

George Zlati

Tratat de criminalitate informatică

Vol. I

Cuprins

Prefață.....	XXV
Listă de abrevieri	XXVII
Introducere.....	1
Titlul I. Conceptul de „criminalitate informatică” și aspecte terminologice	5
Capitolul I. Criminalitatea informatică	5
Secțiunea 1. Conceptul de „criminalitate informatică”	5
§1. Infracțiuni îndreptate împotriva sistemelor ori datelor informatice.	
Sistemul informatic ca obiect al conduitei infracționale	15
§2. Infracțiuni unde sistemul informatic este doar un mijloc pentru a comite	
infracțiunea. Sistemul informatic ca subiect al conduitei infracționale	15
§3. Conduite infracționale ce sunt incidente pentru comiterea	
altor infracțiuni tradiționale.....	16
Secțiunea a 2-a. Caracterele și tratamentul juridic al criminalității informatice	18
Secțiunea a 3-a. Statele pionier din perspectiva legiferării în domeniul criminalității	
informatice.....	20
§1. SUA	21
§2. Germania	21
§3. Austria	23
§4. Italia	25
§5. Alte sisteme de drept	28
Capitolul II. Aspecte terminologice.....	29
Secțiunea 1. Noțiunea de „sistem informatic”	29
§1. Definiția sistemului informatic în instrumentele juridice internaționale	
și europene.....	30
1.1. Convenția Consiliului Europei privind criminalitatea informatică	
și Raportul explicativ al Convenției privind criminalitatea informatică	30
1.2. Decizia-cadru 2005/222/JAI privind atacurile împotriva sistemelor	
informatice [abrogată].....	33
1.3. Directiva 2013/40/UE privind atacurile împotriva sistemelor informatice	
[în vigoare].....	33
§2. Definiția sistemului informatic în dreptul intern	36
2.1. Definiția sistemului informatic în art. 35 din Legea nr. 161/2003	37
2.2. Definiția sistemului informatic în art. 181 alin. (1) C.pen.	37
§3. Definiția sistemului informatic în dreptul comparat	38
3.1. Sisteme de drept în care noțiunea de „sistem informatic” beneficiază	
de o definiție legală	39

3.1.1. Definiția sistemului informatic în SUA – la nivel federal.....	39
3.1.2. Definiția sistemului informatic în SUA – la nivel statal	40
3.1.3. Definiția sistemului informatic în alte state	41
3.2. Sisteme de drept în care noțiunea de „sistem informatic” nu beneficiază de o definiție legală	42
§4. Sistemul informatic în jurisprudența instanțelor naționale și a Curții Constituționale	45
4.1. Sistemul informatic și recursul în interesul legii – Decizia ICCJ nr. 15/2013	45
4.2. Interpretarea noțiunii de „sistem informatic” în practica judiciară.....	47
4.3. Sistemul informatic în jurisprudența Curții Constituționale	49
4.3.1. Aspecte generale cu privire la Decizia CCR nr. 633/2017.....	49
4.3.2. Criticile de neconstituționalitate	49
4.3.3. Considerentele Curții Constituționale.....	51
§5. Importanța calificării corecte a unui dispozitiv ca fiind un sistem informatic.....	54
5.1. Relevanța noțiunii de „sistem informatic” din perspectiva dreptului penal substanțial.....	54
5.2. Relevanța noțiunii de „sistem informatic” din perspectiva dreptului procesual penal.....	56
5.3. Relevanța noțiunii de „sistem informatic” din perspectiva tehnicii legislative.....	56
§6. Analiza criteriilor legale desprinse din definiția sistemului informatic	58
6.1. Sistemul informatic ca dispozitiv.....	58
6.2. Prelucrarea automată a datelor informatice	62
6.3. Prelucrarea automată a datelor prin intermediul unui program informatic	64
§7. Exemple de sisteme informatice și exemple problematice	66
7.1. Servere prin care se furnizează anumite servicii ori pe care sunt găzduite anumite pagini web	66
7.2. Sistemul electronic de tranzacționare pe piața de capital.....	69
7.3. Bazele de date	69
7.4. Paginile web.....	70
7.5. Rețelele de socializare.....	71
7.6. Bancomatele (<i>automated teller machine</i> – ATM)	72
7.7. Terminalele POS (<i>point of sale</i>).....	73
7.8. Dispozitivul tip <i>skimmer</i>	74
7.9. Telefoanele mobile inteligente (<i>smartphones</i>)	75
7.10. Terminalele de comunicații	76
7.11. Ceasurile inteligente (<i>smartwatch</i>).....	78
7.12. Televizoarele inteligente (Smart tv).....	79
7.13. Imprimanta, faxul și scanner-ul.....	79
7.14. Reportofoanele digitale.....	80
7.15. Dispozitivele de distribuire automată a biletelor.....	81
7.16. Camerele de supraveghere digitale.....	81
7.17. Aparatele de jocuri de noroc	82
7.18. Dispozitivele din categoria <i>Internet of Things</i> (IoT)	83
7.19. Cartela SIM (<i>Subscriber Identity Module</i>).....	84

