nu putem vorbi despre o arestare în adevăratul sens al termenului, ci eventual de *prinderea* persoanelor implicate în transporturi ilegale, ulterior, față de acestea, putându-se lua măsurile preventive cuvenite, în condițiile legii.

Legiuitorul a ales să nu condiționeze aplicarea metodei speciale de cercetare de gravitatea unei fapte anume, ci a ales să se raporteze la *obiectele care pot fi supuse traficului*, acestea fiind obiecte obținute sau care pot fi întrebuințate la activități ilicite și obiecte a căror deținere este reglementată sau interzisă prin lege. Nu este necesar ca transportarea bunului să constituie, prin ea însăși, o infracțiune, situație incidentă în cazul unor simple bunuri furate, dar, în cazul unor bunuri reglementate mai strict – substanțe interzise, precum drogurile –, însăși transportarea lor va constitui infracțiune, în acest sens fiind necesară menționarea cauzei de impunitate prevăzută de art. 151 alin. (7) C.pr.pen.

Chiar dacă vor fi îndeplinite condițiile de mai sus, autorizarea metodei speciale de cercetare este supusă unei condiții de subsidiaritate, putând fi întrebuințată numai dacă descoperirea sau arestarea persoanelor implicate „*nu ar putea fi făcută în alt mod sau ar presupune dificultăți deosebite ce ar prejudicia ancheta ori un pericol pentru siguranța persoanelor sau a unor bunuri de valoare*".

(3) Dispozițiile prezentului articol se aplică în mod corespunzător și în cazul în care asistența este solicitată de autoritățile judiciare române".

Prin expresia „nu ar putea fi făcută în alt mod sau ar presupune dificultăți deosebite care ar prejudicia ancheta" vom înțelege că metoda specială de cercetare trebuie să fie necesară în cauză, fie absolut, fie relativ, sens în care facem trimitere la explicațiile date în cazul metodei speciale de cercetare a utilizării investigatorilor sub acoperire sau a colaboratorilor[1].

În cazul în care nefolosirea metodei de cercetare ar putea presupune *un pericol pentru siguranța persoanelor*, credem că legiuitorul a avut în vedere nu numai situațiile în care persoane terțe ar putea fi afectate, ci și situația în care persoanele care realizează transportul pot fi în pericol. Se poate imagina o situație în care pentru transportul unor droguri se întrebuințează o plută artizanală care nu are posibilitatea de a se deplasa pe mare, într-o astfel de situație, organele de urmărire penală fiind obligate fie să nu desfășoare livrarea supravegheată, fie să o sisteze, dacă a fost deja începută, și să procedeze la prinderea, respectiv salvarea persoanelor implicate în transport. În alte situații, pericolul pentru siguranța persoanelor va trebui să fie evaluat numai prin raportare la persoane determinate (sau determinabile), cunoscute de organele de urmărire penală.

În ceea ce privește *pericolul pentru bunuri de valoare*, situația este discutabilă, întrucât, în cazul bunurilor furate, tocmai livrarea supravegheată ar putea pune în pericol aceste bunuri, existând riscul de a nu mai putea fi recuperate dacă livrarea supravegheată va eșua. În atare situație, apare ca preferabilă recuperarea directă a bunurilor, cu consecința pierderii posibilității descoperirii și prinderii persoanelor implicate în transport. *De lege ferenda*, considerăm că ar trebui eliminată această condiție, care, de altfel, este împrumutată de legiuitor de la alte metode speciale de supraveghere sau cercetare.

În cea de-a doua situație, conform art. 151 alin. (2) lit. b) C.pr.pen., „*dacă descoperirea ori dovedirea infracțiunilor săvârșite în legătură cu livrarea de transporturi ilegale sau suspecte ar fi imposibilă ori foarte dificilă în alt mod*". Apreciem că singura diferență între acest text de lege și cel cuprins la art. 151 alin. (1) lit. a) C.pr.pen. este lipsa mențiunilor privind infracțiunile care pot fi cercetate prin întrebuințarea metodei de investigație a livrării supravegheate. Apreciem că, *de lege ferenda*, se impune reunirea celor două condiții alternative.

S-a considerat că metoda specială de cercetare nu poate conduce, de principiu, la restrângerea drepturilor fundamentale ale vreunei persoane, astfel că legiuitorul nu a condiționat măsura de vreun control de proporționalitate[2]. Nu putem fi de acord cu afirmația că nu ar exista, chiar și de principiu, o restrângere a drepturilor fundamentale ale unei persoane, în condițiile în care vom admite că măsura este realizată prin monitorizarea unui transport de la origine până la destinație atât timp cât vor fi urmărite toate persoanele care realizează operațiuni privind transportul. Dimpotrivă, credem că reglementarea metodei speciale este deficitară din acest punct de vedere, impunându-se ca, în cazul utilizării investigatorilor sub acoperire și a colaboratorilor, măsura să poată fi autorizată numai atunci când este necesară și proporțională cu restrângerea drepturilor persoanei vizate într-un caz concret. Afirmăm acest lucru, întrucât legislația specială anterioară intrării în vigoare a Codului de procedură penală limita folosirea livrării supravegheate atunci când puteau fi lezate valori sociale importante, respectiv siguranța națională, ordinea sau sănătatea publică[3].

Întrucât legiuitorul a considerat că se impun condiții speciale privind autorizarea livrării supravegheate în funcție de caracterul său național sau transfrontalier, în cele ce urmează vom trata distinct condițiile legale care se impun a fi îndeplinite suplimentar față de cele analizate deja.

[1] *V. supra*, Titlul XII, Capitolul II.

[2] *M. Bulancea, R. Slăvoiu*, în M. Udroiu (coord.), Codul de procedură penală, 2017, p. 734.

[3] Conform art. 16 alin. (3) din Legea nr. 39/2003, în forma în vigoare până la 1 februarie 2014.

Secțiunea a 2-a. Condiții speciale în cazul livrării supravegheate naționale

Înainte de a analiza condițiile speciale propriu-zise ale livrării supravegheate, trebuie făcute câteva precizări asupra sensului includerii *intrării, circulației sau ieșirii* de pe teritoriul țării a bunurilor vizate, întrucât sunt susceptibile de confuzii în practică. Potrivit art. 151 alin. (2[1]) C.pr.pen., „*livrarea supravegheată poate fi realizată pe teritoriul țării numai dacă procurorul care supraveghează sau efectuează urmărirea penală se asigură că autoritățile care au, potrivit legii, atribuții în legătură cu verificarea sau supravegherea intrării, circulației sau ieșirii de pe teritoriul țării a bunurilor vizate*".

Deși, aparent, noțiunile de „ieșire din țară" și „de intrare în țară" par a fi inaplicabile în cazul unui transport național vizat de livrarea supravegheată, întrucât cele două acțiuni – intrarea și ieșirea din țară – presupun o activitate transfrontalieră; nu este neapărat așa în situația în care numai procurorul național dispune livrarea supravegheată și activitatea presupune numai activitate de trecere a frontierei între România și un stat vecin.

Astfel, putem fi în situația unei livrări supravegheate naționale atunci când organele de urmărire penală sunt sesizate că urmează să intre în țară un transport ilegal în scurt timp, fără ca acesta să fi fost urmărit din țara de origine. Într-o asemenea situație, se va putea dispune livrarea supravegheată, iar autoritățile vamale dinspre sensul de intrare în țară vor fi încunoștințate să permită accesul în țară al transportului, mai apoi, organele abilitate vor urmări transportul până la destinația din țară. În jurisprudență s-a considerat că va putea fi întrebuințată livrarea supravegheată pentru un colet cu amfetamină care deja sosise în țară și se afla în custodia organelor de urmărire penală, el fiind înmânat, mai apoi, făptuitorului de către un investigator sub acoperire care s-a prezentat drept funcționar al Poștei Române, predându-i coletul indicat[1]. Nu putem fi de acord cu o asemenea soluție, aceasta neavând elementul transnațional constând în intrarea în țară a coletului, întrucât acesta deja se afla pe teritoriul țării la momentul la care s-a emis ordonanța de livrare supravegheată[2]. Mai mult, activitatea investigatorului sub acoperire poate fi clasificată doar drept participare autorizată la anumite activități, întrucât transportul coletului cu amfetamină poate fi încadrat la *operațiuni privind droguri*, conform art. 138 alin. (11) C.pr.pen.

În cazul unei livrări supravegheate naționale prin care se va permite ieșirea din țară a unui bun, apreciem că o atare situație va fi limitată, întrucât va presupune ca persoana urmărită să fie surprinsă imediat după ieșirea din țară. Este discutabil dacă o asemenea situație nu ar fi, în realitate, o formă transfrontalieră a livrării supravegheate.

În cazul circulației pe teritoriul țării, nu se ridică probleme semnificative, livrarea supravegheată putând viza deplasarea oricărui transport dintr-o locație în alta din țară, pentru a descoperi și prinde persoanele responsabile de transport ilegal.

Pentru a se dispune livrarea supravegheată națională, este necesar ca procurorul să se asigure că autoritățile care au, potrivit legii, atribuții în legătură cu verificarea sau supravegherea intrării, circulației sau ieșirii de pe teritoriul țării a bunurilor vizate *să păstreze confidențialitatea activităților desfășurate* și *să garanteze supravegherea permanentă a transportului ilegal sau suspect*.

[1] Trib. Covasna, s. pen., sent. nr. 45 din 31 octombrie 2017, pe *portal.just.ro*

[2] C. Ap. Craiova, s. pen., dec. nr. 327 din 7 martie 2014, pe *portal.just.ro* – în această speță, organele de urmărire penală au dispus livrarea supravegheată și, prin organele de poliție, au preluat de la autoritățile bulgare un pachet conținând heroină, apoi au procedat la aducerea sa în țară, la substituirea substanței în colet și l-au remis colaboratorului care l-a transmis, mai apoi, inculpaților.

Prin „păstrarea confidențialității activităților desfășurate" nu vom înțelege doar existența unui obligații de păstrare a secretului profesional, ci și o evaluare din partea procurorului a capacității operative a organelor implicate de a nu divulga, în mod neintenționat, activitățile desfășurate. Un exemplu negativ ar fi urmărirea transportului de o mașină de poliție dotată cu girofar sau de o mașină tip Dacia Logan albă, cu numere începând cu prefixul MAI. Dimpotrivă, acțiunile organelor care pun în aplicare livrarea supravegheată vor trebui să fie păstrate secrete față de cei care realizează transportul ilicit prin activități complexe, precum: multiple echipe de filaj, utilizarea unor autovehicule care să nu ridice suspiciuni, derularea supravegherii pe arii teritoriale determinate de către fiecare echipă etc.

„Garantarea supravegherii permanente a transportului ilegal sau suspect" constituie o condiție legală care conduce la posibile interferențe cu metoda specială de supraveghere tehnică a *supravegherii, audio, video sau prin fotografiere*, întrucât presupune urmărirea persoanei de către autorități, fără a fi emis un mandat de supraveghere tehnică de către judecătorul de drepturi și libertăți. Între cele două situații există asemănări clare, întrucât vor presupune o monitorizare continuă a persoanei, însă vor exista suficiente diferențe pentru delimitarea de aceasta. În primul rând, se va monitoriza o activitate de transport ilegal, și nu întreaga viață privată a unei persoane, nefiind posibilă monitorizarea decât în spații publice. În al doilea rând, textul de lege este suficient de clar și previzibil pentru ca o persoană implicată în activități ce pot face obiectul livrării supravegheate să înțeleagă că poate fi monitorizată. În al treilea rând, nu vor putea fi realizate înregistrări video sau audio ori fotografii pentru surprinderea persoanei sau a transportului, organele care pun în aplicare măsura fiind ținute numai să *supravegheze permanent transportul*. În vederea asigurării că această condiție poate fi respectată, procurorul poate apela la judecătorul de drepturi și libertăți să autorizeze, în condițiile legii, orice metodă specială de supraveghere tehnică adecvată.

Secțiunea a 3-a. Condiții speciale în cazul livrării supravegheate transfrontaliere

În situația unei livrări supravegheate transfrontaliere, legea prevede trei condiții care trebuie să fie îndeplinite în cazul acestei variante a metodei speciale de cercetare. Acestea vor trebui să fie avute în vedere de organele de urmărire penală în acele situații în care nu se prevăd condiții diferite prin tratatele internaționale la care România este parte [art. 151 alin. (4) C.pr.pen.].

Conform art. 151 alin. (3) C.pr.pen., procurorul care va emite ordonanța de autorizare a livrării supravegheate va trebui să ia măsuri și să se asigure că autoritățile vor îndeplini anumite obligații instituite de Codul de procedură penală. Față de livrările supravegheate naționale, procurorul *ia măsuri* pentru punerea în aplicare a metodei speciale de cercetare de către statul solicitat, acestea trebuind să constea în apelarea la mecanismele de cooperare internațională în materie penală. În esență, va trebui să comunice cu organele de urmărire penală și cu autoritățile competente din statele de tranzit pentru ca acestea să asigure punerea în aplicare a livrării supravegheate pe teritoriul lor. Măsurile pe care va trebui să le ia sunt: *i)* să ceară acordul autorităților străine; *ii)* să planifice în comun cu autoritățile străine modul de desfășurare pe teritoriul fiecărui stat a livrării supravegheate și *iii)* să comunice rezultatul livrării supravegheate. Alături de aceste două condiții, apreciem că procurorul va fi obligat să comunice toate informațiile necesare pentru realizarea livrării supravegheate de către statul solicitat.

Prima condiție, prevăzută de art. 151 alin. (3) lit. a) C.pr.pen., constă în *obținerea acordului* autorităților statelor tranzitate pentru intrarea pe teritoriul acestora a transportului ilegal sau suspect și pentru ieșirea acestuia de pe teritoriul statului. Această condiție este esențială, întrucât procurorul român nu își poate exercita puterea conferită de lege decât pe teritoriul statului român[1]. Chiar și în cazul emiterii unui ordin european de anchetă, procurorul va trebui să se asigure de consimțământul autorităților străine, obținut, în principal, prin recunoașterea de către acestea a ordinului. Trebuie avut în vedere că orice transport ilegal, în special de substanțe periculoase, va prezenta un pericol pentru ordinea, sănătatea sau siguranța publică a statului tranzitat, sens în care pot fi luate măsuri prin care acest risc să fie diminuat, acestea putând fi condiționate de statul străin. De pildă, statul străin va impune ca drogurile transportate să fie substituite de îndată și transportul să se realizeze cu substanțe înlocuitoare, în tot sau în parte.

A doua condiție, prevăzută de art. 151 alin. (3) lit. b) C.pr.pen., constă în obținerea de garanții din partea autorităților competente ale statelor tranzitate că *transportul ilegal sau suspect este supravegheat permanent de către autoritățile competente*. Sub acest aspect, facem trimitere la explicațiile date mai sus, cu particularitatea că procurorul va putea solicita încuviințarea unor măsuri de supraveghere tehnică (interceptarea comunicațiilor) sau de cercetare și va putea să procedeze la punerea lor în executare prin ordinul european de anchetă.

A treia condiție, prevăzută de art. 151 alin. (3) lit. c) C.pr.pen., este o condiție aparentă, ea instituind de fapt o obligație a procurorului ulterioară desfășurării livrării supravegheate. Această obligație constă în faptul că *procurorul, organele de poliție sau alte autorități de stat competente sunt înștiințate în ceea ce privește rezultatul urmăririi penale împotriva persoanelor acuzate de infracțiuni care au constituit obiectul metodei speciale de cercetare*. Nu putem considera că suntem în situația unei condiții legale, ci a unei obligații ulterioare, întrucât, la momentul la care se dispune autorizarea livrării supravegheate, urmărirea penală nu poate fi finalizată. Era preferabil ca legiuitorul să prevadă distinct această obligație. Încunoștințarea autorităților statului străin este necesară pentru buna cooperare internațională în materie penală, întrucât acestea sunt obligate să justifice propriile acțiuni realizate, dar și să aibă posibilitate să soluționeze propriile urmăriri penale deschise cu privire la respectivul transport.

[1] *Gh. Vâșcea*, Elemente de drept comparat privind reglementarea livrării supravegheate, în Revista de Investigare a Criminalității, vol. 9, nr. 2/2016, p. 86.

Capitolul IV
Procedura de autorizare a livrării supravegheate

Mai înainte de a discuta procedura de autorizare, se impune a face câteva mențiuni cu privire la organul de urmărire penală care va dispune asupra măsurii, din perspectiva competenței și a tacticii, privitor la forma cea mai des întâlnită a livrării supravegheate – livrarea supravegheată transfrontalieră[1].

În combaterea criminalității transfrontaliere cu obiecte interzise, urmărirea penală se va realiza, cel mai adesea, de țara de destinație a obiectelor, întrucât punerea în circulație a acestora va afecta ordinea publică din acea țară mai mult, și mai puțin pe cea din statele prin care transportul a tranzitat, ca atare țara de destinație va avea interesul cel mai înalt de a putea descoperi, prinde și trage la răspundere penală toate persoanele implicate. În susținerea acestei poziții, arătăm că, potrivit art. 151 alin. (3) C.pr.pen., legea condiționează autorizarea măsurii de *asigurările primite de procuror de la statele de tranzit cu privire la respectarea condițiilor speciale* la livrarea supravegheată transfrontalieră. Textul este imprecis, întrucât nu are în vedere și ipoteza în care țara noastră este stat solicitat ca stat tranzit sau stat de origine, situație ce rezultă din coroborarea art. 151 C.pr.pen. cu art. 237 din Legea nr. 302/2004, republicată.

Din interpretarea dispozițiilor legale amintite mai sus rezultă că livrarea supravegheată se va autoriza de procurorul național atât în cazul în care România este stat solicitant, cât și atunci când țara noastră este stat solicitat. Chiar și în situația în care România nu va efectua, în final, urmărirea penală pentru faptele cercetate, ci va fi doar stat solicitat, va fi necesară autorizarea livrării supravegheate de procurorul național pentru a fi pusă în aplicare livrarea supravegheată pe teritoriul național cât timp transportul tranzitează țara noastră. Cu alte cuvinte, livrarea supravegheată se va autoriza atât de statul străin solicitant, cât și de către statul român. Necesitatea autorizării și în cazul în care țara noastră este stat solicitat poate fi justificată și prin prisma dispozițiilor art. 151 alin. (7) C.pr.pen., potrivit cărora „*punerea în aplicare a livrării supravegheate nu constituie infracțiune*", pentru incidența acestui text de lege fiind necesar să existe o autorizare din partea organelor competente naționale.

În situația în care România este stat de destinație, urmărirea penală la care se face referire în art. 151 C.pr.pen. va fi una a organelor de urmărire penală române, care vor și proceda la tragerea la răspunderea penală a infractorilor. Nu trebuie omis faptul că autoritățile române trebuie să cunoască dinainte faptul că transportul ilicit se va realiza și că țara noastră va fi destinația, aceasta realizându-se prin diverse surse de informare (informatori, colaboratori, organe de poliție străine etc.), inclusiv instituțiile și organele competente din alte state. În doctrină s-a constatat și un pericol crescut pentru statul de destinație în cazul folosirii excesive a măsurii speciale de cercetare, existând riscul susținerii traficului ilicit de droguri, mai ales dacă nu există o supraveghere adecvată asupra autorizării măsurii[2].

La cealaltă extremă vor sta statele de origine a obiectelor sau substanțelor interzise (în cazul drogurilor – America de Sud pentru cocaină, Afganistan pentru heroină și alte opiacee, Olanda pentru canabis), care vor avea un interes minim în a cerceta traficul de droguri. Trebuie

[1] Astfel cum am arătat într-o secțiune precedentă, anterior emiterii O.U.G. nr. 18/2016, livrarea supravegheată putea fi numai transfrontalieră.

[2] *N. Boister*, op. cit., p. 169.

avut în vedere și contextul politic în care se află aceste state, pentru că vor avea un regim mai permisiv cu privire la respectivele bunuri sau vor suferi din cauza războiului, și statul nu își va putea exercita autoritatea pentru a combate fenomenul infracțional. Totuși, trebuie avut în vedere că și acest stat va putea fi solicitat prin metoda specială de cercetare [în calitate de stat de tranzit, în accepțiunea art. 151 alin. (3) C.pr.pen.], pentru a substitui o parte sau întregul bunurilor traficate.

Deși, în cazul livrării supravegheate transfrontaliere, țara noastră, în calitate de stat de origine, poate solicita, prin procurorul competent, livrarea supravegheată pentru descoperirea și prinderea în țara de destinație a persoanelor care pornesc un transport ilegal din România, o atare măsură nu pare fezabilă. Din punct de vedere tactic, această situație nu este preferabilă, deoarece ar presupune desfășurarea majorității procedurilor judiciare în statul de destinație, organele române trebuind să apeleze la metode de cooperare judiciară internațională pentru a realiza urmărirea penală, ceea ce ar îngreuna procesul penal. În cel mai bun caz, pentru o bună administrare a justiției, va fi realizat un transfer de proceduri, în condițiile legii. Mai lesne va fi dacă autoritățile române vor informa organele de urmărire penală din statul de destinație (prin transmitere spontană de informații[1]), urmând ca acestea să efectueze urmărirea penală și să dispună livrarea supravegheată, în acest caz, România putând fi stat solicitat și, în această calitate, va fi autorizată măsura și de către procurorul național.

Statele de tranzit vor fi cele pe teritoriul cărora transportul trece în condițiile livrării supravegheate, acestea trebuind să fie de acord cu intrarea, circulația și ieșirea de pe teritoriul lor a obiectelor traficate. Cu alte cuvinte, vor trebui să se asigure că transportul de obiecte ilegale își continuă mersul către destinație, în eventualitatea în care s-ar ivi vreun eveniment neprevăzut, acestea trebuind să intervină. De pildă, în situația în care infractorii ar bănui că sunt supravegheați, ar putea să întrerupă transportul sau să încerce să se întoarcă în țara de origine. Într-o asemenea situație, livrarea supravegheată va eșua, însă se va putea organiza un flagrant în statul de tranzit, organele de urmărire penală din respectivul stat putând începe urmărirea penală pentru faptele comise pe teritoriul respectivului stat.

Deși art. 151 C.pr.pen. pare a sugera că statul român nu va putea fi stat solicitat, în realitate, procurorul național va fi obligat să dispună livrarea supravegheată în condițiile legii române și atunci când el nu va efectua în final urmărirea penală în cauză, fiind sesizat de instituțiile și organele competente dintr-un stat străin. Potrivit art. 237 alin. (1) din Legea nr. 302/2004, republicată, „*autoritățile judiciare române competente autorizează, la cerere, în condițiile prevăzute de legea română, livrări supravegheate, în cadrul unor proceduri penale privind infracțiuni care pot da loc la extrădare*".

În concluzie, autorizarea metodei speciale de cercetare a livrării supravegheate se va face de către procurorul român pentru livrările supravegheate care au stat de destinație țara noastră, pornesc din țara noastră sau doar tranzitează țara, atât în situația în care România este un stat solicitant și va efectua în continuare urmărirea penală, cât și atunci când este doar stat solicitat.

Sub aspectul *procedurii de autorizare*, Codul de procedură penală nu prevede o procedură distinctă pentru autorizarea metodei speciale de cercetare, în măsura în care condițiile legale vor fi îndeplinite, procurorul dispunând prin ordonanță autorizarea livrării supravegheate,

[1] Conform art. 236 alin. (1) din Legea nr. 302/2004, republicată, „autoritățile judiciare române pot, fără cerere prealabilă, să transmită autorităților competente ale unui stat străin informațiile obținute în cadrul unei anchete, atunci când consideră că acestea ar putea ajuta statul destinatar să inițieze o procedură penală sau când informațiile ar putea conduce la formularea unei cereri de asistență judiciară".

aceasta trebuind să conțină toate mențiunile cuprinse în art. 286 alin. (2) C.pr.pen., precum și mențiunile speciale prevăzute de art. 151 alin. (5) C.pr.pen.[1], pe care le vom detalia în cele ce urmează.

Numele suspectului sau inculpatului, dacă sunt cunoscute, reprezintă o mențiune pe care nu o socotim ca fiind necesară, întrucât trebuia să fie prevăzută în ordonanță ca efect al dispozițiilor art. 286 alin. (2) lit. c) C.pr.pen., fiind redundantă mențiunea prevăzută de legiuitor.

Motivele concrete care justifică măsura reprezintă o mențiune pe care o socotim utilă, însă nu este necesară prin prisma dispozițiilor art. 286 alin. (2) lit. d) C.pr.pen. Cu toate acestea, este important, față de caracterul de metodă specială de investigație, ca procurorul să își motiveze temeinic măsura și să detalieze mai ales îndeplinirea condițiilor speciale ale măsurii, dar și proporționalitatea acesteia.

Indicarea bunurilor care fac obiectul livrării va constitui o mențiune obligatorie, însă nu va presupune mari probleme pentru procuror, întrucât această informație va fi tot timpul cunoscută, chiar dacă nu în totalitate. De pildă, nu se vor cunoaște puritatea drogurilor transportate sau chiar natura lor exactă, în cazul în care sunt susceptibile de variante multiple, natura obiectelor furate etc. Nu va fi necesar să se indice cantitatea exactă a acestora, fiind suficient să fie aproximată prin raportare la mijlocul de transport folosit. *Dovezile din care rezultă caracterul ilicit al bunurilor* vor trebui să fie incluse prin raportare la necesitatea motivării ordonanței prin care se autorizează livrarea supravegheată, dar vor avea însemnătate mai mare atunci când bunurile care fac obiectul măsurii ar putea fi deținute în mod legal.

Bunurile care urmează a fi sustrase sau substituite adaugă la dispozițiile legale ideea că se pot și sustrage bunurile, nu numai substitui. Apreciem că organele de urmărire penală ar trebui să procedeze, de regulă, la substituirea bunurilor, nu la luarea lor, pentru a nu ridica suspiciuni cu privire la operațiune[2]. Pe lângă natura bunurilor substituite, se va indica și cantitatea lor. În condițiile în care nu se cunoaște exact cantitatea transportată, se va putea indica numai cantitatea care va rămâne în transportul ilegal, urmând ca restul să fie completat prin înlocuire. *Bunurile care vor fi înlocuite* vor trebui să fie precizate prin substanță, cantitate și volum, după caz[3].

Timpul și locul efectuării livrării și itinerariul care urmează a fi parcurs sunt elemente importante, deoarece indică organelor care trebuie să pună în aplicare măsura când se așteaptă ca transportul să sosească. Legiuitorul a arătat că aceste informații vor fi prevăzute numai dacă sunt cunoscute, ținând seama de cât de fidele sunt informațiile puse la dispoziția procurorului. Deși poate nu vor fi cunoscute, toate statele implementează un sistem de consemne la frontiera de stat pe baza unui sistem informatic, situație în care ofițerii poliției de frontieră vor putea

[1] Conform art. 151 alin. (5) C.pr.pen., mențiunile suplimentare inserate în plus față de art. 286 alin. (2) C.pr.pen. vor fi:

„a) numele suspectului sau inculpatului, dacă sunt cunoscute;

b) motivele concrete care justifică măsura;

c) indicarea bunurilor care fac obiectul livrării supravegheate și a dovezilor din care rezultă caracterul ilicit al acestora, a bunurilor care urmează a fi sustrase sau substituite, precum și a bunurilor care urmează a le înlocui pe acestea, după caz;

d) timpul și locul efectuării livrării sau, după caz, itinerarul ce urmează a fi parcurs în vederea efectuării livrării, dacă acestea sunt cunoscute;

e) modalitățile în care va fi efectuată supravegherea;

f) datele de identificare a persoanelor autorizate să supravegheze livrarea".

[2] A se vedea și *L. Iliescu*, Noile reglementări legislative privind livrările supravegheate în unele state membre din Uniunea Europeană, în Studii de Securitate Publică, vol. 3, nr. 2/2014, p. 223.

[3] A se vedea, pentru identitate de rațiune, *C. Harfield, K. Harfield*, Covert Investigation, 2018, p. 141.

constata că transportul depistat face obiectul livrării supravegheate şi vor încunoştinţa de îndată procurorul. Apoi, se va putea asigura supravegherea continuă a transportului şi se va descoperi itinerariul său şi destinaţia sa finală.

Modalităţile în care va fi efectuată supravegherea vor detalia planul care trebuie să fie respectat de toate componentele echipelor care pun în aplicare metoda specială de cercetare, precizându-se tacticile care urmează să fie folosite, responsabilităţile, mijloacele tehnice care vor fi utilizate, iar dacă au fost autorizate măsuri de supraveghere tehnică, să se indice în ce constau acestea, cu menţionarea încheierii de autorizare, a persoanelor vizate şi a perioadei de timp pentru care au fost autorizate. În măsura în care o parte a persoanelor care pun în aplicare livrarea supravegheată are competenţa de a pune în aplicare măsurile de supraveghere tehnică, procurorul va trebui să dispună separat, prin ordonanţă, punerea în executare a acestora de către respectivele persoane (organe de cercetare penală, investigatori sub acoperire, colaboratori etc), în conformitate cu dispoziţiile art. 142 C.pr.pen.

Prin „datele de identificare a persoanelor autorizate să supravegheze livrarea", legiuitorul sugerează că nu va fi suficient ca procurorul să precizeze numai unitatea de poliţie sau autoritatea competentă să asigure livrarea supravegheată, ci şi să individualizeze toate persoanele autorizate[1]. Prin „date de identificare" vom înţelege cel puţin menţionarea numelui complet al persoanei, funcţia şi instituţia de care aparţine. După cum am mai arătat, livrarea supravegheată presupune ca procurorul să coordoneze şi să controleze fiecare membru al echipelor care vor pune în aplicare măsura. Cu toate acestea, ne exprimăm anumite rezerve atunci când va fi în discuţie o livrare supravegheată transfrontalieră prin mai multe state tranzitate, întrucât va fi foarte greu să se asigure identificarea fiecărei persoane care va contribui la succesul măsurii.

Un ultim aspect important pentru autorizarea livrării specializate este că, pentru fiecare livrare supravegheată, procurorul va fi obligat să emită o nouă ordonanţă care să conţină toate menţiunile la care am făcut referire mai sus. Prin aceasta considerăm că legiuitorul a impus ca, pentru fiecare transport – mijloc de transport sau persoană care transportă –, să fie emisă câte o ordonanţă separată, nu câte o ordonanţă pentru fiecare operaţiune, în cazul în care sunt implicate mai multe transporturi.

[1] *Ibidem*, pp. 136-137.

Capitolul V
Punerea în aplicare a livrării supravegheate

Secțiunea 1. Procedura punerii în aplicare a livrării supravegheate

Spre deosebire de terminologia utilizată în cadrul altor metode speciale de supraveghere sau cercetare, legiuitorul a folosit o altă expresie pentru a desemna punerea în executare a măsurii, apreciind că, în cazul livrării supravegheate, vom avea o *punere în aplicare a măsurii*, fapt care decurge din cuprinsul art. 151 alin. (6) C.pr.pen. Diferența este justificată, întrucât livrarea supravegheată este o metodă de investigare care presupune un efort considerabil din partea mai multor instituții ale statului, neputându-se realiza numai de către organele de urmărire penală. În schimb, legiuitorul a vrut să indice prin expresia de „punere în aplicare" și faptul că va putea fi incidentă posibilitatea unei delegări din partea procurorului cu privire la măsură.

Conform art. 151 alin. (6) teza a II-a C.pr.pen., „*procurorul stabilește, coordonează și controlează modul de punere în aplicare a livrării supravegheate*", ceea ce semnifică, în opinia noastră, că punerea în executare se va putea realiza numai de către procuror, acesta exercitând control direct asupra celorlalți participanți, care nu vor realiza decât acte de punere în aplicare materială a măsurii[1].

Prin atributul de „stabilire", legiuitorul a vrut să indice că procurorul urmează a stabili, din punct de vedere tactic, modalitatea concretă în care se va realiza livrarea supravegheată, ce acțiuni vor fi întreprinse, care vor fi echipele de poliție participante, care vor fi organele specializate însărcinate cu facilitarea accesului în țară ori ieșirea din țară a transportului sau controlarea deplasării transportului în țară. În plus, procurorul va decide și dacă se impune folosirea altor metode speciale de supraveghere sau cercetare, obținând, după caz, autorizarea din partea judecătorului de drepturi și libertăți. Tot sub aspectul planificării tactice a livrării supravegheate, procurorul este cel care va determina momentul la care se va realiza flagrantul sau condițiile în care livrarea supravegheată poate fi sistată, luând măsuri pentru pregătirea organelor care pun aplicare măsura să acționeze în asemenea situații[2].

Prin „coordonare", legiuitorul a vrut să arate că procurorul va fi cel care se va ocupa de modul în care fiecare echipă (organ, instituție, persoană) care pune în aplicare măsura va conlucra în mod operativ, asigurându-se că se respectă planul stabilit dinainte și că se lucrează către atingerea aceluiași scop. În concret, se va asigura că fiecare persoană care pune în aplicare măsura va ști ce are de făcut, când trebuie să facă acel lucru și cum să colaboreze cu celelalte persoane care acționează în punerea în aplicare a măsurii, iar, dacă o persoană nu își îndeplinește sarcinile, să ia măsurile corective impuse. Livrarea supravegheată este o metodă de investigație care impune un contact nemijlocit și continuu între procuror și persoanele care pun în aplicare măsura.

Prin „controlarea punerii în aplicare a livrării supravegheate", legiuitorul a vrut să stabilească rolul decizional al procurorului în realizarea livrării supravegheate, în special prin

[1] *C. Olaru*, op. cit., p. 88.
[2] *Em. Stancu*, op. cit., pp. 700-701.

deciziile pe care le ia în funcție de evenimentele care au loc în timpul punerii în aplicare. Livrarea supravegheată nu este o metodă specială a cărei punere în aplicare poate fi prevăzută complet de la început, existând numeroase situații când, deși se cunoaște țara de destinație a transportului, nu se va ști adresa concretă ori, pe parcursul punerii în aplicare a măsurii, infractorii (sau persoana care realizează transportul) iau o decizie neașteptată pentru organele de urmărire penală. Atributul de control nu poate fi delegat, impunându-se ca procurorul să ia decizii pe moment asupra livrării supravegheate, dispunând de îndată măsurile care vor trebui luate de persoanele însărcinate cu punerea în aplicare.

O altă problemă de interes este aplicarea dispozițiilor art. 151 alin. (1) C.pr.pen. cu privire la *sustragerea ori substituirea totală sau parțială a bunurilor care fac obiectul livrării*, aceasta fiind o posibilitate comună ambelor forme de livrarea supravegheată – națională sau internațională.

Prin „sustragerea bunurilor care fac obiectul măsurii" vom înțelege acțiunea organelor de urmărire penală de a lua din posesia detentorilor care realizează transportul obiectul sau obiectele pentru care s-a dispus livrarea supravegheată.

Prin „substituire" nu vom înțelege numai confiscarea bunurilor, fiind obligatoriu ca acestea să fie înlocuite cu substanțe (de exemplu, făină, în cazul unor droguri[1]), obiecte sau recipiente care să aibă proprietăți similare ca greutate și volum, pentru a evita distrugerea acestora sau dispariția lor (de exemplu, bunuri de lux sustrase și aflate în detenția hoților pentru a preveni valorificarea lor[2]). În terminologia specifică, dacă infracțiunile cercetate privesc operațiuni cu droguri sau precursori, o livrare supravegheată cu substituirea drogurilor[3] va fi denumită o „livrare supravegheată curată"[4], și una prin care nu se realizează această substituire se va numi „livrare supravegheată murdară sau efectivă"[5].

În măsura în care obiectele substituite se află în spații private, s-a arătat în doctrină că va fi necesară autorizarea prealabilă din partea judecătorului de drepturi și libertăți[6], fără a se indica procedeul probatoriu care va trebui utilizat, în opinia noastră, acesta trebuind să fie o percheziție domiciliară.

Substituirea bunurilor se va decide de către procuror și se va pune în aplicare fie de către poliție sau de către o altă autoritate competentă, fie, în cazul în care există autorizare în acest sens, de un investigator sub acoperire sau un colaborator. În cazul unei livrări supravegheate transfrontaliere, problema substituirii se impune a fi stabilită de comun acord de către procuror și autoritățile naționale ale fiecărui stat tranzitat[7].

Substituirea se va face în condiții de confidențialitate, fiind important ca persoanele care realizează transportul să nu cunoască împrejurarea că bunurile transportate au fost înlocuite. În literatura de specialitate a fost analizată și posibilitatea unei duble substituiri, atunci când ar exista riscul pierderii unui transport[8]. Astfel, situația relevată a fost descoperirea desfășurării unui transport maritim de droguri, organele de urmărire penală din statul de destinație colaborând cu autoritățile din statul de origine pentru substituirea integrală a drogurilor în primă fază, pentru ca, apoi, acestea să fie transportate de un informator pe calea aerului până

[1] *M. Udroiu*, Procedură penală, vol. I, 2019, p. 617.
[2] *Ibidem*, p. 616.
[3] ICCJ, s. pen., dec. nr. 1641 din 14 mai 2014, pe *www.scj.ro*
[4] *N. Boister*, op. cit., p. 169.
[5] *I.M. De Lucas Martín, C.-E. Ștefan*, op. cit., pp. 155-156.
[6] *M. Udroiu*, Procedură penală, vol. I, 2019, p. 618.
[7] *I.M. De Lucas Martín, C.-E. Ștefan*, op. cit., p. 154.
[8] *C. Olaru*, op. cit., p. 89.

în țara de destinație, unde, în faza a doua, drogurile vor fi reintroduse, putându-se continua livrarea supravegheată pe cale terestră[1].

Cu ocazia sustragerii sau substituirii obiectelor, dacă acestea privesc substanțe, vor fi în mod obligatoriu supuse unor analize de laborator pentru identificarea lor, determinarea purității etc.

Livrarea supravegheată națională apare, de regulă, atunci când se descoperă că un colet destinat circulației naționale printr-un serviciu de poștă sau curierat ar conține substanțe sau obiecte interzise[2]. Într-o asemenea situație, procurorul va putea dispune livrarea supravegheată prin substituirea bunurilor, reintroducând în circuitul poștei sau curieratului respectivul colet și supraveghind circulația sa către destinație pentru a identifica persoanele care vin să îl ridice. Alternativ livrării supravegheate se va putea autoriza utilizarea unui investigator sub acoperire și participarea autorizată la anumite activități, dacă livrarea coletului se va face de către organele de urmărire penală.

În cazul unei livrări supravegheate transfrontaliere, este posibil ca sursa informării organelor de urmărire penală cu privire la pregătirea unui transport de obiecte ilicite să provină din statul de origine, impunându-se ca procurorul să stabilească relații personale cu autoritățile din statul de origine pentru definirea cadrului în care se va realiza livrarea supravegheată mai înainte de a dispune prin ordonanță. Ulterior emiterii ordonanței, dar, pe baza înțelegerilor negociate anterior (modalitatea de realizare a supravegherii, substituirea sau sustragerea obiectelor etc.), va asigura informarea autorităților și organelor competente străine că se poate demara punerea în executare a măsurii. În plus, la finalizarea livrării supravegheate, procurorul va avea obligația de a comunica procurorului, organelor de poliție sau altor autorități de stat din statele de tranzit rezultatele livrării supravegheate.

Atunci când România este stat solicitat, potrivit dispozițiilor art. 237 din Legea nr. 302/2004, republicată, procurorul național va trebui să emită o ordonanță de livrare supravegheată și să se asigure că metoda specială este pusă în aplicare de către autoritățile române asemenea situației în care România ar fi fost statul solicitant. Din oficiu sau la solicitarea autorităților și organelor competente din statul de destinație sau a statului care va proceda la efectuarea urmăririi penale, procurorul va putea propune judecătorului de drepturi și libertăți autorizarea unor metode speciale de supraveghere tehnică sau cercetare.

În privința valorii probante a livrării supravegheate, astfel cum am arătat deja, metoda specială de investigații nu va conduce la obținerea de probe în procesul penal prin ea însăși, dar va da prilejul organelor de urmărire penală să descopere informații utile administrării unor alte probe sau să creeze contextul pentru administrarea de probe în timpul livrării supravegheate prin intermediul altor metode speciale de supraveghere sau cercetare.

Conform art. 151 alin. (8) C.pr.pen., la finalul livrării supravegheate, organele de poliție sau autoritățile competente de pe teritoriul României sunt obligate să întocmească un proces-verbal cu privire la activitățile desfășurate, pe care îl vor înainta procurorului. Apreciem că fiecare organ în parte va fi dator să realizeze un astfel de proces-verbal, urmând ca, prin însumarea tuturor, să poată fi reflectată întreaga punere în aplicare a livrării supravegheate de pe teritoriul României[3]. Acest proces-verbal nu va include, în cazul livrării supravegheate transfrontaliere, decât activități naționale, acestea trebuind să fie completate cu acte emise de autoritățile din statele de tranzit. Toate rezultatele activității de livrare supravegheată vor fi transmise organelor

[1] *I.M. De Lucas Martín, C.-E. Ștefan*, op. cit., p. 149.
[2] *Ibidem*, p. 152.
[3] În același sens, *C. Olaru*, op. cit., p. 90.

de urmărire penală competente din statul solicitat[1]. În consecință, rezultatul punerii în aplicare a livrării supravegheate nu se va materializa într-un act singular emis de procuror, astfel că nu va rezulta direct niciun mijloc de probă.

Secțiunea a 2-a. Organele care pot fi chemate să pună în aplicare livrarea supravegheată

O caracteristică aparte a livrării supravegheate este că această metodă specială de cercetare nu poate fi pusă în aplicare de către organele de urmărire penală, presupunând contribuția mai multor autorități de stat, de la poliție până la autorități competente în domenii specializate.

Conform art. 151 alin. (6) C.pr.pen., „*livrarea supravegheată este pusă în aplicare de către poliție sau de altă autoritate competentă. Procurorul stabilește, coordonează și controlează modul de punere în aplicare a livrării supravegheate*".

În cele ce urmează vom face câteva precizări privind persoanele abilitate, potrivit legii, să pună în aplicare livrarea supravegheată, dar și despre posibilitatea folosirii colaboratorilor.