7.20. Instrumentele de plată electronică (cardurile bancare).....	85
7.21. Autovehiculele moderne	86
7.22. Internetul	87
7.23. Rețeaua de comunicații electronice.....	87
§8. O reconceptualizare a noțiunii de „sistem informatic”?.....	89
8.1. Redefinirea noțiunii de „sistem informatic”	90
8.1.1. Simplificarea definiției	90
8.1.2. Restrângerea definiției prin raportare la funcția principală a dispozitivului.....	91
8.1.3. Restrângerea definiției prin raportare la autonomia dispozitivului.....	92
8.1.4. Restrângerea definiției prin introducerea unui criteriu negativ.....	92
8.1.5. Restrângerea definiției prin introducerea unei liste negative	93
8.2. O interpretare restrictivă a definiției actuale.....	93
8.2.1. Soluționarea controverselor privind utilizarea unor aparate casnice	95
8.2.2. Soluționarea controverselor privind utilizarea unui televizor inteligent.....	95
8.2.3. Soluționarea controverselor privind interacțiunea cu un mijloc de stocare	96
8.2.4. Soluționarea controverselor privind utilizarea unei multifuncționale.....	96
Secțiunea a 2-a. Noțiunea de „mijloc de stocare a datelor informatice”	96
§1. Definiția noțiunii de „mijloc de stocare a datelor informatice”	96
§2. Relevanța noțiunii de „sistem informatic” din perspectiva dreptului procesual penal și a dreptului substanțial penal.....	97
§3. Exemple relevante de mijloace (suport) de stocare a datelor informatice	98
3.1. Suportii optici (CD, DVD, Blu-Ray etc.)	98
3.2. Hard disk, memory card, memory stick.....	98
3.3. Instrumentele de plată electronică (cardul bancar)	98
3.4. Cartela SIM.....	99
Secțiunea a 3-a. Noțiunile de „program informatic” și „date informatice”	100
§1. Definiția „datelor informatice” și a „programelor informatice” în instrumentele juridice internaționale și europene.....	100
1.1. Convenția privind criminalitatea informatică, Raportul explicativ al Convenției privind criminalitatea informatică și Decizia-cadru 2005/222/JAI privind atacurile împotriva sistemelor informatice [abrogată]	100
1.2. Directiva 2013/40/UE privind atacurile împotriva sistemelor informatice.....	101
§2. Definiția „programelor” și „datelor informatice” în dreptul intern	101
2.1. Definiția „programelor” și „datelor informatice” în art. 35 din Legea nr. 161/2003	101
2.2. Definiția „programelor” și „datelor informatice” în art. 181 alin. (2) C.pen.....	101
2.3. Definiția „datelor informatice” în Legea nr. 455/2001	102
§3. Exemple de date informatice.....	102
3.1. Calificarea unei înregistrări tehnice drept „date informatice”	103
3.2. Calificarea juridică a informației stocate pe o bandă magnetică.....	103
§4. Raportul dintre datele informatice și programele informatice.....	103
4.1. Exemple de programe informatice licite.....	104
4.2. Exemple de programe informatice malițioase	104
4.3. Firmware	104

§5. Importanța identificării unui program informatic.....	105
Secțiunea a 4-a. Noțiunea de „instrument de plată electronică”	105
§1. Definiția instrumentelor de plată în dreptul european.....	105
1.1. Decizia-cadru 2001/413/JAI de combatere a fraudei și a falsificării mijloacelor de plată, altele decât numerarul [abrogată]	106
1.2. Directiva (UE) 2019/713 privind combaterea fraudelor și a contrafacerii în legătură cu mijloacele de plată fără numerar și de înlocuire a Deciziei-cadru 2001/413/JAI a Consiliului.....	106
§2. Definiția instrumentului de plată electronică în dreptul intern.....	107
Titlul II. Accesul neautorizat la un sistem informatic (art. 360 C.pen.).....	111
Prezentare generală.....	111
Capitolul I. Raportul dintre reglementarea națională și instrumentele juridice supranaționale	112
Secțiunea 1. Sursa de inspirație a legiuitorului național.....	112
§1. Recomandarea Consiliului Europei din 1989	112
§2. Convenția Consiliului Europei privind Criminalitatea informatică din 2001 și Raportul explicativ al acesteia	114
§3. Decizia-cadru 2005/2002/JAI privind atacurile împotriva sistemelor informatice [abrogată].....	116
§4. Directiva 2013/40/EU privind atacurile împotriva sistemelor informatice [în vigoare]	117
Secțiunea a 2-a. Modul de transpunere în dreptul intern	118
§1. Diferențe și observații critice	118
§2. O posibilă încălcare a marjei de apreciere?	120
Capitolul II. Decizii ale Curții Constituționale, Recursuri în interesul legii și Decizii ale Curții Europene a Drepturilor Omului	125
Secțiunea 1. Decizii ale Curții Constituționale.....	125
§1. Decizia CCR nr. 183/2018 (despre măsurile de securitate)	125
§2. Decizia CCR nr. 353/2018 (despre accesul neautorizat)	127
Secțiunea a 2-a. Recursul în interesul legii – Decizia ICCJ nr. 15/2013.....	128
§1. Analiză punctuală a dispozitivului Deciziei nr. 15/2013	128
§2. Relevanța Deciziei nr. 15/2013 din perspectiva noțiunii de „acces la un sistem informatic”.....	129
2.1. Fondul problemei	129
2.2. Opiniile exprimate cu privire la relația dintre montarea <i>skimmer</i> -ului la bancomat și accesul neautorizat la acesta.....	130
2.2.1. Opinia procurorului general	130
2.2.2. Opinia judecătorului raportor	131
2.2.3. Opinia Facultăților de Drept și a Institutului de Cercetări Juridice din cadrul Academiei Române	131
2.3. Considerentele Înaltei Curți de Casație și Justiție	132
2.4. Critici punctuale la adresa deciziei ICCJ nr. 15/2013	133

Secțiunea a 3-a. Curtea Europeană a Drepturilor Omului (<i>Bărbulescu c. României</i>).....	134
§1. Generalități	134
§2. Starea de fapt relevantă	135
§3. Considerentele Curții	135
§4. Câteva concluzii generale	135
4.1. Cu privire la accesul discreționar la date	136
4.2. Cu privire la existența unei notificări aduse la cunoștința angajatului.....	136
4.3. Cu privire la proporționalitatea și necesitatea monitorizării	136
§5. Efectele hotărârii <i>Bărbulescu</i> cu privire la incidența art. 360 C.pen.	137
Capitolul III. Rațiunea și necesitatea incriminării.....	139
Secțiunea 1. Necesitatea unei incriminări autonome.....	139
§1. Raportul cu violarea de domiciliu	139
§2. Raportul cu violarea secretului corespondenței	141
§3. Necesitatea unei incriminări autonome.....	142
Secțiunea a 2-a. Limitele incriminării.....	143
§1. Limitele accesului neautorizat în forma de bază – art. 360 alin. (1) C.pen.....	143
§2. Agravanta accesului neautorizat cu scopul special de a obține date informatice – art. 360 alin. (2) C.pen.	144
§3. Agravanta accesului neautorizat la un sistem informatic protejat de măsuri de securitate – art. 360 alin. (3) C.pen.	145
Capitolul IV. Analiza conținutului infracțiunii de acces neautorizat la un sistem informatic.....	147
Secțiunea 1. Obiectul juridic	147
Secțiunea a 2-a. Natura infracțiunii de acces neautorizat la un sistem informatic	149
Secțiunea a 3-a. Subiecții infracțiunii	151
§1. Subiectul activ	151
§2. Subiectul pasiv.....	153
2.1. Identificarea subiectului pasiv.....	153
2.2. Teoria titularului sistemului informatic – existența unui drept de folosință consolidat	157
2.3. Există un subiect pasiv colectiv?	159
2.4. Există un subiect pasiv secundar?	160
2.5. Pluralitatea de subiecți pasivi vs. pluralitatea de sisteme informatice accesate.....	160
2.5.1. Situația pluralității de subiecți pasivi, dar a unității sistemului informatic accesat	162
2.5.2. Situația pluralității de subiecți pasivi și a pluralității de sisteme informatice accesate	162
2.5.3. Situația unității de subiect pasiv, dar a pluralității de sisteme informatice accesate	163
2.5.4. Situația partajării accesului la sistemul informatic între mai multe persoane	164
2.6. Concluzii.....	164
2.6.1. Cu privire la consecințele pluralității de subiecți pasivi/sisteme informatice	164
2.6.2. Cu privire la consecințele identificării corecte a subiectului pasiv	165

Secțiunea a 4-a. Latura obiectivă. Cadrul general	165
§1. Tipologia accesului neautorizat la un sistem informatic, în dreptul comparat	166
§2. Sistemul informatic vs. mijlocul de stocare a datelor informatice	169
2.1. Contextualizare	169
2.2. Ipoteza în care mijlocul de stocare este parte integrantă a sistemului informatic accesat	171
2.3. Ipoteza în care mijlocul de stocare este extras fizic și conectat la sistemul informatic al agentului	171
2.4. Ipoteza în care se accesează un mijloc de stocare de la distanță	172
Secțiunea a 5-a. Conduita comisivă – accesul (la un sistem informatic)	173
§1. Cadrul general	173
1.1. Lipsa unei definiții legale în dreptul penal substanțial	173
1.2. Art. 138 alin. (3) C.proc.pen. – un punct de plecare pentru definirea noțiunii de „acces”?	174
1.3. Accesul – o conduită comisivă	175
§2. Interpretarea noțiunii	176
2.1. Interpretarea gramaticală	177
2.2. Interpretarea legală (în dreptul comparat), doctrinară și jurisprudențială	178
2.2.1. Definiția legală a noțiunii de „acces” în dreptul comparat	178
2.2.2. Noțiunea de „acces” în literatura de specialitate și în jurisprudență	179
A) Definiții doctrinare	179
B) Definiții jurisprudențiale	181
2.3. Decizia ICCJ nr. 15/2013 – recurs în interesul legii	183
2.4. Conceptualizarea noțiunii de „acces”	183
2.4.1. Cadrul general	183
2.4.2. Perspectiva „internă” a accesului [sau a „realității virtuale”]	184
2.4.3. Perspectiva „externă” a accesului [sau a „realității fizice”]	184
2.4.4. Identificarea unor trăsături esențiale ale accesului	185
A) Existența unei interacțiuni logice cu un sistem informatic	185
B) Urmarea interacțiunii logice – posibilitatea de a beneficia de funcțiile ori/și resursele sistemului informatic	186
Secțiunea a 6-a. Conduita incriminată din perspectiva art. 360 c.pen.	187
§1. Cadrul general	187
§2. Accesul propriu-zis – reglementat expres	188
§3. Depășirea limitelor autorizării – reglementat prin art. 35 alin. (2) din Legea nr. 161/2003?	188
§4. Menținerea accesului după retragerea ori expirarea autorizării – ipoteză nereglementată	192
§5. Accesul nelimitat vs. accesul limitat (în tot sau doar într-o parte a sistemului informatic)	193
Secțiunea a 7-a. Ipoteze particulare de acces la un sistem informatic	193
§1. Accesul propriu-zis la un sistem informatic	194
1.1. Autentificarea în cadrul unui sistem informatic	194
1.2. Folosirea de la distanță [<i>remote access</i>] a unui sistem informatic prin intermediul Team Viewer	195