§1. Poliția Română

În realizarea livrării supravegheate, un rol foarte important îl vor avea lucrătorii de poliție, în special în realizarea supravegherii permanente a transportului care va face obiectul livrării supravegheate. Este lesne de înțeles de ce Poliția Română va avea un rol important în cadrul punerii în aplicării a metodei speciale de cercetare, date fiind capacitățile logistice ale acestei instituții, numărul deosebit de mare de angajați și specializarea acestora pe toate domeniile de combatere a infracționalității, inclusiv prin raportare la activitatea de culegere și valorificare de informații operative.

De interes vor fi atribuțiile poliției în domeniul supravegherii și controlului circulației pe drumurile publice, ceea ce va permite lucrătorilor de poliție să realizeze supravegherea permanentă în cazul unui transport pe drumurile publice[2]. În plus, poliția va desfășura activități specifice (inclusiv cele privind prevenirea și combaterea infracționalității) în domeniul transporturilor feroviare, aeriene și navale, putând sprijini punerea în aplicare a livrării supravegheate.

O ipoteză care trebuie avută în vedere este că legea nu exclude posibilitatea folosirii unui investigator sub acoperire pentru punerea în aplicare a livrării supravegheate. Întrucât investigatorii sub acoperire sunt lucrători operativi în cadrul poliției judiciare, aceștia ar putea fi folosiți cel puțin pentru o parte dintre operațiuni. De pildă, se va putea dispune ca un investigator sub acoperire să substituie bunurile care fac obiectul transportului și să le înlocuiască cu altele sau să livreze un colet preluat de la o unitate poștală[3]. Apreciem că, într-o asemenea situație, va fi nevoie de autorizarea utilizării investigatorilor sub acoperire și a colaboratorilor, precum și livrarea supravegheată.

---

[1] *Ibidem*.

[2] Conform art. 26 alin. (1) pct. 21 din Legea nr. 218/2002, Poliția Română „supraveghează și controlează circulația pe drumurile publice, în afara cazurilor exceptate prin lege, și colaborează cu alte autorități publice, instituții, asociații și organizații neguvernamentale, pentru îmbunătățirea organizării și sistematizării circulației, asigurarea stării tehnice a autovehiculelor, perfecționarea pregătirii conducătorilor auto și luarea unor măsuri de educație rutieră a participanților la trafic".

[3] ICCJ, s. pen., dec. nr. 2907 din 30 octombrie 2014, pe *www.scj.ro*; *H. Fejzullah*, Covert and Technical Surveillance Measures and Investigation, în Acta Universitatis Danubius. Juridica, vol. 15, no. 3/2019, p. 46.

§2. Autoritatea Vamală

În realizarea livrărilor supravegheate, indiferent de legislația aplicabilă, un rol deosebit îl vor avea autoritățile vamale naționale, care vor controla mărfurile care sunt introduse sau scoase dintr-o țară, cu această ocazie, putând descoperi transporturi de bunuri ilicite. Ipoteza optimă pentru desfășurarea livrării supravegheate este descoperirea obiectelor ilicite de către autoritățile vamale fără ca persoana care realizează transportul să poată bănui că a fost descoperită[1]. De cele mai multe ori, aceste situații apar atunci când transportul ilicit este introdus într-un container naval, un colet, un bagaj de cală (în cazul transportului aerian) sau, în orice caz, este lăsat nesupravegheat[2].

Autoritățile vamale au un rol determinant nu numai în punctele de trecere a frontierei, acestea putând activa pe tot teritoriul țării, procedând la controlul tuturor mărfurilor supuse reglementărilor vamale. Activitatea autorităților vamale naționale este reglementată de Codul vamal[3].

Conform art. 14 alin. (1) C.vamal, „*autoritatea vamală poate controla mărfurile supuse reglementărilor vamale în orice loc s-ar afla pe teritoriul țării*". În aplicarea acestei dispoziții legale, Codul vamal mai precizează că autoritatea vamală poate:

a) verifica, în condițiile legii, clădiri, depozite, terenuri, *mijloace de transport* susceptibile de a transporta mărfuri supuse unui regim vamal sau care ar trebui supuse unui regim vamal, precum și orice alte obiective (cea mai importantă atribuție, care permite controlul oricărui transport de mărfuri și, astfel, descoperirea obiectelor ilicite transportate – n.n.);

b) preleva, în condițiile legii, probe pe care le analizează în laboratoarele proprii sau agreate, în vederea identificării și expertizării mărfurilor (inclusiv substanțe bănuite a fi narcotice, medicamente etc. – n.n.);

c) efectua investigații, supravegheri și verificări în cazurile în care sunt semnalate situații de încălcare a reglementărilor vamale;

d) desfășura activitățile necesare pentru gestionarea riscurilor;

e) exercita controlul ulterior la sediul agenților economici asupra schimbului de mărfuri dintre România și alte țări, în scopul verificării respectării reglementărilor vamale;

f) identifica, pe bază de documente, persoanele care se află în raza de activitate a biroului vamal, precum și persoanele care au legătură cu mărfurile și se află în locurile verificate potrivit lit. a);

g) participa, în condițiile legii, la realizarea livrărilor supravegheate (există o prevedere legală expresă asupra posibilității de a pune în aplicare ordonanța procurorului de livrare supravegheată – n.n.);

h) coopera direct cu alte instituții centrale române sau cu administrații vamale străine, în condițiile legii și cu respectarea obligațiilor ce decurg din convențiile și înțelegerile la care România este parte;

i) culege, prelucra și utiliza informații specifice necesare pentru prevenirea și combaterea încălcării reglementărilor vamale, inclusiv prin gestionarea, potrivit legii, a unor baze de date privind schimbul de mărfuri.

---

[1] *L. Giurea*, Metodele și tehnicile speciale de investigare a traficului de droguri, în Pro Patria Lex, vol. 13, nr. 2/2014, p. 246.

[2] *I.M. De Lucas Martín, C.-E. Ștefan*, op. cit., pp. 152-153.

[3] Legea nr. 86/2006 privind Codul vamal (M. Of. nr. 350 din 19 aprilie 2006).

Activitatea autorității vamale prin raportare la metoda specială a livrării supravegheate va avea în vedere două posibilități esențiale: *descoperirea obiectelor ilicite cu ocazia controlului mărfurilor*[1] și *punerea în aplicare a livrării supravegheate*.

Activitatea autorității vamale se poate răsfrânge și asupra persoanelor, în anumite situații, putându-se realiza un control corporal sumar atunci când există indicii de fraudă din partea unei persoane[2]. Acest control sumar se va putea desfășura și asupra corpului persoanelor, în cazul în care s-ar aprecia că acestea transportă asupra lor droguri sau precursori[3], pe baza consimțământului valabil exprimat. Agenții vamali vor realiza un control corporal, în caz de refuz, solicitând concursul organelor de urmărire penală pentru examinarea fizică și reținerea persoanei.

De îndată ce sunt descoperite mărfuri ilicite într-un transport sau asupra unei persoane, potrivit art. 100 alin. (7) C.vamal, autoritatea vamală este obligată să sesizeze organele de urmărire penală. Ulterior, după emiterea ordonanței procurorului, autoritatea vamală va putea pune în aplicare livrarea supravegheată cu privire la respectivul transport.

§3. Colaboratorii autorizați de procuror

În situația în care livrarea supravegheată debutează ca urmare a depistării unui transport, s-a afirmat că persoana care este prinsă conducând mijlocul de transport cu bunuri ilicite (cărăuș, curier de droguri) ar putea fi antrenată în operațiunea de livrare supravegheată, chiar dacă, față de aceasta, se va desfășura o urmărire penală pentru faptele comise[4]. Și în măsura în care acceptăm ideea că o livrare supravegheată se va putea realiza cu sprijinul unei asemenea persoane, care va beneficia de cauze de reducere a pedepsei prevăzute de legislația specială, nu va fi suficientă livrarea supravegheată, fiind necesară autorizarea de către procuror a participării autorizate la anumite activități și a utilizării investigatorilor sub acoperire și a colaboratorilor, întrucât continuarea transportului de către colaborator va constitui o infracțiune. Totodată, față de dispozițiile exprese ale art. 151 alin. (6) C.pr.pen., nu este posibilă folosirea colaboratorilor pentru punerea în aplicare a livrării supravegheate, o atare omisiune impunându-se a fi reglementată, *de lege ferenda*, prin permiterea punerii în aplicare a măsurii de către colaboratori.

---

[1] Conform art. 10 C.vamal, controlul poate privi și persoanele fizice care tranzitează frontiera de stat. Astfel, „autoritatea vamală are dreptul să efectueze controlul vamal al mijloacelor de transport și al mărfurilor, precum și al bunurilor și valorilor aparținând persoanelor fizice, prezentate la introducerea sau la scoaterea lor din țară".

[2] Conform art. 10 alin. (3) C.vamal, se consideră că există indicii temeinice de fraudă atunci când agentul vamal:

„a) descoperă în timpul controlului indicii cu privire la existența unor mărfuri nedeclarate sau ascunse;

b) deține informații despre intenția persoanei controlate de a săvârși contravenții sau infracțiuni vamale;

c) posedă date că persoana controlată a săvârșit contravenții sau infracțiuni vamale;

d) constată comportamente neobișnuite din partea persoanei controlate".

[3] Conform art. 11 C.vamal,

„1) Autoritatea vamală, când are informații cu privire la persoanele care, la trecerea frontierei de stat, ar transporta droguri sau precursori ai acestora ascunși în corpul lor, poate, pe baza consimțământului acestora, să le supună unui examen de investigare medicală.

2) În caz de refuz, agentul vamal solicită parchetului în a cărui rază de competență se află biroul vamal autorizarea pentru examinarea medicală și reținerea persoanei. Rezultatele examinării medicale se prezintă parchetului în scopul aplicării procedurilor penale".

[4] *I.M. De Lucas Martín, C.-E. Ștefan*, op. cit., p. 150.

Capitolul VI
Concluzii

Livrarea supravegheată este o metodă specială de cercetare care exista la momentul intrării în vigoare a Codului de procedură penală, fiind întrebuințată în cazul infracțiunilor de gravitate mare privind traficul de narcotice și activitățile grupurilor de criminalitate organizată. Legislația actuală constituie o combinare a legislației speciale aplicabilă anterior intrării în vigoare a Codului de procedură penală.

Natura metodei speciale de cercetare este cea de tehnică specială de investigație, ea neputând conduce în mod direct la obținerea de probe în procesul penal. Cu toate acestea, metoda specială de cercetare nu a fost gândită niciodată ca o măsură care să fie aplicată singură, ci va trebui asociată cu alte metode speciale de supraveghere sau cercetare. Finalitatea livrării supravegheate va fi investigarea unei infracțiuni sau identificarea persoanelor implicate în realizarea de infracțiuni ce implică transporturi ilegale de bunuri. Aceasta va fi urmată, cel mai adesea, de organizarea flagrantului la sfârșitul livrării supravegheate, ceea ce va conduce la prilejul prinderii infractorilor și obținerea de probe.

Livrarea supravegheată își va avea aplicabilitatea maximă atunci când va fi întrebuințată pentru a combate criminalitatea transfrontalieră, în special în cazul traficului de droguri, implicând cooperarea dintre procuror și autoritățile din statele de origine și de tranzit.

În afara unor mici carențe, fie de ordin terminologic, fie datorate lipsei de coroborare a textelor din legea procesuală penală, livrarea supravegheată este reglementată, în prezent, într-un mod adecvat, pentru a contribui la atingerea scopului măsurii, deși este de o complexitate deosebit de mare aplicarea sa în practică. Ca urmare a acestei complexități, prin raportare la numărul de persoane implicate, eforturile materiale necesare, asigurarea unei cooperări internaționale între instituții, coordonarea și controlul permanent al procurorului, realizarea unei supravegheri permanente a transportului, utilizarea măsurii speciale se pretează numai în cauze de mare importanță și pentru descoperirea și prinderea unor grupări infracționale importante.

Titlul XV
Tehnici speciale de investigare prevăzute de legea specială

Capitolul I
Aspecte generale

Secțiunea 1. Noțiunea de „securitate națională"

În ultimul titlu al prezentei lucrări, am decis să abordăm tehnicile speciale de investigare prevăzute în Legea nr. 51/1991 privind securitatea națională a României, republicată[1] (în continuare, „Legea nr. 51/1991"), întrucât cunosc o reglementare procedurală diferită față de cele prevăzute de Codul de procedură penală, însă, cu similarități și diferențe care trebuie să fie evidențiate. În urma intrării în vigoare a Codului de procedură penală, au fost abrogate toate dispozițiile din legile speciale care prevedeau tehnici speciale de investigare, cu excepția celor prevăzute în cuprinsul Legii nr. 51/1991. Ca atare, legislația specială în domeniul tehnicilor speciale de investigare a infracțiunilor se rezumă numai la această din urmă lege. Motivul pentru care au fost menținute separat aceste tehnici speciale de investigare este că reprezintă o formă originară a tuturor metodelor speciale de supraveghere sau cercetare prevăzute de Codul de procedură penală, toate tehnicile speciale avându-și originea în activitatea de culegere de informații desfășurată de serviciile secrete ale unui stat. Este necesar ca orice stat să beneficieze de o marjă de libertate pentru a-și îndeplini funcțiile de „politică înaltă", o marjă care poate fi susținută numai prin proceduri specializate cu un caracter secret[2].

Conceptul de „securitate națională" este definit de legiuitor în cuprinsul art. 1 din Legea nr. 51/1991, în care „*prin «securitatea națională a României» se înțelege starea de legalitate, de echilibru și de stabilitate socială, economică și politică necesară existenței și dezvoltării statului național român ca stat suveran, unitar, independent și indivizibil, menținerii ordinii de drept, precum și a climatului de exercitare neîngrădită a drepturilor, libertăților și îndatoririlor fundamentale ale cetățenilor, potrivit principiilor și normelor democratice statornicite prin Constituție*". În doctrină s-a subliniat că elementul definitoriu al conceptului de „siguranță națională" îl reprezintă garanția oferită de stat privind apărarea eficientă a democrației, statului de drept, ordinii constituționale și valorilor fundamentale stabilite prin Constituție[3]. În acest context, va fi deosebit de important să vedem cum organele din domeniul securității statului pot restrânge drepturile și libertățile fundamentale ale unei persoane, în special dreptul la viață privată, pentru a apăra la nivel general aceste valori, precum și statul, și dacă astfel de restrângeri sunt necesare și proporționale într-o societate democratică.

[1] Legea nr. 51 din 29 iulie 1991 privind securitatea națională a României (republicată în M. Of. nr. 190 din 18 martie 2014).

[2] *S. Grădinaru*, Supravegherea tehnică, 2014, p. 89.

[3] *D.C-tin Mâță*, op. cit., p. 46.

În contextul studierii tehnicilor speciale de investigare prevăzute de Legea nr. 51/1991, va avea o mare importanță modalitatea în care legiuitorul a considerat că se pot combate amenințările la adresa securității naționale, întrucât vor influența determinant procesul de autorizare a activităților specifice de culegere de informații. Potrivit art. 2 alin. (1) din Legea nr. 51/1991, „*securitatea națională se realizează prin cunoașterea, prevenirea și înlăturarea amenințărilor interne sau externe ce pot aduce atingere valorilor prevăzute în art. 1*". Cele trei acțiuni, de cunoaștere, prevenire și înlăturare, vor trebui privite ca un scop în realizarea securității naționale și vor trebui evaluate în mod gradual într-un examen de proporționalitate, alături de drepturile și libertățile fundamentale ale persoanei. Apreciem că, gradual, în funcție de cele trei scopuri, se vor putea autoriza tehnici speciale de investigare mai intruzive și pentru o perioadă mai lungă, însă acesta nu va fi și singurul criteriu, amenințarea la adresa securității naționale trebuind să fie încadrată și în categoriile stabilite de lege. Pentru problemele discutate în prezenta lucrare sunt importante și dispozițiile legale prin care se definește amenințarea la adresa siguranței naționale.

Potrivit art. 3 din Legea nr. 51/1991, constituie „amenințări la adresa securității naționale a României" următoarele:

„*a) planurile și acțiunile care vizează suprimarea sau știrbirea suveranității, unității, independenței sau indivizibilității statului român;*

b) acțiunile care au ca scop, direct sau indirect, provocarea de război contra țării sau de război civil, înlesnirea ocupației militare străine, aservirea față de o putere străină ori ajutarea unei puteri sau organizații străine de a săvârși oricare din aceste fapte;

c) trădarea prin ajutarea inamicului;

d) acțiunile armate sau orice alte acțiuni violente care urmăresc slăbirea puterii de stat;

e) spionajul, transmiterea secretelor de stat unei puteri sau organizații străine ori agenților acestora, procurarea ori deținerea ilegală de documente sau date secrete de stat, în vederea transmiterii lor unei puteri sau organizații străine ori agenților acestora sau în orice alt scop neautorizat de lege, precum și divulgarea secretelor de stat sau neglijența în păstrarea acestora;

f) subminarea, sabotajul sau orice alte acțiuni care au ca scop înlăturarea prin forță a instituțiilor democratice ale statului ori care aduc atingere gravă drepturilor și libertăților fundamentale ale cetățenilor români sau pot aduce atingere capacității de apărare ori altor asemenea interese ale țării, precum și actele de distrugere, degradare ori aducere în stare de neîntrebuințare a structurilor necesare bunei desfășurări a vieții social-economice sau apărării naționale;

g) acțiunile prin care se atentează la viața, integritatea fizică sau sănătatea persoanelor care îndeplinesc funcții importante în stat ori a reprezentanților altor state sau ai organizațiilor internaționale, a căror protecție trebuie să fie asigurată pe timpul ședерii în România, potrivit legii, tratatelor și convențiilor încheiate, precum și practicii internaționale;

h) inițierea, organizarea, săvârșirea sau sprijinirea în orice mod a acțiunilor totalitariste sau extremiste de sorginte comunistă, fascistă, legionară sau de orice altă natură, rasiste, antisemite, revizioniste, separatiste care pot pune în pericol sub orice formă unitatea și integritatea teritorială a României, precum și incitarea la fapte ce pot periclita ordinea statului de drept;

i) actele teroriste, precum și inițierea sau sprijinirea în orice mod a oricăror activități al căror scop îl constituie săvârșirea de asemenea fapte;

j) atentatele contra unei colectivități, săvârșite prin orice mijloace;

k) sustragerea de armament, muniție, materii explozive sau radioactive, toxice sau biologice din unitățile autorizate să le dețină, contrabanda cu acestea, producerea, deținerea, înstrăinarea,

transportul sau folosirea lor în alte condiții decât cele prevăzute de lege, precum și portul de armament sau muniție, fără drept, dacă prin acestea se pune în pericol securitatea națională;

l) inițierea sau constituirea de organizații sau grupări ori aderarea sau sprijinirea sub orice formă a acestora, în scopul desfășurării vreuneia din activitățile enumerate la lit. a)-k), precum și desfășurarea în secret de asemenea activități de către organizații sau grupări constituite potrivit legii.

m) orice acțiuni sau inacțiuni care lezează interesele economice strategice ale României, cele care au ca efect periclitarea, gestionarea ilegală, degradarea ori distrugerea resurselor naturale, fondurilor forestier, cinegetic și piscicol, apelor și altor asemenea resurse, precum și monopolizarea ori blocarea accesului la acestea, cu consecințe la nivel național sau regional".

Față de conținutul legal al categoriilor de fapte care constituie sau pot constitui amenințări la securitatea națională, apreciem că este rolul legiuitorului de a stabili faptele de maximă importanță pentru care se impune o protecție cât mai mare și, în vederea asigurării acesteia, se impune ca activitatea serviciilor din domeniul securității naționale să fie autorizată[1]. Comparând dispozițiile din Legea nr. 51/1991 cu cele din Codul de procedură penală, considerăm că vor avea un rol asemănător cu cel al art. 139 alin. (2) C.pr.pen., în care se definesc infracțiunile pentru care se poate încuviința supravegherea tehnică a unei persoane. Ca atare, dispozițiile trebuie să fie clare și previzibile și să cuprindă categorii de fapte care sunt de o gravitate mare. Spre deosebire de Codul de procedură penală, toate faptele incluse în art. 3 din Legea nr. 51/1991 le considerăm a fi grave și impun luarea de măsuri drastice pentru combaterea amenințărilor la securitatea națională.

Ținând seama de necesitatea ca legea să aibă o calitate de a fi clară și previzibilă, sunt criticabile dispozițiile art. 3 lit. f) din Legea nr. 51/1991, care consideră că vor putea constitui o amenințare la securitatea națională și „*alte acțiuni care (…) aduc atingere gravă drepturilor și libertăților fundamentale ale cetățenilor români (…) ori altor asemenea interese ale țării*". Dispozițiile citate au făcut obiectul a două decizii pronunțate de Curtea Constituțională, prin care s-a constatat a fi neconstituționale, până la acest moment, legiuitorul omițând să pună în acord legislația cu aceste hotărâri.

Prin Decizia Curții Constituționale nr. 91/2018[2] a fost analizată, printre altele, constituționalitatea dispozițiilor art. 3 lit. f) din Legea nr. 51/1991 în privința expresiei „alte acțiuni care (…) aduc atingere gravă drepturilor și libertăților fundamentale ale cetățenilor români", stabilindu-se că această sintagmă este neconstituțională. Această dispoziție fost criticată în momentul în care se urmărea constatarea caracterului nelegal al probelor obținute prin realizarea de activități specifice culegerii de informații într-o cauză de corupție, anterior intrării în vigoare a Codului de procedură penală. Folosirea de activități specifice s-a realizat în contextul în care se aprecia că infracțiunile de corupție de competența D.N.A. sunt considerate amenințări grave care pot constitui amenințări la securitatea națională, argumentându-se că dispozițiile criticate din cuprinsul art. 3 lit. f) din Legea nr. 51/1991 ar permite acest lucru. În

[1] *I. Drăghici*, Importanța serviciilor de informații în identificarea deficiențelor de natură a periclita siguranța națională, în Pro Patria Lex, vol. 10, nr. 2/2012, p. 284.

[2] CCR, Dec. nr. 91 din 28 februarie 2018 referitoare la excepția de neconstituționalitate a dispozițiilor art. 3, art. 10, art. 11 alin. (1) lit. d) și art. 13 din Legea nr. 51/1991 privind securitatea națională a României, precum și a dispozițiilor art. 13 din Legea nr. 51/1991 privind securitatea națională a României, în forma anterioară modificării prin Legea nr. 255/2013 pentru punerea în aplicare a Legii nr. 135/2010 privind Codul de procedură penală și pentru modificarea și completarea unor acte normative care cuprind dispoziții procesual penale (M. Of. nr. 348 din 20 aprilie 2018).

analiza sa, Curtea Constituțională a constatat că legea nu definește ce constituie o faptă care aduce o atingere **gravă** drepturilor și libertăților fundamentale, reținând că: „*din modul de reglementare a sintagmei analizate, rezultă că se poate circumscrie unei amenințări la adresa securității naționale orice faptă/acțiune cu sau fără conotație penală care afectează un drept sau o libertate fundamentală. Cu alte cuvinte, sfera de aplicare a dispoziției criticate este atât de largă, încât față de orice persoană se poate reține exercitarea unei acțiuni care constituie amenințare la adresa securității naționale*"[1]. Curtea constată că dispozițiile legale sunt lipsite de claritate și nu instituie reguli suficient de precise pentru a determina în concret circumstanțele și condițiile în care pot fi împuternicite organele din domeniul securității naționale să recurgă la activități specifice de culegere de informații care constituie tehnici speciale de investigare. Ca atare, Curtea a reținut că: „*având în vedere aceste aspecte și caracterul intruziv al măsurilor de supraveghere tehnică, Curtea reține că este obligatoriu ca aceasta să se realizeze într-un cadru normativ clar, precis și previzibil, atât pentru persoana supusă acestei măsuri, cât și pentru organele de urmărire penală și pentru instanțele de judecată. În caz contrar, s-ar ajunge la posibilitatea încălcării într-un mod aleatoriu/abuziv a drepturilor fundamentale, esențiale într-un stat de drept, privind viața intimă, familială și privată și secretul corespondenței. Este îndeobște admis că drepturile prevăzute la art. 26 și art. 28 din Constituție nu sunt absolute, însă limitarea lor trebuie să se facă cu respectarea dispozițiilor art. 1 alin. (5) din Legea fundamentală, iar gradul de precizie a termenilor și noțiunilor folosite trebuie să fie unul ridicat, dată fiind natura măsurilor intruzive reglementate*"[2], constatând că sintagma „aduc atingere gravă drepturilor și libertăților fundamentale ale cetățenilor români", prevăzută în art. 3 lit. f), încalcă prevederile art. 1 alin. (5) din Constituție privind principiul legalității, art. 26 din Constituție privind viața privată și art. 53 din Constituție privind restrângerea exercițiului unor drepturi sau al unor libertăți. În urma constatării ca neconstituțională a sintagmei arătate, se va restrânge aplicarea abuzivă a activităților de culegere de informații prevăzute de Legea nr. 51/1991 în cazul unor amenințări care nu sunt definite în mod expres în cuprinsul legii.

Prin Decizia Curții Constituționale nr. 802/2018[3] a fost analizată constituționalitatea sintagmei „ori altor asemenea interese ale țării", cuprinsă în art. 3 lit. f) din Legea nr. 51/1991, stabilindu-se că aceasta este neconstituțională. În mod similar cu decizia anterior analizată, problema relevată de Curte a fost că textul legal este lipsit de claritate și previzibilitate, întrucât un organ judiciar sau un organ din domeniul securității naționale nu poate proceda la stabilirea competenței sale în a autoriza sau realiza activități care constituie tehnici speciale de investigare prevăzute de Legea nr. 51/1991. Curtea reține că: „*sfera de cuprindere a sintagmei «altor asemenea interese ale țării» rămâne la libera apreciere a organului abilitat să aplice legea, fără a putea fi circumstanțiată de destinatarul normei. Astfel, prin corelarea între forma/modalitatea de manifestare a activităților prevăzute de art. 3 lit. f) din Legea nr. 51/1991 cu scopul urmărit/valoarea lezată prin acea activitate, în acest caz posibilitatea aducerii atingerii «altor interese ale țării», nu se mai poate determina limita de aplicare a dispoziției de lege criticate. Caracterul deschis al sintagmei criticate determină posibilitatea introducerii sau excluderii de elemente în/*

[1] *Ibidem*, §83.

[2] *Ibidem*, §85.

[3] CCR, Dec. nr. 802 din 6 decembrie 2018 referitoare la excepția de neconstituționalitate a sintagmei „ori altor asemenea interese ale țării", cuprinsă în dispozițiile art. 3 lit. f) din Legea nr. 51/1991 privind securitatea națională a României, și a dispozițiilor art. 4 alin. (2) din Legea nr. 255/2013 pentru punerea în aplicare a Legii nr. 135/2010 privind Codul de procedură penală și pentru modificarea și completarea unor acte normative care cuprind dispoziții procesual penale (M. Of. nr. 218 din 20 martie 2019).

din această categorie, acțiune care se răsfrânge și asupra limitelor de aplicare a dispoziției de lege criticate. În acest mod, limitele de aplicare a dispoziției de lege criticate nu mai pot fi cunoscute de destinatarii normei, care, astfel, nu își pot corecta conduita și nu pot fi capabili să prevadă, într-o măsură rezonabilă, consecințele care pot apărea dintr-un act determinat"[1]. Astfel cum am arătat și prin decizia precedentă a Curții Constituționale, problema de constituționalitate este legată de o lipsă de previzibilitate a legii care va permite ca organul care autorizează sau care realizează activitățile specifice culegerii de informații să își stabilească singur competența prin interpretarea normei legale, un atare aspect afectând mai multe dispoziții ale legii supreme. În consecință, Curtea Constituțională a constatat ca fiind neconstituționale dispozițiile art. 3 lit. f) din Legea nr. 51/1991 în ceea ce privește sintagma „ori alte asemenea interese ale țării", întrucât încalcă art. 1 alin. (5) din Constituție privind principiul legalității, art. 26 din Constituție privind viața privată și art. 53 din Constituție privind restrângerea exercițiului unor drepturi sau al unor libertăți.

În considerarea categoriilor de acțiuni care pot constitui amenințări la adresa securității naționale, legiuitorul a prevăzut mai multe mijloace specifice de cunoaștere, prevenire și combatere a acestora, fiind reglementate în Legea nr. 51/1991 în scopul exclusiv de a menține securitatea națională. Ca atare, securitatea națională este un scop cu un caracter distinct față de cel avut în vedere de legiuitor în stabilirea metodelor speciale de supraveghere sau cercetare din Codul de procedură penală, acest aspect trebuind să fie avut în vedere pe parcursul întregii analize a tehnicilor speciale de investigare prevăzute de Legea nr. 51/1991.

Secțiunea a 2-a. Utilitatea reglementării tehnicilor speciale de investigare privind securitatea națională

În cazul metodelor speciale de supraveghere sau cercetare, am arătat în prezenta lucrare că un mare avantaj al Codului de procedură penală a fost unificarea tuturor tehnicilor speciale prevăzute anterior în Codul de procedură penală din 1968 și în legislația specială într-o singură lege, încercându-se a se omogeniza aceste măsuri și a le face accesibile organelor de urmărire penală în orice cauză. În cazul tehnicilor speciale de investigare din domeniul siguranței naționale, legiuitorul a avut o altă viziune, preferând să le reglementeze în continuare în Legea nr. 51/1991 sub denumirea de „activități specifice de culegere de informații". Utilitatea reglementării lor în mod distinct față de tehnicile speciale de investigare din Codul de procedură penală trebuie să aibă în vedere: *i)* necesitatea existenței unor metode eficiente de combatere a amenințărilor la adresa siguranței naționale; *ii)* caracterul diferit al procedurii folosirii activităților specifice; *iii)* nevoia de a crea o diferență între acestea și metodele speciale de supraveghere sau cercetare, pentru a nu crea confuzie între scopurile celor două tipuri de măsuri.

În privința utilității reglementării tehnicilor speciale de investigare pentru a fi folosite în cazul culegerii de informații, considerăm că problema este oarecum retorică, deoarece procesul penal a împrumutat aceste metode din activitatea desfășurată de serviciile secrete și le folosește. Totuși, prin raportare la caracterul intruziv al tehnicilor speciale de investigare și al caracterului grav al restrângerii drepturilor fundamentale ale omului, era obligatorie reglementarea acestora pentru a fi respectat dreptul la viață privată, garantat de art. 8 Conv.EDO. În fapt, necesitatea reglementării tehnicilor speciale de investigare în domeniul securității naționale are același

[1] *Ibidem*, §80.

temei[1] ca în cazul celor destinate folosirii în procesul penal, singura diferență dintre acestea fiind scopul pentru care sunt utilizate[2].

Activitățile specifice desfășurate de organele din domeniul securității naționale nu se vor rezuma numai la sfera tehnicilor speciale de investigare, legea prevăzând și alte activități specifice pentru culegerea de informații, care nu sunt considerate de legiuitor a constitui restrângeri la drepturile fundamentale ale persoanei. De interes pentru prezenta lucrare nu vor fi decât cele care se vor încadra între tehnicile speciale de investigare.

S-a considerat că necesitatea reglementării distincte a tehnicilor speciale de investigare aplicabile pentru asigurarea securității naționale este datorată competențelor organelor cu atribuții în domeniul securității naționale[3] care reclamă o reglementare specială în vederea îndeplinirii rolului acestora în societate[4].

Pentru a eficientiza folosirea unor tehnici speciale de investigare în scopul apărării siguranței naționale, s-a impus prevederea lor în legislația specială împreună cu o procedură de autorizare distinctă, care să prevină riscul de divulgare a informațiilor clasificate[5]. Spre deosebire de metodele speciale de supraveghere sau cercetare, tehnicile speciale de investigare prevăzute de Legea nr. 51/1991 vor fi autorizate numai la propunerea unui organ competent din domeniul siguranței naționale adresată procurorului general al P.I.C.C.J., care o va analiza sub aspectul legalității temeiniciei și care va putea cere președintelui Înaltei Curți de Casație și Justiție autorizarea măsurilor. Ca atare, procedura de autorizare se va desfășura la un nivel înalt, între conducătorii organelor judiciare române, pentru a se asigura cel mai înalt nivel de secretizare a operațiunii. Fiind restrângeri ale drepturilor și libertăților persoanei, era firească instituirea unei proceduri judiciare de autorizare, neputând fi admis ca un organ din ramura executivului să procedeze la restrângerea dreptului unei persoane, întrucât nu va exista nicio garanție împotriva abuzului. Organele din domeniul securității naționale, în special S.R.I., D.G.P.I. și fosta Direcție Generală de Protecție și Anticorupție, au fost criticate pentru excese și chiar abuzuri desfășurate în contextul realizării activităților specifice, impunându-se ca acțiunile care restrâng drepturile persoanei să fie sever controlate de o autoritate independentă[6]. Mai mult, era imperios necesară prevederea unei proceduri separate și pentru a nu crea o situație complet derogatorie față de principiul autorizării tehnicilor speciale de supraveghere din Codul de procedură penală, nefiind justificat ca pentru unele tehnici identice celor prevăzute în Cod să nu existe o procedură de autorizare judiciară, punând tehnicile de investigare din Legea nr. 51/1991 într-o poziție privilegiată.

O altă diferență care impune un regim legal distinct este implicarea organelor de urmărire penală în procedură, în cazul tehnicilor speciale de investigare prevăzute de Legea nr. 51/1991,

---

[1] *V. supra*, Titlul I, Capitolul II.2.

[2] *P. Ungureanu*, Utilizarea supravegherii tehnice în prevenirea și contracararea amenințărilor la adresa securității naționale. Asemănările și deosebirile între supravegherea tehnică realizată în domeniul instrucției penale și cel al securității naționale, în Revista de Investigare a Criminalității nr. 1/2015, p. 89.

[3] *V. infra*, Titlul XV, Capitolul I.3.

[4] *V. Trif*, op. cit., p. 200.

[5] Potrivit art. 10 alin. (1) din Legea nr. 51/1991,

„(1) Activitatea de informații pentru realizarea securității naționale are caracter secret de stat.

(2) Informațiile din acest domeniu nu pot fi comunicate decât în condițiile prezentei legi".

[6] Sub acest aspect, este suficient să avem în vedere încheierea unor protocoale secrete între aceste instituții și Ministerul Public, prin care s-a urmărit creșterea puterii și a numărului de atribuții ale serviciilor secrete în detrimentul organelor de urmărire penală. *V. supra*, Titlul IV, Capitolul IV.

procurorul fiind implicat numai în procedura de autorizare, urmând ca punerea în executare să se facă în mod discreționar de către organele din domeniul siguranței naționale.

În ceea ce privește nevoia de diferențiere între cele două feluri de tehnici speciale de investigare, legiuitorul a încercat să facă o cât mai bună delimitare a regimului lor juridic, inclusiv sub aspectul denumirii lor. Expresia folosită de legiuitor pentru a desemna metodele speciale de investigare este una diferită de cea folosită în Codul de procedură penală, în cuprinsul Legii nr. 51/1991 fiind reglementate „activități specifice culegerii de informații". S-a susținut că aceste procedee investigative corespund, prin conținutul și finalitatea lor, tehnicilor speciale de investigare[1]. Suntem de acord în mod deplin că, sub aspectul conținutului lor, corespund tehnicilor speciale de investigare, însă suntem în total dezacord că finalitatea acestora ar fi aceeași. Metodele speciale de supraveghere sau cercetare constituie procedee probatorii în procesul penal, reglementarea acestora fiind necesară atât pentru protejarea dreptului la viață privată, cât și pentru respectarea caracterului echitabil al procesului penal, spre deosebire de activitățile specifice culegerii de informații, care nu vor putea fi valorificate ca probe în procesul penal[2]. Acestea din urmă vor putea fi folosite numai în scopul apărării securității naționale, nefiind admisibil ca scopul lor să fie deturnat către unul judiciar, dat fiind faptul că autorizarea lor se va face printr-un control de proporționalitate, cu ingerință adusă vieții private a individului, prin raportare la necesitatea apărării securității naționale, o valoare mai importantă decât prevenirea și sancționarea comiterii de infracțiuni. Diferența dintre valorile sociale ocrotite va permite o mai ușoară încuviințare a unei ingerințe a statului în viața privată a unei persoane atunci când se impune înlăturarea unei amenințări la adresa securității naționale.

În considerarea celor expuse mai sus, apreciem că există o necesitate în a separa tehnicile speciale de investigare destinate prevenirii și combaterii săvârșirii de infracțiuni în funcție de scop, rezultatul acestora fiind probe în procesul penal, și cele care sunt menite să asigure siguranța statului, care vor putea conduce numai la o eventuală sesizare a organelor de urmărire penală. Aceasta constituie diferența cea mai importantă dintre cele două tipuri de tehnici speciale de investigare și cea care are relevanță cu privire la tema prezentei lucrări, întrucât nu va permite o imixtiune între domeniul siguranței naționale și cel judiciar.

Această diferență este subliniată și de Curtea Constituțională, care arată că: „*scopul în care sunt utilizate activitățile întreprinse în domeniul securității naționale este diferit de cel al activității procesual penale. Primele se axează pe cunoașterea, prevenirea și înlăturarea amenințărilor interne sau externe cu scopul realizării securității naționale, iar celelalte au ca scop tragerea la răspundere penală a persoanelor care au săvârșit infracțiuni. Astfel, într-o interpretare sistematică și teleologică, rezultă că Legea nr. 51/1991 și Codul de procedură penală au finalități diferite, care se reflectă și în scopul pentru care este dispusă autorizarea unor activități specifice culegerii de informații care presupun restrângerea exercițiului unor drepturi sau libertăți fundamentale ale omului/măsura supravegherii tehnice*"[3].

[1] *D.C-tin Mâță*, op. cit., p. 364; *C. Olaru*, op. cit., p. 7.

[2] Conform art. 21 alin. (1) din Legea nr. 51/1991, „datele și informațiile de interes pentru securitatea națională, rezultate din activitățile autorizate, dacă indică pregătirea sau săvârșirea unei fapte prevăzute de legea penală, sunt reținute în scris și transmise organelor de urmărire penală, potrivit art. 61 din Codul de procedură penală, însoțite de mandatul emis pentru acestea, la care se adaugă propunerea de declasificare, după caz, totală sau în extras, potrivit legii, a mandatului. Convorbirile și/sau comunicările interceptate, redate în scris, și/sau imaginile înregistrate se transmit organelor de urmărire penală în integralitate, însoțite de conținutul digital original al acestora".

[3] CCR, Dec. nr. 91 din 28 februarie 2018 (M. Of. nr. 348 din 20 aprilie 2018).

Nevoia de a se crea o diferență între cele două tipuri de tehnici speciale de investigare este dată de importanța evitării unei interferențe nedorite între acestea, neputând fi permisă imixtiunea determinantă în desfășurarea procesul penal a organelor din domeniul siguranței naționale. Acestea nu se vor putea substitui niciodată organelor de urmărire penală, neputând administra probe în locul acestora, și orice act rezultat din activitatea de culegere de informații nu va putea fi valorificat ca probă în procesul penal. Asta nu va însemna că organele din domeniul securității naționale vor putea să ignore situațiile în care constată săvârșirea de infracțiuni, fiind obligate, în temeiul art. 61 C.pr.pen., să sesizeze organele de urmărire penală, activitățile specifice de culegere de informații putând avea ca rezultat această sesizare. Credem că o atare situație nu contrazice cele enunțate mai sus, întrucât descoperirea săvârșirii unei infracțiuni va fi una întâmplătoare, neputându-se proceda la autorizarea unor activități specifice de culegere de informații având ca scop doar sesizarea organelor de urmărire penală.

Secțiunea a 3-a. Organele cu competențe în domeniul securității naționale

Spre deosebire de tehnicile speciale de investigare care pot fi puse în executare de procuror sau de către organele de cercetare penală ori lucrători specializați de poliție, activitățile specifice de culegere de informații pot fi realizate numai de organe din domeniul securității naționale, acestea fiind menționate în cuprinsul Legii nr. 51/1991, reglementarea activităților desfășurate de acestea fiind detaliate în legislația care vizează fiecare serviciu în parte.

Toate organele din domeniul securității naționale au o particularitate comună, respectiv au profilul unor servicii de informații, adică organe care au ca obiect de activitate principal culegerea de informații. Obiectul culegerii de informații trebuie să includă cel puțin acele categorii de informații care pot contribui la realizarea securității naționale.

Potrivit dispozițiilor art. 8 alin. (1) din Legea nr. 51/1991, „*activitatea de informații pentru realizarea securității naționale se execută de Serviciul Român de Informații, organul de stat specializat în materia informațiilor din interiorul țării, Serviciul de Informații Externe, organul de stat specializat în obținerea din străinătate a datelor referitoare la securitatea națională, și Serviciul de Protecție și Pază, organul de stat specializat în asigurarea protecției demnitarilor români și a demnitarilor străini pe timpul prezenței lor în România, precum și în asigurarea pazei sediilor de lucru și reședințelor acestora*". Aceste trei organe sunt enumerate de legiuitor în mod distinct, deoarece reprezintă autorități administrative autonome[1], care au un statut special, instituit prin lege, de înființare proprie și care nu se află în subordinea niciunui alt organ, decât a comisiilor de specialitate ale Parlamentului, desemnate pentru controlul acestora. În doctrină s-a subliniat faptul că o problemă deosebită este limitarea acestui control la primirea și ascultarea rapoartelor anuale de activitate ale acestor instituții[2]. Prin regulile de funcționare a comisiilor, nu se va putea avea un acces direct și nemijlocit la informațiile în baza cărora serviciile de informații funcționează.

[1] Conform art. 69 din Codul administrativ, „Autoritățile administrative autonome prevăzute la art. 51 alin. (1) sunt autorități ale administrației publice centrale a căror activitate este supusă controlului Parlamentului, în condițiile prevăzute de legile lor de înființare, organizare și funcționare și care nu se află în raporturi de subordonare față de Guvern, de ministere sau față de organele de specialitate ale acestora".

[2] *D.C-tin Mâță*, Considerații generale în legătură cu rolul Justiției în Mecanismul de Apărare a Securității Naționale, în Dreptul nr. 9/2015, p. 78.

După cum vom vedea în prezența secțiune, fiecare dintre cele trei organe amintite are un set de atribuții prin care încearcă evitarea suprapunerii activităților desfășurate, cel mai bun exemplu fiind relația dintre S.R.I. și S.I.E. În schimb, S.P.P. va interacționa, în domeniul tehnicilor speciale de investigare, numai cu S.R.I.