1.3. Accesarea unui cont bancar online.....	196
1.4. Autentificarea (accesul) fără drept la interfața de administrare a unei pagini web	197
1.5. Accesarea unui bancomat prin intermediul unui instrument de plată electronică	198
1.6. Alterarea fără drept a unei pagini web, prin înlocuirea ori modificarea modului în care aceasta este afișată [în engleză, <i>defacing</i>]	199
§2. Depășirea limitelor autorizării ori menținerea neautorizată a accesului.....	199
2.1. Folosirea în continuare a unei baze de date prin intermediul unui cod de acces, deși perioada de încercare (<i>trial access</i>) a expirat.....	200
2.2. Accesarea unei baze de date în mod autorizat, continuată de cereri SQL [<i>SQL queries</i>], în vederea accesării unor informații privilegiate	200
2.3. Continuarea accesului la un sistem informatic fără plata redevenței	201
2.4. Primirea datelor de autentificare într-un cont de e-mail pentru o verificare punctuală și omisiunea cu intenție a deconectării	201
§3. Ipoteze particulare ce nu vizează un acces la un sistem informatic.....	201
3.1. Transmiterea unui e-mail	201
3.2. Transmiterea unui program informatic.....	202
3.3. Atacurile de tip <i>denial-of-service</i> [<i>DoS attack</i>].....	203
3.4. Scanarea porturilor [<i>port scanning</i>].....	203
3.5. Obținerea de date informatice prin <i>phishing</i>	204
3.6. Contrafacerea de pagini web	205
3.7. Punerea în vânzare, pe Internet, a unor bunuri fictive	205
3.8. Captarea informației lizibile pe monitor	206
3.9. Interacțiunea fizică cu un bancomat	207
3.10. Efectuarea de plăți la un terminal POS.....	207
3.11. Efectuarea de plăți online	209
§4. Ipoteze particulare ce ar putea ridica probleme deosebite.....	210
4.1. Accesarea unor adrese URL (nepublice) ale unor pagini web (publice)	210
4.2. Copierea fără drept de date informatice din sistemul informatic aparținând unei terțe persoane	212
4.3. Copierea fără drept de date informatice într-un sistem informatic aparținând unei terțe persoane	212
4.4. Utilizarea unui program informatic tip <i>keylogger</i> , pentru a intercepta datele introduse de la tastatură de către victimă	213
4.5. Restricționarea accesului la anumite date informatice de către administratorul sistemului informatic.....	214
4.6. Infectarea unor sisteme informatice cu un program malițios (virus)	214
Secțiunea a 8-a. Lipsa autorizării – noțiunea „fără drept”.....	215
§1. Cadrul general.....	215
§2. Noțiunea „fără drept” și alte noțiuni interschimbabile.....	216
§3. Ipoteze particulare ale accesului „fără drept” în doctrină și jurisprudență	217
3.1. Lipsa autorizării exprese din partea administratorului de rețea.....	217
3.2. Utilizarea fără drept a unui card de carburant.....	217

3.3. Introducerea de anunțuri fictive pe platforma eBay.....	218
3.4. Crearea de conturi fictive pe platforma eBay.....	218
3.5. Accesarea, de către un funcționar bancar, a aplicației „CARD PIN” și „CARD FORM”, prin utilizarea fără drept a unui cod de acces	219
3.6. Accesarea, de către un funcționar bancar, a unei componente a sistemului informatic care era restricționată pentru categoria de angajați din care acesta făcea parte	219
3.7. Accesarea, de către angajat, a unei pagini web restricționate, cu un scop fraudulos	219
3.8. Utilizarea unui laptop bun comun al soților	220
3.9. Accesarea contului de Internet Banking de către unul dintre soți	220
3.10. Accesarea unui cont de e-mail ori de Facebook de către unul dintre soți.....	221
3.11. Accesarea contului de Skype al soției.....	221
3.12. Accesarea unui cont de e-mail prin folosirea unui parole primite anterior	222
3.13. Verificarea situației fiscale a unor contribuabili din altă jurisdicție.....	222
3.14. Transferul de materiale pornografice cu minori pe sistemul informatic folosit de angajat	222
\$4. Orientări jurisprudențiale relevante în dreptul comparat.....	222
4.1. Jurisprudența Curții de Casație italiene.....	222
4.2. Teorii ale accesului „fără drept” în dreptul american	225
4.2.1. Teoria contractuală [<i>contract-based approach</i>]	226
4.2.2. Teoria încălcării unei obligații de loialitate ori fiduciare [<i>agency-based approach</i>]	230
4.2.3. Teoria depășirii unor măsuri de securitate [<i>code-based approach</i>]	231
4.2.4. Teoria revocării autorizării.....	232
\$5. Identificarea unui <i>framework</i> rezonabil pentru noțiunea „fără drept”	234
5.1. Stabilirea unor puncte de reper.....	234
5.2. Soluționarea limitelor autorizării pentru accesul între soți.....	236
5.3. Accesul la sistemul informatic al copilului.....	237
Secțiunea a 9-a. Urmarea.....	237
Secțiunea a 10-a. Vinovăția (latura subiectivă).....	238
Secțiunea a 11-a. Momentul consumării și tentative	239
\$1. Cadrul general.....	239
\$2. Momentul consumării infracțiunii.....	240
\$3. Ipoteze ce se situează în sfera tentativei	241
3.1. Simpla pornire a unui sistem informatic	241
3.2. Inițializarea [<i>boot-area</i>] unui sistem de operare de pe un CD sau USB stick.....	242
3.3. Depășirea parțială a măsurilor de securitate ce împiedică cu totul accesul la sistemul informatic.....	243
3.4. Accesarea bancomatului fără a fi operațional serverul bancar	243
\$4. Ipoteze care se situează în sfera actelor preparatorii	244
\$5. Teoria tentativei neidonee – o soluție de compromis	245
\$6. Desistarea și împiedicarea producerii rezultatului	246
6.1. Desistarea.....	246
6.2. Împiedicarea producerii rezultatului.....	247