Alături de cele trei autorități administrative autonome, Legea nr. 51/1991 instituie posibilitatea ca Ministerul Apărării Naționale, Ministerul Afacerilor Interne și Ministerul Justiției să își organizeze structuri de informații cu atribuții specifice domeniilor lor de activitate, activitatea care urmează va fi controlată de Parlament, cu mențiunea că fiecare dintre acestea va fi subordonată conducerii ministerului din care face parte[1]. Sfera de activitate a acestor organe va fi mai restrânsă și va viza strict domeniul de activitate al acestora. După cum vom vedea, controlul parlamentar este unul iluzoriu, fiind necesară introducerea unui mecanism efectiv de guvernanță a serviciilor de informații care să permită direcționarea serviciilor secrete către obiective stabilite de organele reprezentative ale statului[2].

Toate organele din domeniul securității naționale, fie autorități administrative autonome, fie organe în subordinea autorităților administrative centrale, vor putea desfășura activități de culegere de informații, vor putea deține și folosi mijloace tehnice specifice pentru activitatea de culegere de informații, inclusiv echipamente tehnice a căror deținere este interzisă de lege particularilor, precum mijloacele tehnice de interceptare a comunicațiilor. În funcție și de specificul activității, organele din domeniul securității naționale vor putea avea și unități militare combatante, astfel că activitatea de culegere de informații va putea fi exploatată direct de către aceste instituții, în măsura în care se impune înlăturarea unui pericol la adresa securității naționale.

Legislația specială din domeniul securității naționale, mai ales cea care reglementează activitatea organelor din domeniul securității naționale, a fost criticată în mod just ca fiind neunitară, greu accesibilă și lipsită de previzibilitate[3]. În cele ce urmează vom analiza succint fiecare organ din domeniul securității naționale, subliniindu-le pe cele care pot pune în aplicare tehnicile speciale de investigație prevăzute de Legea nr. 51/1991.

§1. Serviciul Român de Informații

S.R.I. este principalul organ din domeniul securității naționale, având competențe extinse care includ și activități susceptibile de a contribui la realizarea actelor de urmărire penală. Activitatea S.R.I. este reglementată prin Legea nr. 14/1992 privind organizarea și funcționarea Serviciului Român de Informații[4], stabilindu-se, prin art. 2, ca atribuție generală, că: „*Serviciul Român de Informații organizează și execută activități pentru culegerea, verificarea și valorificarea informațiilor necesare cunoașterii, prevenirii și contracarării oricăror acțiuni care constituie, potrivit legii, amenințări la adresa siguranței naționale a României*". Aceasta este doar

[1] Conform art. 9 din Legea nr. 51/1991:
„(1) Ministerul Apărării Naționale, Ministerul Afacerilor Interne și Ministerul Justiției își organizează structuri de informații cu atribuții specifice domeniilor lor de activitate.
(2) Activitatea de informații a acestor organe se desfășoară în conformitate cu prevederile prezentei legi și este controlată de Parlament".

[2] *Z.K. Goldman*, în Z.K. Goldman, S.J. Rascoff, Global Intelligence Oversight. Governing Security in the Twenty-First Century, Oxford University Press, New York, 2016, pp. 207-208.

[3] *S. Grădinaru*, Supravegherea tehnică, 2014, p. 97.

[4] Legea nr. 14 din 24 februarie 1992 privind organizarea și funcționarea Serviciului Român de Informații (M. Of. nr. 33 din 3 martie 1992).

o atribuție generală, întrucât prin lege se stabilesc mai multe responsabilități pentru acest serviciu de informații, de la verificarea regimului documentelor clasificate, atunci când nu intră în competența altui serviciu secret, până la verificarea corporală a pasagerilor care se vor îmbarca pe aeronave, dar și activități de combatere a terorismului prin unități de intervenție specializată.

Activitatea desfășurată de S.R.I. cuprinde mai multe domenii de activitate concrete, cel despre care am făcut numeroase referințe în prezenta lucrare fiind organizarea și administrarea în subordinea sa a Centrului Național de Interceptare a Comunicațiilor. Sub acest aspect, sunt importante prevederile art. 8 alin. (2) din Legea nr. 14/1992, în care se arată că: „*pentru relația cu furnizorii de comunicații electronice destinate publicului, Centrul Național de Interceptare a Comunicațiilor din cadrul Serviciului Român de Informații este desemnat cu rolul de a obține, prelucra și stoca informații în domeniul securității naționale. La cererea organelor de urmărire penală, Centrul asigură accesul nemijlocit și independent al acestora la sistemele tehnice în scopul executării supravegherii tehnice prevăzute la art. 138 alin. (1) lit. a) din Codul de procedură penală*". Din aceasta rezultă că C.N.I.C. poate fi folosit de către S.R.I. în mod direct în activitatea de culegere de informații, dar și de către organele de urmărire penală în punerea în executare a supravegherii tehnice prin interceptarea comunicațiilor. În acest din urmă caz, organele de urmărire penală vor acționa în mod independent, S.R.I. punând la dispoziție doar infrastructura tehnică necesară și oferind servicii de mentenanță și suport tehnic. În cazul în care infracțiunile cercetate sunt cele contra securității naționale sau de terorism, S.R.I. va putea, prin ofițeri care vor avea calitatea de organe de cercetare penală specializate, să pună în executare mandatele de supraveghere tehnică emise de judecătorul de drepturi și libertăți, ca urmare a dispoziției exprese a procurorului.

Reamintim faptul că, în cazul interceptării comunicațiilor telefonice în sistem centralizat, toate autoritățile statului, inclusiv alte servicii de informații, vor trebui să folosească echipamentele C.N.I.C.

În situația în care se desfășoară activități de culegere de informații prin utilizarea tehnicilor speciale de investigare, S.R.I. va trebui să obțină autorizarea legală prevăzută în Legea nr. 51/1991, nefiind permise activități care pot constitui restrângeri ale drepturilor și libertăților persoanei[1]. Rezultatele unor astfel de activități de culegere de informații vor putea fi valorificate de S.R.I. și, în măsura în care vor constitui infracțiuni, vor putea sta la baza sesizării organelor de urmărire penală.

Deși au existat numeroase decizii ale Curții Constituționale care au vizat activitățile desfășurate de S.R.I. în legătură cu activitatea organelor de urmărire penală, Legea nr. 14/1992 nu a fost încă adaptată la aceste decizii. De pildă, potrivit art. 12 alin. (2) din Legea nr. 14/1992, „*la solicitarea organelor judiciare competente, cadre anume desemnate din Serviciul Român de Informații pot acorda sprijin la realizarea unor activități de cercetare penală pentru infracțiuni privind siguranța națională*", acesta reprezentând temeiul legal al constituirii echipelor comune de anchetă dintre procurori și S.R.I., precum și desfășurarea de către S.R.I. a unor activități de verificare operativă în teren la solicitarea procurorului. Corelativ, întâlnim și o obligație din

[1] Conform art. 10 alin. (1) din Legea nr. 14/1992: „În situațiile care constituie amenințări la adresa securității naționale, Serviciul Român de Informații, prin cadre desemnate în acest scop, desfășoară activități specifice culegerii de informații care presupun restrângerea exercitării unor drepturi sau libertăți fundamentale ale omului, efectuate potrivit procedurii prevăzute în Legea nr. 51/1991, cu modificările ulterioare, care se aplică în mod corespunzător".

partea organelor de urmărire penală de a comunica S.R.I. orice date sau informații privitoare la siguranța națională care rezultă din activitatea de urmărire penală. Dispozițiile anterioare se impun a fi considerate neconstituționale, întrucât legiuitorul a prevăzut o interferență neîncuviințată a S.R.I. în activitatea de urmărire penală, preluând nepermis din atribuțiile și puterile procurorului.

§2. Serviciul de Informații Externe

Activitatea S.I.E. este reglementată prin Legea nr. 1/1998 privind organizarea și funcționarea Serviciului de Informații Externe, republicată[1], iar, la art. 1 din legea menționată, se arată că: „*Serviciul de Informații Externe este organul de stat specializat în domeniul informațiilor externe privind siguranța națională și apărarea României și a intereselor sale*". Ținând seama de aria de activitate a acestui serviciu de informații, Legea nr. 1/1998, republicată, nu prevede dispoziții exprese privind întrebuințarea de tehnici speciale de investigare, din contră, legiuitorul instituie o interdicție de a se folosi mijloace de obținere, verificare sau valorificare a datelor și a informațiilor care să lezeze în vreun fel drepturile sau libertățile fundamentale ale cetățenilor, viața particulară, onoarea sau reputația lor ori sa îi supună la îngrădiri ilegale[2]. Mai mult, încălcarea acestei reguli s-ar pedepsi conform legii. Din modul de exprimare al legiuitorului, s-ar înțelege că interdicția de a restrânge drepturile și libertățile fundamentale s-ar aplica numai cetățenilor români, astfel că, *per a contrario*, nu ar exista o interdicție de a aplica măsuri de acest tip persoanelor care nu au cetățenia română. Nu credem că acesta este sensul legal, ci acesta trebuie să fie raportat la dispozițiile art. 14 din Legea nr. 51/1991, în care sunt reglementate activitățile specifice de culegere de informații care pot constitui restrângeri ale drepturilor unei persoane, neputând fi aplicate de către S.I.E., întrucât activitatea se va desfășura în afara granițelor țării. Cu alte cuvinte, deși admitem că S.I.E. va putea folosi tehnici speciale de investigare, competența sa pentru domeniul extern al siguranței naționale nu va permite o autorizare a tehnicilor speciale, deoarece acestea, fiind autorizate de o instanță națională, presupun aplicarea lor numai pe teritoriul țării, ceea ce ar însemna că trebuie aplicate de către S.R.I. În doctrină s-a reținut în sens invers, că activitatea S.I.E. va trebui să fie în conformitate cu o interpretare mai strictă a dispozițiilor legale menționate, neavând posibilitatea să recurgă la acte care să restrângă drepturile și libertățile fundamentale ale persoanei[3].

Faptul că S.I.E. poate să întreprindă activități de culegere de informații care pot consta și în tehnici speciale de investigare rezultă din dispozițiile art. 10 alin. (1) din Legea nr. 1/1998, republicată, în care se prevede că: „*Serviciul de Informații Externe este autorizat să folosească persoane juridice sub acoperire, înființate în condițiile legii, să utilizeze metode specifice, să creeze și să dețină mijloace adecvate pentru obținerea, verificarea, protecția, evaluarea, valorificarea și stocarea datelor și informațiilor referitoare la siguranța națională*". Din dispozițiile legale citate rezultă și o tehnică specială de investigare, necunoscută în legislația procesuală penală – înființarea de persoane juridice sub acoperire, aceasta fiind considerată ca o atare tehnică în

[1] Legea nr. 1 din 6 ianuarie 1998 privind organizarea și funcționarea Serviciului de Informații Externe (republicată în M. Of. nr. 511 din 18 octombrie 2000).

[2] Conform art. 10 alin. (3) din Legea nr. 1/1998, republicată: „Folosirea mijloacelor de obținere, verificare și valorificare a datelor și a informațiilor nu trebuie să lezeze în nici un fel drepturile sau libertățile fundamentale ale cetățenilor, viața particulară, onoarea sau reputația lor ori sa îi supună la îngrădiri ilegale".

[3] *D.C-tin Mâță*, op. cit., p. 368.

pct. 27 al Memorandumului explicativ al Recomandării (2005) 10 a Comitetului de Miniștri[1], în care, prin „tehnici speciale de investigare" se înțelege, între altele: *operațiuni sub acoperire, operațiuni sub acoperire disimulate*, dându-se ca exemplu *o societate comercială sub acoperire*.

În opinia noastră, chiar dacă dispozițiile legale cuprinse în Legea nr. 51/1991 ar permite desfășurarea de către S.I.E. a activităților de culegere de informații prin tehnici speciale de investigare, acestea nu se vor putea desfășura pe teritoriul țării și, astfel, nu va trebui să fie urmată procedura de autorizare prevăzută de legea română.

§3. Serviciul de Protecție și Pază

Al treilea serviciu secret al României menționat expres în cuprinsul Legii nr. 51/1991 este S.P.P., a cărui organizare și funcționare este reglementată prin Legea nr. 191/1998[2]. Domeniul de activitate al S.P.P. este asigurarea protecției demnitarilor români, a demnitarilor străini pe timpul ședерii lor în România, a familiilor acestora, precum și asigurarea pazei sediilor de lucru și a reședințelor acestora. Activitatea acestui serviciu secret se realizează atât pe teritoriul țării, cât și în afara ei, dar numai pentru apărarea demnitarilor români.

Atribuțiile S.P.P. sunt stabilite prin art. 14 din Legea nr. 191/1998, în care sunt enumerate mai multe activități de culegere de informații care pot fi desfășurate de către acest organ, inclusiv cele care au o legătură cu tehnicile speciale de investigare prevăzute de Legea nr. 51/1991. Astfel, conform art. 14 alin. (1) lit. d) din Legea nr. 191/1998, S.P.P. „*poate efectua, cu respectarea Legii nr. 51/1991 privind siguranța națională a României, verificări prin: solicitarea și obținerea de obiecte, înscrisuri sau relații oficiale de la instituții publice; consultarea de specialiști ori experți; primirea de sesizări sau note de relații; fixarea unor momente operative prin mijloace tehnice sau prin constatări personale*", acestea corespunzând cu activitățile specifice de culegere de informații prevăzute la art. 13 alin. (1) lit. a)-e) din Legea nr. 51/1991. Acestea vor fi activitățile specifice care, în viziunea Legii nr. 51/1991, nu presupun o restrângere a drepturilor și libertăților fundamentale ale cetățeanului și nu presupun nici autorizarea prealabilă a instanței competente.

În privința activităților specifice culegerii de informații care vor constitui tehnici speciale de investigare, vor fi aplicabile dispozițiile art. 14 alin. (1) lit. e) din Legea nr. 191/1998, care prevăd că S.P.P. poate „*solicita procurorului, în cazuri justificate, cu respectarea prevederilor Codului de procedură penală, autorizarea efectuării unor activități potrivit Legii nr. 51/1991, în scopul culegerii de informații pentru îndeplinirea misiunilor specifice. Operațiunile tehnice pentru realizarea acestor activități se execută de către Serviciul Român de Informații*". Este evident că acest articol, deși face trimitere la „unele activități", se referă la cele prevăzute de art. 14 din Legea nr. 51/1991, întrucât sunt singurele care se pot autoriza prin intervenția procurorului în vederea sesizării instanței competente. Nu considerăm că mențiunea privind realizarea operațiunilor tehnice de către S.R.I. trebuie să fie interpretată ca fiind o delegare, ci semnifică implicarea S.R.I. numai în privința acelor activități pentru care S.P.P. nu deține mijloace tehnice suficiente, cel mai clar exemplu fiind activitatea de interceptarea comunicațiilor care

[1] Memorandumul explicativ al Recomandării (2005) 10 a Comitetului de Miniștri al Consiliului Europei, pe *www.coe.int*

[2] Legea nr. 191 din 19 octombrie 1998 privind organizarea și funcționarea Serviciului de Protecție și Pază (M. Of. nr. 402 din 22 octombrie 1998).

se va realiza numai de către C.N.I.C. din cadrul S.R.I.[1]. În sens contrar, s-a susținut că toate operațiunile tehnice specifice culegerii de informații vor fi desfășurate de S.R.I.[2].

În privința valorii probante a rezultatelor activităților desfășurate de S.P.P., observăm că Legea nr. 191/1998 conține un anacronism foarte grav, pentru că, prin dispozițiile art. 14 alin. (1) lit. f), pare a da valoarea de probă acestor rezultate. Conform art. 14 alin. (1) lit. f) din Legea nr. 191/1998, S.P.P. „*consemnează rezultatele activităților prevăzute la lit. d) și e) în acte de constatare, întocmite cu respectarea prevederilor Codului de procedura penală, care pot constitui mijloace de probă*". Cu alte cuvinte, se reglementează că activitățile specifice de culegere de informații la care am făcut referire mai sus, inclusiv cele care constituie tehnici speciale de investigare, vor putea fi folosite ca probe în procesul penal. Analizând dispoziția criticată, observăm că forma avută în vedere datează din anul 2002[3], mai înainte de intrarea în vigoare a Codului de procedură penală anterior, permițând folosirea rezultatelor activităților specifice ca mijloace de probă în procesul penal[4], ceea ce nu s-a preluat în cuprinsul legislației procesuale penale actuale. Observăm că textul legal anterior citat este în disonanță și cu dispozițiile Legii nr. 51/1991, care indică posibilitatea folosirii rezultatelor activităților specifice numai ca date și informații pentru sesizarea organelor de urmărire penală. Astfel, anacronismul arătat este dat de o lipsă de corelare dintre Legea nr. 191/2008, Legea nr. 51/1991 și Codul de procedură penală în vigoare, iar remediul va consta în posibilitatea folosirii rezultatelor activităților specifice numai în vederea sesizării organelor de urmărire penală.

§4. Ministerul Apărării Naționale – Direcția Generală de Informații a Apărării

Un organ în domeniul securității naționale esențial pentru orice țară este serviciul de informații militar, care este reglementat, în România, prin Legea nr. 346/2006 privind organizarea și funcționarea Ministerului Apărării Naționale, republicată[5], ca o direcție distinctă în cadrul ministerului, sub denumirea de „Direcția Generală de Informații a Apărării"[6]. Această direcție are o competență generală în domeniul militar al securității naționale, atât internă, cât și externă. Ceea ce o face distinctă de alte servicii este că are în vedere numai aspectele militare ale siguranței naționale, astfel că nu privește activitatea desfășurată de persoane civile, dar se observă că există o oarecare suprapunere cu activitatea S.R.I. În realitate, astfel cum rezultă din

[1] După cum am mai arătat în prezenta lucrare, C.N.I.C. are 4 fluxuri de interceptare, trei sunt asociate P.I.C.C.J., D.N.A. și D.I.I.C.O.T., iar una va fi dedicată serviciilor de informații. *V. supra*, Titlul IV, Capitolul V.

[2] *D.C-tin Mâță*, op. cit., p. 368.

[3] Ultima modificare a art. 14 alin. (1) lit. f) din Legea nr. 191/1998 a avut loc prin art. I pct. 2 din O.U.G. nr. 103 din 29 august 2002 (M. Of. nr. 669 din 9 septembrie 2002).

[4] *S. Grădinaru*, Supravegherea tehnică, 2014, p. 96.

[5] Legea nr. 346 din 21 iulie 2006 privind organizarea și funcționarea Ministerului Apărării Naționale (republicată în M. Of. nr. 867 din 2 noiembrie 2017).

[6] Conform art. 15 alin. (1) din Legea nr. 346/2006, republicată: „Direcția generală de informații a apărării asigură obținerea, prelucrarea, verificarea, stocarea și valorificarea informațiilor și datelor referitoare la factorii de risc și amenințările interne și externe, militare și nonmilitare, care pot afecta securitatea națională în domeniul militar, acționează pentru prevenirea, descurajarea și contracararea oricăror riscuri sau amenințări care pot afecta securitatea națională a României în domeniul militar, coordonează aplicarea măsurilor contrainformative și cooperarea atât cu serviciile/structurile departamentale naționale și de informații, cât și cu cele ale statelor membre ale alianțelor, coalițiilor și organizațiilor internaționale la care România este parte și elaborează politicile, coordonează și controlează, la nivelul Ministerului Apărării Naționale, potrivit legii, activitățile referitoare la protecția informațiilor clasificate naționale, NATO, UE și a informațiilor clasificate care fac obiectul tratatelor, înțelegerilor și acordurilor bilaterale sau multilaterale în domeniul apărării la care România este parte".

dispozițiile art. 15 alin. (1) din Legea nr. 346/2006, republicată, direcția va colabora și cu alte organe din domeniul securității naționale din țară sau din străinătate. Un exemplu în acest sens este lupta împotriva terorismului, care se va încadra atât în competența S.R.I., cât și a D.G.I.A., în funcție de specificul amenințării și de locul în care are loc aceasta.

În realizarea activităților specifice de culegere de informații, D.G.I.A. va putea avea și unități combatante care să fie trimise în teatre de război, dar și să desfășoare activitatea sa în mod deschis sau sub acoperire.

De importanță pentru lucrarea de față este posibilitatea D.G.I.A. de a folosi tehnici speciale de investigare în activitatea de culegere de informații. Din perspectiva Legii nr. 346/2006, republicată, nu se precizează în mod clar că pot să folosească asemenea tehnici sau că ar putea să solicite autorizarea de astfel de tehnici, însă este permisă achiziționarea de către acest serviciu de informații a unor „categorii de tehnică și bunuri specifice". Categoria aceasta de bunuri specifice poate însemna absolut orice bun, ținând seama atât de domeniul militar al structurii, cât și cel de serviciu de informații. Apreciem că D.G.I.A. va putea solicita și, ulterior, pune în aplicare tehnicile speciale de investigare prevăzute de art. 14 din Legea nr. 51/1991. Această concluzie rezultă din art. 9 alin. (2) din Legea nr. 51/1991, în care se arată că structurile de informații din cadrul Ministerului Apărării Naționale își vor desfășura activitatea de informații în conformitate cu prevederile Legii nr. 51/1991, putând face aplicarea și a dispozițiilor legale privind autorizarea tehnicilor speciale de investigare din domeniul securității naționale.

§5. Ministerul Afacerilor Interne – Direcția Generală de Protecție Internă

Un alt serviciu de informații aflat în subordinea unui minister este D.G.P.I. a Ministerului Afacerilor Interne, care funcționează în temeiul O.U.G. nr. 76/2016[1]. Activitatea D.G.P.I. va consta în desfășurarea de activități de identificare, contracarare și înlăturare a amenințărilor, vulnerabilităților și factorilor de risc la adresa informațiilor, patrimoniului, personalului, misiunilor, procesului decizional și capacității operaționale ale structurilor Ministerului Afacerilor Interne, precum și a celor care pot duce la tulburarea gravă a ordinii publice, astfel cum rezultă din art. 1 din O.U.G. nr. 76/2016. Din definiția dată rezultă o competență vagă și deosebit de largă în special în privința „amenințărilor, vulnerabilităților și factorilor de risc", care pot duce la tulburarea gravă a ordinii publice, oferind serviciului de informații o competență generală în a desfășura o multitudine de activități. În cuprinsul atribuțiilor D.G.P.I. nu sunt clarificate aceste aspecte, reținându-se în art. 10 lit. a) din O.U.G. nr. 76/2016 că D.G.P.I. „*desfășoară activități de informații, contrainformații și de protecție în scopul identificării, prevenirii și contracarării amenințărilor, vulnerabilităților și factorilor de risc care pot conduce la tulburarea gravă a ordinii publice sau care vizează informațiile, patrimoniul, personalul, misiunile, procesul decizional și capacitatea operațională ale structurilor Ministerului Afacerilor Interne*". Din punctul nostru de vedere, este de înțeles ca acest serviciu să contracareze amenințările care pot afecta structura componentelor Ministerului Afacerilor Interne, dar nu apreciem că în sfera protejării ordinii publice vor putea fi încadrate și activitățile din domeniul judiciar.

În mod similar altor servicii de informații, D.G.P.I. va putea întrebuința activități specifice culegerii de informații, în sensul art. 13-14 din Legea nr. 51/1991, având posibilitatea de a

[1] O.U.G. nr. 76 din 2 noiembrie 2016 privind înființarea, organizarea și funcționarea Direcției Generale de Protecție Internă a Ministerului Afacerilor Interne (M .Of. nr. 891 din 8 noiembrie 2016).

solicita autorizarea tehnicilor speciale de investigare prevăzute în această lege[1]. Punerea în executare se va realiza de către ofițerii serviciului de informații, datele și informațiile obținute vor putea fi folosite de D.G.P.I. ori, dacă se obțin informații care nu fac parte din domeniul de activitate, se vor transmite celorlalte organe în domeniul securității naționale. În măsura în care se vor obține date și informații privind pregătirea sau săvârșirea unei infracțiuni, potrivit art. 13 alin. (2) din O.U.G. nr. 76/2016, se vor transmite organelor de urmărire penală în conformitate cu art. 61 C.pr.pen., putând sta la baza sesizării organelor de urmărire penală.

O limitare necesară a activității D.G.P.I. o constituie imposibilitatea efectuării de către acest serviciu a actelor de urmărire penală, o atare interdicție fiind instituită de art. 15 alin. (1) din O.U.G. nr. 76/2016. Legiuitorul se referă la imposibilitatea efectuării de acte de cercetare penală, și nu de urmărire penală, în acest sens trebuie să avem în vedere că nu poate exista nicio implicare a D.G.P.I. în activitatea de urmărire penală, nici măcar în domeniul concursului tehnic al unor măsuri. Ca atare, rolul D.G.P.I. în activitățile organelor de urmărire penală vor fi limitate numai la transmiterea unor date și informații rezultate din activitățile de culegere de informații desfășurate în conformitate cu dispozițiile Legii nr. 51/1991. În niciun caz, D.G.I.P.I. nu va putea pune în executare supravegherea tehnică autorizată de judecătorul de drepturi și libertăți, conform art. 138 și urm. C.pr.pen., întrucât această instituție nu are și nu poate dobândi atribuții specifice poliției judiciare.

§6. Ministerul Justiției – Direcția Generală de Protecție și Anticorupție

Astfel cum se arată în cuprinsul art. 9 alin. (1) din Legea nr. 51/1991, Ministerul Justiției își organizează structuri de informații cu specific în domeniul de activitate, respectiv în domeniul judiciar. Dintre toate autoritățile centrale deja menționate, Ministerul Justiției nu mai are nicio structură de informații, încă din anul 2006 fiind desființată Direcția Generală de Protecție și Anticorupție[2], întrucât s-a apreciat că nu este necesară o astfel de structură în cadrul ministerului. Deși avea atribuții în domeniul securității naționale, aceasta era corespunzătoare Direcției Generale a Penitenciarelor și avea o funcție aparent limitată, doar cu privire la sistemul penitenciar, dacă ne raportăm la dispozițiile art. 4 din H.G. nr. 637/2004, abrogată în prezent[3]. Analizând aceste atribuții, observăm că se suprapun cu atribuțiile mai largi ale

[1] Conform art. 12 din O.U.G. nr. 76/2016:

„(1) În vederea identificării amenințărilor, vulnerabilităților și factorilor de risc care pot conduce la tulburarea gravă a ordinii publice sau care vizează informațiile, patrimoniul, personalul, misiunile, procesul decizional ori capacitatea operațională ale structurilor Ministerului Afacerilor Interne, Direcția Generală de Protecție Internă desfășoară activitățile prevăzute la art. 13 lit. a)-e) din Legea nr. 51/1991, republicată, cu completările ulterioare.

(2) În situațiile care constituie amenințări la adresa securității naționale care vizează tulburarea gravă a ordinii publice sau informațiile, patrimoniul, personalul, misiunile, procesul decizional ori capacitatea operațională ale structurilor Ministerului Afacerilor Interne, Direcția Generală de Protecție Internă desfășoară activitățile prevăzute la art. 14 alin. (2) din Legea nr. 51/1991, republicată, cu completările ulterioare, cu respectarea prevederilor art. 14 alin. (1) și art. 15-21 din aceeași lege, care se aplică în mod corespunzător".

[2] Înființată prin H.G. nr. 637 din 29 aprilie 2004 privind funcționarea și atribuțiile Direcției Generale de Protecție și Anticorupție din subordinea Ministerului Justiției (M. Of. nr. 417 din 11 mai 2004), desființată prin H.G. nr. 127/2006 privind desființarea Direcției Generale de Protecție și Anticorupție din subordinea Ministerului Justiției (M. Of. nr. 125 din 9 februarie 2006), prin reorganizarea Serviciului Independent de Protecție și Anticorupție (S.I.P.A.).

[3] Conform art. 4 din H.G. nr. 637/2004 (abrogată prin H.G. nr. 127/2006), „Direcția Generală de Protecție și Anticorupție desfășoară activități de obținere, verificare, prelucrare, stocare și valorificare a informațiilor în domeniul siguranței naționale, corespunzătoare Direcției Generale a Penitenciarelor, Regiei Autonome «Multi-product», unităților și întreprinderilor subordonate acestora, îndeplinind următoarele atribuții principale:

a) cunoașterea, prevenirea și înlăturarea amenințărilor la adresa siguranței naționale, a faptelor sau evenimentelor cu consecințe periculoase în rândul efectivelor de deținuți, precum și a oricăror situații sau împrejurări din care pot rezultă asemenea pericole;

S.R.I., astfel că nu era necesară menținerea unei structuri de informații separate doar pentru pericolele la securitatea națională provenite din mediul penitenciar.

Ceea ce a făcut din D.G.P.A. și din S.I.P.A. o instituție controversată a fost posibilitatea folosirii acestui serviciu de informații în cursul urmăririi penale, sub acest aspect, art. 6 alin. (3) din H.G. nr. 637/2004 prevăzând: „*la solicitarea Ministerului Public, Direcția Generală de Protecție și Anticorupție execută acțiuni operative în sprijinul investigării și documentării unor dosare de urmărire penală*". Aceasta semnifica posibilitatea folosirii serviciului secret în cursul urmăririi penale și, prin raportare la specificul domeniului de activitate, trebuia să privească angajați aflați în subordinea, sub autoritatea sau în relație de coordonare cu Ministerul Justiției, inclusiv procurorii sau judecătorii. Apreciem că era inadecvată existența acestui serviciu secret dacă scopul său real era monitorizarea personalului din justiție, în special a magistraților, dar și posibilitatea de a realiza activități în domeniul securității naționale. Ținând seama și de legislația procesuală penală anterioară, puteau fi strânse probe împotriva unor magistrați prin activitatea de culegere de informații, desfășurată la solicitarea procurorului, ceea ce punea sub semnul întrebării independența justiției. Mai mult, conform art. 7 alin. (1) din H.G. nr. 637/2004, personalul D.G.P.A. era format inclusiv din cadre militare în activitate, ceea ce este de neconceput în contextul unui instituții cu caracter civil și în subordinea unei conduceri civile.

Din cele prezentate mai sus, rezultă că, în domeniul securității naționale, sunt implicate numeroase organe cu activitate de culegere de informații, atât cu competențe generale, cât și specializate, în funcție de domeniul în care activează sau a cărei autoritate centrală i se subordonează, după caz. Având în vedere domeniul de activitate și particularitățile situației, apreciem că toate aceste organe vor putea solicita autorizarea folosirii tehnicilor speciale de investigare ca modalitate concretă de culegere a informațiilor.

Secțiunea a 4-a. Activitățile specifice culegerii de informații prevăzute de Legea nr. 51/1991

În desfășurarea activității organelor din domeniul securității naționale se are în vedere modalitatea legală de a fi combătute amenințările la securitatea națională, astfel cum ele sunt

b) identificarea persoanelor aflate în detenție (arestați preventiv sau condamnați) care au avut legături cu organizații sau grupări teroriste, preluarea sub control a canalelor de legătură pe care acestea și le creează cu exteriorul, în situațiile în care există indicii că întrețin în continuare contacte cu structuri extremist-teroriste ori cu persoane implicate în trafic cu arme, droguri și ființe umane;

c) identificarea persoanelor aflate în detenție care intenționează organizarea unor acțiuni violente în penitenciare sau îndreptate împotriva personalului administrației penitenciare, precum și a magistraților, cadrelor de poliție ori a altor persoane aflate în diverse împrejurări în mediul penitenciar; prevenirea faptelor sau împrejurărilor ce pot constitui premise la producerea unor evenimente de natura celor prevăzute;

d) prevenirea oricăror acțiuni de destabilizare a mediului penitenciar;

e) conlucrarea cu instituțiile abilitate în realizarea acțiunilor de protejare a persoanelor incluse în Programul de protecție a martorilor, care se află în stare de arest preventiv sau execută o pedeapsă privativă de libertate;

f) protecția contrainformativă a personalului din Direcția Generală a Penitenciarelor și unitățile subordonate față de orice acțiuni care urmăresc angrenarea acestuia în fapte ce constituie amenințări la adresa siguranței naționale ori în săvârșirea de infracțiuni sau fapte antisociale;

g) prevenirea și contracararea, împreună cu factorii abilitați, a faptelor, situațiilor și împrejurărilor de nerespectare de către personalul Direcției Generale a Penitenciarelor și al unităților subordonate a actelor normative care reglementează activitatea profesională și conduita acestora, a fenomenelor ce pot favoriza ori genera evenimente grave, a actelor de corupție sau a altor fapte și manifestări ce constituie încălcări ale legii".

prevăzute de art. 2 alin. (1) din Legea nr. 51/1991, în care se arată că „*securitatea națională se realizează prin cunoașterea, prevenirea și înlăturarea amenințărilor interne sau externe*". Dintre modalitățile de combatere, prima este cea de cunoaștere, activitate care se va realiza prin aplicarea unor tehnici specifice serviciilor de informații, denumite „activități specifice culegerii de informații". Aceasta reprezintă o categorie foarte largă, în care pot fi incluse toate metodele folosite în prezent sau care pot fi imaginate pentru a obține informații în vederea asigurării statului, unele dintre acestea putând implica restrângerea drepturilor și libertăților fundamentale ale persoanelor.

Din cuprinsul Legii nr. 51/1991 ar rezulta că există două categorii de activități specifice culegerii de informații: *i)* activități specifice care nu presupun restrângerea drepturilor și libertăților fundamentale și *ii)* activități specifice care presupun restrângerea drepturilor și libertăților fundamentale. Primele vor putea fi întrebuințate fără nicio autorizare judiciară prealabilă, cele din urmă vor trebui autorizate de instanța competentă și executate numai în baza unui mandat de siguranță națională.

§1. Activitățile specifice culegerii de informații care nu presupun restrângerea drepturilor și libertăților fundamentale ale omului

Activitățile specifice care, potrivit legii, nu presupun o restrângere a drepturilor și libertăților fundamentale sunt cele cuprinse în art. 13 lit. a)-e) din Legea nr. 51/1991 și permit serviciilor din domeniul securității naționale următoarele: „*a) să solicite și să obțină obiecte, înscrisuri sau relații oficiale de la autorități sau instituții publice, respectiv să solicite de la persoane juridice de drept privat ori de la persoane fizice; b) să consulte specialiști ori experți; c) să primească sesizări sau note de relații; d) să fixeze unele momente operative prin fotografiere, filmare sau prin alte mijloace tehnice ori să efectueze constatări personale cu privire la activități publice desfășurate în locuri publice, dacă această activitate este efectuată ocazional; e) să solicite obținerea datelor generate sau prelucrate de către furnizorii de rețele publice de comunicații electronice ori furnizorii de servicii de comunicații electronice destinate publicului, altele decât conținutul acestora, și reținute de către aceștia potrivit legii*".

Din tehnicile arătate mai sus, două ar putea fi considerate tehnici speciale de investigare: fixarea de momente operative prin fotografiere, filmare sau prin alte mijloace tehnice ori efectuarea constatărilor personale cu privire la activități publice desfășurate în locuri publice, în mod ocazional, și obținerea de date generate sau prelucrate de către furnizorii de rețele publice de comunicații electronice ori de către furnizorii de servicii de comunicații electronice destinate publicului. În opinia noastră, ambele vor constitui tehnici speciale de investigare și au un conținut similar cu cel al unor metode speciale de supraveghere sau cercetare prevăzute de Codul de procedură penală.

Prima măsură, prevăzută de art. 13 lit. d) din Legea nr. 51/1991, reprezintă o supraveghere video, audio sau prin fotografiere în spații publice, care se impune a fi autorizată de un organ judiciar, constituind o ingerință gravă adusă dreptului la viață privată. Legiuitorul încearcă să diminueze aparența de gravitate a ingerinței prin referiri la caracterul ocazional al măsurii și prin limitarea măsurii numai la activități publice desfășurate în spații publice, însă nu oferă nicio garanție împotriva abuzului. Sub umbrela caracterului ocazional se pot ascunde deosebit de multe abuzuri care pot fi comise de organele din domeniul securității statului, această formă de activitate fiind tributară celor folosite de Direcția Securității Statului. Lesne este de înțeles că „ocazional", pentru un ofițer al unui serviciu (de pildă, S.R.I.), poate să însemne, în realitate,

că „de fiecare dată când are ocazia" să supravegheze o persoană va fi abilitat să facă acest lucru. De pildă, va fi ocazională desfășurarea de activități de supraveghere a unui politician atunci când se va îmbarca pe un zbor într-un aeroport național, observându-se data, ora și persoanele de care este însoțit de către ofițerii S.R.I. care realizează controlul de securitate. Termenul de „ocazional" nu are nicio justificare legală, întrucât fie o persoană reprezintă o amenințare la adresa securității naționale și va fi monitorizată, fie nu, ca atare, nu sunt necesare „verificări ocazionale". În același timp, chiar și pentru supravegherea tehnică ocazională a unei persoane în spații publice, Codul de procedură penală impune obținerea unui mandat, indiferent de întinderea supravegherii în timp, nefiind nicio condiție privind caracterul continuu sau sistematic.

A doua măsură, cea prevăzută de art. 13 lit. e) din Legea nr. 51/1991 constituie vechea formă a metodei speciale de cercetare prevăzută de art. 152 C.pr.pen., care a rămas neaplicabilă ca urmare a pronunțării Deciziei nr. 440/2014 a Curții Constituționale. Deși textul nu a fost supus controlului de constituționalitate, tehnica de culegere de informații a devenit inaplicabilă la momentul publicării deciziei, întrucât a fost văduvită de cadrul legal necesar, prevăzut de Legea nr. 82/2012. În aplicarea jurisprudenței Curții de Justiție a Uniunii Europene, în Hotărârea Digital Rights, Curtea Constituțională a reținut că era necesară o autorizare din partea unei instanțe pentru accesarea datelor stocate în baza Legii nr. 82/2012, sens în care dispozițiile legale erau incomplete[1] și contraveneau necesității unei protecții adecvate a drepturilor fundamentale ale persoanei. În urma unor modificări legislative, legea care stă la baza întrebuințării metodei speciale de cercetare prevăzute de art. 152 C.pr.pen. este la acest moment Legea nr. 506/2004, în care se reglementează atât datele care pot fi obținute, cât și procedura de obținere a lor[2].

În mod bizar, deși nu se amintește în Legea nr. 51/1991 despre o autorizare a obținerii datelor generate sau prelucrate de către furnizorii de rețele publice de comunicații electronice ori furnizorii de servicii de comunicații electronice destinate publicului, altele decât conținutul acestora, în cuprinsul Legii nr. 506/2004 se prevede obligativitatea obținerii unui mandat de siguranță națională, precum în cazul autorizării activităților specifice de culegere de informații care restrâng drepturile și libertățile persoanei. Astfel, conform art. 12^1 alin. (2) din Legea nr. 506/2004, „*solicitările privind datele prevăzute la alin. (1)* (date de trafic și localizare – n.n.), *formulate de către organele de stat cu atribuții în domeniul apărării și securității naționale, sunt supuse dispozițiilor art. 14, 15 și art. 17-23 din Legea nr. 51/1991 privind securitatea națională a României, republicată*". Putem concluziona astfel că există o necorelare legislativă nefericită, fiind obligatorie modificarea Legii nr. 51/1991, pentru a corespunde cu legislația specială din domeniul comunicațiilor, care limitează și obiectul măsurii la datele de trafic și de localizare, dar impune și obligația obținerii unui mandat de siguranță națională.

După cum se vede, inclusiv măsuri apreciate în sensul că nu ar restrânge drepturile și libertățile fundamentale ale unei persoane vor putea constitui forme de supraveghere și vor putea fi considerate tehnici speciale de investigare, presupunând autorizarea prealabilă a unei autorități independente, precum o instanță.

[1] CCR, Dec. nr. 440/2014, §67.

[2] *V. supra*, Titlul X, Capitolul III.2.

§2. Activitățile specifice culegerii de informații care presupun restrângerea drepturilor și libertăților fundamentale ale omului

A doua categorie de activități specifice culegerii de informații o reprezintă cele care vor presupune restrângerea drepturilor și libertăților fundamentale ale persoanelor, fiind în mod neîndoielnic tehnici speciale de investigare folosite în domeniul securității naționale. La aceste tehnici, regăsim prima referință în cadrul art. 13 lit. f) din Legea nr. 51/1991, în care se menționează că organele din domeniul securității naționale sunt îndreptățite „*să efectueze activități specifice culegerii de informații care presupun restrângerea exercițiului unor drepturi sau libertăți fundamentale ale omului desfășurate cu respectarea prevederilor legale*".

În cuprinsul art. 14 alin. (2) din Legea nr. 51/1991 sunt prevăzute activitățile specifice care atrag o restrângere a drepturilor și libertăților fundamentale ale persoanei, acestea suprapunându-se metodelor speciale de supraveghere sau cercetare. În concret, ele pot consta în:

„*a) interceptarea și înregistrarea comunicațiilor electronice, efectuate sub orice formă;*

b) căutarea unor informații, documente sau înscrisuri pentru a căror obținere este necesar accesul într-un loc, la un obiect ori deschiderea unui obiect;

c) ridicarea și repunerea la loc a unui obiect sau document, examinarea lui, extragerea informațiilor pe care acesta le conține, precum și înregistrarea, copierea sau obținerea de extrase prin orice procedee;

d) instalarea de obiecte, întreținerea și ridicarea acestora din locurile în care au fost depuse, supravegherea prin fotografiere, filmare sau prin alte mijloace tehnice ori constatări personale, efectuate sistematic în locuri publice sau efectuate în orice mod în locuri private;

e) localizarea, urmărirea și obținerea de informații prin GPS sau prin alte mijloace tehnice de supraveghere;

f) interceptarea trimiterilor poștale, ridicarea și repunerea la loc a acestora, examinarea lor, extragerea informațiilor pe care acestea le conțin, precum și înregistrarea, copierea sau obținerea de extrase prin orice procedee;

g) obținerea de informații privind tranzacțiile financiare sau datele financiare ale unei persoane, în condițiile legii".

După cum lesne se poate observa, majoritatea activităților specifice se suprapun cu metodele speciale de supraveghere sau cercetare, însă există și anumite particularități care se impune a fi surprinse, motiv pentru care, în continuare, vom proceda la o succintă analiză a lor, relevând și elementele de diferențiere dintre ele și tehnicile speciale de investigare prevăzute în Codul de procedură penală.

Interceptarea și înregistrarea comunicațiilor electronice, efectuate sub orice formă, constituie o tehnică specială de investigare identică celei prevăzute de art. 138 alin. (1) lit. a) C.pr.pen. Chiar dacă nu se detaliază în ce constă metoda, legiuitorul fiind mai puțin explicit, nefiind menționate ca în cuprinsul art. 138 alin. (2) C.pr.pen. componentele interceptării comunicațiilor, apreciem că explicațiile date anterior în cazul măsurii vor fi pe deplin aplicabile în ceea ce privește aspectele concrete de punere în executare[1]. Cel mai facil mod de realizare a interceptării va fi interceptarea comunicațiilor telefonice realizată prin C.N.I.C., aflat în subordinea S.R.I. În considerarea opiniei expuse deja în prezenta lucrare[2], credem că acest centru va trebui să dobândească statutul de autoritate administrativă autonomă, nefiind justificat nici din

[1] *V. supra*, Titlul IV, Capitolul III.2.

[2] *V. supra*, Titlul IV, Capitolul V.

perspectiva asigurării securității naționale ca toate serviciile de informații să deruleze interceptările comunicațiilor telefonice prin intermediul unei unități din structura unui alt serviciu. În cazurile în care interceptarea nu va presupune interceptarea comunicațiilor prin telefon în sistem centralizat, fiecare serviciu de informații va folosi tehnica sa proprie, în funcție de dotările specifice. Precum în cazul măsurii prevăzute de Codul de procedură penală, conversațiile nemijlocite dintre indivizi nu fac obiectul acestei tehnici, fiind considerate înregistrări ale convorbirilor ambientale[1].

Căutarea unor informații, documente sau înscrisuri pentru a căror obținere este necesar accesul într-un loc, la un obiect ori deschiderea unui obiect constituie o tehnică specială de investigare necunoscută în legislația procesuală penală. În doctrină se arată că această tehnică cuprinde două activități separate[2]: căutarea unor informații, documente sau înscrisuri și pătrunderea într-un loc, la un obiect ori deschiderea unui obiect. Reglementarea tehnicii speciale a fost criticată în doctrină ca fiind neadecvată, întrucât căutarea de informații nu este o tehnică în sine, ci un obiectiv al accesului[3]. Această tehnică prezintă similarități cu percheziția domiciliară prevăzută în Codul de procedură penală, dar nu poate fi asimilată acesteia, deoarece nu reprezintă un act de urmărire penală ce poate conduce la obținerea de probe, ci un act care se desfășoară în secret[4]. Posibilitatea realizării unor percheziții cu caracter secret ca tehnică specială de investigare este menționată inclusiv în Recomandarea (2005) 10 a Comitetului de Miniștri[5]. Prin noțiunea de „loc" vom înțelege un loc privat care nu se va limita numai la domiciliul persoanei, ci și la reședința sau locul unde își desfășoară activitatea profesională[6]. În opinia noastră, termenul „loc" va trebui să aibă aceeași semnificație cu termenul de „domiciliu" din accepțiunea Curții Europene a Drepturilor Omului[7]. Accesul va reprezenta pătrunderea într-un spațiu privat al unei persoane, fiind justificată necesitatea de a se recurge la o autorizare prealabilă din partea unei instanțe. Credem că, prin raportare la varianta unui acces în vederea deschiderii unui obiect, se va impune o autorizare și dacă obiectul respectiv reprezintă un vehicul în care se presupune că vor exista informații, documente sau înscrisuri. Legiuitorul omite să precizeze însă ce se va întâmpla cu informațiile, documentele sau înscrisurile găsite, sens în care tehnica specială a fost criticată, pe bună dreptate, ca fiind complementară următoarei măsuri pe care o vom analiza[8].

Ridicarea și repunerea la loc a unui obiect sau document, examinarea lui, extragerea informațiilor pe care acesta le conține, precum și înregistrarea, copierea sau obținerea de extrase prin orice procedee constituie o altă tehnică specială de investigare prin care vor fi culese informații în vederea protejării securității naționale. Aceasta va fi subsumată *stricto sensu* unei operațiuni de culegere de informații, întrucât va permite, spre deosebire de tehnica tratată anterior, să se obțină în orice mod informațiile care pot fi găsite[9]. Un element esențial al acestei activități specifice este păstrarea caracterului secret al operațiunii prin păstrarea sau restabilirea

[1] *D.C-tin Mâță*, op. cit., p. 371.

[2] *Ibidem*, pp. 371-372.

[3] *M. Udroiu, R. Slăvoiu, O. Predescu*, Tehnici speciale, 2009, p. 30.

[4] *Ibidem*, p. 31.

[5] Memorandumul explicativ al Recomandării (2005) 10 a Comitetului de Miniștri al Consiliului Europei, pe *www.coe.int*

[6] *D.C-tin Mâță*, op. cit., p. 372; *M. Udroiu, R. Slăvoiu, O. Predescu*, Tehnici speciale, 2009, p. 31.

[7] *V. supra*, Titlul II, Capitolul IV.

[8] *M.V. Tudoran*, Teoria și practica interceptărilor, 2012, p. 183; *M. Udroiu, R. Slăvoiu, O. Predescu*, Tehnici speciale, 2009, p. 47.

[9] *M. Udroiu, R. Slăvoiu, O. Predescu*, Tehnici speciale, 2009, p. 47.

situației de fapt în aceleași coordonate ca înainte de intervenția organelor din domeniul securității naționale[1]. Aceasta rezultă din activitățile pe care le presupune tehnica, precum ridicarea și repunerea la loc a unui obiect sau document și fixarea conținutului acestuia în orice mod adecvat. Practic, tehnica este o formă clasică de spionaj în care, după ce se realizează pătrunderea într-un spațiu privat, ofițerul sub acoperire culege informațiile căutate prin orice procedeu posibil și reface situația de fapt pentru a nu trezi suspiciuni[2]. Această metodă nu are un echivalent în legislația procesuală penală, întrucât, în cazul unei percheziții domiciliare, nu se va proceda la repunerea la loc a obiectelor, din contră, acțiunile organelor de urmărire penală vor lăsa semne vizibile, dincolo de lipsa unui caracter secret.

Pentru a se obține informațiile căutate, organele din domeniul securității naționale vor putea examina un obiect atunci când este timp suficient pentru a face acest lucru[3], dar au și posibilitatea de a extrage informațiile conținute fie prin copiere, fie prin înregistrare sau orice alt procedeu. Cel mai cunoscut mod de a se realiza extragerea este fotografierea obiectului, documentului sau înscrisului, dacă această metodă este suficientă. Întrucât tehnicile și metodele de lucru trebuie să țină pasul cu tehnologia, va fi necesar să poată fi extrase și informații conținute de un sistem informatic, sub acest aspect, tehnica fiind similară atât cu percheziția informatică, cât și cu accesul la un sistem informatic. De altfel, în prezent, cele mai importante informații pot fi obținute prin extragerea lor dintr-un sistem informatic, cu mențiunea că metodele folosite vor trebui să evite crearea de urme digitale care să ridice suspiciuni persoanei vizate de măsură, fără a fi necesară o menținere a integrității datelor informatice, precum în cazul percheziției informatice.

Instalarea de obiecte, întreținerea și ridicarea acestora din locurile în care au fost depuse, supravegherea prin fotografiere, filmare sau prin alte mijloace tehnice ori constatări personale, efectuate sistematic în locuri publice sau efectuate în orice mod în locuri private constituie o tehnică specială de investigare prin care se realizează o supraveghere a unei persoane. Această activitate va fi similară cu metoda specială a supravegherii video, audio sau prin fotografiere, prevăzută de art. 138 alin. (1) lit. c) C.pr.pen., însă diferă de aceasta prin faptul că include, în mod expres, în cuprinsul acesteia posibilitatea de pătrundere în spații private pentru instalarea tehnicii operative. În mod paradoxal, față de dispozițiile art. 140 alin. (5) lit. h) C.pr.pen., în care se face referire la activarea sau dezactivarea unor mijloace tehnice de înregistrare, Legea nr. 51/1991, în mod corect, prevede instalarea, menținerea și dezinstalarea lor, fiind evident că legiuitorul nu poate prezuma că o persoană ar deține în casă mijloace tehnice ce se impune numai a fi activate. În literatura de specialitate s-a considerat că, pentru a fi pusă în executare instalarea, întreținerea și ridicarea, se va impune și autorizarea măsurii complementare a *căutării unor informații, documente sau înscrisuri pentru a căror obținere este necesar accesul într-un loc*, pentru a se permite accesul legal într-un spațiu privat[4].

În ceea ce privește realizarea înregistrărilor, s-a arătat că acestea pot fi obținute și prin sistemele deținute de particulari și instalate în spații publice, organelor din domeniul securității naționale permițându-li-se accesul la acestea, fie pentru folosire în timp real, fie pentru a prelua înregistrări gata stocate[5]. Înregistrările pot fi, asemenea supravegherii tehnice prevăzute de

[1] *D.C-tin Mâță*, op. cit., p. 373.
[2] *M. Udroiu, R. Slăvoiu, O. Predescu*, Tehnici speciale, 2009, p. 51.
[3] *D.C-tin Mâță*, op. cit., p. 373.
[4] *Ibidem*, p. 374.
[5] *Ibidem*.

Codul de procedură penală, video, audio, audiovideo sau prin fotografiere. Chiar și varianta observării este prevăzută în cazul activității specifice culegerii de informații, legiuitorul menționând că aceasta va trebui să fie realizată *prin constatări personale.* În cazul acesta, nu va fi necesară folosirea vreunui mijloc tehnic de observare, putând fi vorba și de un simplu filaj al persoanei urmărite. După cum am arătat în prezenta secțiune, această supraveghere va trebui să fie autorizată de un organ independent, chiar dacă nu va avea caracter sistematic sau continuu, fiind obligatorie autorizarea și atunci când va avea caracter ocazional.

Localizarea, urmărirea și obținerea de informații prin GPS sau prin alte mijloace tehnice de supraveghere se va desfășura în același mod și prin aceleași mijloace ca în cazul metodei speciale de supraveghere prevăzute de Codul de procedură penală[1]. În privința acestei tehnici speciale de investigare, nu va exista nicio diferență între cele două reglementări sub aspectul activităților care vor fi autorizate, ele desfășurându-se într-un mod identic. Evident, distincțiile vor ține de regimul juridic diferit al actelor specifice culegerii de informații, de organele care le pun în executare și de regulile care guvernează punerea în executare, acestea din urmă nefiind publice. Cel mai utilizat mijloc de localizare va fi sistemul GPS sau prin obiecte atașate persoanei care va transmite locația[2].

Interceptarea trimiterilor poștale, ridicarea și repunerea la loc a acestora, examinarea lor, extragerea informațiilor pe care acestea le conțin, precum și înregistrarea, copierea sau obținerea de extrase prin orice procedee constituie o tehnică specială de investigare hibridizată, având trăsături comune cu metoda specială de cercetare a reținerii, predării și percheziționării corespondenței, dar și cu activitățile specifice de culegere de informații. Tehnica specială de investigare va afecta secretul corespondenței, presupunând obținerea corespondenței unei persoane, deschiderea acesteia și verificarea conținutului său, urmată de „extragerea informațiilor pe care le conține, înregistrarea sau obținerea de extrase prin orice procedee", o acțiune prevăzută de legiuitor pentru a se putea obține informații indiferent de conținutul corespondenței. În înțelesul noțiunii de „trimitere poștală"[3] vor intra și colete care pot conține obiecte care, la rândul lor, vor putea conține informații. Ne referim la un sistem informatic sau chiar la un suport de stocare trimis prin poștă, acesta putând fi reținut, iar datele informatice extrase, doar ca urmare a aplicării acestei tehnici speciale. Spre deosebire de Codul de procedură penală, nu va fi necesară o autorizare suplimentară pentru o percheziție informatică a sistemului informatic sau a suportului de stocare, întrucât dispozițiile legale permit copierea și obținerea de extrase de pe conținutul corespondenței, indiferent care ar fi natura acesteia. O altă diferență foarte importantă este că, în cazul tehnicii speciale de investigare prevăzută de Legea nr. 51/1991, este menționată și repunerea la loc a trimiterilor poștale, ceea ce va presupune retransmiterea corespondenței după ce conținutul a fost copiat sau extras, fără ca persoana vizată să afle acest lucru. În cazul metodei speciale de cercetare prevăzută de Codul de procedură penală, atunci când trimiterea poștală va avea legătură cu cauza, aceasta va constitui mijloc de probă în procesul penal și va fi reținută de organul de urmărire penală. În funcție

[1] *V. supra*, Titlul VII, Capitolul III.3. și Capitolul III.4.

[2] *D.C-tin Mâță*, op. cit., p. 375.

[3] Conform O.U.G. nr. 13/2013 privind serviciile poștale, la art. 2 pct. 13, „trimiterea poștală" este definită ca: „bun adresat, aflat în forma finală în care urmează să fie transportat și livrat la adresa indicată de expeditor pe trimiterea în sine, pe ambalaj sau într-o listă de distribuție. Pe lângă trimiterile de corespondență, în această categorie sunt incluse, de exemplu, imprimatele, sacii «M», pachetele mici, coletele poștale care conțin bunuri cu sau fără valoare comercială și mandatele poștale pe suport hârtie. În această categorie nu sunt incluse trimiterile hibrid".

de specificul trimiterii poștale și de modul în care aceasta se prezintă, serviciile de informații vor putea alege să retransmită trimiterea poștală după ce au extras informațiile conținute sau, pentru a nu divulga secretul operațiunii, să o păstreze.

Obținerea de informații privind tranzacțiile financiare sau datele financiare ale unei persoane, în condițiile legii, reprezintă o tehnică specială de investigare cu multe similarități cu metoda specială de cercetare prevăzută de Codul de procedură penală. Chiar dacă are aceeași formulare ca metoda specială de cercetare, diferența principală va fi scopul pentru care sunt obținute datele privind tranzacțiile financiare, acestea având valoare de informații obținute în urma activităților specifice și neputând fi valorificate ca probe. În privința instituțiilor care ar putea comunica date privind tranzacțiile financiare, acestea vor fi instituțiile de credit, entitățile financiare și alte persoane fizice și juridice, astfel cum am explicat într-o secțiune anterioară[1].

Putem identifica o problemă deosebită, întrucât nu există o dispoziție legală care să permită organelor din domeniul securității naționale să încalce secretul bancar al relației dintre client și bancă ori secretul profesional dintre client și o entitate financiară, întrucât aceste organe nu au calitatea de procuror sau instanță. Conform art. 111 alin. (1) din O.U.G. nr. 99/2006, o instituție de credit este ținută să păstreze confidențialitatea tranzacțiilor desfășurate de un client al său, cu excepția unor situații prevăzute în mod limitativ de lege. Numai în cuprinsul art. 114 din O.U.G. nr. 99/2006 se arată că „*instituțiile de credit sunt obligate să furnizeze procurorului sau instanței de judecată, la solicitarea acestora, informații de natura secretului bancar, dispozițiile privind metodele speciale de supraveghere sau cercetare din Codul de procedură penală aplicându-se în mod corespunzător*", or, organelor din domeniul securității naționale nu le-a fost acordată nicio dispensă la aflarea secretului bancar. Dispozițiile citate nu sunt singurele care permit ridicarea secretului bancar, de interes fiind și cele cuprinse în art. 113 alin. (2) din O.U.G. nr. 99/2006[2], care permit divulgarea secretului bancar în condiții restrictive prevăzute de lege. Dintr-o analiză a dispozițiilor legale amintite, apreciem că singurul caz care s-ar putea încadra, ipotetic, ar fi cel de la art. 113 alin. (2) lit. c) din O.U.G. nr. 99/2016, care ar permite divulgarea unor informații care constituie secret bancar „*la solicitarea scrisă a altor autorități sau instituții ori din oficiu, dacă prin lege specială aceste autorități sau instituții sunt îndrituite, în scopul îndeplinirii atribuțiilor lor specifice, să solicite și/sau să primească astfel de informații și sunt identificate clar informațiile care pot fi furnizate de către instituțiile de credit în acest scop*". În opinia noastră, textul nu este aplicabil organelor din domeniul securității naționale, întrucât

[1] *V. supra*, Titlul VIII, Capitolul III.

[2] Conform art. 113 alin. (2) din O.U.G. nr. 99/2006:

„(2) Informații de natura secretului bancar pot fi furnizate, în măsura în care acestea sunt justificate de scopul pentru care sunt cerute ori furnizate, în următoarele situații:

a) la solicitarea titularului de cont sau a moștenitorilor acestuia, inclusiv a reprezentanților legali și/sau statutari, ori cu acordul expres al acestora;

b) în cazurile în care instituția de credit justifică un interes legitim;

c) la solicitarea scrisă a altor autorități sau instituții ori din oficiu, dacă prin lege specială aceste autorități sau instituții sunt îndrituite, în scopul îndeplinirii atribuțiilor lor specifice, să solicite și/sau să primească astfel de informații și sunt identificate clar informațiile care pot fi furnizate de către instituțiile de credit în acest scop;

d) la solicitarea scrisă a soțului titularului de cont, atunci când face dovada că a introdus în instanță o cerere de împărțire a bunurilor comune, sau la solicitarea instanței.

e) la solicitarea instanței, în scopul soluționării diferitelor cauze deduse judecății.

f) la solicitarea executorului judecătoresc, în scopul realizării executării silite, pentru existența conturilor debitorilor urmăriți.

g) la solicitarea notarului, în cadrul procedurii succesorale notariale".

acestea nu au atribuții în domeniul financiar și nici în legile lor de organizare sau funcționare nu sunt incluse dispoziții cu referire la aflarea datelor privind tranzacțiile financiare ale unor persoane. În plus, față de caracterul secret și intruziv al tehnicilor speciale de investigare, nu va putea fi folosit acest text de lege, deoarece, alături de dispozițiile din Legea nr. 51/1991, nu oferă un cadru legal clar și previzibil pentru aplicarea tehnicii, fiind contrare dispozițiilor art. 8 Conv.EDO[1]. Cu alte cuvinte, în lipsa unor dispoziții în legea specială, nu vom putea considera că tehnica specială este prevăzută de lege în mod complet, nefiind întrunită prima condiție a art. 8 par. 2 Conv.EDO, respectiv ca ingerința adusă dreptului la viață privată să fie prevăzută de lege.

O altă problemă deosebită în aplicarea tehnicii speciale a obținerii datelor privind tranzacțiile financiare ale unei persoane este că se va impune justificarea cererii adresate unei instituții bancare, or, acest lucru trebuie să fie făcut prin prezentarea autorizării primite de organele din domeniul securității naționale, într-un mod identic organelor de urmărire penală. Pentru a se da crezare susținerilor serviciilor secrete, instituția de credit sau o altă entitate financiară va trebui să primească o copie a mandatului de siguranță națională în aceleași condiții în care ar primi un mandat de supraveghere tehnică. Problema legislativă din această situație este că serviciul secret nu va putea prezenta mandatul unei entități financiare sau unei instituții de credit, întrucât acesta va avea caracter secret, fiind clasificat, ținând seama că reprezintă o parte din activitatea de informații care, potrivit art. 10 din Legea nr. 51/1991, reprezintă secret de stat. Totodată, nici nu este prevăzută vreo procedură de declasificare a mandatului.

Având în vedere viciile arătate mai sus, apreciem că dispozițiile privind folosirea tehnicii speciale de investigare a obținerii datelor privind tranzacțiile financiare ale unei persoane nu vor putea fi aplicate în lipsa unui cadru legal prevăzut în legislația specială din domeniul financiar și în lipsa prevederii obligației comunicării mandatului declasificat, prin care serviciile secrete să își poată justifica solicitările către instituțiile de credit sau alte entități financiare.

În concluzie, activitățile specifice culegerii de informații care presupun restrângerea drepturilor și libertăților fundamentale ale persoanei sunt prevăzute într-un mod similar metodelor speciale de supraveghere sau cercetare, însă permit puteri sporite organelor din domeniul securității naționale și au o reglementare, pe alocuri, deficitară, prin raportare la lipsa garanțiilor necesare într-o societate democratică pentru apărarea dreptului la viață privată.

[1] CEDO, cauza *Kruslin c. Franța*, Hotărârea din 24 aprilie 1990, §36, pe *hudoc.echr.coe.int*

Capitolul II
Aspecte procedurale privind autorizarea tehnicilor speciale de investigare prevăzute de Legea nr. 51/1991

Secțiunea 1. Condițiile legale pentru autorizarea tehnicilor speciale care constituie activități specifice culegerii de informații

În conformitate cu dispozițiile Legii nr. 51/1991, activitățile specifice culegerii de informații care presupun o restrângere a drepturilor și libertăților fundamentale ale unei persoane impun o autorizare prealabilă din partea unui organ independent, respectiv cea a președintelui Înaltei Curți de Casație și Justiție, care va putea fi dată numai atunci când sunt îndeplinite anumite condiții legale. Ținând cont de faptul că toate tehnicile speciale de investigare, indiferent de regimul lor juridic, vor presupune o intruziune în viața privată a unei persoane, vor fi ținute să respecte condițiile stabilite prin art. 8 par. Conv.EDO și prin jurisprudența stabilită de Curte, pentru a fi evitat abuzul autorităților în relația cu particularii.

Condițiile legale de autorizare a tehnicilor speciale de investigare sunt prevăzute la art. 14 alin. (1) din Legea nr. 51/1991, în care se arată că activitățile de culegere de informații care presupun restrângerea drepturilor sau libertăților fundamentale ale omului se efectuează numai în situațiile în care: *i)* nu există alte posibilități ori sunt posibilități limitate pentru cunoașterea, prevenirea sau contracararea riscurilor ori amenințărilor la adresa securității naționale; *ii)* acestea sunt necesare și proporționale, date fiind circumstanțele situației concrete; *iii)* a fost obținută autorizația prevăzută de lege.

Textul legal instituie, în realitate, două condiții legale: subsidiaritatea folosirii tehnicilor speciale de investigare și proporționalitatea restrângerii drepturilor și libertăților persoanei cu scopul urmărit – cunoașterea, prevenirea și înlăturarea amenințărilor la adresa securității naționale.

În comparație cu metodele speciale de supraveghere sau cercetare, lipsește un element pe care îl apreciem esențial – suspiciunea rezonabilă privind săvârșirea unei infracțiuni sau, prin adaptare la domeniul securității naționale, o suspiciune rezonabilă a existenței unei amenințări la adresa securității naționale. Prevederea unei astfel de condiții legale este esențială, deoarece permite organului competent să autorizeze măsura, posibilitatea de a evalua dacă există sau nu un motiv serios pentru a se autoriza tehnicile speciale de investigare, în lipsa acestuia, neputându-se exercita un control de proporționalitate.

Deși Legea nr. 51/1991 prevede atât în cazul propunerii de autorizare, cât și în cuprinsul conținutului încheierii de autorizare mențiunea privind „*date sau informații din care să rezulte existența unei amenințări la adresa securității naționale, prin prezentarea faptelor și circumstanțelor pe care se întemeiază propunerea*", o atare precizare nu reprezintă o condiție legală, nefiind suficient să existe numai date și informații din care să rezulte o amenințare la adresa siguranței naționale, ci trebuie inclus și un standard probatoriu care să condiționeze autorizarea tehnicilor speciale de investigație numai la acele amenințări care au un caracter suficient de bine probat cât să justifice o suspiciune rezonabilă privind existența unei amenințări. Trebuie să corelăm această nevoie și cu dispozițiile art. 2 din Legea nr. 51/1991, care arată că

securitatea națională se realizează prin cunoaștere, prevenție și înlăturare de amenințări, or, textul acesta este prea larg pentru a releva un standard de probă. Practic, se va putea oricând argumenta necesitatea autorizării unor tehnici speciale de investigare pentru cunoașterea unei potențiale amenințări la adresa securității naționale, fără ca instanța să aprecieze dacă este sau nu îndeplinit un anumit standard de probă privind existența unei amenințări[1]. Situația este cu atât mai gravă încât la momentul autorizării nu va exista un dosar al cauzei, nu va exista nici un control transparent asupra obținerii datelor și informațiilor și nu se va cunoaște nici dacă acestea au fost obținute în mod licit de către serviciile secrete. Deși o instanță este chemată să stabilească asupra temeiniciei autorizării unor tehnici speciale de investigare, aceasta nu ar putea constata că lipsește amenințarea la adresa securității naționale, ci va prelua în mod automat acest aspect de la serviciile secrete. În opinia noastră, un control *a priori* de acest fel nu este unul eficient, conducând la posibilitatea autorizării automate a oricărei propuneri venite din partea unui serviciu secret[2].

Prima condiție prevăzută de lege, cea a subsidiarității folosirii tehnicilor speciale de investigare, se va considera îndeplinită *dacă nu există alte posibilități ori sunt posibilități limitate pentru cunoașterea, prevenirea sau contracararea riscurilor ori amenințărilor la adresa securității naționale*. Condiția este similară cu cea prevăzută în cazul supravegherii tehnice de la art. 139 alin. (1) lit. c) C.pr.pen., în care formularea este că „*probele nu ar putea fi obținute în alt mod sau obținerea lor ar presupune dificultăți deosebite ce ar prejudicia ancheta ori există un pericol pentru siguranța persoanelor sau a unor bunuri de valoare*", cu observația că textul legal cuprins în Legea nr. 51/1991 pare a fi mai clar, previzibil și lipsit de prevederi care ar putea fi folosite în mod abuziv de autorități. În prezenta lucrare am criticat alegerea legiuitorului de a prevedea în cuprinsul Codului de procedură penală condiția subsidiarității prin raportare și la pericolul pentru siguranța persoanelor sau a unor bunuri de valoare[3], deoarece nu constituie o situație în care să se aplice procedee probatorii, fiind de bun-simț ca, în cazul amenințărilor la adresa securității naționale, să nu fie menționate asemenea criterii.

În domeniul securității naționale, condiția subsidiarității va avea un caracter atenuant, întrucât întreaga activitate de culegere de informații are un caracter secret, neputându-se dezvălui nicio componentă a acesteia. Astfel, procedeele non-intruzive sunt limitate, organele din domeniul securității naționale neavând posibilitatea de a desfășura acte de urmărire penală, precum audierea unor persoane, deoarece acestea ar trăda secretul operațiunii. Cu toate acestea, nu suntem de acord cu formularea variantei „*sunt posibilități limitate pentru cunoașterea, prevenirea sau contracararea riscurilor ori amenințărilor*", deoarece lasă loc de interpretări care nu sunt utile în asigurarea unor garanții împotriva abuzului. Întotdeauna vor exista posibilități limitate în a afla informații despre o anumită faptă sau o persoană, acest lucru nu înseamnă că vor trebui folosite toate măsurile opresive și intruzive ale statului. Prin tehnicile speciale de investigare nu trebuie create posibilități nelimitate pentru organele de urmărire penală sau, în acest caz, pentru organele din domeniul securității naționale, ci trebuie oferit minimul de măsuri intruzive prin care să se realizeze scopul. Din acest punct de vedere, autorizarea unor activități specifice intruzive, în condițiile în care există posibilități de cunoaștere, prevenire sau contracarare, dar ele sunt limitate, vine în opoziție cu însăși ideea de

[1] *V. supra*, Titlul III, Capitolul I.2.

[2] CEDO, cauza *Iordachi ș.a. c. Moldova*, Hotărârea din 10 februarie 2009, §50; cauza *Roman Zakharov c. Rusia*, Hotărârea din 4 decembrie 2015, §230.

[3] *V. supra*, Titlul III, Capitolul I.4.

subsidiaritate. *De lege ferenda*, considerăm că se impune modificarea criteriului legal prevăzut de art. 14 alin. (1) lit. a) din Legea nr. 51/1991, iar tehnicile speciale să poată fi autorizate numai atunci când informațiile nu pot fi obținute prin alte procedee.

A doua condiție prevăzută de lege pentru autorizarea activităților specifice de culegere de informații ce restrâng drepturile și libertățile fundamentale ale omului o constituie proporționalitatea, conform art. 14 alin. (1) lit. b) din Legea nr. 51/1991, stipulându-se că măsurile pot fi autorizate dacă „*acestea sunt necesare și proporționale, date fiind circumstanțele situației concrete*". Termenul de „necesitate" a măsurii este introdus în mod greșit de legiuitor în contextul proporționalității, deoarece doar întărește condiția prevăzută de art. 14 alin. (1) lit. a) din Legea nr. 51/1991. Mai degrabă, termenul de „necesar" trebuie folosit în contextul necesității unei restrângeri a drepturilor și libertăților persoanei, ceea ce ar fi însemnat că era o componentă a proporționalității, făcând trimitere la condițiile prevăzute de art. 8 par. 2 Conv.EDO (restrângerea dreptului la viață privată trebuie să fie necesară într-o societate democratică).

După cum am subliniat și în cazul supravegherii tehnice, proporționalitatea nu va fi influențată numai de criteriile condițiilor legale prevăzute de art. 14 alin. (1) din Legea nr. 51/1991, ci și de existența unei suspiciuni rezonabile suficient de bine conturate pentru a justifica ingerința adusă, dar și de lipsa unei măsuri mai puțin restrictive care să conducă la același rezultat. Cu alte cuvinte, neîntrunirea oricăreia dintre condițiile legale prevăzute de art. 14 alin. (1) din Legea nr. 51/1991 va determina și lipsa de proporționalitate a măsurii[1].

Încercând să adapteze cerința proporționalității din Codul de procedură penală, legiuitorul a impus condiția *proporționalității măsurii cu restrângerea drepturilor și libertăților fundamentale* prin raportare la *circumstanțele situației concrete*, ceea ce va corespunde cu expresia folosită în cuprinsul Codului de procedură penală de „particularitățile cauzei".

Proporționalitatea trebuie analizată atât raportat la autorizarea de activități specifice în întregime, cât și cu privire la tehnicile speciale de investigare concrete ce sunt solicitate prin propunerea procurorului. Ca și în cazul supravegherii tehnice, o autorizare a tuturor tehnicilor speciale prevăzute de art. 14 alin. (2) din Legea nr. 51/1991 față de aceeași persoană o socotim ca fiind excesivă și depășind proporționalitatea măsurii.

Cel mai important aspect va fi ca analiza de la momentul judecării propunerii de autorizare să privească tehnicile concrete propuse, întrucât aceeași măsură generală poate genera ingerințe asupra vieții private de diferite gravități, în funcție de modalitatea lor concretă. Astfel cum am arătat și în cazul supravegherii tehnice, judecătorul va trebui să dispună, de pildă, asupra proporționalității supravegherii video a locului de muncă al unei persoane ori a interiorului domiciliului acestei persoane, cele două situații fiind complet diferite, raportat la întinderea restrângerii dreptului la viață privată.

Prin „circumstanțele situației" vom înțelege acele împrejurări specifice care vor impune utilizarea activităților de culegere de informații intruzive, deoarece un altfel de mijloc nu ar fi propice pentru a cunoaște, preveni sau înlătura amenințarea la adresa securității naționale. Lesne poate fi imaginată situația în care o grupare teroristă activează în mod acoperit pe teritoriul țării și folosește mijloace de comunicare la distanță și întâlniri secrete pentru a discuta sau a transfera bunuri în vederea realizării de activități teroriste, situație care nu va presupune numai efectuarea unei urmăriri penale, ci și luarea de măsuri pentru prevenirea unui atentat la securitatea națională.

[1] V. *supra*, Titlul III, Capitolul I.3.

Chiar dacă scopul urmărit, menținerea securității naționale, este unul de maximă importanță, este necesar ca proporționalitatea să aibă în vedere situațiile prevăzute de art. 2 alin. (1) din Legea nr. 51/1991, în sensul în care măsuri mai puțin intruzive vor trebui luate mai degrabă în cazul unei cunoașteri a amenințărilor interne sau externe decât în cazul prevenirii sau înlăturării lor. Practic, gradual față de aceste situații, vor putea fi autorizate măsuri mai intruzive. Credem că o simplă cunoaștere a unei potențiale amenințări nu este suficientă pentru a justifica activități de culegere de informații care restrâng drepturile fundamentale ale omului. În situația prevenirii unor amenințări, suntem de părere că deja trebuie să existe anumite suspiciuni privind desfășurarea unor acțiuni, o amenințare la adresa securității naționale și, în cazul înlăturării amenințării, aceasta trebuia deja să existe și să fie temeinic probată pentru a se autoriza măsurile cele mai intruzive.

Un criteriu de care trebuie să se țină cont este durata măsurii, care, spre deosebire de supravegherea tehnică, va putea fi mult mai mare, existând posibilitatea emiterii unui mandat valabil pentru 6 luni de zile, cu posibilitatea de a se prelungi succesiv până la durata maximă de 2 ani.

Secțiunea a 2-a. Formularea propunerii de autorizare

În cadrul oricărei proceduri de autorizare a unei tehnici speciale de investigare nu va fi suficientă îndeplinirea condițiilor legale pentru a se dispune autorizarea, fiind necesară o sesizare formulată de un organ competent, întrucât instanța nu se poate sesiza din oficiu. Spre deosebire de metodele speciale de supraveghere sau cercetare, în cazul activităților specifice culegerii de informații, dreptul de a formula o cerere de autorizare va aparține unui organ din domeniul securității naționale, însă care nu va putea să se prezinte în fața instanței competente, ci va trebui să supună cererea sa procurorului competent. Practic, în cazul supravegherii realizate în temeiul legii securității naționale, va exista un control dublu: unul preliminar, din partea procurorului general al P.I.C.C.J., și unul principal, desfășurat de președintele Înaltei Curți de casație și Justiție.

Atunci când organele din domeniul securității naționale vor considera că se impune autorizarea unor tehnici speciale de investigare, vor formula o propunere scrisă către procurorul general al P.I.C.C.J., care, conform art. 15 alin. (1) din Legea nr. 51/1991, va trebui să conțină:

„*a) numele și funcția persoanei care formulează propunerea;*

b) data și locul emiterii propunerii;

c) date sau informații din care să rezulte existența unei amenințări la adresa securității naționale, prin prezentarea faptelor și circumstanțelor pe care se întemeiază propunerea;

d) motivația pentru care se impun activități specifice;

e) categoriile de activități pentru care se propune solicitarea autorizării;

f) dacă este necesară încuviințarea pătrunderii în spații private pentru desfășurarea de activități specifice;

g) perioada pentru care se propune solicitarea autorizării;

h) identitatea persoanei supusă măsurii, dacă aceasta este cunoscută;

i) locul unde urmează a fi executate activitățile propuse, dacă acesta este cunoscut".

Înainte de a analiza fiecare dintre mențiunile obligatorii, trebuie să precizăm faptul că toate aceste mențiuni vor trebui să se regăsească și în cuprinsul propunerii formulate de procurorul

general, ceea ce ne ridică semne de întrebare asupra unui aparent formalism al procedurii atunci când procurorul general va admite propunerea și va sesiza președintele Înaltei Curți de Casație și Justiție. Practic, nu există nicio garanție că procurorul nu va copia în mod mecanic propunerea făcută de organele din domeniul securității naționale și o va transmite mai apoi la Înalta Curte de Casație și Justiție.

Unele aspecte comune nu vor prezenta probleme deosebite, precum *numele și funcția persoanei care formulează propunerea* sau *data și locul emiterii propunerii*, acestea fiind elemente care se regăsesc și în cazul propunerii de autorizare a supravegherii tehnice.

Datele sau informațiile din care să rezulte existența unei amenințări la adresa securității naționale, prin prezentarea faptelor și circumstanțelor pe care se întemeiază propunerea reprezintă o mențiune obligatorie din cuprinsul propunerii, prin care se va prezenta contextul faptic în care se solicită autorizarea tehnicilor speciale de investigare. Fără a exista date sau informații concrete privind existența unei amenințări la securitatea națională nu se vor putea încuviința activități de culegere de informații, chiar dacă aceasta nu este o condiție legală impusă de art. 14 alin. (1) din Legea nr. 51/1991. Prin „existența unei amenințări" nu trebuie să înțelegem doar că în prezent ar exista o amenințare, ci și că se impune autorizarea de tehnici speciale de investigare pentru cunoașterea sau prevenirea amenințărilor la adresa securității naționale, în sensul art. 2 alin. (1) din Legea nr. 51/1991. După cum am arătat în secțiunea precedentă[1], legiuitorul nu a inclus un standard față de care să fie evaluate datele și informațiile în scopul aprecierii dacă datele și informațiile prezentate sunt suficiente pentru a se considera că există sau ar putea exista o amenințare la adresa securității naționale.

Motivația pentru care se impun activități specifice vizează scopul pentru care trebuie să fie autorizate tehnicile speciale de investigare. Dacă, în cazul supravegherii tehnice, am apreciat că scopul pentru care se autorizează măsura este un element de mai puțină importanță, deoarece scopul supravegherii tehnice este cel de a obține probe în procesul penal, în cazul activităților specifice culegerii de informații, scopul va avea un rol mai important. Susținem această concluzie prin faptul că, potrivit art. 2 din Legea nr. 51/1991, activitatea de culegere de informații poate să se desfășoare pentru mai multe scopuri – cunoașterea unei amenințări la adresa securității naționale, dar și prevenirea sau înlăturarea unei asemenea amenințări. Mai concret, organele din domeniul securității naționale vor trebui să arate ce fel de informații vor putea obține și de ce s-ar dovedi acestea necesare și utile. Față de diferența dintre gradul de periculozitate a amenințării reflectat și prin scopul potențial al măsurii, instanța competentă va trebui să aprecieze dacă scopul urmărit justifică folosirea unor tehnici speciale de investigare cu caracter intruziv.

Categoriile de activități pentru care se propune solicitarea autorizării constituie cel mai important element al propunerii de autorizare, dar și cel mai problematic, fiind o reinterpretare a prevederilor Codului de procedură penală asupra necesității indicării metodei speciale de supraveghere care se cere a fi autorizată. Spre deosebire de Codul de procedură penală, în care se impune a fi *indicate măsurile de supraveghere tehnică care se solicită a fi dispuse*, în cuprinsul Legii nr. 51/1991, se solicită numai indicarea unor categorii de activități de culegere de informații, și nu măsurile concrete. Aceasta înseamnă că legiuitorul a dorit să acorde un standard de protecție mai restrâns în cazul acestor tehnici speciale de investigare și garanții contra abuzului mai puține, situație cu care nu putem fi de acord. Simpla autorizare a categoriilor de măsuri dintre cele prevăzute de art. 14 alin. (2) din Legea nr. 51/1991 nu este acceptabilă,

[1] *V. supra*, Titlul XV, Capitolul II.1.

deoarece diminuează posibilitatea instanței competente să determine proporționalitatea măsurii care se dorește a fi autorizată. În opinia noastră, textul legal este în discordanță cu art. 8 par. 2 Conv.EDO, întrucât poate conduce la autorizarea generalizată a unor tehnici speciale de investigare. De exemplu, în cazul obținerii datelor privind tranzacțiile financiare ale unei persoane, vor putea fi obținute date și informații de la orice entitate financiară, pentru orice perioadă de timp, fără ca în propunere să trebuiască să se menționeze expres aceste elemente. Într-un alt exemplu, nu va trebui menționat tipul de comunicații electronice care vor fi interceptate, fiind suficient ca propunerea să vizeze doar această tehnică specială, fără a se indica dacă vor fi interceptate comunicații telefonice, prin Whatsapp sau prin e-mail. *De lege ferenda*, se impune ca propunerea să conțină o indicare a măsurilor concrete care se doresc a fi autorizate în beneficiul serviciilor de informații.

Precizarea privind necesitatea pătrunderii în spații private constituie un element facultativ pentru propunerea formulată de organele din domeniul securității naționale, care va avea legătură cu un alt element care trebuie prevăzut, respectiv locul în care se vor desfășura activitățile specifice. Corelând dispozițiile amintite cu conținutul unui eventual mandat, observăm că nu se specifică prin această dispoziție spațiul privat autorizat. Sensul urmărit de legiuitor a fost unul vag, permițând, aparent, ca organele din domeniul securității naționale să dobândească posibilitatea de a pătrunde în orice spațiu privat. Credem că orice pătrundere într-un spațiu privat necesită explicitări, organul din domeniul securității naționale trebuind să indice numărul de pătrunderi, scopul acestora și locul în care se vor desfășura, aceste elemente fiind obligatoriu, ulterior, să se regăsească în mandat, precum în cazul supravegherii tehnice prevăzute de Codul de procedură penală[1].

Perioada pentru care se propune solicitarea măsurii constituie un element care nu se regăsește și în Codul de procedură penală, nefiind menționat în cuprinsul art. 140 alin. (2) C.pr.pen. Inserarea lui în cuprinsul propunerii este utilă pentru a se aprecia mai bine gravitatea atingerii aduse vieții private a persoanei care urmează a fi supusă unor activități specifice de culegere de informații, sens în care este util ca procurorul și, ulterior, judecătorul să cunoască acest element pentru a înțelege pe deplin scopul măsurii propuse, dar și ce ingerință poate aduce.

Identitatea persoanei supuse măsurii, dacă aceasta este cunoscută, constituie un element care trebuie prevăzut în propunere, fiind firesc să se precizeze față de cine se ia măsura, pentru a se cunoaște identitatea persoanei căreia i se vor restrânge drepturile și libertățile fundamentale. Va fi de interes să se cunoască identitatea persoanei și prin prisma calității pe care o are, în special dacă îndeplinește o funcție de demnitate publică în stat, este magistrat, conducător al unor autorități publice locale etc.

Locul unde urmează a fi executate activitățile propuse, dacă acesta este cunoscut, poate constitui un element esențial pentru autorizarea activităților de culegere de informații, întrucât se impune autorizarea cât mai precisă a fiecărei locații care va fi avută în vedere. În mod evident, va avea relevanță această mențiune numai în cazul unora dintre tehnicile speciale; de pildă, nu va avea mare însemnătate la localizarea unei persoane, întrucât tocmai acest element se impune a fi aflat prin tehnică, sau la interceptarea comunicațiilor. O situație aparte este atunci când va fi necesar accesul în spații private, caz în care vor trebui să fie prevăzute expres toate locațiile unde vor putea pătrunde ofițerii serviciilor secrete. Nu putem concepe o pătrundere a serviciilor secrete într-un spațiu privat fără o autorizare, indiferent că se deplasează pentru a instala sau dezinstala mijloace tehnice de înregistrare sau pentru a căuta, copia și extrage

[1] *V. supra*, Titlul VI, Capitolul II.3.

informații, documente sau înscrisuri. Posibilitatea dată de legiuitor de a fi autorizate locuri numai în măsura în care ele sunt cunoscute este una abuzivă, impunându-se a fi abrogată, pentru că generalizează mandatul pe care îl au organele din domeniul securității naționale și permit incursiuni în orice spațiu privat, apreciat de acestea ca fiind locul unde se pot desfășura activități specifice.