Secțiunea a 12-a. Formele agravate ale accesului ilegal la un sistem informatic.....	247
§1. Scopul obținerii de date informatice [art. 360 alin. (2) C.pen.]	247
1.1. Cadrul general.....	247
1.2. Conținutul scopului special.....	248
1.3. Relația cu alte infracțiuni.....	249
§2. Încălcarea măsurilor de securitate.....	250
2.1. Cadrul general.....	250
2.2. Rațiunea agravantei	251
2.3. Natura măsurilor de securitate – fizice, organizaționale ori doar logice?	253
2.4. Caracteristicile măsurilor de securitate	256
2.4.1. Natura și specificul măsurilor de securitate	256
2.4.2. Controlul accesului.....	257
2.4.3. Scopul controlului accesului	258
2.4.4. Efectivitatea măsurilor de securitate.....	258
2.4.5. Fiabilitatea (eficacitatea) măsurilor de securitate.....	259
2.5. Proceduri de interdicere ori de restricționare a accesului	260
2.5.1. Parole sau coduri de acces	260
2.5.2. Criptarea datelor informatice.....	261
2.5.3. Utilizarea unor elemente biometrice	261
2.5.4. Setarea adreselor MAC [<i>media access control adress</i>]	261
2.5.5. Securizarea unui browser web	262
2.6. Dispozitive de interdicere ori restricționare a accesului	262
2.7. Programe informatice ce interzic ori restricționează accesul	262
2.8. Modalitățile prin care sunt „încălcate” măsurile de securitate	263
2.8.1. Obținerea frauduloasă a datelor de la victimă	263
2.8.2. Folosirea datelor de autentificare după pierderea autorizării	263
2.8.3. Utilizarea unor date reale în vederea autentificării	264
2.9. Consecințele inexistenței unor măsuri de securitate.....	265
Capitolul V. Raportul infracțiunii de acces neautorizat la un sistem informatic	
cu alte infracțiuni.....	266
Secțiunea 1. Relația cu alte infracțiuni informatice	266
§1. Relația cu falsul informatic (art. 325 C.pen.)	266
§2. Relația cu fraudă informatică (art. 249 C.pen.)	266
§3. Relația cu alterarea integrității datelor informatice (art. 362 C.pen.).....	267
§4. Relația cu operațiuni ilegale cu dispozitive sau programe informatice (art. 365 C.pen.)	267
Secțiunea a 2-a. Relația cu alte infracțiuni din Codul penal.....	268
§1. Relația cu infracțiunea de violare a vieții private (art. 226 C.pen.).....	268
§2. Relația cu infracțiunea de furt (art. 228 C.pen.).....	269
2.1. Accesarea sistemului informatic ulterior momentului sustragerii acestuia	269
2.2. Sustragerea unor componente din diferite sisteme informatice și accesarea sistemului informatic alcătuit din acestea	271
§3. Relația cu infracțiunea de furt de folosință [art. 230 alin. (2) C.pen.].....	271
§4. Relația cu infracțiunea de tănuire (art. 270 C.pen.).....	272

§5. Relația cu infracțiunea de violare a secretului corespondenței [art. 302 alin. (1) C.pen.]	272
5.1. Aplicabilitatea art. 360 C.pen. – accesarea serverului de e-mail	274
5.1.1. Accesarea contului de poștă electronică prin intermediul unui browser web.....	275
5.1.2. Accesarea contului de poștă electronică prin intermediul unei aplicații de poștă electronică	277
5.2. Aplicabilitatea art. 302 alin. (1) C.pen. – deschiderea unei corespondențe sau a unei comunicări?	277
5.3. Concurs de infracțiuni sau de calificări?	278
§6. Relația cu infracțiunea privind efectuarea de operațiuni financiare în mod fraudulos [art. 250 alin. (1) C.pen.]	279
§7. Relația cu infracțiunea privind fraudă la votul electronic (art. 388 C.pen.)	280
Secțiunea a 3-a. Relația cu alte infracțiuni din legislația specială	281
§1. Relația cu infracțiunile privind drepturile de autor (Legea nr. 8/1996)	281
§2. Relația cu infracțiunile privind concurența neloială (Legea nr. 11/1991).....	282
§3. Relația cu infracțiunea (infracțiunile) de terorism (Legea nr. 535/2004)	283
§4. Relația cu infracțiunea privind supravegherea tehnică neautorizată (Legea nr. 51/1991)	285
Capitolul VI. Reformarea art. 360 C.pen.	286
Secțiunea 1. O reformă conceptuală?	286
Secțiunea a 2-a. Propuneri referitoare la modificarea art. 360 C.pen.	287
§1. Introducerea „încălcării măsurilor de securitate” ca element constitutiv al formei de bază.....	287
§2. Clarificarea noțiunii de „acces” și introducerea unor teze alternative de comitere a faptei.....	287
§3. Extinderea accesului la mijloacele de stocare a datelor informatice	288
§4. Abrogarea art. 360 alin. (2) C.pen.	288
§5. Introducerea unei clauze de subsidiaritate	288
Secțiunea a 3-a. Intervenții <i>de lege ferenda</i> ce ar trebui evitate.....	289
§1. Introducerea plângerii prealabile.....	289
§2. Introducerea unor cauze de atipicitate.....	289
§3. Alte intervenții <i>de lege ferenda</i>	290
Titlul III. Frauda informatică (art. 249 C.pen.)	291
Aspecte introductive	291
Capitolul I. Raportul dintre reglementarea națională și instrumentele juridice supranaționale	293
Secțiunea 1. Sursa de inspirație a legiuitorului național.....	293
§1. Recomandarea Consiliului Europei din 1989 privind infracțiunile informatice.....	293
§2. Convenția Consiliului Europei privind Criminalitatea informatică din 2001 și Raportul explicativ al Convenției privind criminalitatea informatică.....	295
§3. Decizia-cadru 2005/2002/JAI privind atacurile împotriva sistemelor informatice [abrogată]	296

§4. Directiva 2013/40/EU privind atacurile împotriva sistemelor informatice [în vigoare]	297
§5. Decizia-cadru 2001/413/JAI de combatere a fraudei și a falsificării mijloacelor de plată, altele decât numerarul [abrogată]	297
§6. Directiva (UE) 2019/713 privind combaterea fraudelor și a contrafacerii în legătură cu mijloacele de plată fără numerar [în vigoare]	300
Secțiunea a 2-a. Modul de transpunere în dreptul intern	304
§1. Transpunerea în dreptul intern a art. 8 din Convenția privind criminalitatea informatică	304
§2. Transpunerea în dreptul intern a art. 6 din Directiva (UE) 2019/713	305
Capitolul II. Rațiunea și necesitatea incriminării fraudei informatice	308
Capitolul III. Analiza conținutului infracțiunii de fraudă informatică	316
Secțiunea 1. Obiectul infracțiunii	316
§1. Obiectul juridic	316
§2. Obiectul material	321
Secțiunea a 2-a. Subiecții infracțiunii	323
§1. Subiectul activ	323
§2. Subiectul pasiv	326
2.1. Despre pluralitatea de subiecți pasivi	327
2.2. Identificarea subiectului pasiv principal	328
2.3. Existența unui subiect pasiv secundar	330
Secțiunea a 3-a. Latura obiectivă a fraudei informatice	331
§1. Sistemul informatic și datele informatice	332
§2. Modalități de comitere a fraudei informatice	333
2.1. Observații generale	333
2.1.1. Infracțiune cu conținut alternativ	334
2.1.2. Infracțiune comisivă și comisivă prin omisiune	334
2.2. Analiza conduitei comise	337
2.3. Modalitatea introducerii de date informatice	338
2.3.1. Observații generale	338
2.3.2. Situația premisă	338
2.3.3. Ipoteze de comitere a fraudei informatice prin introducerea de date informatice	340
A) Furtul [transferul neautorizat] de monede virtuale	340
B) Achiziționarea de telefoane mobile la valoare zero prin activarea în sistemul informatic a unor reduceri de preț	344
C) Folosirea fără drept a unui tichet pentru reîncărcarea cartelei PrePay	344
D) Transferul de credit pe o cartelă telefonică PrePay	345
E) Mărirea „artificială” a soldului contului bancar	348
F) Obținerea frauduloasă a unui bilet de transport în comun de la un automat de bilete	349
G) Introducerea mențiunii „plătit” cu privire la un anumit debit stocat într-o bază de date	350
H) Folosirea frauduloasă a unei multifuncționale, prin utilizarea unei cartele falsificate	350