Odată ce propunerea este formulată în scris de către organul din domeniul securității naționale și conține mențiunile amintite mai sus, ea va fi transmisă către procurorul general al P.I.C.C.J.[1]. Chiar dacă competența de a analiza propunerea aparține procurorului general, astfel cum se indică și în lege, acesta va desemna procurori din cadrul P.I.C.C.J., care vor fi responsabili cu analizarea legalității și temeiniciei unor astfel de propuneri, ceea ce nu exclude posibilitatea de a se desemna numai pe el însuși. Legiuitorul a instituit un termen de 24 de ore pentru ca procurorul general sau procurorul desemnat de acesta să se pronunțe asupra propunerii și, în cazuri care reclamă urgență, ar trebui să se pronunțe de îndată. Instituirea unor astfel de termene o socotim a fi nepotrivită, întrucât importanța securității naționale reclamă o analiză profundă asupra implicațiilor pe care le are omisiunea luării unor măsuri de prevenire sau înlăturare a unor amenințări la securitatea națională. În plus, din interpretarea textului legal s-ar putea deduce că urgența nu va fi stabilită de procuror, ci de organul din domeniul securității naționale, deoarece procurorul poate aprecia oricând caracterul urgent al cererii și se poate pronunța imediat după ce este sesizat. Caracterul grăbit al trecerii prin filtrul procurorului constituie un indiciu asupra caracterului de formalitate al controlului.

Conform art. 15 alin. (3) din Legea nr. 51/1991, dacă procurorul desemnat socotește că propunerea formulată este „nejustificată", acesta o va respinge printr-o ordonanță motivată. Considerăm nefericită alegerea legiuitorului de a folosi termenul de „nejustificată", întrucât reprezintă o contradicție cu dispozițiile art. 15 alin. (2) din Legea nr. 51/1991, prin care se instituie un control de legalitate și de temeinicie din partea procurorului, dar un caracter nejustificat ar trebui să însemne numai o lipsă de temeinicie a propunerii.

În cazul în care propunerea este întemeiată și sunt întrunite condițiile prevăzute de lege, aceasta se va admite și însuși procurorul general sau înlocuitorul său de drept (procurorul general adjunct – n.n.) va solicita în scris președintelui Înaltei Curți de Casație și Justiție să încuviințeze măsurile de supraveghere cerute. Observăm astfel că în cuprinsul art. 15 alin. (4) din Legea nr. 51/1991 se face referire la un alt procuror decât cel desemnat prin dispozițiile anterioare, respectiv la înlocuitorul de drept al procurorului general. Solicitarea în scris care trebuie transmisă Înaltei Curți de Casație și Justiție va trebui să conțină aceleași mențiuni ca propunerea formulată de organul din domeniul securității naționale. Din cuprinsul dispozițiilor art. 15 alin. (2)-(5) C.pr.pen. nu rezultă în mod expres posibilitatea ca procurorul general al P.I.C.C.J. să modifice propunerea formulată anterior de un organ din domeniul securității naționale, având posibilitatea numai de a respinge propunerea sau de a o admite, caz în care va face o propunere către organul judiciar competent, care va conține mențiunile din cuprinsul propunerii formulate de serviciul secret. Din modul de redactare a dispozițiilor legale rezultă un control formal exercitat de către procurorul general și de către procurorii anume desemnați, putându-se interpreta o preferință legală în sensul admiterii propunerii și transmiterii către instanța competentă pentru autorizare.

[1] Conform art. 15 alin. (2) din Legea nr. 51/1991, „propunerea se înaintează procurorului general al Parchetului de pe lângă Înalta Curte de Casație și Justiție și este examinată sub aspectul legalității și temeiniciei, în termen de 24 de ore de la înregistrare ori de îndată în cazurile urgente, de procurori anume desemnați de acesta".

Secțiunea a 3-a. Autorizarea tehnicilor speciale de investigare prevăzute de Legea nr. 51/1991

Asemenea dispunerii supravegherii tehnice de către judecătorul de drepturi și libertăți, la autorizarea unor activități specifice culegerii de informații se impune verificarea îndeplinirii condițiilor legale de autorizare prevăzute de art. 14 alin. (1) din Legea nr. 51/1991, procedura fiind prevăzută de art. 15-18 din Legea nr. 51/1991. Această verificare se face pe baza propunerii transmise de către procurorul general al P.I.C.C.J.

Competența de încuviințare a tehnicilor speciale de investigare prevăzute de Legea nr. 51/1991 va reveni, potrivit art. 15 alin. (6) din Legea nr. 51/1991, judecătorului din cadrul Înaltei Curți de Casație și Justiție anume desemnat de președintele Înaltei Curți de Casație și Justiție să judece astfel de propuneri. Acest judecător nu va fi considerat un judecător de drepturi și libertăți conform Codului de procedură penală, însă va acționa în mod similar cu acesta, exercitând o funcție similară, dar în alt domeniu și în afara unui cadru procesual.

Judecarea propunerii de încuviințare a tehnicilor speciale de investigare are loc de urgență, în camera de consiliu, fără ca legiuitorul să menționeze că prezența procurorului ar fi obligatorie[1]. Spre deosebire de dispozițiile Codului de procedură penală, în care se arată că judecarea propunerii se va face în aceeași zi, în cazul autorizării activităților specifice culegerii de informații, nu se precizează un termen clar, ci numai se menționează judecarea de urgență. Întrucât toate tehnicile speciale de supraveghere sau cercetare au un caracter secret, este evident că judecarea propunerii procurorului va trebui să se facă în cameră de consiliu, fără participarea publicului. Prezența procurorului nu numai că nu este menționată ca fiind obligatorie, dar este discutabil dacă judecarea cauzei se poate realiza în prezența sa, textul legal evidențiind, în realitate, că judecarea propunerii se va face întotdeauna în lipsa procurorului. Astfel, conform art. 15 alin. (7) din Legea nr. 51/1991, „*în cazul în care judecătorul, examinând solicitarea, apreciază că nu sunt suficiente informații, solicită suplimentarea de îndată, în scris, a argumentelor prezentate*", reflectând că procedura este una scrisă și nu permite procurorului să prezinte oral argumentele propunerii sale.

Soluțiile pe care le poate pronunța judecătorul din cadrul Înaltei Curți de Casație și Justiție sunt fie *respingerea propunerii*, fie *admiterea ei* și emiterea, de îndată, a *mandatului de autorizare a activităților specifice prevăzute de Legea securității naționale*.

Respingerea propunerii se va dispune conform art. 18 din Legea nr. 51/1991 atunci când judecătorul va constata că propunerea este nejustificată. Din nou, respingerea ca nejustificată este o soluție care nu are corespondent în procedura penală; apreciem că desemnează o respingere ca nefondată a cererii. Socotim că vor trebui să fie incidente aceleași tipuri de soluții prevăzute de Codul de procedură penală[2].

În cazul oricăreia dintre soluțiile adoptate de către judecător, aceasta nu va putea fi supusă niciunei căi de atac, însă procurorul va fi îndreptățit să formuleze o nouă cerere de încuviințare, în cazul respingerii, dacă vor fi îndeplinite cerințele prevăzute de art. 18 alin. (2) din Legea nr. 51/1991. Formularea unei a doua cereri de încuviințare a tehnicilor speciale de investigare va putea fi făcută numai în măsura în care au apărut sau s-au descoperit date sau informații noi, necunoscute la momentul soluționării cererii anterioare. Apreciem că această condiție nu

[1] Conform art. 15 alin. (6) din Legea nr. 51/1991, „solicitarea este examinată, de urgență, în camera de consiliu de unul din judecătorii anume desemnați de președintele Înaltei Curți de Casație și Justiție".

[2] *V. supra*, Titlul III, Capitolul II.2.

trebuie să fie considerată una formală, ea trebuind să fie verificată în mod temeinic de către judecător, raportat la starea de fapt descrisă în cuprinsul primei cereri de încuviințare.

În cazul *admiterii propunerii de încuviințare a activităților specifice*, judecătorul este îndreptățit să încuviințeze numai acele tehnici speciale care sunt proporționale și necesare pentru cauză, urmând să le respingă pe toate celelalte. Totodată, judecătorul se poate pronunța și asupra conținutului concret, în măsura în care propunerea formulată de procurorul general este suficient de detaliată. Admiterea cererii se face prin încheierea judecătorului care va proceda la emiterea imediată a unui mandat. În cuprinsul dispozițiilor legale nu se face nicio mențiune privind întocmirea minutei, ceea ce constituie o omisiune nepermisă din partea legiuitorului și o diferență față de supravegherea tehnică reglementată prin Codul de procedură penală.

Activitățile specifice culegerii de informații pot fi dispuse pentru o perioadă maximă de 6 luni, însă, conform art. 17 alin. (4) din Legea nr. 51/1991, aceasta poate fi prelungită, fiecare prelungire neputând depăși 3 luni[1]. Socotim cele două termene a fi excesive, constituind o situație care nu poate fi concepută într-o societate democratică – autorizarea unor măsuri de supraveghere extrem de intruzive pentru o primă durată care poate egala durata totală a măsurilor de supraveghere tehnică din procesul penal. Atât durata maximă inițială, cât și durata pentru care se pot prelungi autorizările se impun a fi reduse, deoarece au un caracter disproporționat față de drepturile și libertățile fundamentale ale unei persoane.

Totodată, conform art. 17 alin. (4) din Legea nr. 51/1991, durata maximă a autorizărilor *cu privire la aceleași date și informații din care să rezulte existența unei amenințări la adresa securității naționale* este de 2 ani. Spre deosebire de art. 144 alin. (3) C.pr.pen., în care se prevede că durata totală a măsurilor de supraveghere tehnică cu privire la aceeași persoană nu poate depăși 6 luni, Legea nr. 51/1991 nu limitează durata maximă la o persoană, ci numai la datele și informațiile din care rezultă că există o amenințare la adresa securității naționale. Deoarece nu se referă și la o persoană anume, este posibilă desfășurarea unor activități de culegere de informații paralele cu privire la aceeași persoană, ținând cont de date și informații diferite. Durata totală pentru care pot fi autorizate activitățile specifice restrictive de drepturi și libertăți fundamentale este excesivă și nejustificată, întrucât pune la îndoială însăși existența unei amenințări la securitatea națională, dacă pentru combaterea ei este nevoie de o activitate de 2 ani din partea organelor din domeniul securității naționale.

În cazul în care judecătorul constată că propunerea formulată de procurorul general al P.I.C.C.J. este justificată și sunt întrunite condițiile art. 14 alin. (1) din Legea nr. 51/1991, dispune autorizarea prin încheiere motivată a activităților specifice culegerii de informații. Încheierea trebuie să cuprindă, conform art. 17 alin. (1) din Legea nr. 51/1991:

„*a) denumirea instanței, data, ora și locul emiterii;*

b) date și informații din care să rezulte existența unei amenințări la adresa securității naționale, prin prezentarea faptelor și circumstanțelor care justifică măsura;

c) activitățile specifice autorizate, dintre cele prevăzute la art. 14 alin. (2);

d) identitatea persoanei care este afectată de activitățile specifice, prin restrângerea drepturilor și libertăților fundamentale, dacă aceasta este cunoscută;

[1] Conform art. 17 alin. (4) din Legea nr. 51/1991, „durata de valabilitate a autorizării activităților este cea necesară pentru desfășurarea acestora, dar nu mai mult de 6 luni. Autorizarea poate fi prelungită în aceleași condiții, pentru motive temeinic justificate, fiecare prelungire neputând depăși 3 luni. Durata maximă a autorizărilor cu privire la aceleași date și informații din care să rezulte existența unei amenințări la adresa securității naționale este de doi ani. Activitățile specifice încetează înainte de expirarea duratei pentru care au fost autorizate, îndată ce au încetat motivele care le-au justificat".

e) organele care efectuează activitățile autorizate;

f) persoanele fizice sau juridice care au obligația de a acorda sprijin la executarea activităților autorizate;

g) precizarea locului sau a localităților în care se vor desfășura activitățile autorizate, dacă acestea sunt cunoscute;

h) durata de valabilitate a autorizației".

Mențiunile cuprinse în încheiere corespund cu cele care trebuie să fie prevăzute, în mod obligatoriu, în propunerea formulată de organele din domeniul securității naționale și de propunerea procurorului general al P.I.C.C.J., în conformitate cu dispozițiile art. 15 alin. (1) din Legea nr. 51/1991. În ceea ce privește organele care efectuează activitățile autorizate, nu va fi suficient să se indice numai instituția autorizată (de pildă, S.R.I.), ci și unitatea militară care va realiza activitățile, prin menționarea indicativului unității (de exemplu, U.M. 0198, U.M. 0603) sau a numelui acesteia (D.G.P.I. Cluj).

Mențiunea privind sprijinul la executarea activităților autorizate se referă la aceleași persoane prevăzute și în cuprinsul art. 142 alin. (3) C.pr.pen., respectiv la persoanele care acordă sprijin tehnic, precum furnizorii de rețele publice sau de servicii de comunicații electronice.

După admiterea propunerii de utilizare a tehnicilor speciale ca activități specifice de culegere de informații, judecătorul din cadrul Înaltei Curți de Casație și Justiție emite, conform art. 17 alin. (2) din Legea nr. 51/1991, *un mandat*, care va conține mai multe elemente comune cu încheierea[1]. Față de conținutul încheierii, mandatului îi vor lipsi *datele și informațiile din care să rezulte existența unei amenințări la adresa securității naționale, prin prezentarea faptelor și circumstanțelor care justifică măsura*, astfel că se vor putea cunoaște date despre amenințarea la securitatea națională care a fost avută în vedere la emiterea sa. Din acest punct de vedere, mandatul se aseamănă la conținut cu mandatul de supraveghere tehnică prevăzut de Codul de procedură penală. O diferență majoră față de mandatul de supraveghere tehnică este că mandatul emis în temeiul Legii securității naționale va avea caracter clasificat și încadrat în categoria documentelor strict secrete, aspect care rezultă din interpretarea dispozițiilor art. 21 alin. (1) din Legea nr. 51/1991, care fac referire la declasificarea mandatului[2]. În același timp, menționăm că, potrivit art. 20 alin. (4) din Legea nr. 51/1991, „*procedura de autorizare a activităților specifice, precum și desfășurarea activităților autorizate se fac cu respectarea prevederilor legale privind protecția informațiilor clasificate*", aceasta însemnând că fiecare element al autorizării sau punerii în executare a activităților specifice va fi clasificat.

Asemenea Codului de procedură penală, legiuitorul a prevăzut și posibilitatea autorizării provizorii a activităților specifice culegerii de informații, în situațiile în care urgența situației nu permite obținerea unei autorizații din partea judecătorului anume desemnat din cadrul Înaltei Curți de Casație și Justiție. O atare prevedere este susceptibilă de aceleași critici pe care

[1] Conform art. 17 alin. (2) din Legea nr. 51/1991, „judecătorul emite, totodată, un mandat cuprinzând elementele prevăzute la alin. (1) lit. a) și c)-h)".

[2] Conform art. 21 alin. (1) din Legea nr. 51/1991, „datele și informațiile de interes pentru securitatea națională, rezultate din activitățile autorizate, dacă indică pregătirea sau săvârșirea unei fapte prevăzute de legea penală, sunt reținute în scris și transmise organelor de urmărire penală, potrivit art. 61 din Codul de procedură penală, însoțite de mandatul emis pentru acestea, la care se adaugă propunerea de declasificare, după caz, totală sau în extras, potrivit legii, a mandatului. Convorbirile și/sau comunicările interceptate, redate în scris, și/sau imaginile înregistrate se transmit organelor de urmărire penală în integralitate, însoțite de conținutul digital original al acestora".

deja le-am exprimat în cazul supravegherii tehnice[1], nefiind justificată existența ei, mai ales în condițiile în care o propunere a serviciilor secrete poate fi admisă de urgență de procuror și, ulterior, tot de urgență să fie judecată de judecătorul desemnat din cadrul Înaltei Curți de Casație și Justiție. Conform art. 19 alin. (1) din Legea nr. 51/1991, „*atunci când întârzierea obținerii autorizării ar prejudicia grav finalitatea activităților specifice necesare, acestea se pot efectua cu autorizarea procurorului, pe o durată de maximum 48 de ore, urmând ca autorizarea judecătorului să fie solicitată de îndată ce există posibilitatea, dar nu mai târziu de expirarea acestui termen. Judecătorul se pronunță asupra cererii de îndată*". Legiuitorul nu menționează ce trebuie să conțină ordonanța procurorului, dar apreciem că aceasta va trebui să aibă aceleași elemente ca încheierea judecătorului. Spre deosebire de procedura reglementată în Codul de procedură penală, în termenul de 48 de ore prevăzut pentru autorizarea provizorie, procurorul va trebui să și sesizeze judecătorul desemnat din cadrul Înaltei Curți de Casație și Justiție, fără a fi menționată o sancțiune care ar interveni în cazul depășirii termenului.

În procedura de confirmare a autorizării provizorii, procurorul poate cere judecătorului anume desemnat din cadrul Înaltei Curți de Casație și Justiție să dispună continuarea activităților, aplicându-se prevederile art. 15-17 din Legea nr. 51/1991. Practic, în mod similar Codului de procedură penală, se poate formula o cerere de autorizare a activităților specifice de culegere de informații în procedura confirmării autorizării provizorii. Această solicitare poate fi admisă sau respinsă, în cazul admiterii, procedându-se la emiterea unui mandat.

Judecarea confirmării se va face fără prezența procurorului, în cameră de consiliu, judecătorul putând dispune confirmarea măsurii autorizate de procuror și păstrarea materialelor obținute sau, după caz, încetarea de îndată și distrugerea acestora. Legiuitorul nu menționează dacă, alături de cererea de confirmare, procurorul va trebui să transmită și rezultatele activității de culegere de informații, dacă va transmite un original sau copii ale acestora. Față de Codul de procedură penală, credem că formularea este una inferioară, neputându-se vorbi de materiale rezultate, întrucât informațiile obținute nu pot avea înfățișare materială, eventual numai dacă informațiile sunt conținute de un mijloc material, atunci vom putea vorbi despre unele materiale rezultate. Era necesar ca legiuitorul să nu lase loc de interpretare asupra faptului că informațiile obținute nu vor putea fi folosite și că suportul pe care se află urmează a fi distrus. O altă exprimare deficitară privește folosirea expresiei „încetare", fiind nepotrivită, dacă măsura dispusă de procuror era nelegală, impunându-se infirmarea ordonanței motivate a procurorului și constatarea nelegalității activităților desfășurate. Încetarea punerii în executare a unor tehnici speciale de investigare se poate dispune numai dacă măsura a fost autorizată cu respectarea condițiilor legale, în caz contrar, măsura nu încetează, ci este desființată *ex tunc*, iar toate rezultatele ei trebuie să fie distruse.

În situația în care autorizarea provizorie dispusă de procuror se va infirma în condițiile art. 19 alin. (3) din Legea nr. 51/1991, în termen de 7 zile, procurorul va proceda la distrugerea rezultatelor activităților specifice de culegere de informații, informând ulterior judecătorul desemnat din cadrul Înaltei Curți de Casație și Justiție.

[1] *V. supra*, Titlul III, Capitolul II.3.

Secțiunea a 4-a. Punerea în executare a mandatului emis în baza Legii nr. 51/1991

Potrivit conținutului încheierii de autorizare a activităților specifice, dar și potrivit cuprinsului mandatului emis de judecătorul din cadrul Înaltei Curți de Casație și Justiție, punerea în executare se va realiza de către un organ din domeniul securității naționale. Cu toate că legea nu menționează dacă între organul care a propus autorizarea măsurii și cel care o pune în executare va exista identitate, apreciem că această chestiune se subînțelege, întrucât autorizarea se va emite în beneficiul persoanei care o solicită, nefiind firesc să se impună obligații asupra unui terț, fie și el organ din domeniul securității naționale. Spre deosebire de metodele speciale de supraveghere sau cercetare, procurorul nu va exercita niciun control sau o supraveghere a punerii în executare, activitățile specifice fiind desfășurate independent de serviciile secrete. O atare situație o apreciem ca fiind o gravă ignorare a dreptului la viață privată, neexistând nicio garanție efectivă că organele din domeniul securității naționale vor respecta autorizația primită și nu vor comite abuzuri împotriva persoanelor supravegheate.

Modalitatea concretă de punere în executare va fi similară cu cea din cazul supravegherii tehnice, fiind variată în funcție de fiecare tehnică specială care va fi autorizată. Bunăoară, din moment ce activitățile serviciilor de informații sunt sursa metodelor speciale de supraveghere sau cercetare, modalitatea concretă de punere în executare, tehnicile folosite, echipamentele și mijloacele tehnice utilizate vor fi similare, sens în care nu le vom reaminti în prezenta secțiune, ținând seama că prezenta lucrare a analizat deja, în detaliu, fiecare tehnică în parte.

Pentru a putea fi puse în executare, unele activități specifice vor presupune participarea unor persoane care sprijină punerea în executare, precum furnizorii de rețele publice de comunicații electronice sau furnizorii de servicii de comunicații electronice. Acestora, precum și persoanelor care solicită autorizarea, autorizează sau pun în executare activitățile specifice culegerii de informații li se impune respectarea prevederilor legale privind informațiile clasificate, ele fiind ținute să păstreze secretul operațiunii[1].

Dacă pe parcursul punerii în executare a mandatului emis de judecător se descoperă că tehnicile speciale autorizate sunt insuficiente, se poate proceda la completarea mandatului emis, prin formularea unei solicitări în acest sens[2]. O atare situație poate fi incidentă atunci când activitățile specifice culegerii de informații se pot dovedi insuficiente, necesitând fie autorizarea de activități noi, fie desfășurarea activităților în locuri față de care nu s-a emis o autorizare ori au existat modificări ale numerelor de telefon folosite de o persoană. Spre deosebire de Codul de procedură penală, legiuitorul a folosit expresia de „completare a mandatului", cu care nu putem fi de acord. Mandatul este doar rezultatul soluției date de judecătorul desemnat din cadrul instanței competente, este numai un instrument, în opinia noastră, fiind mai corect să operăm cu expresia de „completare a autorizării". Prin acest concept de „completare a mandatului" se ajunge la situația în care se suplimentează doar anumite activități specifice,

[1] Conform art. 20 alin. (1) din Legea nr. 51/1991, „persoanele care solicită autorizarea, autorizează, pun în executare sau sprijină punerea în executare a autorizării beneficiază de protecția legii și sunt obligate să păstreze secretul asupra datelor și informațiilor de care iau cunoștință cu acest prilej și să respecte prevederile legale privind protecția informațiilor clasificate".

[2] Conform art. 17 alin. (3) din Legea nr. 51/1991, „în situațiile în care este necesar să se autorizeze noi activități decât cele inițiale, desfășurarea acestora în alte locuri sau localități, dacă sunt cunoscute, ori atunci când au intervenit schimbări ale numerelor de apel, mandatul inițial se completează în mod corespunzător, cu aplicarea procedurii prevăzute de art. 15".

fără a fi modificate alte elemente din cuprinsul mandatului. Un element important este cel al expirării mandatului, o completare a acestuia neînsemnând și prelungirea valabilității sale. Practic, activitățile specifice nou autorizate vor fi valabile numai pentru restul de timp rămas până la expirarea mandatului inițial.

În cursul punerii în executare a activităților specifice culegerii de informații, este posibil să se constate că măsurile luate și-au atins scopul mai înainte de expirarea autorizării, sens în care se impune încetarea acestora. Conform art. 17 alin. (4) teza finală din Legea nr. 51/1991, *„activitățile specifice încetează înainte de expirarea duratei pentru care au fost autorizate, îndată ce au încetat motivele care le-au justificat*". În mod similar Codului de procedură penală, se impune a se dispune încetarea măsurilor de supraveghere atunci când temeiurile care au impus autorizarea lor nu mai subzistă[1]. Deși, aparent, din textul de lege citat s-ar părea că măsurile încetează de drept, o atare situație nu este posibilă, fiind necesară emiterea unui act prin care să se dispună încetarea măsurii. Deși nu se bucură de o reglementare coerentă, Legea nr. 51/1991 prevede expres că încetarea se va dispune de către organul care pune în executare măsura[2], respectiv de către un organ din domeniul securității naționale. Spre deosebire de Codul de procedură penală în care procurorul dispune încetarea măsurilor de supraveghere tehnică, în această situație, însuși serviciul secret va dispune întreruperea, de îndată ce temeiurile care le-au justificat au încetat. Odată ce au fost întrerupte activitățile specifice, serviciul secret va informa procurorul general al P.I.C.C.J., care, la rândul lui, va informa judecătorul din cadrul Înaltei Curți de Casație și Justiție.

În privința consemnării rezultatelor punerii în executare a activităților specifice autorizate de judecătorul desemnat din cadrul Înaltei Curți de Casație și Justiție, Legea nr. 51/1991 este deficitară, în sensul în care nu se face nicio precizare cu privire la modul în care vor arăta rezultatele, consemnând, pe alocuri, aspecte despre acestea. De pildă, se instituie obligația ca organele din domeniul securității naționale să îl informeze pe procurorul general al P.I.C.C.J. despre rezultatele obținute în urma activităților specifice și dacă au fost luate unele măsuri, fără a se detalia forma sub care trebuie să arate informarea, dacă se transmit și rezultatele, dacă aceasta se va face la expirarea măsurii sau pe parcurs etc.[3]. Un indiciu despre faptul că rezultatele activităților de culegere de informații vor avea formă scrisă sau cel puțin materială rezultă din dispozițiile art. 21 alin. (1) din Legea nr. 51/1991, în care se arată că datele și informațiile obținute din activitățile specifice pot fi folosite pentru sesizarea organelor de urmărire penală, sens în care *„datele și informațiile de interes pentru securitatea națională, rezultate din activitățile autorizate, dacă indică pregătirea sau săvârșirea unei fapte prevăzute de legea penală, sunt reținute în scris și transmise organelor de urmărire penală, potrivit art. 61 din Codul de procedură penală*". Nu se menționează dacă prin consemnarea lor în scris se vor reda procese-verbale ca în cazul supravegherii tehnice, dar, dată fiind natura de tehnici speciale de investigare, rezultatele vor trebui consemnate într-un mod similar, chiar dacă nu

[1] *V. supra*, Titlul III, Capitolul III.3.

[2] Conform art. 20 alin. (2) din Legea nr. 51/1991, „organele care pun în executare activitățile autorizate sunt obligate să le întrerupă de îndată atunci când temeiurile care le-au justificat au încetat și să îl informeze despre aceasta pe procurorul general al Parchetului de pe lângă Înalta Curte de Casație și Justiție. Procurorul general al Parchetului de pe lângă Înalta Curte de Casație și Justiție informează Înalta Curte de Casație și Justiție despre întreruperea activităților autorizate atunci când temeiurile care le-au justificat au încetat".

[3] Conform art. 20 alin. (3) din Legea nr. 51/1991, „aceleași organe au obligația să îl informeze în scris pe procurorul general al Parchetului de pe lângă Înalta Curte de Casație și Justiție despre rezultatul activităților autorizate prin mandat și despre măsurile luate, conform legii".

va fi respectată forma prevăzută de Codul de procedură penală. În acest sens sunt relevante și dispozițiile art. 21 alin. (1) teza finală din Legea nr. 51/1991, în care se arată că: „*convorbirile și/sau comunicările interceptate, redate în scris, și/sau imaginile înregistrate se transmit organelor de urmărire penală în integralitate, însoțite de conținutul digital original al acestora*", astfel că se vor realiza note de redare a convorbirilor și comunicărilor, într-un mod similar cu dispozițiile art. 143 alin. (4) C.pr.pen. Evident, nu va exista nicio garanție privind redarea integrală, acestea nu vor fi certificate de procuror, nu se prevede în ce act vor fi descrise, vor fi redate de un ofițer al unui serviciu secret etc. Din acest punct de vedere, este dificil de definit o anumită formă a datelor și informațiilor obținute, sens în care trebuie subliniat că acestea nu vor putea fi folosite ca probe într-un proces penal, întrucât nici măcar regulile de consemnare a lor nu sunt compatibile cu cele ale Codului de procedură penală.

Capitolul III
Valorificarea rezultatelor utilizării tehnicilor speciale prevăzute de Legea nr. 51/1991

Secțiunea 1. Valoarea probantă a rezultatelor utilizării tehnicilor speciale prevăzute de Legea nr. 51/1991

În considerarea faptului că tehnicile speciale de investigare prevăzute de art. 14 alin. (2) din Legea nr. 51/1991 au fost reglementate în scopul cunoașterii, prevenirii și înlăturării amenințărilor la securitatea națională, posibilitatea folosirii acestora în cursul procesului penal este una care impune o analiză, în special având în vedere faptul că, în Codul de procedură penală, sunt reglementate tehnici similare prin metodele speciale de supraveghere sau cercetare. Întrucât nu poate fi acceptat ca organele din domeniul securității naționale să realizeze acte de urmărire penală, ele nefiind organe judiciare, nu va putea exista o implicare directă a acestora în desfășurarea urmăririi penale sau realizarea unor anchete paralele cu urmărirea penală. Cu alte cuvinte, procedeele investigative speciale de securitate națională nu pot fi incluse în sfera procesului penal[1]. Cu toate acestea, din activitățile specifice culegerii de informații vor putea reieși date și informații privind pregătirea săvârșirii ori săvârșirea unor infracțiuni, organele din domeniul securității naționale putând avea o contribuție incidentală la desfășurarea urmăririi penale.

Sub imperiul Codului de procedură penală anterior, au fost expuse trei opinii în privința folosirii tehnicilor speciale de investigare prevăzute de Legea nr. 51/1991 în procesul penal: *i)* posibilitatea folosirii lor numai în faza actelor premergătoare; *ii)* folosirea lor atât în cadrul actelor premergătoare, cât și în cursul urmăririi penale; *iii)* folosirea lor în faza actelor premergătoare, a urmăririi penale și a judecății[2]. Sub acest aspect, s-a argumentat că erau incidente dispozițiile art. 20-22 din Legea nr. 535/2004 privind prevenirea și combaterea terorismului[3], prin care se puteau autoriza astfel de activități, întrucât reprezentau atât amenințări la securitatea națională, cât și infracțiuni[4]. În plus, s-a arătat că o influență mare în sensul folosirii în procesul penal a rezultatelor activităților specifice culegerii de informații o constituiau și dispozițiile art. 224 alin. (2) și (3) C.pr.pen. anterior ce reglementau actele premergătoare[5].

Sub imperiul Codului de procedură penală anterior, dispozițiile art. 224 alin. (2) C.pr.pen. anterior permiteau desfășurarea unor activități înainte de a se dispune începerea urmăririi penale[6], cu scopul de a se strânge date pentru verificarea actului de sesizare și de a se putea

---

[1] *M. Udroiu, R. Slăvoiu, O. Predescu*, Tehnici speciale, 2009, p. 71.

[2] *Ibidem*, p. 70.

[3] Legea nr. 535 din 25 noiembrie 2004 privind prevenirea și combaterea terorismului (M. Of. nr. 1161 din 8 decembrie 2004).

[4] *S. Grădinaru*, Supravegherea tehnică, 2014, p. 96.

[5] *M. Udroiu, R. Slăvoiu, O. Predescu*, Tehnici speciale, 2009, pp. 70-71.

[6] Conform art. 224 alin. (2) C.pr.pen. anterior: „De asemenea, în vederea strângerii datelor necesare organelor de urmărire penală pentru începerea urmăririi penale, pot efectua acte premergătoare și lucrătorii operativi din Ministerul de Interne, precum și din celelalte organe de stat cu atribuții în domeniul siguranței naționale, anume desemnați în acest scop, pentru fapte care constituie, potrivit legii, amenințări la adresa siguranței naționale".

verifica dacă se impune începerea urmăririi penale. Aceste activități se puteau realiza și de către lucrători operativi din cadrul Ministerului Afacerilor Interne (D.G.P.I.) sau de către alte organe de stat din domeniul securității naționale. Ținând seama de specificul acestor activități, s-a apreciat că în cadrul acestora vor intra și tehnicile speciale de investigare prevăzute de art. 14 alin. (2) din Legea nr. 51/1991. Ca valoare probantă, Codul de procedură penală menționa în cuprinsul art. 224 alin. (3) C.pr.pen. că „*procesul-verbal prin care se constată efectuarea unor acte premergătoare poate constitui mijloc de probă*". În practica mai veche, rezultatele activităților de culegere de informații erau incluse în acest proces-verbal, mai ales dacă constau în redarea convorbirilor interceptate[1]. În opinia noastră, chiar și sub imperiul vechii reglementări procesuale penale, nu puteau fi valorificate ca probe rezultatele obținute în urma activităților specifice culegerii de informații, întrucât se desfășurau cu un alt scop decât cel al strângerii probelor și puteau fi întrebuințate, ca oricare act premergător, numai pentru începerea urmăririi penale, nu și pentru probarea săvârșirii unei infracțiuni.

Codul de procedură penal actual și forma actuală a Legii nr. 51/1991 au clarificat acest aspect, în prezent, activitățile specifice culegerii de informații neputând fi folosite ca probe în procesul penal, ci putând fi folosite ca date și informații care să stea la baza sesizării organelor de urmărire penală, fiind eliminată faza actelor premergătoare și instituindu-se obligația administrării probelor numai după emiterea ordonanței de începere a urmăririi penale, conform art. 305 alin. (1) C.pr.pen.

Conform art. 21 alin. (1) din Legea nr. 51/1991, „*datele și informațiile de interes pentru securitatea națională, rezultate din activitățile autorizate, dacă indică pregătirea sau săvârșirea unei fapte prevăzute de legea penală, sunt reținute în scris și transmise organelor de urmărire penală, potrivit art. 61 din Codul de procedură penală, însoțite de mandatul emis pentru acestea, la care se adaugă propunerea de declasificare, după caz, totală sau în extras, potrivit legii, a mandatului. Convorbirile și/sau comunicările interceptate, redate în scris, și/sau imaginile înregistrate se transmit organelor de urmărire penală în integralitate, însoțite de conținutul digital original al acestora*". Acest text legal instituie o obligație pentru organele din domeniul securității naționale de a transmite toate datele și informațiile rezultate, dacă din acestea se apreciază că rezultă săvârșirea unei fapte prevăzute de legea penală. Este interesant faptul că nu va conta gravitatea infracțiunii, nefiind necesar ca aceasta să fie dintre cele pentru care s-ar putea încuviința supravegherea tehnică, respectiv să fie una dintre infracțiunile amintite la art. 139 alin. (2) C.pr.pen. Considerăm că legislația are un neajuns, deoarece pune pe o poziție superioară din acest punct de vedere tehnicile speciale de investigare prevăzute de art. 14 alin. (2) din Legea nr. 51/1991, în condițiile în care legea procesuală penală limitează mai strict folosirea în altă cauză a unor date și informații rezultate din supravegherea tehnică[2].

În procedura de comunicare a datelor și informațiilor rezultate din activitățile specifice, organele din domeniul securității naționale vor comunica și mandatul emis pentru acesta și propunerea de declasificare totală sau în extras a mandatului, de aici rezultând că se vor comunica procurorului documente clasificate, alături de propunerea de declasificare a lor. Credem că legiuitorul a greșit când s-a referit numai la declasificarea mandatului, întrucât și rezultatele activităților de culegere de informații au caracter secret, potrivit legii. Practic, legea impune declasificarea informațiilor clasificate dacă din ele rezultă o faptă penală, însă nu

[1] *V. Dabu, L. Radu*, Legalitatea interceptărilor în faza actelor premergătoare, în Revista de Drept Penal nr. 1/2012, p. 79.

[2] V. *supra*, Titlul III, Capitolul IX.2.

trebuie ignorat faptul că emitentul informațiilor clasificate (organul din domeniul securității naționale) va trebui să își dea acordul, aceasta reprezentând o excepție legală. Cu toate acestea, nu există nicio garanție că astfel de informații vor fi transmise dacă declasificarea ar afecta interesele organului emitent al lor, sens în care se va putea declasifica în extras mandatul, omițându-se anumite elemente care vor rămâne clasificate. Deși înțelegem că menținerea unui grad de secretizare este importantă, apreciem că un organ de urmărire penală nu poate folosi date și informații clasificate pentru sesizarea sa, fiind imperios necesar ca, înainte de a se sesiza, să fi obținut declasificarea mandatului și a rezultatelor activităților specifice și ca acestea să fie depuse la dosarul cauzei. Numai așa se poate elucida în mod transparent practica organelor de urmărire penală de a dovedi veleități de oracol, prin sesizări din oficiu deosebit de precise, fără indicarea niciunei surse și cu descrierea amănunțită a faptelor sesizate. Considerăm că ascunderea unei sesizări din partea unor organe din domeniul securității naționale este ilegală, întrucât împiedică persoana acuzată să poată contesta legalitatea obținerii datelor și informațiilor care au stat la baza sesizării.

Alături de mandat și propunerea de declasificare, se vor transmite, în scris, și convorbirile și comunicările redate în scris (sub forma de note de redare), dar și imaginile și înregistrările audiovideo, care vor fi transmise și în formă digitală.

Din punctul de vedere al legii procesuale penale, vor fi aplicabile dispozițiile art. 61 alin. (1) C.pr.pen., în care se arată că „*ori de câte ori există o suspiciune rezonabilă cu privire la săvârșirea unei infracțiuni, sunt obligate să întocmească un proces-verbal despre împrejurările constatate: (...) c) organele de ordine publică și siguranță națională, pentru infracțiunile constatate în timpul exercitării atribuțiilor prevăzute de lege*". Dispozițiile din Codul de procedură penală se coroborează cu dispozițiile Legii nr. 51/1991, instituind aceeași obligație de informare a organelor de urmărire penală, însă Codul de procedură penală prevede și forma pe care trebuie să o aibă actul trimis de organele din domeniul securității naționale.

Conform art. 61 alin. (5) C.pr.pen., „*procesul-verbal încheiat în conformitate cu prevederile alin. (1) constituie act de sesizare a organelor de urmărire penală și nu poate fi supus controlului pe calea contenciosului administrativ*", legiuitorul rezolvând definitiv orice discuție privind valoarea probantă a rezultatelor activităților de culegere de informații prevăzute de art. 14 alin. (2) din Legea nr. 51/1991, prin aceea că a instituit valoarea lor de act de sesizare. Fiind doar un act de sesizare, nu vor putea avea niciodată calitatea de probe datele și informațiile obținute și nici procesul-verbal nu va avea calitatea de mijloc de probă. Dispozițiile art. 61 alin. (5) C.pr.pen. vor trebui să fie coroborate cu cele ale art. 291 C.pr.pen., procesul-verbal constituind actul de sesizare a organelor de urmărire penală[1], fiind nelegală o folosire a datelor și informațiilor obținute pentru o sesizare din oficiu, conform art. 292 C.pr.pen.

Chiar dacă problema valorii probante a rezultatelor tehnicilor speciale de investigare folosite de organele din domeniul securității statului a fost elucidată de legiuitor, aceste organe nu și-au pierdut năravul de a se implica în activitatea organelor de urmărire penală, iar acestea din urmă nu au refuzat un sprijin în administrarea de probe din partea serviciilor secrete. Printr-o fraudă la lege s-a ajuns ca dispozițiile art. 139 alin. (3) C.pr.pen. privind înregistrările care nu au nevoie de autorizare să fie interpretate în sensul în care activitățile specifice culegerii de informații să fie considerate „orice alte înregistrări care nu sunt interzise de lege", în scopul justificării lor ca mijloc de probă. Pentru a combate o astfel de abordare deosebit de periculoasă, Curtea Constituțională s-a pronunțat prin Decizia nr. 55/2020, în care a constatat că: „*dispozițiile*

[1] *G. Bodoroncea*, în M. Udroiu (coord.), Codul de procedură penală, 2017, p. 233.

art. 139 alin. (3) teza finală din Codul de procedură penală sunt constituționale în măsura în care nu privesc înregistrările rezultate ca urmare a efectuării activităților specifice culegerii de informații care presupun restrângerea exercițiului unor drepturi sau libertăți fundamentale ale omului desfășurate cu respectarea prevederilor legale, autorizate potrivit Legii nr. 51/1991"[1]. Astfel cum am arătat deja în prezenta lucrare, ca urmare a deciziei Curții Constituționale amintite, rezultatele activităților specifice vor fi lipsite de orice valoare probantă cât timp nu este reglementată o procedură clară și previzibilă de contestare a legalității autorizării și punerii în executare a acestora[2]. În motivarea deciziei, Curtea Constituțională a avut în vedere scopul diferit pentru care se autorizează activitățile specifice culegerii de informații, datele și informațiile obținute neputând fi folosite ca probe în procesul penal în considerarea evidentei restrângeri a dreptului la viață privată, semnalând o viitoare abandonare a utilizării serviciilor de informații în desfășurarea urmăririi penale.

O altă problemă aparte relevată de doctrină este cea a descoperirii unor bunuri a căror deținere este interzisă de lege, în timpul realizării activităților de culegere de informații, prin tehnica ridicării și punerii la loc a unui obiect, document sau înscris, fiind identificate două ipoteze[3]: *i)* dacă obiectele identificate atestă pregătirea unei infracțiuni flagrante la regimul securității naționale, a unui atentat sau act terorist, ofițerii din cadrul serviciilor secrete vor lua măsura ridicării obiectelor și reținerii făptuitorului; *ii)* dacă bunurile descoperite atestă săvârșirea unei alte infracțiuni, atunci vor proceda la sesizarea organului de urmărire penală competent.