2.3.4. Ipoteze privind introducerea de date informatice, problematice din perspectiva reținerii fraudei informatice.....	351
A) Publicarea de anunțuri de vânzare sau licitații fictive pe Internet	351
B) Frauda constând în transmiterea de mesaje prin mijloace de comunicare electronică	356
C) Activitatea de <i>phishing</i> și <i>pharming</i>	358
D) Trimiterea de corespondență electronică nesolicitată (<i>spam</i>)	361
E) Folosirea datelor de identificare ale unui instrument de plată electronică	362
F) Efectuarea de tranzacții offline.....	363
G) Retragera de numerar de la bancomat, imediat după retragerea sumei de la ghișeu bancii.....	364
H) Folosirea unui <i>spyware dialer</i> /utilizarea frauduloasă a serviciului VoIP (<i>Voice over IP</i>)	365
I) Comandarea frauduloasă de produse în calitate de agent de vânzări.....	367
J) Folosirea unor coduri <i>paysafecard</i> pentru efectuarea de plăți online	368
K) „Minarea” de monede virtuale (<i>crypto-jacking</i>)	370
L) Tipărirea unor bancnote falsificate	374
2.4. Modalitatea modificării de date informatice.....	375
2.4.1. Observații generale.....	375
2.4.2. Ipoteze de comitere a fraudei informatice prin modificarea de date informatice	376
A) Efectuarea unui transfer de fonduri	376
B) Modificarea soldului dintr-un cont bancar printr-o intervenție asupra bazei de date.....	376
C) Menținerea ca activat a unui anumit serviciu, în vederea facturării suplimentare.....	377
D) Modificarea „creditului” disponibil pe o platformă online.....	378
E) Rotunjirea sumelor la momentul efectuării unui transfer de fonduri	378
F) Modificarea programului informatic aferent unui aparat de joc de noroc pentru a nu mai fi necesară plata de credite suplimentare.....	379
2.4.3. Ipoteze privind modificarea de date informatice problematice din perspectiva reținerii fraudei informatice	379
A) Alterarea conținutului unei pagini web.....	379
B) Modificarea sumei ce apare afișată pe ecranul terminalului POS	380
C) Modificarea limitei zilnice de retragere de numerar de la bancomat	382
2.5. Modalitatea ștergerii de date informatice.....	383
2.5.1. Observații generale.....	383
2.5.2. Ipoteze de ștergere a datelor informatice relevante din perspectiva art. 249 C.pen.	384
2.5.3. Ipoteze privind ștergerea de date informatice, problematice din perspectiva reținerii fraudei informatice.....	385
A) Ștergerea datelor informatice prin utilizarea unui magnet.....	385
B) Ștergerea unor debite ori a unor debitori din baza de date	386
2.6. Modalitatea restricționării accesului la datele informatice	387
2.6.1. Observații generale.....	387

2.6.2. Ipoteze de restricționare a accesului la datele informatice, care se pliază pe art. 249 C.pen.....	387
2.6.3. Ipoteze privind restricționarea accesului la datele informatice, problematice din perspectiva reținerii fraudei informatice	387
A) Restricționarea accesului la anumite conturi prin schimbarea parolei de acces.....	387
B) Nerestituirea unor sume de bani ajunse din eroare în contul agentului.....	389
C) Conduita tip <i>ransomware</i>	389
2.7. Modalitatea împiedicării în orice mod a funcționării unui sistem informatic	391
2.7.1. Observații generale.....	391
2.7.2. Ipoteze de împiedicare a funcționării unui sistem informatic posibil relevante din perspectiva art. 249 C.pen.	392
A) Manipularea jocurilor electronice de noroc	392
B) Interacțiunea logică cu un bancomat	394
2.7.3. Ipoteze privind împiedicarea în orice mod a funcționării unui sistem informatic, problematice din perspectiva reținerii fraudei informatice	396
A) Interacțiunea fizică cu un bancomat (metoda „furculița”)	396
B) Dezactivarea unor dispozitive electronice de protecție împotriva sustragerii bunului	399
C) Obținerea fără drept a unui bun de la un automat.....	401
D) Atacuri informatice tip DOS (<i>denial-of-service</i>)	401
2.8. Conduita omisivă improprie (comisiva prin omisiune).....	401
§3. Lipsa autorizării – noțiunea „fără drept”	402
§4. Urmarea	404
4.1. Observații generale.....	404
4.2. Producerea unei pagube.....	404
§5. Obținerea unui beneficiu material	409
5.1. Clarificarea noțiunii	409
5.2. Beneficiu material just vs. beneficiu material injust	410
§6. Raportul de cauzalitate.....	411
Secțiunea a 4-a. Vinovăția (latura subiectivă).....	411
§1. Forma de vinovăție	411
§2. Scopul special – obținerea unui beneficiu material.....	412
Secțiunea a 5-a. Unitatea naturală sau legală a infracțiunii.....	414
Secțiunea a 6-a. Momentul consumării și tentativa	415
§1. Momentul consumării infracțiunii.....	415
§2. Tentativa.....	415
2.1. Cadrul general.....	415
2.2. Ipoteze care se situează în sfera tentativei	416
2.3. Ipoteze care se situează în sfera actelor preparatorii.....	416
2.3.1. Accesul neautorizat la un sistem informatic	416
2.3.2. Activitatea de <i>phishing</i>	417
§3. Desistarea și împiedicarea producerii rezultatului.....	418
3.1. Desistarea.....	418
3.2. Împiedicarea producerii rezultatului.....	419
3.3. Consecințele desistării ori ale împiedicării producerii rezultatului.....	420