În privința primei situații, dacă, în cazul desfășurării activităților specifice culegerii de informații, se va constata o infracțiune flagrantă, atunci vom fi într-o situație mai specială în care, deși nu vor putea fi folosite rezultatele activităților specifice culegerii de informații, constatarea infracțiunii flagrante se va putea realiza, întrucât atât dispozițiile legii procesuale penale[4], cât și ale Legii nr. 14/1992 prevăd acest lucru (în cazul S.R.I.)[5]. Considerăm situația clară, ținând seama de dezlegările date de Curtea Constituțională în privința acțiunilor ce pot constitui amenințări la adresa securității naționale, organele de stat din domeniul securității naționale acționând asemenea unui organ din domeniul ordinii publice care constată o infracțiune flagrantă, în urma acesteia putând rezulta probe în procesul penal. Însă, ceea ce este anterior constatării infracțiunii flagrante va rămâne în afara procesului penal sub actuala legislație, deși întrevedem ca utilă și o contestare a legalității desfășurării activităților specifice,

[1] CCR, Dec. nr. 55 din 4 februarie 2020 (M. Of. nr. 517 din 17 iunie 2020).

[2] *Ibidem*, §60.

[3] *D.C-tin Mâță*, op. cit., p. 373.

[4] Conform art. 61 alin. (2)-(4) C.pr.pen.: „(2) Organele prevăzute la alin. (1) au obligația să ia măsuri de conservare a locului săvârșirii infracțiunii și de ridicare sau conservare a mijloacelor materiale de probă. În cazul infracțiunilor flagrante, aceleași organe au dreptul de a face percheziții corporale sau ale vehiculelor, de a-l prinde pe făptuitor și de a-l prezenta de îndată organelor de urmărire penală.

(3) Când făptuitorul sau persoanele prezente la locul constatării au de făcut obiecții ori precizări sau au de dat explicații cu privire la cele consemnate în procesul-verbal, organul de constatare are obligația de a le consemna în procesul-verbal.

(4) Actele încheiate împreună cu mijloacele materiale de probă se înaintează, de îndată, organelor de urmărire penală".

[5] Conform art. 12 alin. (1) din Legea nr. 14/1992, „în cazul constatării unei infracțiuni flagrante la regimul siguranței naționale stabilit de lege, a unui atentat sau act terorist ori a unor tentative sau acte preparatorii la asemenea infracțiuni, dacă sunt pedepsite de lege, cadrele Serviciului Român de Informații pot reține pe făptuitor, predându-l de îndată organelor judiciare competente împreună cu actul de constatare și corpurile delicte".

sens în care, supunându-se regulilor nulității, chiar și constatarea infracțiunii flagrante ar putea fi lovită de o nulitate derivată.

În cazul celei de-a doua situații, dacă din activitatea specifică rezultă că bunurile descoperite și bănuite a fi deținute ilegal vor atrage răspunderea penală pentru infracțiuni care nu au legătură cu domeniul securității naționale, se va putea proceda, în temeiul art. 21 alin. (1) din Legea nr. 51/1991 coroborat cu art. 61 C.pr.pen., la sesizarea organelor de urmărire penală, rezultatele activităților specifice neputând fi folosite ca probe în procesul penal.

Secțiunea a 2-a. Contestarea legalității și temeiniciei utilizării tehnicilor speciale prevăzute de Legea nr. 51/1991

În realizarea oricărui act juridic trebuie pornit de la premisa bunei-credințe și a legalității actului, impunându-se ca persoana care se consideră vătămată ca urmare a unui act ilicit să probeze atât existența actului ilicit, cât și vinovăția persoanei care l-a realizat și să justifice existența unui prejudiciu. Deoarece organele din domeniul securității naționale nu pot fi exceptate de la această regulă fundamentală, ele trebuie să poată fi trase la răspundere pentru activitățile nelegale desfășurate prin activitățile de culegere de informații.

Am ales în prezenta secțiune să analizăm posibilitatea contestării legalității și temeiniciei activităților specifice desfășurate de organele din domeniul securității naționale, întrucât aceasta a reprezentat o problemă deosebită în cazul metodelor speciale de supraveghere sau cercetare, Codul de procedură penală având un caracter deficitar sub acest aspect. Deoarece activitățile specifice culegerii de informații se desfășoară în afara unui proces penal și nu vor putea constitui decât sursa de date și informații care poate sta la baza sesizării organelor de urmărire penală, se impun câteva considerații asupra: *i)* dreptului persoanei supuse unei tehnici speciale de a fi informată asupra acesteia; *ii)* dreptului persoanei supuse unei tehnici speciale de a contesta legalitatea și temeinicia ei.

§1. Informarea persoanei supuse unei tehnici speciale de investigare prevăzute de Legea nr. 51/1991

Posibilitatea ca o persoană supusă unei tehnici speciale de investigare folosite în temeiul Legii nr. 51/1991 să fie informată asupra desfășurării împotriva sa a unor astfel de măsuri intruzive este prevăzută de art. 21 alin. (2)-(3) din Legea nr. 51/1991. Afirmăm că legea stabilește o posibilitate, și nu un drept al persoanei, într-un mod care este chiar mai formal decât procedura informării persoanei supravegheate prevăzută de art. 145 C.pr.pen., deoarece nu se stabilește nicio obligație în sarcina serviciului secret care a realizat activitățile de culegere de informații să informeze, în toate cazurile, persoana supusă măsurilor. În același timp, nu se stabilește nici vreun termen în care să se realizeze informarea.

Conform art. 21 alin. (2) din Legea nr. 51/1991, „*în cazul în care datele și informațiile rezultate din activitățile autorizate nu sunt suficiente pentru sesizarea organelor de urmărire penală și nici nu justifică desfășurarea în continuare de activități de informații cu privire la acea persoană, din dispoziția conducătorului organului de stat cu atribuții în domeniul securității naționale se dispune notificarea persoanei ale cărei drepturi sau libertăți au fost afectate prin activitățile autorizate, cu privire la activitățile desfășurate față de aceasta și perioadele în care s-au desfășurat*".

Informarea persoanei supuse activităților specifice culegerii de informații poate opera numai în situația în care au existat activități care produceau o restrângere a drepturilor și libertăților fundamentale ale omului, respectiv activitățile specifice prevăzute de art. 14 alin. (2) din Legea nr. 51/1991, precum și activitățile specifice prevăzute de art. 13 lit. f) din Legea nr. 51/1991, care constituie tehnici speciale de investigare. Aceasta se va realiza din dispoziția conducătorului organului de stat cu atribuții în domeniul securității naționale, respectiv de către persoana care deține funcția de conducere a unui serviciu de informații. O atare prevedere o socotim a fi una care nu dă nicio eficiență informării, deoarece impune ca aceasta să se realizeze la dispoziția unei persoane aflate în vârful ierarhiei unei structuri, existând toate șansele ca această persoană să omită să dispună informarea. Mai mult, față de dispozițiile art. 145 C.pr.pen., informarea va trebui dispusă de către conducătorul organului din domeniul securității naționale, nu doar să se realizeze de către acesta, diferit de modul în care procurorul realizează informarea[1]. Textul poate fi interpretat în sensul în care dreptul persoanei supravegheate nu se naște ca urmare a legii, ci ca urmare a deciziei unui organ de stat. Sub acest aspect, este discutabil dacă acesta este un drept, deoarece nu prezintă nicio garanție procedurală de a fi respectat în vreo situație.

Totodată, informarea se va realiza numai dacă datele și informațiile obținute nu sunt folosite în vederea sesizării organelor de urmărire penală în condițiile art. 61 C.pr.pen., situație în care informarea nu se va realiza nici de organul din domeniul securității naționale și nici de către procuror.

Informarea nu va avea loc nici dacă datele și informațiile rezultate din activitățile specifice nu justifică o continuare a desfășurării de activități de informații cu privire la acea persoană, ceea ce semnifică faptul că informarea va opera în funcție de necesitatea desfășurării de activități specifice față de o persoană anume, nu față de o amenințare la adresa securității naționale. Distincția este importantă, deoarece, ținând seama de durata excesiv de mare pentru care se pot autoriza activitățile specifice culegerii de informații, se poate ca mandatul să înceteze pentru o anumită persoană mai înainte de a înceta față de altele. Din acest punct de vedere, apreciem că situația poate conduce la o evitare a informării persoanei față de care a încetat, în urma unei analize a dispozițiilor care permit omiterea informării și care sunt cuprinse în art. 21 alin. (3) din Legea nr. 51/1991, în care se stipulează că: „*notificarea prevăzută la alin. (2) nu se va face dacă: a) ar putea conduce la periclitarea îndeplinirii atribuțiilor de serviciu ale organelor de stat cu atribuții în domeniul securității naționale, prin dezvăluirea unor surse ale acestora, inclusiv ale serviciilor de securitate și informații ale altor state; b) ar putea afecta apărarea securității naționale; c) ar putea aduce atingere drepturilor și libertăților unor terțe persoane; d) ar putea duce la deconspirarea metodelor și mijloacelor, inclusiv a tehnicilor speciale de investigare concrete, utilizate în cazul respectiv de organele de stat cu atribuții în domeniul securității naționale*". În concret, s-ar putea susține că atât timp cât mandatul emis de judecătorul anume desemnat din cadrul Înaltei Curți de Casație și Justiție este încă în perioada sa de valabilitate, notificarea unei persoane care cădea sub incidența mandatului ar putea afecta apărarea securității naționale.

În continuarea analizei dispozițiilor care privesc informarea persoanei supuse unor activități specifice de culegere de informații, arătăm că aceasta nu va putea fi informată dacă „*ar putea conduce la periclitarea îndeplinirii atribuțiilor de serviciu ale organelor de stat cu*

[1] Conform art. 145 alin. (1) C.pr.pen., „după încetarea măsurii de supraveghere tehnică, procurorul informează, în scris, în cel mult 10 zile, pe fiecare subiect al unui mandat despre măsura de supraveghere tehnică ce a fost luată în privința sa".

atribuții în domeniul securității naționale, prin dezvăluirea unor surse ale acestora, inclusiv ale serviciilor de securitate și informații ale altor state". Aceasta semnifică faptul că, dacă, prin informarea asupra realizării activităților, s-ar divulga implicarea unor surse (de regulă, alte persoane) și aceasta ar afecta activitatea serviciilor interne sau din alte state, persoana nu va putea fi informată, ipoteză pe care noi o socotim a fi excesivă prin raportare la măsurile care se realizează. Din similaritatea lor cu supravegherea tehnică, activitățile specifice culegerii de informații presupun un caracter secret, care va conduce la imposibilitatea dezvăluirii unor aspecte concrete, dar acestea vor fi neesențiale sau vor putea fi considerate informații clasificate. Criteriul folosit de legiuitor este unul prea general și nu are nicio legătură cu o informare cel puțin sumară a persoanei supravegheate cu privire la activitățile concrete. De exemplu, va trebui realizată informarea și atunci când vecinul persoanei supuse măsurii a colaborat (sau era agent operativ) la realizarea activităților specifice în domiciliul persoanei, omițându-se elementele care ar putea conduce la identificarea vecinului. Legiuitorul a preferat să suprime dreptul la informare decât să reglementeze o informare care să apere atât drepturile individului, cât și protejarea securității naționale.

A doua situație este atunci când informarea *ar putea afecta apărarea securității naționale*, caz pe care îl apreciem ca fiind valid în situațiile în care amenințările la adresa securității naționale au un caracter complex și încă persistă anumite suspiciuni cu privire la respectiva persoană, existând date și informații referitoare la o altă amenințare la adresa securității naționale. De pildă, în funcție de particularitățile situației, o persoană poate fi implicată în mai multe activități care pot fi considerate amenințări la adresa securității naționale, pentru fiecare dintre acestea, emițându-se mandate de autorizare a activităților specifice, unul dintre acestea expirând sau încetând înainte de altele. În mod evident, informarea persoanei ar putea să afecteze apărarea securității naționale, deoarece ar putea să o determine să fie mai precaută și să nu mai poată fi asigurat scopul prevăzut de art. 2 din Legea nr. 51/1991. Cu toate acestea, apreciem că legiuitorul trebuia să introducă un termen maxim până la care se putea amâna informarea persoanei, în funcție de persistența unor date și informații că aceasta ar fi implicată și în alte activități care ar afecta securitatea națională.

Al treilea criteriu de omitere a informării constă în posibilitatea ca informarea să aducă *atingere drepturilor și libertăților unei terțe persoane*. Un atare criteriu îl considerăm neadecvat, întrucât nu se relevă în ce mod desfășurarea de activități specifice față de o persoană ar afecta în vreun mod un terț. Mai mult decât atât, nu vedem în ce mod ar fi afectate drepturile și libertățile unui terț din moment ce activitățile specifice s-au desfășurat prin aplicarea legii și informarea constituie tot o posibilitate prevăzută de lege. Credem că, în realitate, legiuitorul a urmărit să apere unele persoane de eventuale răzbunări din partea persoanei care a fost supusă măsurii, dacă aceasta din urmă ar bănui că ar fi colaborat cu organele din domeniul securității naționale. Nu apreciem că un atare risc justifică neinformarea persoanei, ci, dacă există un pericol real că acest lucru s-ar întâmpla, pot fi sesizate organele de urmărire penală.

Al patrulea caz în care nu se va realiza informarea persoanei supuse activităților specifice va fi întrunit dacă informarea *ar putea duce la deconspirarea metodelor și mijloacelor, inclusiv a tehnicilor speciale de investigare concrete, utilizate în cazul respectiv de organele de stat cu atribuții în domeniul securității naționale*. Nu considerăm că un asemenea caz este unul justificat, întrucât tehnicile speciale de investigare sunt cele prevăzute de lege, nefiind legal să se folosească tehnici noi, aceasta putând veni în contradicție cu respectarea art. 8 Conv.EDO. Acest caz de omisiune a informării îl considerăm ca fiind anacronic, întrucât folosirea unor

tehnici speciale de investigare este deja de notorietate, ele fiind prevăzute și în cuprinsul Codului de procedură penală, unde sunt detaliate. Desigur, pot exista proceduri sau mijloace concrete care vor reprezenta secret de stat, însă informarea unei persoane supuse activităților specifice culegerii de informații nu implică și prezentarea tehnicii folosite, a modului cum a fost folosită sau a capacităților sale tehnice. De exemplu, în cazul unei înregistrări în mediu ambiental, nu va fi importantă informația privind modelul de cameră, capacitățile sale, costul producător, fiind suficient să se indice unde au avut loc înregistrările și natura lor – video, audio, audiovideo sau fotografiere.

Spre deosebire de informarea persoanei privind supravegherea tehnică, în cazul desfășurării unor activități specifice culegerii de informații, legea nu instituie posibilitatea ca persoana care a fost supusă acestor măsuri să poată cunoaște conținutul rezultatelor obținute. Practic, informarea persoanei va fi mai degrabă o formalitate, deoarece nu îi va fi dezvăluit rezultatul reflectat în înregistrări sau în note de redare.

Având în vedere limitările expuse mai sus, informarea persoanei supuse unor activități specifice nu poate constitui un drept al acesteia, legiuitorul instituind mai degrabă o facultate a organelor de stat din domeniul securității naționale în a încunoștința persoana supravegheată, ținând seama de cazurile vagi și generale pentru care nu se va dispune informarea, dar și de lipsa unei obligații sancționabile de a realiza informarea ori a unui termen în care aceasta se va realiza.

§2. Contestarea întrebuințării tehnicilor speciale de investigare prevăzute de Legea nr. 51/1991

După cum am văzut, dreptul persoanei de a fi informată cu privire la desfășurarea de activități specifice culegerii de informații, față de aceasta, nu este un drept efectiv, putând fi limitat în mod discreționar de organele de stat din domeniul securității naționale, fapt care afectează în mod determinant și dreptul persoanei de a contesta măsura. După cum am arătat și în cazul informării persoanei care a făcut obiectul supravegherii tehnice, informarea reprezintă doar o condiție pentru a se exercita un control de legalitate și de temeinicie asupra măsurii[1]. Dacă, în cazul Codului de procedură penală, legea instituie posibilitatea contestării măsurilor de supraveghere tehnică numai în camera preliminară și numai de către persoana care are calitatea de inculpat, Legea nr. 51/1991 pare să acorde mai multe posibilități unei persoane care se consideră vătămată prin acțiunile organelor de securitate națională. În realitate, după cum vom vedea, un control judiciar efectiv nu va exista.

Conform art. 22 din Legea nr. 51/1991, „*orice persoană care se consideră vătămată în drepturile sau libertățile sale fundamentale ca urmare a activităților specifice culegerii de informații efectuate de organele de informații sau de cele cu atribuții în domeniul securității naționale se poate adresa, potrivit legii, comisiilor parlamentare sau organelor judiciare, astfel:*

a) comisiilor însărcinate să exercite control parlamentar, potrivit legilor de organizare și funcționare a organelor de informații sau a celor cu atribuții în domeniul securității naționale;

b) instanței de judecată, în condițiile Legii nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date, cu modificările și completările ulterioare;

[1] *V. supra*, Titlul III, Capitolul VI.3.

c) instanțelor judecătorești, pentru repararea daunelor materiale și morale suferite, potrivit legii civile;

d) organelor judiciare, prin formularea de plângeri și căi de atac potrivit Codului de procedură penală;

e) altor comisii sau organe judiciare, potrivit procedurilor reglementate de legi speciale".

În continuare vom analiza fiecare dintre aceste posibilități, pentru a constata limitele și avantajele acestora și dacă ele corespund cu cerințele art. 8 par. 2 Conv.EDO referitor la instituirea de garanții privind protejarea dreptului la viață privată.

Petiționarea comisiilor parlamentare însărcinate cu exercitarea controlului parlamentar al organelor din domeniul securității naționale nu poate constitui un remediu efectiv pentru acțiunile nelegale ale unui serviciu secret, întrucât nu vor putea permite anularea activităților desfășurate[1]. Controlul comisiei parlamentare nu poate să ia forma aceluiași control pe care îl poate exercita un judecător, fiind necesar ca orice control de legalitate să fie realizat de autoritatea judecătorească, ramura îndrituită potrivit Constituției să aibă această atribuție. De altfel, un control din partea unei comisii parlamentare[2] va fi și unul lipsit de eficiență, așa cum vom observa dacă vom analiza Regulamentul de organizare și funcționare a Comisiei comune permanente a Camerei Deputaților și Senatului pentru exercitarea controlului parlamentar asupra activității S.R.I.[3]. Conform art. 8 alin. (1) lit. d) din regulament, comisia comună permanentă „*examinează cazurile în care s-au semnalat încălcări ale legii în activitatea S.R.I. și se pronunță asupra măsurilor ce se impun pentru restabilirea legalității*", astfel că îi este recunoscută o atribuție specifică în sensul Legii nr. 51/1991. Din păcate, nu există nicio procedură parlamentară specifică prin care să se determine cum va avea loc soluționarea petiției și care vor fi măsurile dispuse de comisie pentru repararea prejudiciului și restabilirea legalității, astfel că simpla mențiune ca atribuție nu are niciun efect dacă comisia parlamentară nu va putea face nimic decât, eventual, să constate o încălcare a legii, care nu va servi scopului contestării legalității și temeiniciei activităților specifice. În plus, controlul va fi exercitat asupra activității organelor de stat din domeniul securității naționale, neputând fi supusă controlului încheierea judecătorului desemnat din cadrul Înaltei Curți de Casație și Justiție prin care s-au autorizat activitățile specifice culegerii informații. Ca atare, apreciem că petiționarea comisiilor parlamentare nu poate constitui un remediu eficient pentru o persoană vătămată prin acțiunile desfășurate de organele din domeniul securității naționale.

Formularea unei acțiuni în fața instanței de judecată în condițiile Legii nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date[4] nu este aptă să constituie o garanție efectivă împotriva unui abuz din partea organelor din domeniul securității naționale, întrucât trimiterea din cuprinsul Legii nr. 51/1991 este în contradicție cu dispozițiile legii speciale. Astfel, potrivit art. 2 alin. (7) din

[1] *C. Rotaru*, Tehnici speciale de supraveghere sau cercetare. Supravegherea tehnică – interceptarea convorbirilor și comunicărilor, în Caiete de Drept Penal nr. 1/2011, p. 18.

[2] În prezent funcționează numai două comisii permanente de control ale Parlamentului în domeniul securității naționale ce exercită controlul parlamentar asupra S.R.I., respectiv asupra S.I.E.

[3] Hotărârea nr. 2 din 27 martie 2017 a Birourilor permanente reunite ale Camerei Deputaților și Senatului pentru aprobarea Regulamentului de organizare și funcționare a Comisiei comune permanente a Camerei Deputaților și Senatului pentru exercitarea controlului parlamentar asupra activității Serviciului Român de Informații.

[4] Publicată în M. Of. nr. 790 din 12 decembrie 2001 și abrogată prin art. V alin. (1) al Legii nr. 129/2018.

Legea nr. 677/2001, abrogată, „*prezenta lege nu se aplică prelucrărilor*[1] *și transferului de date cu caracter personal, efectuate în cadrul activităților în domeniul apărării naționale și siguranței naționale, desfășurate în limitele și cu restricțiile stabilite de lege*". Practic, indicarea acestei căi de atac nu are niciun efect, întrucât o prelucrare de către organele din domeniul securității statului este exceptată de la control, dacă se realizează în temeiul dispozițiilor Legii nr. 51/1991. Or, prin raportare la existența unei proceduri legale de autorizare, instanța nu va putea să admită o acțiune decât dacă stabilește, în prealabil, legalitatea activităților desfășurate în baza autorizației emise de judecătorul desemnat din cadrul Înaltei Curți de Casație și Justiție.

O acțiune civilă în obținerea de daune constituie una dintre posibilitățile legale enumerate în cuprinsul art. 22 din Legea nr. 51/1991. Într-adevăr, această posibilitate este una reală, putând fi promovată cu succes o astfel de acțiune în fața unei instanțe civile, însă va presupune dovedirea caracterului ilicit al faptei serviciilor secrete, dar și a daunei. Sub acest aspect, doctrina a identificat jurisprudență de nișă, în care Tribunalul București a admis o astfel de cerere de chemare în judecată, instanța civilă stabilind că interceptarea convorbirilor telefonice ale reclamantului și antrenarea în acest scop a logisticii S.R.I. sunt elementele unei fapte ilicite de interceptare ilegală a convorbirilor telefonice[2]. Situația era una particulară, întrucât s-a demarat un proces penal în paralel, instanța penală neținând cont de nelegalitatea interceptărilor obținute și folosite ca probă în procesul penal (cauza judecându-se sub imperiul reglementării procesuale penale anterioare), apreciindu-se că soluția instanței civile nu constituie o chestiune prealabilă[3]. Astfel, rezultă că printr-o astfel de acțiune nu se va putea obține constatarea nulității actelor de autorizare sau de punere în executare și nici distrugerea rezultatelor activităților specifice culegerii de informații.

Posibilitatea formulării de plângeri și căi de atac potrivit Codului de procedură penală nu este aptă să conducă la constatarea nelegalității procedurii desfășurate, ceea ce constituie esența contestării folosirii unor tehnici speciale de investigare. Deși se vor putea formula plângeri penale împotriva unor persoane particulare, funcționari din cadrul serviciilor de stat din domeniul securității naționale, exercitarea unor căi de atac prevăzute de Codul de procedură penală nu este fezabilă. Analizând dispozițiile Codului de procedură penală, nu se pot exercita căi de atac asupra unor acte decât dacă ele fac parte din procesul penal, or, activitățile specifice culegerii de informații nu constituie acte de urmărire penală. Mai mult, va fi necesară existența unui proces penal față de persoana care a fost supusă măsurii, aceasta neputând sesiza direct instanța penală. Într-o singură situație s-ar putea invoca nelegalitatea autorizării și desfășurării de activități specifice, atunci când însuși actul de sesizare este reclamat ca fiind nelegal, întrucât s-a bazat pe date și informații obținute în mod nelegal de organele din domeniul securității naționale, dar nu credem că legiuitorul a avut în vedere această situație în cuprinsul art. 22 din Legea nr. 51/1991.

În ceea ce privește exercitarea unor căi de atac la *alte comisii sau organe judiciare*, ele nu reprezintă la acest moment o soluție la problema arătată, întrucât nu există asemenea

[1] Conform art. 3 lit. b) din Legea nr. 677/2001, abrogată, unii termeni se definesc astfel: „prelucrarea datelor cu caracter personal – orice operațiune sau set de operațiuni care se efectuează asupra datelor cu caracter personal, prin mijloace automate sau neautomate, cum ar fi colectarea, înregistrarea, organizarea, stocarea, adaptarea ori modificarea, extragerea, consultarea, utilizarea, dezvăluirea către terți prin transmitere, diseminare sau în orice alt mod, alăturarea ori combinarea, blocarea, ștergerea sau distrugerea".

[2] Trib. București, s. a IV-a civ., sent. nr. 709 din 11 mai 2007, pronunțată în dosar nr. 2770/3/2006, *apud V. Trif*, op. cit., p. 231.

[3] *Ibidem*.

reglementări speciale care să prevadă căi de atac, drept urmare mențiunea din cuprinsul Legii nr. 51/1991 rămâne fără obiect.

Credem că aspectele surprinse legate de procedura informării persoanei supravegheate, potrivit art. 145 C.pr.pen., sunt aplicabile și în cazul activităților desfășurate în baza Legii nr. 51/1991, deoarece și aceste tehnici reprezintă tot o formă de restrângere a drepturilor și libertăților fundamentale ale unei persoane, astfel că vor fi supuse aceloraşi condiții. Din jurisprudența Curții Europene a Drepturilor Omului rezultă că atât posibilitatea de a fi informat asupra desfășurării unor tehnici speciale, cât și posibilitatea de a contesta măsura și a obține anularea autorizării ei sau a punerii sale în executare constituie garanții pentru protejarea dreptului la viață privată. Din acest punct de vedere, atât procedura de informare, cât mai ales cea de contestare nu sunt în acord cu art. 8 par. 2 Conv.EDO, întrucât informarea este aproape facultativă și contestarea nu permite persoanei să obțină anularea activităților specifice efectuate și distrugerea rezultatelor obținute.

Într-o cauză, Curtea Europeană a Drepturilor Omului a constatat că dreptul de a fi notificat cu privire la desfășurarea unei supravegheri tehnice față de o persoană este în mod indisolubil legat de dreptul la un recurs judiciar efectiv împotriva măsurii, în cazul în care s-ar considera ca fiind una abuzivă[1]. Nu s-ar concepe posibilitatea de contestare în lipsa unei notificări cu privire la măsura de supraveghere nici dacă persoana nu ar avea dreptul de a contesta *a posteriori* măsura. Mergând mai departe, jurisprudența Curții a recunoscut necesitatea reglementării în dreptul intern a unui recurs efectiv *a posteriori* cu privire la măsurile de supraveghere tehnică, reamintind constatările din cauza *Roman Zakharov c. Rusia* privind condiționarea posibilității de a exercita un recurs efectiv de informare a persoanei supravegheate[2]. Acest recurs efectiv nu trebuie să fie unul în sensul obținerii unor daune, ci trebuie să privească legalitatea măsurii și să deschidă posibilitatea concretă ca persoana supravegheată să obțină anularea măsurilor luate împotriva sa[3].

Astfel cum am arătat în prezenta secțiune, contestarea legalității și temeiniciei autorizării și punerii în executare a activităților specifice culegerii de informații prevăzute de Legea nr. 51/1991 nu are caracterul unui recurs efectiv la acest moment, întrucât nu oferă posibilitatea de a se obține constatarea nelegalității măsurilor, desființarea acestora și distrugerea tuturor rezultatelor acestora. Din acest punct de vedere, situația constatată de Curtea Constituțională privind neconstituționalitatea dispozițiilor art. 145 C.pr.pen. care nu permit contestarea legalității supravegherii tehnice este similară și în cazul art. 22 din Legea nr. 51/1991. Mai mult decât atât, nici măcar dreptul de informare al persoanei supuse activităților specifice nu este suficient de bine reglementat, acesta fiind, în realitate, un drept iluzoriu, în condițiile în care organele de stat în domeniul securității naționale pot evita informarea persoanei prin invocarea unor temeiuri legale generale și lipsite de claritate.

[1] CEDO, cauza *Roman Zakharov c. Rusia*, Hotărârea din 4 decembrie 2015, §234, pe *hudoc.echr.coe.int*
[2] CEDO, cauza *Irfan Güzel c. Turcia*, Hotărârea din 7 mai 2017, §98, pe *hudoc.echr.coe.int*
[3] CEDO, cauza *Xavier Da Silveira c. Franța*, Hotărârea din 21 aprilie 2010, §48, pe *hudoc.echr.coe.int*

Capitolul IV
Concluzii

Asigurarea securității naționale este o obligație pentru orice țară, indiferent de regimul politic al acesteia, tehnicile speciale de investigare fiind dezvoltate mai ales prin activitățile desfășurate de serviciile secrete. Prin cunoașterea, prevenirea și înlăturarea amenințărilor se poate ajunge la menținerea valorilor supreme ale statului, dar și la garantarea existenței în continuare a acestuia.

În domeniul securității naționale, actorii principali nu vor fi organele judiciare, ci organele de stat din domeniul securității naționale ce își realizează activitatea atât pe plan intern, cât și pe plan extern în mod continuu. Toate aceste servicii contribuie într-un mod nevăzut la asigurarea securității naționale, prin activități secrete și metode specifice care nu pot fi divulgate. Totuși, întrucât unele dintre aceste metode vor restrânge drepturile și libertățile fundamentale ale persoanelor vizate, legiuitorul a instituit un control *a priori* prin care se vor autoriza astfel de tehnici de către un organ judiciar independent. Deși această condiție este îndeplinită, supravegherea și controlul nu vor fi realizate de un astfel de organ și nici măcar de către procuror; odată obținută autorizarea, organele din domeniul securității naționale nefiind controlate într-un mod efectiv. Îngrijorătoare este și situația reglementării unor termene deosebit de lungi pentru care se pot autoriza tehnici speciale de investigare, ceea ce le face cu atât mai intruzive. Mai mult, în procesul de autorizare nu se poate cerceta temeinicia informațiilor care au condus la formularea unor propuneri de autorizare a tehnicilor speciale de investigare, nefiind indicat niciun standard probator care trebuie respectat. Această situație afectează grav și posibilitatea de a cerceta complet proporționalitatea și subsidiaritatea măsurii, Legea nr. 51/1991 prevăzând condiții nepermis de largi în comparație cu dispozițiile Codului de procedură penală.

Valoarea probantă a rezultatelor activităților specifice culegerii de informații va fi una redusă, acestea putând fi folosite numai pentru a sta la baza procesului-verbal de sesizare a organelor de urmărire penală prevăzut de art. 61 alin. (5) C.pr.pen. Sub nicio formă activitățile de culegere de informații nu vor putea fi folosite ca procedee probatorii ori datele și informațiile care rezultă din acestea să fie folosite ca probe. Ținând seama de configurația prezentă a procesului penal, activitățile specifice se desfășoară în afara procesului penal și nu pot fi introduse în acesta nici prin interpretări ale dispozițiilor Codului de procedură penală, precum s-a încercat în cazul înregistrărilor pentru care nu este necesară autorizarea [art. 139 alin. (3) C.pr.pen.]. Organele din domeniul securității statului nu se vor putea substitui niciodată organelor de urmărire penală și activitatea lor în cadrul procesului penal va fi strict cea limitată de legea procesuală penală.

Contestarea legalității și temeiniciei tehnicilor speciale de investigare desfășurate împotriva unei persoane în temeiul Legii nr. 51/1991 nu poate fi socotită ca fiind o instituție reglementată într-un mod adecvat, întrucât persoanei supravegheate nu i se oferă un remediu efectiv împotriva intruziunii aduse vieții sale private. Persoana supravegheată nu se va putea adresa unei instanțe pentru a cere anularea actelor desfășurate împotriva sa și distrugerea rezultatelor activităților specifice ce au lezat-o, putând, cel mult, obține despăgubiri din partea unei instanțe civile sau tragerea la răspundere penală a unor funcționari responsabili, ceea ce

este insuficient. De altfel, persoana supravegheată are un drept iluzoriu de a fi informată cu privire la activitățile desfășurate împotriva sa, legea prevăzând cazuri generale și neclare în care se poate omite în mod absolut și fără un termen determinat încunoștințarea sa. În același timp, chiar dacă ar fi încunoștințată asupra faptului că a făcut obiectul unei supravegheri din partea serviciilor secrete, aceasta nu va avea dreptul de a-i fi prezentate activitățile specifice desfășurate ori de a cunoaște rezultatele lor, dreptul de informare fiind unul formal.

Bibliografie selectivă

I. Tratate, cursuri și monografii

Alămoreanu, Sorin, Elemente de criminalistică, Ed. Alma Mater, Sibiu, 2000;

Ashworth, Andrew, Positive obligations in Criminal Law, Hart Publishing, Portland, 2013;

Ashworth, Andrew; Redmayne, Mike, The Criminal Process, Fourth Edition, Oxford University Press, Oxford, 2014;

Ashworth, Andrew; Zedner, Lucia, Preventive Justice, Oxford University Press, Oxford, 2014;

Ball, Kristie; Haggerty, Kevin D.; Lyon, David, Routledge Handbook of Surveillance Studies, Ed. Routledge, Abingdon, Oxfordshire, 2012;

Barbara, John J. (coord.), Handbook of Digital and Multimedia Forensic Evidence, Humana Press, Totowa, New Jersey, 2008;

Barbu, Alina; Tudor, Georgiana; Șinc, Alexandra Mihaela, Codul de procedură penală adnotat cu jurisprudență națională și europeană, Ed. Hamangiu, București, 2016;

Basarab, Matei, Drept penal. Partea generală, vol. I, ed. a IV-a, revăzută și adăugită, Ed. Lumina Lex, București, 2002;

Bogdan, Sergiu; Șerban, Doris Alina; Zlati, George, Noul Cod penal. Partea specială. Analize, explicații, comentarii. Perspectiva clujeană, Ed. Universul Juridic, București, 2014;

Boister, Neil, An Introduction to Transnational Criminal Law, First Edition, Oxford University Press, Oxford, 2012;

Boțic, Sebastian, Regula exclusiunii. Excluderea probelor obținute nelegal în procesul penal, Ed. Universul Juridic, București, 2016;

Brown, Darryl K.; Turner, Jenia I.; Weisser, Bettina (coord.), The Oxford Handbook of Criminal Process, Oxford University Press, Oxford, 2019;

Choo, Andrew L-T, Evidence, Fifth Edition, Oxford University Press, Oxford, 2018;

Ciopec, Flaviu, Drept procesual penal. Partea generală, Ed. C.H. Beck, București, 2017;

Cohen, Elliot D., Mass Surveillance and State Control: the total information awareness project, Ed. Palgrave Macmillan, New York, 2010;

Crișu, Anastasiu, Drept procesual penal. Partea generală (conform noului Cod de procedură penală), ed. a 3-a, revizuită și actualizată, Ed. Hamangiu, București, 2018;

Damaška, Mirjan, Evaluation of Evidence. Pre-modern and Modern Approaches, Cambridge University Press, Cambridge, 2019;

Del Carmen, Rolando V., Criminal Procedure. Law and Practice, 8th Edition, Ed. Wadsworth Cengage Learning, Belmont, 2010;

De Lucas Martín, Ignacio Miguel; Ștefan, Cristian-Eduard, Livrările supravegheate transnaționale în contextul investigării traficului de droguri, Ed. Magic Print, București, 2016;

Dongoroz, Vintilă; Bulai, Constantin; Kahane, Siegfried; Iliescu, Nicoleta; Antoniu, George; Stănoiu, Rodica, Explicații teoretice ale Codului de procedură penală român. Partea generală, vol. I, Ed. Academiei Republicii Socialiste România, București, 1975;

Donohue, Laura K., The Future of Foreign Intelligence. Privacy and Surveillance in a Digital Age, Oxford University Press, Oxford, 2016;

Finn, Johnathan, Capturing the Criminal Image: From Mug Shot to Surveillance Society, University of Minnesota Press, Minneapolis, 2009;

Fitzgerald, Dennis G., Informants, Cooperating Witnesses, and Undercover Investigations. A Practical Guide to Law, Policy and Procedure, Second Edition, CRC Press, Boca Raton, Florida, 2015;

Fuchs, Christian; Boersma, Kees; Albrechtslund, Anders; Sandoval, Marisol, Internet and Surveillance, The Challenges of Web 2.0 and Social Media, Ed. Routledge, New York, 2012;

Goold, Benjamin J.; Lazarus, Liora (coord.), Security and Human Rights, Hart Publishing, Oxford, 2007;

Goold, Benjamin J.; Lazarus, Liora; Swiney, Gabriel, Public protection, Proportionality and the Search for Balance, în Ministry of Justice Research Series 10/07, London, 2007;

Grădinaru, Daniel, Investigarea infracțiunilor contra intereselor financiare ale U.E., Ed. C.H. Beck, București, 2016;

Grădinaru, Sandra, Supravegherea tehnică în Noul Cod de procedură penală, Ed. C.H. Beck, București, 2014;

Goldman, Zachary K.; Rascoff, Samuel J., Global Intelligence Oversight, Governing Security in the Twenty-First Century, Oxford University Press, New York, 2016;

Hall, Daniel E., Criminal Law and Procedure, Fifth Edition, Ed. Delmar Cengage, New York, 2009;

Harfield, Clive; Harfield, Karen, Covert Investigation, Fifth Edition, Oxford University Press, Oxford, 2018;

Harris, David J.; O'Boyle, Michael; Warbrick, Carla, Law of the European Convention on Human Rights, Ed. Butterworths, London, 1995;

Hirsch Ballin, Marianne F.H., Anticipative Criminal Investigation: Theory and Counterterrorism Practice in the Netherlands and the United States, Ed. Springer, Haga, 2012;

Hsieh, Kuo-Hsing, The Exclusionary Rule of Evidence. Comparative Analysis and Proposals for Reform, Ed. Ashgate, Farnham, 2014;

Ionescu, Lucian; Sandu, Dumitru, Identificarea criminalistică, ed. a 2-a, Ed. C.H. Beck, București, 2011;

Jamieson, Allan; Moenssens, Andre (coord.), Wiley Encyclopedia of Forensic Science, vol. 5, Ed. Wiley-Blackwell, Chichester, 2009;

Jackson, John D.; Langer, Maximo; Tillers, Peter, Crime, Procedure and Evidence in a Comparative and International Context Essays in Honour of Professor Mirjan Damaska, Ed. Hart Publishing, Portland, Oregon, 2008;

Jeffreys-Jones, Rhodri, We Know all About You. The Story of Surveillance in Britain and America, Oxford University Press, Oxford, 2017;

Jenkins, Peter, Advanced Surveillance: The Complete Manual of Surveillance Training, Intel Publications, Oxenhope, 2003;

Kerr, Ian; Steeves, Valerie; Lucock, Carole, Lessons from the Identity Trail. Anonymity, Privacy and Identity in a Networked Society, Oxford University Press, New York, 2009;

Kirchner, Richard Jr., Surveillance and Threat Detection: Prevention versus Mitigation, Ed. Elsevier, Woburn, 2014;

Kostoris Roberto E. (coord.), Handbook of European Criminal Procedure, Ed. Springer, Cham, 2018;

Krotoszynski, Ronald J. Jr., Privacy Revisited. A Global Perspective on the Right to Be Left Alone, Oxford University Press, Oxford, 2016;

Leslie, Daniel Adeoye, Legal Principles for Combatting Cyberlaundering, Ed. Springer, Cham, 2014;

Livescu, Monica (coord.), Avocatura în România. 150 de ani în linia întâi a luptei pentru Drept, Ed. Hamangiu, București, 2015;

Lombardo Giuseppe (coord.); Nardo, Massimo; Roversi, Valeria; Craiu, Nicolae; Moldoveanu, Cornel; Banu, Laura; Ricca, Piero, Manual de instruire privind combaterea spălării banilor și a finanțării terorismului, Imprimeria Națională, București, 2009;

Maras, Marie-Helen, Cybercriminology, Oxford University Press, New York, 2017;

Mareș, Mihai, Nulitățile în procesul penal, Ed. Hamangiu, București, 2019;

Marx, Gary T., Windows into the Soul, Surveillance and Society in an Age of High Technology, Ed. University of Chicago Press, Chicago, 2016;

Mateuț, Gheorghiță, Tratat de procedură penală. Partea generală, vol. I, Ed. C.H. Beck, București, 2007;

Mateuț, Gheorghiță, Tratat de procedură penală. Partea generală, vol. II, Ed. C.H. Beck, București, 2012;

Mateuț, Gheorghiță, Procedură penală. Partea generală, Ed. Universul Juridic, București, 2019;

Mâță, Dan Constantin, Securitatea națională. Concept. Reglementare. Mijloace de ocrotire, Ed. Hamangiu, București, 2016;

McKay, Simon, Covert Policing Law and Practice, Second Edition, Oxford University Press, Oxford, 2015;

McKay, Simon, The Investigatory Powers Act 2016, Oxford University Press, Oxford, 2017;

Meiklejohn, Alexander, Free Speech and Its Relation to Self-Government, Harper Brothers Publishers, New York, 1948;

Moisă, Cristina, Probele în procesul penal, Ed. Hamangiu, București, 2017;

Neagu, Ion, Tratat de procedură penală. Partea generală, ed. a III-a, revăzută și adăugită, Ed. Universul Juridic, București, 2013;

Nouwt, Sjaak; de Vries, Berend R.; Prins, Corien, Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy, Ed. TMC Asser Press, Haga, 2005;

Olaru, Codruț, Mijloace specifice de investigare a infracțiunilor de criminalitate organizată, Ed. Hamangiu, București, 2014;

Ormerod, David; Perry, David; Murphy, Peter (coord.), Blackstone's Criminal Practice 2019, Oxford University Press, Oxford, 2018;

Panc, Daniela, Securitatea cibernetică la nivel național și internațional. Instrumente normative și instituționale, Ed. Hamangiu, București, 2017;

Pașca, Ioana-Celina, Criminalitatea organizată în perspectiva legislațiilor europene, Ed. Universul Juridic, București, 2015;

Petersen, Julie K., Handbook of Surveillance Technologies, Third Edition, Ed. CRC Press, Boca Raton, Florida, 2012;

Peterson, Gilbert; Sujeet Shenoi (coord.), Advances in Digital Forensics X. 10th IFIP WG 11.9 International Conference, Vienna, Austria, January 8-10, 2014, Revised Selected Papers, Ed. Springer, New York, 2014;

Petre, Adrian; Grigoraș, Cătălin, Înregistrările audio și audio-video, mijloace de probă în procesul penal, Ed. C.H. Beck, București, 2008;

Pop, Traian, Drept procesual penal. Partea generală, Vol. III, Tipografia Națională Cluj S.A., reeditare anastatică, Ed. Universul Juridic, București, 2019;

Pop, Traian, Drept penal comparat. Partea generală, vol. II, Institutul de Arte Grafice „Ardealul", Cluj, 1923;

Pușcașu, Voicu-Ionel; Ghigheci, Cristinel, Codul de procedură penală adnotat, vol. 1 și 2, Ed. Universul Juridic, București, 2019;

Ruggeri, Stefano (coord.), Transnational Inquiries and the Protection of Fundamental Rights in Criminal Proceedings. A study in Memory of Vittorio Grevi and Giovanni Tranchina, Ed. Springer, Berlin, 2013;

Schellekens, M.H.M., Electronic Signatures. Authentication Technology from a Legal Perspective, Ed. TMC Asser Press, Haga, 2004;

Shalhoub-Kevorkian, Nadera, Security Theology, Surveillance and the Politics of Fear, Cambridge University Press, Cambridge, 2015;

Shavers, Brett, Placing the Suspect Behind the Keyboard. Using Digital Forensics and Investigative Techniques to Identify Cybercrime Suspects, Ed. Elsevier, Waltham, Massachusetts, 2013;

Shi, Yun-Qing; Kim, Hyoung Joong; Pérez-González, Fernando; Yang, Ching-Nun (coord.), Digital Forensics and Watermarking. 13th International Workshop, IWDW 2014, Taipei, Taiwan, October 1-4, 2014, Revised Selected Papers, Ed. Springer, New York, 2014;

Shimonski, Robert; Zenir, John; Bishop, Allison, Cyber Reconnaissance, Surveillance and Defense, Ed. Elsevier, Waltham, 2015;

Shuy, Roger W., Deceptive ambiguity by Police and Prosecutors, Oxford University Press, New York, 2017;

Spencer, John R., Hearsay Evidence in Criminal Proceedings, Ed. Hart Publishing, Portland, Oregon, 2008;

Stancu, Emilian, Tratat de Criminalistică, ed. a V-a, revăzută și adăugită, Ed. Universul Juridic, București, 2010;

Staniforth, Andrew, Blackstone's Handbook of Cyber Crime Investigation, Oxford University Press, Oxford, 2017;

Streteanu, Florin, Tratat de drept penal. Partea generală, vol. I, Ed. C.H. Beck, București, 2008;

Șandru, Simona, Protecția datelor personale și viața privată, Ed. Hamangiu, București, 2016;

Tanoviceanu, Ion, Curs de procedură penală română, Ed. Atelierele Grafice SOCEC & Co., București, 1913;

Theodoru, Grigore Gr., Tratat de Drept procesual penal, ed. a 3-a, Ed. Hamangiu, București, 2013;

Trif, Valentin, Metode de supraveghere tehnică în cadrul procesului penal, Ed. C.H. Beck, București, 2019;

Tudoran, Mihai Viorel, Teoria și practica interceptărilor și înregistrărilor audio sau video judiciare, Ed. Universul Juridic, București, 2012;

Udroiu, Mihail, Dicționar de drept penal și de procedură penală, Ed. C.H. Beck, București, 2009;

Udroiu, Mihail, Procedură penală. Partea generală. Sinteze și grile, ed. a 3-a, Ed. C.H. Beck, București 2016;

Udroiu, Mihail, Procedură penală. Partea generală, ed. a 6-a, vol. I și II, Ed. C.H. Beck, București, 2019;

Udroiu, Mihail (coord.), Andone-Bontaș, Amalia; Bodoroncea, Georgina; Bulancea, Marius Bogdan; Constantinescu, Victor; Grădinaru, Daniel; Jderu, Claudia; Kuglay, Irina; Meceanu, Constantin; Postelnicu, Lucreția; Tocan, Isabelle; Trandafir, Andra-Roxana, Codul de procedură penală. Comentariu pe articole, ed. 1, Ed. C.H. Beck, București, 2015;

Udroiu, Mihail (coord.); Andone-Bontaș, Amalia; Bodoroncea, Georgina; Bogdan, Sergiu; Bulancea, Marius Bogdan; Chertes, Dan-Sebastian; Chiș, Ioan-Paul; Constantinescu, Victor Horia Dimitrie; Grădinaru, Daniel; Jderu, Claudia; Kuglay, Irina; Meceanu, Constantin-Cristinel; Nedelcu, Iuliana; Postelnicu (Cojocaru), Lucreția Albertina; Răduleț u, Sebastian; Șinc, Alexandra-Mihaela; Slăvoiu, Radu; Tocan, Isabelle; Trandafir, Andra-Roxana; Vasiescu, Mihaela; Zlati, George, Codul de procedură penală. Comentariu pe articole, ed. a 2-a, Ed. C.H. Beck, București, 2017;

Udroiu, Mihail; Predescu, Ovidiu, Protecția europeană a drepturilor omului și procesul penal român, Ed. C.H. Beck, București, 2008;

Udroiu, Mihail; Slăvoiu, Radu; Predescu, Ovidiu, Tehnici speciale de investigare în justiția penală, Ed. C.H. Beck, București, 2009;

Volonciu, Nicolae; Uzlău, Andreea Simona (coord.); Moroșanu, Raluca; Văduva, Victor; Atasiei, Daniel; Ghigheci, Cristinel; Voicu, Corina; Tudor, Georgiana; Gheorghe, Teodor-Viorel; Chiriță, Cătălin Mihai, Noul Cod de procedură penală comentat, Ed. Hamangiu, București, 2014;

Wells, Colin, Abuse of Process, Third Edition, Oxford University Press, Oxford, 2017;

Whitman, James Q., The Origins of Reasonable Doubt. Theological Roots of the Criminal Trial, Yale University Press, Orwigsburg, Pennsylvania, 2008;

Whitman, Michael E.; Mattord, Herbert J., Principles of Information Security, Fifth Edition, Ed. Cengage Learning, Boston, 2016;

Yan, Wei Qi, Introduction to Intelligent Surveillance. Surveillance Data Capture, Transmission, and Analytics, Third Edition, Ed. Springer, Cham, 2019;

Zaharia, George-Cristinel, Traficul de persoane, Ed. C.H. Beck, București, 2012;

Zarafiu, Andrei, Procedură penală. Partea generală. Partea specială, ed. a II-a, Ed. C.H. Beck, București, 2015.

II. Articole, studii de specialitate și prelegeri

Arnett, Chaz, Virtual Shackles: Electronic Surveillance and the Adultification of Juvenile Courts, în The Journal of Criminal Law & Criminology, vol. 108, no. 3/2018;

Băcăuanu, Andrei, Technical Surveillance in the European Union Judicial System. Aspects of Comparative Law, în Acta Universitatis Danubius, vol. 10, no. 1/2018;

Bălan, Iulian, Dreptul la respectarea vieții private și supravegherea video, audio sau prin fotografiere. Partea I, în Pandectele Române nr. 7/2015;

Bălan, Iulian, Dreptul la respectarea vieții private și supravegherea video, audio sau prin fotografiere. Partea a II-a, în Pandectele Române nr. 8/2015;

Bălan, Iulian, Efectuarea supravegherii tehnice. Proba neconstituțională. Studiu de jurisprudență, în Pandectele Române nr. 4/2019;

Beck, James; Magana, Christopher; Imwinkelried, Edward J., The Use of Global Position System (GPS) and Cell Tower Evidence to Establish A Person's Location Part-I, în Criminal Law Bulletin, vol. 49, no. 1/2013;

Beittel, June S., Mexico: Organized Crime and Drug Trafficking Organizations, în Congressional Research Service Report, 2019;

Beyer, Stefanie; Mulazzani, Martin; Schrittwieser, Sebastian; Huber, Markus; Weippl, Edgar, în Gilbert Peterson, Sujeet Shenoi (coord.), Advances in Digital Forensics X. 10th IFIP WG 11.9 International Conference, Vienna, Austria, January 8-10, 2014, Revised Selected Papers, Ed. Springer, New York, 2014;

Black, Matt; Smith, Russell G., Electronic Monitoring in the Criminal Justice System, în Trends an Issues in Crime and Criminal Justice no. 5/2003;

Bloom, Robert M.; Clark, Wlliam T., Small Cells, Big Problems: The Increasing Precision of Cell Site Location Information and The Need For Fourth Amendment Protections, în Journal of Criminal Law & Criminology, vol. 106, no. 2/2016;

Brady, Natalia, Evidence, special investigative techniques and the right to a fair hearing, în revista ERA Forum, vol. 15, no. 1/2014;

Brown, Cameron S.D., Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice, în International Journal of Cyber Criminology (IJCC), vol. 9, no. 1/2015;

Buftea, Gavrilă, Măsuri eficiente împotriva Criminalității Organizate Transnaționale, în Revista de investigare a criminalității, vol. 8, nr. 2/2015;

Ciuncan, Dorin, Supravegherea tehnică (I), în Revista Universul Juridic nr. 1/2015;

Claypoole, Ted; Balough, Richard, Location Tracking and US Law: How Technology alters Expectations, în Journal of Internet Law no. 11/2012;

Dabu, Valerică; Radu, Loredana, Legalitatea interceptărilor în faza actelor premergătoare, în Revista de Drept Penal nr. 1/2012;

Do, Quang; Martini, Ben; Looi, Jonathan; Wang, Yu; Choo, Kim-Kwang, în Gilbert Peterson, Sujeet Shenoi (coord.), Advances in Digital Forensics X. 10th IFIP WG 11.9 International Conference, Vienna, Austria, January 8-10, 2014, Revised Selected Papers, Ed. Springer, New York, 2014;

Dworzecki, Jacek; Kočan Štefan, Fighting Against Organized Crime With the Use of Agent Provocateur. The Experience of Slovak Republic. Outline of Issues, în Internal Security, vol. 10, no. 2/2018;

Egawhary, Elena M., The Surveillance Dimensions of the Use of Social Media by UK Police Forces, în Surveillance & Society, vol. 17, no. 1/2019;

Etsebeth, Verine, Monitoring and Surveillance in the Workplace: Lessons Learnt? Investigating the International Legal Position, în Journal of Digital Forensics, Security and Law, vol. 2, no. 2/2007;

Fábián, Gyula, Accesul la datele stocate de furnizorii serviciilor de comunicații electronice și influența jurisprudenței Curții de Justiție a Uniunii Europene adoptată în cazul „Digital Rights", în aplicarea dreptului național în acest domeniu, în Dreptul nr. 5/2016;

Fazey, Cindy, International Policy on Illicit Drug Trafficking: The formal and Informal Mechanisms, în Journal of Drug Issues, vol. 37, no. 4/2007;

Fehr, Colton, The Constitutionality of Using Production Orders to Obtain Stored Communications Content, în Canadian Criminal Law Review (2018), 23:2;

Fejzullah, Hasani, Covert and Technical Surveillance Measures and Investigation, în Acta Universitatis Danubius. Juridica, vol. 15, no. 3/2019;

Ferguson, Andrew Guthrie, Big Data and Predictive Reasonable Suspicion, în University of Pennsylvania Law Review, vol. 163, no. 2/2015, 163 U. Pa. L. Rev. 327 (2015);

Ferguson, Andrew Guthrie, Predictive Policing and Reasonable Suspicion, în Emory Law Journal, 2 Emory L. J. 259 (2012);

Furini, Marco; Tamanini, Valentina, Location privacy and public metadata in social media platforms: attitudes, behaviors and opinions, în Multimedia Tools and Applications, vol. 74, no. 21/november 2015;

Galetta, Antonio; De Hert, Paul, Complementing the Surveillance Law Principles of the ECtHR with its Environmental Law Principles: An Integrated Technology Approach to a Human Rights Framework for Surveillance, în Utrecht Law Review, 10 Utrecht L. Rev. 55 (2014);

Ghigheci, Cristinel; Neagoe, Vlad, Supravegherea tehnică în lumina noilor soluții ale Curții Constituționale – interpretarea și aplicarea deciziilor în materie ale instanței constituționale, în Caiete de Drept Penal nr. 3/2019;

Giurea, Laurențiu, Metodele și tehnicile speciale de investigare a traficului de droguri, în Pro Patria Lex, vol. 13, no. 2/2014;

Grădinaru, Daniel, Punerea în executare a mandatelor de supraveghere tehnică după Decizia nr. 51/2016 a Curții Constituționale a României, în Curierul Judiciar nr. 6/2017;

Grădinaru, Sandra, Cazurile și condițiile de emitere a mandatului de supraveghere tehnică, în Curierul Judiciar nr. 1/2015;

Heymann, Philip B., An Essay on Domestic Surveillance, în Journal of National Security Law & Policy, vol. 8:421, 2015;

Iancu, Elena-Ana; Șinca, George Marius; Șinca, Tatiana, Considerații referitoare la folosirea interpreților și traducătorilor în activitățile de supraveghere tehnică, în Revista de Criminologie, Criminalistică și Penologie nr. 2/2018;

Iliescu, Ligia, Noile reglementări legislative privind livrările supravegheate în unele state membre din Uniunea Europeană, în Studii de Securitate Publică, vol. 3, nr. 2/2014;

Ivan, Gheorghe; Ioniță, Vasile, Una din problematicile punerii în executare a mandatelor de supraveghere tehnică, în Revista Pro Lege nr. 1/2017;

Kerr, Orin S., Digital Evidence and the New Criminal Procedure, în Columbia Law Review, vol. 105, no. 1/2005;

Kovesi, Laura Codruța, Punerea sub supraveghere a conturilor bancare și a conturilor asimilate conturilor bancare, în Dreptul nr. 8/2003;

Laudan, Larry, Is Reasonable doubt Reasonable?, în Legal Theory, vol. 9, no. 4/2003;

Lee, Gregory D., Drug Informants: Motives, Methods, and Management, în FBI Law Enforcement Bulletin, 1 septembrie 1993;

Leo, Lionel; Chen, Siyuan, Reasonable Suspicion or Real Likelihood: A Question of Semantics, în Singapore Journal of Legal Studies, 2008, Sing. J. Legal Stud. 446 (2008);

Lerner, Craig S., Reasonable Suspicion and Mere Hunches, în Vanderbilt Law Review, 59 Vand. L. Rev. 405 (2006);

Liao, Ming, The Process of Legalizing Special Investigative Techniques in China, în Frontiers of Law in China, vol. 10, no. 3/2015;

Lionte, Andreea Crenguța, Aspecte generale cu privire la activitatea de interceptare și înregistrare a comunicațiilor și comunicării în cadrul procesului penal, în Revista de Investigare a Criminalității nr. 1/2016;

Lupașcu, Dan; Mareș, Mihai, Considerații referitoare la protecția martorilor și procesul echitabil, în Dreptul nr. 11/2017;

Manzhai, Oleksandr V., Procedure Analysis of the Special Investigative Actions through Cyberspace in Countries of Common and Continental Law, în Internal Security, vol. 4, no. 1/2012;

Mateuț, Gheorghiță, Unele considerații privind garantarea secretului profesional al avocatului în lumina noului Cod de procedură penală, publicat în vol. Avocatura în România. 150 de ani în linia întâi a luptei pentru Drept (coord. M. Livescu), Ed. Hamangiu, București, 2015;

Mateuț, Gheorghiță, Observații critice privind noua reglementare a supravegherii tehnice într-o prezentare comparativă, în Caiete de Drept Penal nr. 3/2015;

Matyshova, Aigerim M., Covert Investigative Activities in Kazakhstan: Purpose, Occurring Conflicts and Ways of their Overcoming, în Journal of Advanced Research in Law and Economics, vol. VII, no. 3/2016;

Mâță, Dan Constantin, Considerații generale în legătură cu rolul Justiției în Mecanismul de Apărare a Securității Naționale, în Dreptul nr. 9/2015;

McBrearty, Simon; McKelvey, Nigel; Curran, Kevin, Legal, Ethical and Social Issues in the case of an Intrusive Remote Monitoring Software, în International Journal of Information and Network Security (IJINS), vol. 1, no. 4/2012;

Micu, Bogdan, Aspecte practice specifice obținerii datelor privind tranzacțiile financiare ale unei persoane, în Dreptul nr. 1/2018;

Militaru, George Constantin, Considerații asupra mandatului de supraveghere tehnică privind obținerea datelor referitoare la tranzacțiile financiare ale unei persoane și analiza comparativă cu instituția obținerii de date privind situația financiară a unei persoane, în Dreptul nr. 9/2016;

Moise, Adrian Cristian, Analysis of Offences Concerning Drug Trafficking in Romanian Legislation, în Law Review (Universul Juridic), vol. VIII, no. 2/2018;

Moon, Millard E., How America Lost its Secrets: Edward Snowden, The Man and The Theft, în Journal of Strategic Security, vol. 10, no. 1/2017;

Mutchler, P.; Mayer, J., MetaPhone: The Sensitivity of Telephone Metadata, publicat pe Web Policy, 12 Martie 2014, disponibil la adresa *http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/*;

Neagu, Ion; Damaschin, Mircea, Audio and video interceptions and recordings in criminal law in Romania, în Lex et Scientia International Journal (LESIJ), vol. 1, no. XVI/2009;

Negruț, Gina, Neconstituționalitatea dispozițiilor privind reținerea datelor generate sau prelucrate de furnizorii de rețele publice de comunicații electronice și de furnizorii de servicii de comunicații electronice destinate publicului, în Pro Patria Lex, vol. 15, nr. 2/2015;

O'Mara, Deborah L., How much covert is too much?, în Security, vol. 71, no. 12/2000;

Oostveen, Anne-Marie; Vasalou, Asimina; van den Besselaar, Peter; Brown, Ian, Child Location Tracking in the US and the UK: Same Technology, Different Social Implications, în Surveillance & Society, vol. 12, no. 4/2014;

Ormerod, David, ECHR and the exclusion of evidence: trial remedies for Article 8 breaches, în Criminal Law Review no. 61/2003, London;

Paraschiv, Dan-Ștefan, Pericolul creșterii traficului și consumului ilicit de stupefiante, în Acta Universitatis George Bacovia, vol. 5, nr. 1/2016;

Pașca, Viorel, Principiul egalității armelor în procesul penal român – o realitate sau o ficțiune?, în Revista Universul Juridic nr. 8/2016;

Perera, David, Cellphone network upgrades make location tracking almost as precise as GPS, în FierceGovernmentIT, 28 aprilie 2013, pe *www.fiercegovernmentit.com*;

Perras, Michael; Nebel, Silke, Satellite Telemetry and its Impact on the Study of Animal Migration, în Nature Education Knowledge no. 3(12):4, 2012;

Petroiu, Marius, Epopeea accesului organelor de stat la datele de trafic, de identificare a echipamentelor și de localizare, în Pandectele Române nr. 3/2016;

Pintea, Răzvan Mihăiță, Unele aspecte controversate privind legalitatea probelor obținute prin supravegherea tehnică, în Revista Themis nr. 2/2018;

Polcak, Libor; Hranick, Radek; Martinek, Tomas, On Identities in Modern Networks, în Journal of Digital Forensics, Security and Law, vol. 9, no. 2/2014;

Popa, Rodica Aida, Aspecte teoretice și practice referitoare la metodele speciale de supraveghere sau cercetare prevăzute în Codul de procedură penală, în Dreptul nr. 6/2015;

Radu, Răzvan Horațiu, Reflecții privind efectele Deciziei nr. 51/2016 a Curții Constituționale a României, în Revista Universul Juridic nr. 3/2016;

Richards, Neil M., The Dangers of Surveillance, în Harvard Law Review, vol. 126, 1934, par. 1959 (2013);

Rotaru, Cristina, Tehnici speciale de supraveghere sau cercetare. Supravegherea tehnică – interceptarea convorbirilor și comunicărilor, în Caiete de Drept Penal nr. 1/2011;

Ruiu, Marin; Dariciuc, Carmen, Metode și tehnici speciale de investigare a infracțiunilor de trafic de droguri, în Forum Criminalistic, vol. IX, nr. 1/2016;

Saini, Radhika; Wadhwa, Mohit; Khari, Manju, Vulnerabilities and Attacks in Global System for Mobile Communication (GSM), în International Journal of Advanced Research in Computer Science, vol. 2, no. 3/may-june 2011;

Shah, Bhavin, Wireless Location for Blueforce Tracking, în Law & Order no. 2/2014;

Simon, Matthew; Slay, Jill, Investigating Modern Communication Technologies: The Effect of Internet-based Communication Technologies on the Investigation Process, în Journal of Digital Forensics, Security and Law, vol. 6, no. 4/2011;

Skolnik, Terry, The Suspicious Distinction between Reasonable Suspicion and Reasonable Grounds to Believe, în Ottawa Law Review, 47 Ottawa L. Rev. 223 (2016);

Slăvoiu, Radu, Verificarea legalității procedeelor probatorii în camera preliminară, în Dreptul nr. 1/2018;

Snider, Brett, Can police read or search through your mail?, publicat la data de 16 aprilie 2014, pe *https://blogs.findlaw.com/blotter/2014/04/can-police-read-or-search-through-your-mail.html*;

Sorell, Tom, Preventive Policing, Surveillance and European Counter-Terrorism, în Criminal Justice Ethics, vol. 30, no. 1/2011;

Steele, Campbell C., Attorneys Beware, Metadata's impact on Privilege, Work, Product, and the Ethical Rules, în The University of Memphis Law Review, vol. 25, no. 4/2005;

Suian, Mihai, Considerații privind accesul la un sistem informatic ca metodă de supraveghere tehnică, în Caiete de Drept Penal nr. 3/2016;

Suian, Mihai, Considerații privind accesul la un sistem informatic ca metodă de supraveghere tehnică, în Caiete de Drept Penal nr. 4/2016;

Suian, Mihai, Unele aspecte privind folosirea investigatorilor sub acoperire și a colaboratorilor, în Revista Penalmente Relevant nr. 2/2016;

Suian, Mihai, Obținerea probelor în procesul penal prin intermediul investigatorilor sub acoperire și a colaboratorilor, în Revista de Criminologie, Criminalistică și Penologie nr. 4/2016;

Suian, Mihai, Unele probleme privind folosirea probelor digitale în procesul penal, în Revista de Criminologie, Criminalistică și Penologie nr. 3/2017;

Suian, Mihai, Unele aspecte privind reținerea, predarea și percheziționarea trimiterilor poștale, în Revista Penalmente Relevant nr. 2/2018;

Suleiman, Garba; Umar, Abdulraheem Ojo; Adekunle, Salako Emmanuel, Development and Implementation of Vehicle Movement Notification and Location using GSM, GPS and Web based Information System, în International Journal Computer Network and Information Security no. 8/2018;

Șandru, Simona, Scurte considerații privind monitorizarea datelor de trafic și drepturile de proprietate intelectuală. Abordări europene, în Revista Română de Drept European nr. 4/2013;

Șerb, Stancu; Ungureanu, Petre, Considerations on the use of technical surveillance in criminal proceedings, în Acta Universitatis George Bacovia, vol. 5, no. 2/2016;

Ștefănescu, Ion Traian; Dumitru, Raluca, Considerații referitoare la protecția datelor personale ale salariaților în cadrul raporturilor de muncă, în Dreptul nr. 9/2015;

Taslitz, Andrew E., Cybersurveillance without restraint? The meaning and social value of the probable cause and reasonable suspicion standards in governmental access to third-party electronic records, în The Journal of Criminal Law & Criminology, vol. 103, no. 3/2013;

Thompson, Kimberly R., Cell Phone Snooping: Why Electronic Eavesdropping Goes Unpunished, în The American Criminal Law Review, vol. 35, no. 1, fall 1997;

Tofan, Dana, Câteva reflecții cu privire la Ordonanța de urgență a Guvernului nr. 6/2016 privind unele măsuri pentru punerea în executare a mandatelor de supraveghere tehnică dispuse în procesul penal, în Revista Curierul Judiciar nr. 4/2016;

Trandafir, Andra-Roxana; Marin, Gabriel, Obținerea de informații ori înscrisuri de la instituțiile de credit în cursul urmăririi penale, publicat pe *www.juridice.ro*;

Trandafir, Andra-Roxana, Obținerea de informații și înscrisuri de la instituțiile de credit în cursul urmăririi penale, prelegere susținută în cadrul Conferinței privind aspecte de practică neunitară intervenite de la intrarea în vigoare a Noului Cod penal și Noului Cod de procedură penală, București, 9-10 octombrie 2017, organizată de Institutul Național al Magistraturii – *www.youtube.com*;

Trif, Valentin; Petre, Adrian, Activitățile preliminare realizate de către echipa de cercetare în cazul constatării infracțiunilor de corupție, în Curierul Judiciar nr. 4/2017;

Tudoran, Mihai Viorel, Considerații referitoare la nerespectarea dispozițiilor legale privind autorizarea interceptării și înregistrării de sunete și imagini, în Dreptul nr. 12/2010;

Tudoran, Mihai Viorel, Interceptările și înregistrările audio sau video efectuate asupra raportului avocat-client în procesul penal, în Curierul Judiciar nr. 5/2011;

Ungureanu, Petre, Aspects of human rights infringement by abusive use of technical surveillance measures, în Buletin Științific al Academiei Forțelor Terestre „Nicolae Bălcescu", Sibiu, vol. XX, nr. 1/2015;

Ungureanu, Petre, Utilizarea supravegherii tehnice în prevenirea și contracararea amenințărilor la adresa securității naționale. Asemănările și deosebirile între supravegherea tehnică realizată în domeniul instrucției penale și cel al securității naționale, în Revista de Investigare a Criminalității nr. 1/2015;

Uzlău, Andreea, Considerații privind garanțiile procesual penale în materia respectării confidențialității relației avocat-client, în raport cu unele procedee probatorii, în Revista de Drept Penal nr. 3/2014;

Valdemar, Richard, Cultivating Effective Gang Informants, în Police Magazine din 5 decembrie 2012;

Vâșcea, Gheorghe, Elemente de drept comparat privind reglementarea livrării supravegheate, în Revista de Investigare a Criminalității, vol. 9, nr. 2/2016;

Villacampa, Carolina; Flórez, Katherine, Human Trafficking for criminal exploitation and participation in armed conflicts: the Colombian case, în Crime, Law and Social Change 69, 421-445 (2018);

Volintiru, Alexandru-Nicolae, Aspecte privind obținerea datelor de trafic și de localizare prelucrate de către furnizorii de rețele publice de comunicații ori furnizorii de servicii de comunicații electronice destinate publicului, în Revista Universul Juridic nr. 9/2016;

Vondráček, Martin; Pluskal, Jan; Ryšavý, Ondřej, Automated Man-in-the-Middle Attack Against Wi-Fi Networks, în Journal of Digital Forensics, Security and Law, vol. 13, no. 1/2018;

Weaver, Nicholas, iPhones, the FBI, and Going Dark, pe *www.lawfareblog.com/iphones-fbi-and-going-dark*;

Wang, Youhua; Qiu, Yitao; Ameri, Shideh Kabiri; Jang, Hongwoo; Dai, Zhaohe; Huang YongAn; Lu, Nanshu, Low-cost, μm-thick, tape-free electronic tattoo sensors with minimized motion and sweat artifacts. în Revista Nature (Nature Partner Journals – Flexible Electronics 2) no. 6/2018;

Wolf, Michelle K., Anti-Wiretapping Statutes: Disregarding Legislative Purpose and the Constitutional Pitfalls of Using Anti-Wiretapping Statues to Prevent the Recording of On-Duty Police Officers, în Journal of Gender, Race and Justice no. 15/2012;

Yang, Jie; Varshavsky, Alexander; Liu, Hongbo; Chen, Yingying, Accuracy Characterization of Cell Tower Localization, Conferința UbiComp 2010: Ubiquitous Computing, 12th International Conference, Copenhaga, Danemarca, 26-29 september 2010;

Yoo, John C., The Legality of The National Security Agency's Bulk Data Surveillance Programs, în Harvard Journal of Law & Public Policy, vol. 37, no. 3/2014;

Zlati, George, Percheziția sistemelor informatice și a mijloacelor de stocare a datelor informatice (I), în Caiete de Drept Penal nr. 3/2014;

Zlati, George, Percheziția sistemelor informatice și a mijloacelor de stocare a datelor informatice (II), în Caiete de Drept Penal nr. 4/2014.

III. Ghiduri, manuale, recomandări și alte instrumente

Comisia de la Veneția, Opinie asupra supravegherii video realizată de autorități publice în spații publice și protejarea drepturilor omului, adoptată în a 70-a Sesiune Plenară a Comisiei de la Veneția, 16-17 martie 2007;

Comisia de la Veneția, Opinie asupra supravegherii video realizate de operatori privați în public și în sfera privată și de autorități publice în sfera privată și protejarea drepturilor omului, adoptată în a 71-a Sesiune Plenară a Comisiei de la Veneția, 1-2 iunie 2007;

Comisia comună permanentă a Camerei Deputaților și Senatului pentru exercitarea controlului asupra activității Serviciului Român de Informații, Raportul parțial reprezentând activitatea comisiei în perioada septembrie 2017 - prezent, referitor la mandatele de securitate

națională, mandatele de supraveghere tehnică și la ordonanțele procurorilor pe 48 de ore, 3 octombrie 2018;

Parchetul de pe lângă Înalta Curte de Casație și Justiție, Raportul activității desfășurate de Ministerul Public în anul 2018, pe *www.mpublic.ro*;

Comisia Europeană, Raportul Comisiei Europene privind evoluția situației din România în cadrul mecanismului de cooperare și de verificare din 22 octombrie 2019 (raportul MCV pentru anul 2019), IP/19/6135;

Federal Bureau of Investigations, Manual of Investigative Operations and Guidelines, desecretizat la nivelul anului 1998;

Office of the Inspector General of the U.S.A., The Federal Bureau of Investigation's Compliance with the Attorney General's Investigative Guidelines, Capitolul III. The Attorney General's Guidelines Regarding the Use of Confidential Informants;

U.S. Justice Department, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations (manual oficial), 2002;

Comitetul de Miniștri al Consiliului Europei, Memorandumul explicativ al Recomandării (2005) 10 a Comitetului de Miniștri al Consiliului Europei;

European Data Protection Board, Guidelines 3/2019 on processing of personal data through video devices, adoptată la 10 iulie 2019;

Serviciul Român de Informații, Raport privind activitatea desfășurată în anul 2008;

Protocol privind organizarea cooperării între Serviciul Român de Informații și Parchetul Național Anticorupție, înregistrat sub nr. 002128 din 28.01.2003 la S.R.I. și sub nr. 00112 din 28.01.2003 la P.N.A. Declasificat sub nr. 7516 din 11.09.2018 la S.R.I. și 2657/C/662 din 21.09.2018 la D.N.A.;

Nota anexă la Protocolul privind organizarea cooperării între Serviciul Român de Informații și Parchetul Național Anticorupție din 29.01.2003, înregistrată sub nr. 44/C din 01.03.2004 la P.N.A. și 002461 din 02.03.2004 la S.R.I. Declasificată sub nr. 7517 din 11.09.2018 la S.R.I. și sub nr. 2657/C/662 din 21.09.2018 la D.N.A.;

Protocol de cooperare între Parchetul de pe lângă Înalta Curte de Casație și Justiție și Serviciul Român de Informații pentru îndeplinirea sarcinilor ce le revin în domeniul securității naționale, înregistrat sub nr. 003222 din 28.06.2005 la S.R.I. și sub nr. 002349 din 30.06.2005 la P.I.C.C.J. Declasificat sub nr. 1949/C1 din 03.08.2018 la P.I.C.C.J.;

Protocol de cooperare între Parchetul de pe lângă Înalta Curte de Casație și Justiție și Serviciul Român de Informații pentru îndeplinirea sarcinilor ce le revin în domeniul securității naționale din 04.02.2009, înregistrat sub nr. 003064 din 04.02.2009 la S.R.I. și sub nr. 00750 din 04.02.2009 la P.I.C.C.J. Declasificat sub nr. 884/C din 29.03.2018 la P.I.C.C.J.;

Protocol privind organizarea cooperării între Serviciul Român de Informații și Parchetul de pe lângă Înalta Curte de Casație și Justiție pentru îndeplinirea sarcinilor ce le revin, potrivit legii, înregistrat sub nr. 03656 din 07.12.2016 la S.R.I. și sub nr. 09472 din 08.12.2016 la P.I.C.C.J. Declasificat sub nr. 2104/C1 din 30.08.2018 la P.I.C.C.J.;

Protocol de cooperare din 07.08.2015 între Parchetul de pe lângă Înalta Curte de Casație și Justiție și Departamentul de Informații și Protecție Internă a Ministerului Afacerilor Interne înregistrat sub nr. 0020 din 07.08.2015 la D.I.P.I. și sub nr. 009726 din 06.08.2015 la P.I.C.C.J. Declasificat sub nr. 1590/C1 din 21.06.2018 la P.I.C.C.J.;

Protocolul privind cooperarea între Serviciul Român de Informații și Ministerul Public pentru stabilirea condițiilor concrete de acces la sisteme tehnice ale Centrului Național de

Interceptare a Comunicațiilor, înregistrat sub nr. 9331 din 07.12.2016 la Serviciul Român de Informații și sub nr. 2440/C din 08.12.2016 la Parchetul de pe lângă Înalta Curte de Casație și Justiție;

Înalta Curte de Casație și Justiție, Raport privind verificarea efectuată de președintele Înaltei Curți de Casație și Justiție în temeiul art. 30[1] din Legea nr. 304/2004 privind organizarea judiciară, republicată, cu modificările și completările ulterioare, înregistrat sub nr. 11 din 7 ianuarie 2020, pe *www.scj.ro*

IV. Articole de presă

Punerea sub acuzare a fostului președinte al Franței, Nicolas Sarkozy, pe *www.theguardian.com*;

Supraveghere tehnică în dosarul lui Decebal Traian Remeș, pe *www.hotnews.ro*;

Cazul Airbus, exemplu de mare corupție în Franța, Marea Britanie și S.U.A., pe *www.euronews.com*;

Comisia Europeană analizează oportunitatea interzicerii pentru o durată de 5 ani a tehnologiei de recunoaștere facială pentru camerele de supraveghere publice, pe: *www.bbc.com*; *www.reuters.com*;

Controlul minorităților din China prin sisteme de recunoaștere facială, pe *www.wired.com*;

Datele și informațiile obținute în mod automat de furnizorii de servicii de internet, pe *arstechnica.com*;

Utilizarea submarinelor pentru transportul cocainei pe mare – caz recent descoperit în Spania (2019), pe *www.theguardian.com*;

Noi tendințe în dezvoltarea statului polițienesc modern – *M. Rajagopalan*, This Is What A 21st-Century Police State Really looks like, pe *www.buzzfeednews.com*;

Hotărâre judecătorească recentă a unei instanțe moscovite, prin care s-a constatat legalitatea folosirii sistemelor de recunoaștere facială în Moscova, pe *www.themoscowtimes.com*;

Riscurile folosirii sistemelor de recunoaștere facială curente și eroarea în identificare – *I.A. Hamilton*, British police scanned 8,600 people's faces in London without their consent, resulting in just 1 arrest and 7 false positives, pe *www.businessinsider.nl*;

Wong, J.C., US, UK and Australia urge Facebook to create backdoor access to encrypted messages, în ziarul The Guardian din 4 octombrie 2019, pe *www.theguardian.com*

V. Jurisprudență

1. Jurisprudența Curții Europene a Drepturilor Omului (*hudoc.echr.coe.int*)

CEDO, cauza *Allan c. Marea Britanie*, Hotărârea din 5 februarie 2003;
CEDO, cauza *Altay c. Turcia (nr. 2)*, Hotărârea din 9 iulie 2019;
CEDO, cauza *André ș.a. c. Franța*, Hotărârea din 24 iulie 2008;
CEDO, cauza *Andreou Papi c. Turcia*, Hotărârea din 22 septembrie 2009;
CEDO, cauza *Antović și Mirković c. Muntenegru*, Hotărârea din 28 noiembrie 2017;
CEDO, cauza *Apostu c. România*, Hotărârea din 6 iulie 2015;
CEDO, cauza *Asch c. Austria*, Hotărârea din 26 aprilie 1991;
CEDO, cauza *Axel Springer c. Germania*, Hotărârea din 7 februarie 2012;
CEDO, cauza *B. c. Franța*, Hotărârea din 25 martie 1992;

CEDO, cauza *Bannikova c. Rusia*, Hotărârea din 4 februarie 2011;
CEDO, cauza *Bălteanu c. România*, Hotărârea din 16 iulie 2013;
CEDO, cauza *Bărbulescu c. România*, Hotărârea din 5 septembrie 2017*;*
CEDO, cauza *Beuze c. Belgia*, Hotărârea din 9 noiembrie 2018;
CEDO, cauza *Botta c. Italia*, Hotărârea din 24 februarie 1998;
CEDO, cauza *Brennan c. Marea Britanie*, Hotărârea din 16 octombrie 2001;
CEDO, cauza *Brito Ferrinho Bexiga Villa-Nova c. Portugalia*, Hotărârea din 1 decembrie 2015, definitivă la 1 martie 2016;
CEDO, cauza *Buck c. Germania*, Hotărârea din 28 aprilie 2005;
CEDO, cauza *Burak Hun c. Turcia*, Hotărârea din 15 martie 2010;
CEDO, cauza *Burghartz c. Elveția*, Hotărârea din 22 februarie 1994;
CEDO, cauza *Bykov c. Rusia*, Hotărârea din 10 martie 2009;
CEDO, cauza *Calmanovici c. România*, Hotărârea din 1 iulie 2008;
CEDO, cauza *Campbell c. Marea Britanie*, Hotărârea din 25 martie 1992;
CEDO, cauza *Castraveț c. Moldova*, Hotărârea din 13 martie 2007;
CEDO, cauza *Cășuneanu c. România*, Hotărârea din 16 aprilie 2013;
CEDO, cauza *Centro Europa 7 S.R.L. și Di Stefano c. Italia*, Hotărârea din 7 iunie 2012;
CEDO, cauza *Cēsnieks c. Letonia*, Hotărârea din 11 februarie 2014;
CEDO, cauza *Chapman c. Marea Britanie*, Hotărârea din 18 ianuarie 2001;
CEDO, cauza *Chiragov ș.a. c. Armenia*, Hotărârea din 16 iunie 2015;
CEDO, cauza *Constantin și Stoian c. România*, Hotărârea din 29 decembrie 2009;
CEDO, cauza *Copland c. Marea Britanie*, Hotărârea din 3 iulie 2007;
CEDO, cauza *Cotleț c. România*, Hotărârea din 3 iunie 2003;
CEDO, cauza *Craxi c. Italia (nr. 2)*, Hotărârea din 17 iulie 2003;
CEDO, cauza *Delcourt c. Belgia*, Hotărârea din 17 ianuarie 1970;
CEDO, cauza *Delta c. Franța*, Hotărârea din 19 decembrie 1990;
CEDO, cauza *Delta Pekárny A.S. c. Cehia*, Hotărârea din 2 octombrie 2014;
CEDO, cauza *Demades c. Turcia*, Hotărârea din 31 iulie 2003;
CEDO, cauza *Denisov c. Ucraina*, Hotărârea din 25 septembrie 2018;
CEDO, cauza *Dudgeon c. Marea Britanie*, Hotărârea din 22 octombrie 1981;
CEDO, cauza *Dragojević c. Croația*, Hotărârea din 15 ianuarie 2015;
CEDO, cauza *Dragoș Ioan Rusu c. România*, Hotărârea din 31 octombrie 2017;
CEDO, cauza *Drakšas c. Lituania*, Hotărârea din 31 iulie 2012;
CEDO, cauza *Dumitru Popescu c. România (nr. 2)*, Hotărârea din 26 aprilie 2007;
CEDO, cauza *Elci ș.a. c. Turcia*, Hotărârea din 24 martie 2004;
CEDO, cauza *Erdagöz c. Turcia*, Hotărârea din 22 octombrie 1997;
CEDO, cauza *Fernández Martínez c. Spania*, Hotărârea din 12 iunie 2014;
CEDO, cauza *Fox, Campbell și Hartley c. Marea Britanie*, Hotărârea din 30 august 1990;
CEDO, cauza *Friedl c. Austria*, Hotărârea din 31 ianuarie 1995;
CEDO, cauza *Furcht c. Germania*, Hotărârea din 23 ianuarie 2015;
CEDO, cauza *Gäfgen c. Germania*, Hotărârea din 1 iunie 2010;
CEDO, cauza *Gagiu c. România*, Hotărârea din 24 februarie 2009;
CEDO, cauza *Gorbunov și Gorbachev c. Rusia*, Hotărârea din 1 martie 2016;
CEDO, cauza *Gorgievski c. Macedonia*, Hotărârea din 10 decembrie 2009;
CEDO, cauza *Gorlov ș.a. c. Rusia*, Hotărârea din 2 iulie 2019;

CEDO, cauza *Govell c. Marea Britanie*, Hotărârea din 14 ianuarie 1998;
CEDO, cauza *Guja c. Moldova*, Hotărârea din 12 februarie 2008;
CEDO, cauza *Halabi c. Franța*, Hotărârea din 16 mai 2019;
CEDO, cauza *Halford c. Marea Britanie*, Hotărârea din 25 iunie 1997;
CEDO, cauza *Heino c. Finlanda*, Hotărârea din 15 februarie 2011;
CEDO, cauza *Huvig c. Franța*, Hotărârea din 24 aprilie 1990;
CEDO, cauza *Ibrahim ș.a. c. Marea Britanie*, Hotărârea din 13 septembrie 2016;
CEDO, cauza *Ilgar Mammadov c. Azerbaidjan*, Hotărârea din 13 octombrie 2014;
CEDO, cauza *Iliya Stefanov c. Bulgaria*, Hotărârea din 22 mai 2008;
CEDO, cauza *Iordachi ș.a. c. Moldova*, Hotărârea din 10 februarie 2009;
CEDO, cauza *Irfan Güzel c. Turcia*, Hotărârea din 7 mai 2017;
CEDO, cauza *Kavala c. Turcia*, Hotărârea din 10 decembrie 2019;
CEDO, cauza *Kennedy c. Marea Britanie*, Hotărârea din 18 mai 2010;
CEDO, cauza *Kent Pharmaceuticals ș.a. c. Marea Britanie*, Hotărârea din 11 octombrie 2005;
CEDO, cauza *Khadija Ismayilova c. Azerbaidjan*, Hotărârea din 10 ianuarie 2019;
CEDO, cauza *Khan c. Marea Britanie*, Hotărârea din 12 mai 2000, definitivă la 4 octombrie 2000;
CEDO, cauza *Khodorkovskiy și Lebedev c. Rusia*, Hotărârea din 25 iulie 2013;
CEDO, cauza *Klass ș.a. c. Germania*, Hotărârea din 6 septembrie 1978;
CEDO, cauza *Kök c. Turcia*, Hotărârea din 19 octombrie 2006;
CEDO, cauza *Kopp c. Elveția*, Hotărârea din 25 martie 1998;
CEDO, cauza *Krasniki c. Cehia*, Hotărârea din 28 februarie 2006;
CEDO, cauza *Kruslin c. Franța*, Hotărârea din 24 aprilie 1990;
CEDO, cauza *Lanz c. Austria*, Hotărârea din 30 aprilie 2002;
CEDO, cauza *Laskey, Jaggard și Brown c. Marea Britanie*, Hotărârea din 19 februarie 1997;
CEDO, cauza *Laurent c. Franța*, Hotărârea din 24 mai 2018;
CEDO, cauza *Ludi c. Elveția*, Hotărârea din 15 iunie 1992;
CEDO, cauza *Luordo c. Italia*, Hotărârea din 17 iulie 2003;
CEDO, cauza *M.M. c. Olanda*, Hotărârea din 24 septembrie 2003;
CEDO, cauza *M.N. ș.a. c. San Marino*, Hotărârea din 7 iulie 2015, definitivă la 7 octombrie 2015;
CEDO, cauza *Malininas c. Lituania*, Hotărârea din 1 octombrie 2010;
CEDO, cauza *Malone c. Marea Britanie*, Hotărârea din 2 august 1984;
CEDO, cauza *Marckx c. Belgia*, Hotărârea din 13 iunie 1979;
CEDO, cauza *Matanović c. Croația*, Hotărârea din 4 iulie 2017;
CEDO, cauza *Matheron c. Franța*, Hotărârea din 29 iunie 2005;
CEDO, cauza *Menţeş ș.a. c. Turcia*, Hotărârea din 28 noiembrie 1997;
CEDO, cauza *Merabishvili c. Georgia*, Hotărârea din 28 noiembrie 2017;
CEDO, cauza *Miailhe c. Franța*, Hotărârea din 25 februarie 1993;
CEDO, cauza *Michaud c. Franța*, Hotărârea din 6 martie 2013;
CEDO, cauza *Milinienė c. Lituania*, Hotărârea din 24 septembrie 2008;
CEDO, cauza *Mikulić c. Croația*, Hotărârea din 7 februarie 2002;
CEDO, cauza *Niemietz c. Germania*, Hotărârea din 16 decembrie 1992;
CEDO, cauza *Nițulescu c. România*, Hotărârea din 22 septembrie 2015;
CEDO, cauza *Norwood c. Marea Britanie*, Hotărârea din 16 noiembrie 2004;

CEDO, cauza *Observer și Guardian c. Marea Britanie*, Hotărârea din 26 noiembrie 1991;
CEDO, cauza *Öcalan c. Turcia*, Hotărârea din 12 mai 2005;
CEDO, cauza *Özgür Gündem c. Turcia*, Hotărârea din 16 martie 2000;
CEDO, cauza *P.G. și J.H. c. Marea Britanie*, Hotărârea din 25 septembrie 2001;
CEDO, cauza *Pavel Ivanov c. Rusia*, Hotărârea din 20 februarie 2007;
CEDO, cauza *Peck c. Marea Britanie*, Hotărârea din 28 ianuarie 2003;
CEDO, cauza *Pesukic c. Elveția*, Hotărârea din 6 decembrie 2012;
CEDO, cauza *Petri Sallinen ș.a. c. Finlanda*, Hotărârea din 27 septembrie 2005;
CEDO, cauza *Petrina c. România*, Hotărârea din 6 aprilie 2009;
CEDO, cauza *Petrov c. Bulgaria*, Hotărârea din 22 mai 2008;
CEDO, cauza *Piechowsicz c. Polonia*, Hotărârea din 17 aprilie 2012;
CEDO, cauza *Popovi c. Bulgaria*, Hotărârea din 9 iunie 2016;
CEDO, cauza *Prokopovich c. Rusia*, Hotărârea din 18 noiembrie 2004;
CEDO, cauza *Pruteanu c. România*, Hotărârea din 3 mai 2015;
CEDO, cauza *Ramanauskas c. Lituania*, Hotărârea din 5 februarie 2008;
CEDO, cauza *Ramanauskas c. Lituania (nr. 2)*, Hotărârea din 20 mai 2018;
CEDO, cauza *Rees c. Marea Britanie*, Hotărârea din 17 octombrie 1986;
CEDO, cauza *Reklos și Davourlis c. Grecia*, Hotărârea din 15 ianuarie 2009;
CEDO, cauza *Robathin c. Austria*, Hotărârea din 3 iulie 2012;
CEDO, cauza *Roemen și Schmidt c. Luxemburg*, Hotărârea din 25 februarie 2003;
CEDO, cauza *Roman Zakharov*, Hotărârea din 4 decembrie 2015;
CEDO, cauza *Rybacki c. Polonia*, Hotărârea din 13 ianuarie 2009;
CEDO, cauza *S. c. Elveția*, Hotărârea din 28 noiembrie 1991;
CEDO, cauza *S. și Marper c. Marea Britanie*, Hotărârea din 4 decembrie 2008;
CEDO, cauza *Sagan c. Ucraina,* Hotărârea din 23 octombrie 2018;
CEDO, cauza *Saint-Paul Luxembourg S.A. c. Luxemburg*, Hotărârea din 18 aprilie 2013;
CEDO, cauza *Sakhnovskiy c. Rusia*, Hotărârea din 2 noiembrie 2010;
CEDO, cauza *Saliyev c. Rusia*, Hotărârea din 21 octombrie 2010;
CEDO, cauza *Sanoma Uitgevers B.V. c. Olanda*, Hotărârea din 14 septembrie 2010;
CEDO, cauza *Schönenberger și Durmaz c. Elveția*, Hotărârea din 20 iunie 1988;
CEDO, cauza *Segerstedt-Wiberg ș.a. c. Suedia*, Hotărârea din 6 iunie 2006;
CEDO, cauza *Sepil c. Turcia*, Hotărârea din 12 noiembrie 2013, definitivă la 12 februarie 2014;
CEDO, cauza *Sequeira c. Portugalia*, Hotărârea din 6 mai 2003;
CEDO, cauza *Shannon c. Marea Britanie*, Hotărârea din 6 aprilie 2004;
CEDO, cauza *Shimovolos c. Rusia*, Hotărârea din 21 iunie 2011;
CEDO, cauza *Silver ș.a. c. Marea Britanie*, Hotărârea din 25 martie 1983;
CEDO, cauza *Smirnov c. Rusia*, Hotărârea din 7 iunie 2007;
CEDO, cauza *Société Colas Est ș.a. c. Franța*, Hotărârea din 16 aprilie 2002;
CEDO, cauza *Sommer c. Germania*, Hotărârea din 27 iulie 2017;
CEDO, cauza *Steeg c. Germania*, Hotărârea din 3 iunie 2008;
CEDO, cauza *Stepuleac c. Moldova*, Hotărârea din 6 februarie 2008;
CEDO, cauza *Szafrański c. Polonia*, Hotărârea din 15 decembrie 2015;
CEDO, cauza *Taal c. Estonia*, Hotărârea din 22 noiembrie 2005,
CEDO, cauza *Tchokhonelidze c. Georgia*, Hotărârea din 28 septembrie 2018;

CEDO, cauza *Teixeira de Castro c. Portugalia*, Hotărârea din 9 iunie 1998;
CEDO, cauza *The Sunday Times c. Marea Britanie*, Hotărârea din 26 aprilie 1979;
CEDO, cauza *Toma c. România*, Hotărârea din 24 februarie 2009;
CEDO, cauza *Ulariu c. România*, Hotărârea din 19 noiembrie 2013;
CEDO, cauza *Uzun c. Germania*, Hotărârea din 2 septembrie 2010, definitivă la 2 decembrie 2010;
CEDO, cauza *Valenzuela Contreras c. Spania*, Hotărârea din 30 iulie 1998;
CEDO, cauza *Van Mechelen ș.a. c. Olanda*, Hotărârea din 23 aprilie 1997;
CEDO, cauza *Van Vondel c. Olanda*, Hotărârea din 25 ianuarie 2008;
CEDO, cauza *Vanyan c. Rusia*, Hotărârea din 15 martie 2006;
CEDO, cauza *Vereniging Weekblad Bluf c. Olanda*, Hotărârea din 9 februarie 1995;
CEDO, cauza *Versini-Campinchi și Crasnianski c. Franța*, Hotărârea din 16 iunie 2016;
CEDO, cauza *Vetter c. Franța*, Hotărârea din 31 august 2005;
CEDO, cauza *Vinci Construction și GTM Génie Civil et Services c. Franța*, Hotărârea din 2 aprilie 2015;
CEDO, cauza *Virgil Dan Vasile c. România*, Hotărârea din 15 august 2018;
CEDO, cauza *Visser c. Olanda*, Hotărârea din 14 februarie 2002;
CEDO, cauza *Von Hannover c. Germania (nr. 2)*, Hotărârea din 7 februarie 2012;
CEDO, cauza *Weber și Saravia c. Germania*, Hotărârea din 29 iunie 2006;
CEDO, cauza *Wieser și Bicos Beteiligungen GmbH c. Austria*, Hotărârea din 16 octombrie 2007;
CEDO, cauza *Windisch c. Austria*, Hotărârea din 27 septembrie 1990;
CEDO, cauza *Winterstein ș.a. c. Franța*, Hotărârea din 17 octombrie 2013;
CEDO, cauza *X și Y c. Belgia*, Hotărârea din 13 mai 1982;
CEDO, cauza *X și Y c. Olanda*, Hotărârea din 26 martie 1985;
CEDO, cauza *Xavier Da Silveira c. Franța*, Hotărârea din 21 aprilie 2010;
CEDO, cauza *Yılmaz și Kılıc c. Turcia*, Hotărârea din 17 iulie 2008;
CEDO, cauza *Yevgeniy Zakharov c. Rusia*, Hotărârea din 14 martie 2017;
CEDO, cauza *Yordanova ș.a. c. Bulgaria*, Hotărârea din 24 aprilie 2012;
CEDO, cauza *Z. c. Finlanda*, Hotărârea din 25 februarie 1997;
CEDO, cauza *Zagaria c. Italia*, Hotărârea din 27 noiembrie 2007.

2. Jurisprudența Curții de Justiție a Uniunii Europene (*eur-lex.europa.eu*)

CJUE, cauzele reunite C-293/12 și C-594/12, *Digital Rights Ireland și alții*, Hotărârea din 8 aprilie 2014;
CJUE, cauza C-193/18, *Google c. Germania*, Hotărârea din 13 iunie 2019;
CJUE, cauza C-207/16, *Ministerio Fiscal*, Hotărârea din 2 octombrie 2018;
CJUE, cauzele reunite C-465/00, C-138/01 și C-139/01, *Österreichischer Rundfunk și alții*, Hotărârea din 20 mai 2003;
CJUE, cauza C-142/18, *Skype Communications c. IBPT*, Hotărârea din 5 iunie 2019;
CJUE, cauzele reunite C-203/15 și C-698/15, *Tele2 Sverige AB, Secretary of State for the Home Department și alții*, Hotărârea din 21 decembrie 2016;
CJUE, cauza C-475/12, *UPC DTH*, Hotărârea din 30 aprilie 2014.

3. Jurisprudență străină

U.S., cauza *INS c. Chadwa*, Hotărârea din 23 iunie 1983, 462 U.S. 919 (1983), pe *supreme.justia.com*;

U.S., cauza *Snyder c. Phelps*, Hotărârea din 2 martie 2011, 562 U.S. 443 (2011), pe *supreme.justia.com*;

U.S., cauza *Hustler Magazine, Inc c. Falwell*, Hotărârea din 24 februarie 1988, 485 U.S. 46 (1988), pe *supreme.justia.com*;

U.S., cauza *Terry c. Ohio*, Hotărârea din 10 iunie 1968, 392 U.S. 1 (1968), pe *supreme.justia.com*;

U.S. Court of Appeals, Fifth Circuit, cauza *United States c. Cervantes-Pacheco*, 826 F.2d 310, dec. din 21 august 1987, par. 29, pe *openjurist.org*;

U.S. Court of Appeals, Eleventh Circuit, cauza *United States c. Edenfield*, 995 F.2d 197, dec. din 14 iulie 1993, par. 3, pe *www.leagle.com*;

U.S. District Court, Southern District, Texas, Magistrate no. H-05-557M, dec. din 14 octombrie 2005, pe *www.courtlistener.com*;

U.K. Supreme Court of Judicature, Queen's Bench Division, *Redmond-Bate c. Director of Public Prosecutions*, dec. din 23 iulie 1999, [1999] EWHC Admin 733, pe *www.bailii.org*;

UKHL, cauza *Regina c. Looseley*, UKHL 53, dec. din 25 octombrie 2001, pe *www.bailii.org*;

EWCA, cauza *R. c. Mason și alții*, Dec. din 13 februarie 2002, [2002] EWCA Crim 385, pe *www.bailii.org*;

EWCA, cauza *Jones c. University of Warwick*, Dec. din 4 februarie 2003, [2003] EWCA Civ 151, pe *www.bailii.org*;

EWCA, cauza *Coudrat. c. Commissioners of Her Majesty's Revenue and Customs*, Dec. din 26 mai 2005, [2005] EWCA Civ 616, pe *www.bailii.org*;

EWCA, cauza *Rosenberg c. R.*, Dec. din 20 ianuarie 2006, [2006] EWCA Crim 6, pe *www.bailii.org*;

EWCA, cauza *Regina c. Ian Anthony Jones*, Dec. din 15 mai 2007, EWCA Crim 1118, pe *www.bailii.org*;

EWCA, cauza *Regina c. M.*, Dec. din 18 martie 2011, EWCA Crim 648, pe *www.bailii.org*;

EWCA, cauza *Regina c. Palmer, Gyamfi, Cooke*, Dec. din 7 august 2014, [2014] EWCA Crim 1681, pe *www.bailii.org*;

England and Wales High Court (Queen's Bench Division), cauza *Parker c. Chief Constable of Essex Police*, Dec. din 18 august 2017, [2017] EWHC 2140 (QB), pe *www.bailii.org*;

EWCA, cauza *Regina c. Ali (Humza)*, Dec. din 20 martie 2018, [2018] EWCA Crim 547, §17, pe *www.bailii.org*;

Curtea Constituțională a Africii de Sud, cauza *Coetzee c. Guvernul Africii de Sud*, Dec. din 22 septembrie 1995, §45, pe *www.saflii.org*

4. Jurisprudența Curții Constituționale a României

CCR, Dec. nr. 97 din 7 februarie 2008 (M. Of. nr. 169 din 5 martie 2008);

CCR, Dec. nr. 440 din 8 iulie 2014 (M. Of. nr. 653 din 4 septembrie 2014);

CCR, Dec. nr. 641 din 11 noiembrie 2014 (M. Of. nr. 887 din 5 decembrie 2014);

CCR, Dec. nr. 383 din 27 mai 2015 (M. Of. nr. 535 din 17 iulie 2015);

CCR, Dec. nr. 51 din 16 februarie 2016 (M. Of. nr. 190 din 14 martie 2016);

CCR, Dec. nr. 556 din 12 iulie 2016 (M. Of. nr. 624 din 12 august 2016);
CCR, Dec. nr. 756 din 13 decembrie 2016 (M. Of. nr. 293 din 25 aprilie 2017);
CCR, Dec. nr. 778 din 15 decembrie 2016 (M. Of. nr. 111 din 12 februarie 2016);
CCR, Dec. nr. 244 din 6 aprilie 2017 (M. Of. nr. 529 din 6 iulie 2017);
CCR, Dec. nr. 302 din 4 mai 2017 (M. Of. nr. 566 din 17 iulie 2017);
CCR, Dec. nr. 323 din 9 mai 2017 (M. Of. nr. 640 din 4 august 2017);
CCR, Dec. nr. 554 din 19 septembrie 2017 (M. Of. nr. 1013 din 21 decembrie 2017);
CCR, Dec. nr. 802 din 5 decembrie 2017 (M. Of. nr. 118 din 6 februarie 2018);
CCR, Dec. nr. 855 din 14 decembrie 2017 (M. Of. nr. 150 din 16 februarie 2018);
CCR, Dec. nr. 22 din 18 ianuarie 2018 (M. Of. nr. 177 din 26 februarie 2018);
CCR, Dec. nr. 91 din 28 februarie 2018 (M. Of. nr. 348 din 20 aprilie 2018);
CCR, Dec. nr. 802 din 6 decembrie 2018 (M. Of. nr. 218 din 20 martie 2019);
CCR, Dec. nr. 55 din 17 septembrie 2018 (M. Of. nr. 417 din 28 mai 2019);
CCR, Dec. nr. 261 din 24 aprilie 2018 (M. Of. nr. 622 din 18 iulie 2018);
CCR, Dec. nr. 720 din 20 noiembrie 2018 (M. Of. nr. 183 din 7 martie 2019);
CCR, Dec. nr. 26 din 16 ianuarie 2019 (M. Of. nr. 193 din 12 martie 2019);
CCR, Dec. nr. 250 din 16 aprilie 2019 (M. Of. nr. 500 din 20 iunie 2019);
CCR, Dec. nr. 55 din 4 februarie 2020 (M. Of. nr. 517 din 17 iunie 2020).

5. Jurisprudența instanțelor naționale

C. Ap. București, s. a IV-a civ., dec. civ. nr. 360 din 14 februarie 2006;
C. Ap. Galați, s. pen. și pentru cauze cu minori, dec. pen. nr. 96/A/2013;
C. Ap. Timișoara, dec. pen. nr. 205/A din 23 octombrie 2013, pronunțată în dosar nr. 5502/108/2013, nepublicată;
C. Ap. Craiova, s. pen., dec. nr. 327 din 7 martie 2014, pe *portal.just.ro*;
C. Ap. Cluj, dec. nr. 54/A din 14 ianuarie 2015;
C. Ap. Craiova, dec. pen. nr. 1249/2015;
C. Ap. București, s. a II-a pen., dec. pen. nr. 340 din 23 iunie 2015;
C. Ap. Oradea, încheierea pen. nr. 146/CCP din 21 decembrie 2015;
C. Ap. Oradea, dec. pen. nr. 1/A din 6 ianuarie 2016;
C. Ap. Oradea, dec. pen. nr. 447 din 5 iulie 2017;
C. Ap. București, s. a II-a pen., încheierea din 4 martie 2016, menținută prin încheierea nr. 726 din 18 martie 2016 a ICCJ, s. pen.;
C. Ap. Oradea, s. pen., încheierea nr. 28 din 29 martie 2016 a judecătorului de cameră preliminară din cadrul C. Ap. Oradea, pronunțată în dosar nr. 84/35/2016;
C. Ap. Suceava, s. pen., încheierea nr. 29 din 6 mai 2016;
C. Ap. Bacău, s. pen., încheierea nr. 33 din 13 mai 2016, definitivă prin încheierea nr. 919 din 22 iunie 2016 a ICCJ, s. pen.;
C. Ap. Timișoara, s. pen., încheierea din 19 mai 2016, pe *portal.just.ro*;
C. Ap. Alba Iulia, s. pen., încheierea nr. 77 din 7 iunie 2016;
C. Ap. Timișoara, s. pen., încheierea nr. 98 din 15 iunie 2016;
C. Ap. București, s. I pen., sent. nr. 278 din 13 iulie 2016, pe *portal.just.ro*;
C. Ap. București, s. I pen., încheierea din 1 septembrie 2016, definitivă prin încheierea din 14 octombrie 2016 a ICCJ, s. pen.;
C. Ap. Iași, s. pen., încheierea din 5 septembrie 2016;

C. Ap. București, s. I pen., încheierea nr. 506 din 8 noiembrie 2016;

C. Ap. Cluj, dec. nr. 554 din 5 aprilie 2017;

C. Ap. Timișoara, dec. pen. nr. 132/A din 31 ianuarie 2017;

C. Ap. București, s. a II-a pen., dec. nr. 1123/A din 18 septembrie 2019, pronunțată în dosar nr. 18875/3/2012, nepublicată;

C. Ap. Oradea, s. pen. și pentru cauze cu minori, dec. nr. 703 din 20 decembrie 2019, pronunțată în dosar nr. 4630/83/2006**, nepublicată;

D.N.A., secția de combatere a corupției, dosar nr. 634/P/2014 (cauză personală);

ICCJ, Secțiile Unite, Dec. nr. 17 din 21 noiembrie 2005 (M. Of. nr. 119 din 8 februarie 2006);

ICCJ, Completul pentru dezlegarea unor chestiuni de drept, Dec. nr. 22 din 25 octombrie 2016 (M. Of. nr. 1057 din 28 decembrie 2016);

ICCJ, Completul pentru dezlegarea unor chestiuni de drept, Dec. nr. 2/2018 (M. Of. nr. 307 din 5 aprilie 2018);

ICCJ, s. pen., dec. nr. 5269 din 6 noiembrie 2007, pe *www.scj.ro*;

ICCJ, s. pen., dec. nr. 1641 din 14 mai 2014, pe *www.scj.ro*;

ICCJ, s. pen., dec. nr. 347 din 29 octombrie 2014, în dosar nr. 812/46/2009*, nepublicată;

ICCJ, s. pen., dec. nr. 2907 din 30 octombrie 2014, pe *www.scj.ro*;

ICCJ, s. pen., dec. nr. 3927 din 29 noiembrie 2012, nepublicată;

ICCJ, s. pen., dec. nr. 3147 din 12 decembrie 2014, nepublicată;

ICCJ, s. pen., încheierea nr. 155 din 3 iunie 2015;

ICCJ, s. pen., încheierea nr. 287 din 6 aprilie 2016;

ICCJ, s. pen., dec. nr. 416/A din 27 octombrie 2016, pe *www.scj.ro*;

ICCJ, s. pen. încheierea nr. 1531 din 12 decembrie 2016;

Jud. Baia Mare, s. pen., încheierea din 23 septembrie 2019, pronunțată în dosar nr. 3879/337/2015, nepublicată;

Trib. București, s. a IV-a civ., sent. nr. 709 din 11 mai 2007, pronunțată în dosar nr. 2770/3/2006;

Trib. Dolj, s. pen., sent. nr. 327 din 7 martie 2014, pe *portal.just.ro*;

Trib. Suceava, s. pen., încheierea din 4 mai 2015, definitivă prin încheierea nr. 42 din 26 iunie 2015 a C. Ap. Suceava;

Trib. Harghita, s. pen., încheierea din 18 noiembrie 2015, modificată prin încheierea nr. 3 din 19 ianuarie 2016 a C. Ap. Târgu Mureș;

Trib. Cluj, s. pen., încheierea nr. 63/CP/2016;

Trib. Gorj, s. pen., încheierea din 13 ianuarie 2016, definitivă prin încheierea din 28 martie 2016 a C. Ap. Craiova;

Trib. Ilfov, s. pen., sent. nr. 33 din 4 februarie 2016, pe *portal.just.ro*;

Trib. Mureș, s. pen., încheierea nr. 147 din 31 octombrie 2016;

Trib. Iași, s. pen., sent. nr. 18 din 15 februarie 2017, pe *portal.just.ro*;

Trib. București, s. I pen., încheierea din 2 martie 2017, pronunțată în dosar nr. 7229/3/2017, nepublicată;

Trib. Satu Mare, s. pen., sent. nr. 26/JDL/2017 din 12 aprilie 2017, pe *portal.just.ro*;

Trib. Covasna, s. pen., sent. nr. 45 din 31 octombrie 2017, pe *portal.just.ro*;

Trib. Argeș, s. pen., încheierea nr. 117 din 22 martie 2018, pe *www.rolii.ro*;

Trib. Cluj, s. pen., încheierea nr. 87/CP din 2 octombrie 2019, pronunțată în dosar 1706/117/2018/a1, nepublicată.

Index tematic*

A

abonat 189; 253; 364; 366; 369-370; 380; 385; 397

abuz în serviciu 59

acces ilegal la un sistem informatic 45; 133; 236

acces la un sistem informatic transfrontalier 237

accesul la date în format electronic 398

acord de colaborare 466; 475; 488

activități specifice culegerii de informații 543-548; 550; 554; 557; 570; 572; 574; 576; 584; 586

- categorii:
  - activități specifice care nu presupun restrângerea drepturilor și libertăților cetățenești 557-558
  - activități specifice care presupun restrângerea drepturilor și libertăților cetățenești 559-564
    - căutarea unor informații, documente sau înscrisuri pentru a căror obținere este necesar accesul într-un loc, la un obiect ori deschiderea unui obiect 560
    - instalarea de obiecte, întreținerea și ridicarea acestora din locurile în care au fost depuse, supravegherea prin fotografiere, filmare sau prin alte mijloace tehnice ori constatări personale, efectuate sistematic în locuri publice sau efectuate în orice mod în locuri private 561-562
    - interceptarea și înregistrarea comunicațiilor electronice, efectuate sub orice formă 559-560
    - interceptarea trimiterilor poștale, ridicarea și repunerea la loc a acestora, examinarea lor, extragerea informațiilor pe care acestea le conțin, precum și înregistrarea, copierea sau obținerea de extrase prin orice procedee 562-563
    - localizarea, urmărirea și obținerea de informații prin GPS sau prin alte mijloace tehnice de supraveghere 562
    - obținerea de informații privind tranzacțiile financiare sau datele financiare ale unei persoane, în condițiile legii 563-564
    - ridicarea și repunerea la loc a unui obiect sau document, examinarea lui, extragerea informațiilor pe care acesta le conține, precum și înregistrarea, copierea sau obținerea de extrase 560-561

acțiune de observare a persoanei desfășurată prin mijloace tehnice 271-272

admisibilitate 22; 53; 134-135; 137-138; 152; 159 (*v.* și inadmisibilitate 69; 447)

agent dublu 474

agent sub acoperire 431

Agenția Națională de Administrare Fiscală 210; 324-326; 360

Allan c. Marea Britanie 40; 269; 282

Altay c. Turcia (nr. 2) 43; 141; 147-148; 151

alte organe specializate ale statului 80-81; 84; 85; 88; 103; 166; 170; 187

amenințări la adresa securității naționale 207; 542; 544-545; 547; 549; 558; 565-569; 573-574; 582; 584-585

anchetă proactivă 11; 51; 62; 237; 434; 438; 507

arhivare 85; 92-97; 110-111; 118

arhivare digitală 343

autoritate de lucru judecat 79; 452

* Trimiterile sunt făcute la numărul paginii din lucrare.

autoritate vamală 521; 526; 537-538
avocatul
- suspectului, inculpatului sau al unei alte persoane 347
- subiect al supravegherii tehnice 141-155; 180
  - *Iordachi ș.a. c. Moldova* 143
  - *Kopp c. Elveția* 143
  - *Versini-Campinchi și Crasnianski c. Franța* 144
- obținerea datelor privind tranzacțiile financiare ale avocatului 347-351
  - obținerea datelor privind tranzacțiile financiare ale avocatului atunci când acesta face obiectul urmăririi penale 347
    - *Sommer c. Germania* 350-351
  - obținerea accidentală a datelor privind tranzacțiile financiare ale avocatului 348
    - *M.N. și alții c. San Marino* 349-350
    - *Brito Ferrinho Bexiga Villa-Nova c. Portugalia* 349-350
  - obținerea nelegală a datelor privind tranzacțiile financiare ale avocatului 349
    - *Michaud c. Franța* 350
- reținerea, predarea și percheziționarea trimiterilor poștale ale unui avocat 426-428
- secretul profesional al avocatului 37; 56; 141-149; 342; 347-348; 350; 352; 383

B

Big Data 406

C

caracter specializat și restrâns 446; 448; 452
certificare – noțiune 120
certificat
- digital 98; 100; 104
- calificat 98; 100-103; 201; 397

cheie de criptare
- privată 100; 234-235
- publică 100; 234-235
- criptare *end-to-end* 235

cheltuieli ocazionate de folosirea investigatorilor sub acoperire, a informatorilor și colaboratorilor 478
cod(uri) hash de verificare 99; 102; 120
colaboratori de serviciu 479
completare a mandatului *c.* completare a autorizării 576-577
comunicare *c.* comunicație 188-190
concurs tehnic 12; 46; 80; 83-84; 247; 285; 293; 414; 555
conectare la o rețea de telefonie mobilă 380
conflict de natură constituțională 87; 205
conservarea materialelor rezultate din supravegherea tehnică 95-98; 172
consimțământul abonatului sau utilizatorului 369-370; 385
contract de asistență juridică 151-152
control de constituționalitate 368; 372; 558
controlarea punerii în aplicare a livrării supravegheate 533-534
controlled delivery 514
conturi
- definiție 354-356
  - existența conturilor;
  - conținutul conturilor.

Convenția de la Budapesta privind criminalitatea informatică din anul 2001 228-232; 235; 237; 244; 246; 249-254; 378; 457
copie certificată 118-120; 216; 341
corespondență
- istoric 401-407
- în interpretarea Constituției României 407-408
- în interpretarea Curții Europene a Drepturilor Omului 142; 145-146
- percheziționarea corespondenței 402; 413; 415; 417; 425-427

criminalitate
- informatică 213; 228; 251
- organizată 3; 180; 314-315; 350; 367; 383; 506; 515-516; 519; 539
  - Convenția ONU împotriva criminalității transnaționale organizate din 2000 514
- transfrontalieră 529; 539

cumpărare de influență 476
cyberbullying 249
cyberharrassement 249
cyberstalking 249

D
dare de mită 182; 311; 467; 476
date
- cu caracter personal [*v.* și: Regulamentul (UE) nr. 2016/679, Legea nr. 190/2018] 20; 84; 135; 307; 368; 378; 382-383; 386; 586-588
- de identificare 65; 67; 114; 337; 532
- de localizare 368-369; 374; 377; 380-381; 387-388
- informatice 31; 79; 98-100; 106-107; 111; 119; 121; 133; 145-146; 157; 179; 191-192; 201; 229; 331; 369; 412
  - date conținut 134; 231-232; 234; 259-261; 367
  - date de trafic/privind traficul informațional/*traffic data* 231-232; 368-369; 373; 377-380; 387-388

Decizia Curții Constituționale nr.
- 440/2014 331; 363-368; 371-372; 382; 384-388; 558
- 641/2014 454
- 51/2016 41; 80-81; 83-90; 112; 165; 170; 176; 178; 182; 186-187; 202; 205; 207-208; 210; 215; 217; 221-222; 226; 446
- 244/2017 122; 124; 129-132; 164-165; 173; 179; 398
- 302/2017 40; 87-88; 164-165; 169-171; 209
- 554/2017 77; 168; 170; 175
- 91/2018 543; 547
- 802/2018 544
- 26/2019 87-88; 183; 205-209
- 250/2019 166
- 55/2020 136; 180; 581-582

declasificarea mandatului 564; 574; 580-581
descoperirea unei fapte noi 70; 420; 448
dezvăluirea conținutului tranzacțiilor financiare 312
Digital Rights Ireland și alții 182; 364; 367; 382-386; 388; 395; 558
digitalizarea procesului penal 104
dismissal of the case 471
dispozitiv – noțiune 229
dispozitive mobile tip Stingray 83; 190; 192; 200; 203-205; 218
divulgare de informații către presă într-un dosar de urmărire penală
- *Guja c. Moldova* 29

divulgarea informațiilor secrete de serviciu 84; 247; 483
drept de semnătură pe conturi 326
dreptul la apărare 11; 15; 37; 39; 43-44; 115; 121; 126; 128; 141-143; 147-149; 151; 153-154; 163; 166; 174; 210; 264; 453; 466
dreptul la domiciliu 13; 18; 35-38; 147; 268
- conceptul de „domiciliu" 35

dreptul la liberă exprimare/libertatea de exprimare 13; 25-29; 268; 384
- relația dintre dreptul la libertatea de exprimare și dreptul la viață privată 26
- caracterul relativ al dreptului la liberă exprimare 27
- încălcarea dreptului la liberă exprimare
  - *Sanoma Uitgevers B.V. c. Olanda* 28

dreptul la un proces echitabil 18; 39-44; 73; 143; 213; 215; 458; 461; 507
dreptul persoanei supravegheate de a fi informată cu privire la măsură 122-125
- *Pruteanu c. România* 33; 124; 130; 145
- *Roman Zakharov c. Rusia* 124; 589

E
echipe operative comune 88; 207; 209; 214; 219
excepție de neconstituționalitate 84; 129; 173; 384; 396
expertiză
- criminalistică 120
- informatică 134

extras(e) de cont 327; 329; 336; 343-344; 361

F
filaj 46; 112; 212; 216-217; 270-271; 279; 285-286; 290-291; 301; 527; 562
fishing expeditions 46; 177
flash-roll 442
flagrant (*v.* și organizarea flagrantului) 74; 272; 490; 497; 501; 507-508; 510; 522; 524; 530; 539
fotografierea – concept 270-271
furnizor de rețele publice de comunicații electronice 232-233; 235; 364

furnizor de servicii de certificare acreditat 98; 100; 103; 119
furnizor de servicii de comunicații destinate publicului 235; 299; 380
furnizor de servicii de comunicații electronice destinate publicului 83; 198; 229; 232-235; 254; 364; 376-377
furtul 53; 195; 278; 365; 391-392; 470

G
Govell c. Marea Britanie 8; 185; 268-269
GPS (*Global Positioning System*) 4-5; 23; 82; 113; 269; 294; 298-303; 305-308; 559; 562
gravitatea infracțiunii 52-53; 55; 59; 139; 194-195; 238; 278; 332; 393; 417; 436-437; 495; 497; 580
grup infracțional organizat 57; 184; 365; 417; 436; 458; 460; 464; 466; 472; 475-477; 479-480; 486; 489; 516

H
hărțuire 27; 45; 133; 289
hărțuire online 249
H.K./Prokuratuur 391-392

I
identitate – concept 106
implicare în activități infracționale 435
importanța informațiilor ori a probelor ce urmează a fi obținute 55; 57-58; 194-195; 238; 278; 332; 393; 417; 436-437; 497
informatorul – noțiune 468-470
infracțiune gravă – concept 207-208; 213; 365
infracțiuni conexe 436
integritatea datelor informatice 102-104; 119-121; 192; 235-236; 241; 243; 257; 260
interpret (*v.* și traducător autorizat) 116; 218
intrusive surveillance 282

Î
încetarea măsurii utilizării investigatorilor sub acoperire și a colaboratorilor 441
înregistrări – noțiune 133-134
înregistrări în mediu ambiental 5; 41; 81; 149; 161; 183; 269-270; 288; 300; 449; 586
înșelăciunea 250; 365

K
Khan c. Marea Britanie 8; 22; 40-41; 185; 269-270; 282
Kruslin c. Franța 8; 24; 32; 185; 301; 564

L
legendare 213
libertatea de conștiință 184; 268
livrare supravegheată
- curată 513; 534
- murdară sau efectivă 534
livrare supravegheată transfrontalieră 526-530; 532; 534-535
localizare – noțiune 301
luarea de mită 58-59; 184; 195; 272; 278; 491; 508
lucrători specializați din cadrul poliției – concept 81

M
Malone c. Marea Britanie 8; 23-24; 30-31; 182; 185
mandat de obținere a datelor privind tranzacțiile financiare ale unei persoane 336-337; 341
martor denunțător 467; 475
martor protejat 482-486
- măsuri de protecție 485
- măsuri de asistență 486
metadate 143; 182; 299; 412
Milinienė c. Lituania 510
minută 71; 169; 178; 197; 280; 336; 420; 448; 573

N
note de redare 89; 202; 212; 578; 581; 586
nulitate
- absolută 40; 87-89; 152-153; 164-166; 169; 171-172; 174; 210; 221; 442
- derivată 47; 175; 583
- relativă 40-41; 76-77; 86; 91; 153; 165; 168-173; 325

O
obținerea în timp real a tranzacțiilor financiare ale unei persoane 344

obținerea înscrisurilor referitoare la tranzacțiile sau operațiunile financiare ale unei persoane 345
operațiuni sub acoperire
- de scurtă durată/ocazionale 464
- de durată medie 464
- de durată lungă 464
- adâncă (*deep undercover*) 464-465; 491

P

particularitățile cauzei 55; 57-58; 194-195; 238; 269; 278; 331-332; 393; 417; 436-437; 497; 567
percheziția domiciliară 11; 74; 274; 358; 411; 413-414; 560
percheziționare – noțiune 424
poștă 401
- Legea telegrafo-poștală 403
- serviciu(i) poștal(e) 407-408
  - furnizor de servicii poștale 408-409; 412; 414; 421; 423; 425; 427
    - furnizor de serviciu universal
      - Compania Națională Poșta Română S.A. 408
    - alți furnizori de servicii poștale 409
- trimitere poștală – noțiune 407-410; 562
- Uniunea Poștală Universală 401

predare – noțiune 423
privileged communications 471
probe
- analogice 105
- derivate 78; 153-154; 156; 158; 276; 436; 446; 457-458; 460-461; 474; 487; 489; 503; 510; 521-522
- directe 12; 58; 158; 160; 180; 184; 195; 226; 268; 278; 295; 311; 332; 352
- indirecte 58; 158; 184; 195; 268; 294; 298; 310; 372; 374; 474

procedură specială unică de autorizare 439
proces-verbal de
- consemnare a activităților de supraveghere tehnică 75; 85; 90; 94; 103; 107-112; 114-115; 118; 127-128; 132; 140; 153; 165; 171; 175; 201; 285-286; 306; 502
- redare rezumativă a activităților de supraveghere tehnică 75; 78; 339; 422; 452

proporționalitate(a) 2; 8; 14; 19; 38; 46-47; 5458; 64; 66; 71; 124; 137-138; 161; 163; 177; 179; 194-195; 238; 278; 318; 331-332; 357; 363; 374-375; 393; 412; 417; 436-437; 495; 497; 505; 531; 565; 567-568; 570; 590
- control de proporționalitate 14; 32; 36; 67; 178; 372; 383; 492; 525; 547-548; 565

propunerea organului de cercetare penală – terminologie 440
provocarea infracțiunii
- clasificare:
  - provocarea de către un agent al statului 504
  - provocarea de către un privat cu interese comerciale 505
    - *Shannon c. Marea Britanie*
  - provocarea realizată de un informator 505
    - *Regina c. Ian Anthony Jones*

punct de acces la un sistem informatic 117; 197-198; 200-201; 240-242; 248; 250; 265; 280; 364
- punct de acces rezidențial 379

R

rechizitoriu 69; 127-128
rețea de comunicații electronice – noțiune 233; 376
rețea de informatori 488
reținere – concept 423
rolling wiretap (*v.* și interceptare rostogolită) 197

S

screenshot (*v.* și captură/i de ecran) 134; 236; 240; 258
secret de stat 564; 586
secret(ul) bancar 313; 320-321; 324; 328; 331; 342; 353; 358-359; 362-363; 563
secretul corespondenței 13; 18; 23; 30-35; 384; 402-403; 405-406; 408; 411-412; 415; 420; 424; 427; 544; 562
- *Campbell c. Marea Britanie* 33

- infracțiunea de violarea secretului corespondenței 45; 133; 194
semnătura electronică 98-99; 102-103; 120; 397
semnătura electronică extinsă 99-104; 106-107; 119-120; 201
serviciu de comunicații electronice – noțiune 233; 376
spălarea banilor 52; 161; 187; 311-315; 332; 335; 344; 391; 426; 435; 440; 494-496; 500
spionaj 1; 181; 267; 431; 542; 561
subsidiaritate(a) 2; 7; 14; 19; 24; 33; 46-47; 52; 56; 60-61; 63-64; 74; 124; 134; 138; 163; 178; 196; 238; 279; 317-318; 333; 358; 392; 418; 421; 436; 440; 498; 565-566; 590
suport
- original 106-107; 118
- de stocare a datelor informatice *c.* sistem informatic – concepte 230
supraveghere video cu recunoaștere facială 26; 273; 290-291; 363-364
supravegherea conturilor bancare 314
supravegherea tehnică
- clasificare 275-276
  - în funcție de locul desfășurării activității:
    - supraveghere publică
      - sisteme (*v.* și camere) de supraveghere publică 1; 23; 135; 273; 275; 286; 290; 363
    - supraveghere în spații private 36; 273; 290; 295
  - în funcție de gradul de continuare a supravegherii:
    - supraveghere secvențială 216; 287
    - supraveghere continuă 178
  - în funcție de natura mijlocului de probă care va rezulta din supravegherea tehnică:
    - audio
    - video
    - audiovideo
  - în funcție de procedeul probatoriu care va conduce la obținerea probei:
    - primară
    - derivată 287
suspiciune rezonabilă (*v.* și *reasonable suspicion*) 2; 46-50; 54; 64-68; 74; 78; 91; 154; 177-178; 196; 239; 280; 319; 330; 334; 364-365; 368; 390; 416; 419; 435-436; 494-496; 505; 565; 581

Ș

șantaj sexual (*sextortion*) 249

T

tehnică operativă 81; 262; 283; 308; 450; 453; 464; 467; 482
Tele2 Sverige AB, Secretary of State for the Home Department și alții 182; 368; 370; 382; 384; 386-389; 391-392; 398; 497
termen
- de decădere 76-77; 128; 168; 339
- de prescripție 370
- de recomandare 76; 125
terorism 3; 27; 52; 109; 161; 187; 207; 213; 291; 367; 391; 426; 435; 440; 463; 488; 494; 496; 500; 504; 550
testarea poligraf 402
token 99-100
trafic de influență 58; 491; 510
transport de droguri 272; 470
trimiteri de corespondență 407; 409; 411-412

U

unitate de fond 324; 337; 344; 354
urmărire – noțiune 301
utilizator(i) 189; 202; 224; 229; 230-232; 234; 236; 242; 244-245; 247; 250; 252-253; 255-256; 258; 261; 307; 326; 364; 366; 369-371; 379-381; 385; 397
- utilizator Skype 377
  - *Skype Communications c. IBPT*

V

violarea secretului corespondenței 45; 133; 194; 403