Secțiunea a 7-a. Sancțiunea	420
Secțiunea a 8-a. Frauda informatică în formă agravată	421
§1. Reținerea art. 256 ¹ C.pen.	421
§2. Aplicarea legii penale mai favorabile, prin raportare la art. 256 ¹ C.pen. și Decizia CCR nr. 368/2017	423
Capitolul IV. Raportul dintre infracțiunea de fraudă informatică și alte infracțiuni	425
Secțiunea 1. Relația cu alte infracțiuni informatice	425
§1. Relația cu accesul la un sistem informatic (art. 360 C.pen.)	425
1.1. Cadrul general.....	425
1.2. Posibile controverse.....	426
1.2.1. Reținerea fraudei informatice fără a se reține un acces neautorizat	426
1.2.2. Posibilitatea unei absorbții naturale ori legale.....	428
§2. Relația cu falsul informatic (art. 325 C.pen.)	430
2.1. Cadrul general	430
2.2. Concurs de infracțiuni sau concurs de calificări	432
§3. Relația cu alterarea datelor informatice (art. 362 C.pen.)	433
3.1. Cadrul general.....	433
3.2. Concurs de infracțiuni sau concurs de calificări	436
3.3. Critici formulate împotriva tezei absorbției.....	438
3.4. Eventuale probleme în legătură cu teza absorbției.....	440
3.4.1. Consumarea art. 362 C.pen. și rămânerea în formă tentată a art. 249 C.pen.	440
3.4.2. Lipsa modalității deteriorării datelor informatice în conținutul art. 249 C.pen.	441
§4. Relația cu perturbarea funcționării sistemelor informatice (art. 363 C.pen.)	442
4.1. Cadrul general.....	442
4.2. Concurs de infracțiuni sau concurs de calificări	443
§5. Relația cu efectuarea de operațiuni financiare în mod fraudulos (art. 250 C.pen.)	443
5.1. Cadrul general	443
5.2. Concurs de infracțiuni sau concurs de calificări	444
5.3. Ipoteze problematice	446
5.3.1. Utilizarea unui instrument de plată electronică falsificat (card bancar clonat)	446
5.3.2. Frauda prin metoda „salam” [în engleză, <i>rounding-down fraud</i>].....	446
5.3.3. Interacțiunea logică cu un bancomat, fără a utiliza un instrument de plată electronică.....	447
5.3.4. Folosirea frauduloasă a cardurilor de comerciant.....	449
5.3.5. Efectuarea de plăți online	452
5.3.6. Retragera de numerar, de către funcționarul bancar, de la casieria băncii, prin debitarea contului unui client	452
Secțiunea a 2-a. Relația cu alte infracțiuni din Codul penal	453
§1. Relația cu infracțiunea de înșelăciune (art. 244 C.pen.)	453
1.1. Cadrul general.....	453
1.2. Frauda informatică vs. înșelăciunea tradițională prin mijloace informatice.....	454
1.3. Analiza conceptuală a fraudei informatice în raport cu înșelăciunea	455

1.4. Frauda informatică ca mijloc de săvârșire a infracțiunii de înșelăciune în formă agravată	457
1.5. Criterii pentru delimitarea fraudei informatice de înșelăciunea tradițională	458
1.5.1. Lipsa conduitei autoprejudiciante din partea victimei	458
1.5.2. Sistemul informatic – instrument sau obiect al acțiunii	459
1.5.3. Lipsa unei legături subiective între agent și victimă	459
1.5.4. Irelevanța conduitei victimei	459
1.5.5. Caracterul voluntar sau nevoluntar al transferului de active	460
1.6. Existența unor conduite care se pliază atât pe înșelăciunea tradițională, cât și pe fraudă informatică	460
§2. Relația cu infracțiunea de furt de folosință [art. 230 alin. (2) C.pen.]	461
2.1. Cadrul general	461
2.2. Concurs de infracțiuni sau concurs de calificări	462
2.3. Necesitatea incriminării furtului în scop de folosință	463
§3. Relația cu infracțiunea de abuz de încredere (art. 238 C.pen.)	463
§4. Relația cu infracțiunea de distrugere (art. 253 C.pen.)	464
4.1. Cadrul general	464
4.2. Concurs de infracțiuni ori concurs de calificări?	464
§5. Relația cu infracțiunea de delapidare (art. 295 C.pen.)	465
Secțiunea a 3-a. Relația cu infracțiunea prevăzută de art. 25 lit. c) din O.U.G. nr. 77/2009	466
Capitolul V. Reformarea art. 249 C.pen.	468
Secțiunea 1. Propunerea unei reforme substanțiale	468
§1. Cadrul general	468
§2. Modificarea art. 244 alin. (1) C.pen. prin introducerea unei teze distincte de incriminare	468
§3. Modificarea art. 244 alin. (1) C.pen. prin lărgirea sferei de aplicabilitate	469
§4. Insuficiența modificării art. 244 C.pen.	470
Secțiunea a 2-a. Propuneri <i>de lege ferenda</i> referitoare la modificarea art. 249 C.pen.	470
§1. Cu privire la beneficiul material	470
§2. Cu privire la caracterul injust	471
§3. Referitor la modalitatea împiedicării în orice mod a funcționării unui sistem informatic	471
§4. Referitor la modalitatea deteriorării datelor informatice	471
Secțiunea a 3-a. Alte intervenții <i>de lege ferenda</i>	472
Titlul IV. Falsul informatic (art. 325 C.pen.)	475
Aspecte introductive	475
Capitolul I. Raportul dintre reglementarea națională și instrumentele juridice supranaționale	476
Secțiunea 1. Sursa de inspirație a legiuitorului național	476
§1. Recomandarea Consiliului Europei din 1989	476
§2. Convenția Consiliului Europei privind Criminalitatea informatică din 2001 și Raportul explicativ al Convenției privind criminalitatea informatică	478

§3. Decizia-cadru 2005/2002/JAI privind atacurile împotriva sistemelor informatice [abrogată] și Directiva 2013/40/EU privind atacurile împotriva sistemelor informatice [în vigoare]	480
§4. Directiva UE 2019/713 privind combaterea fraudelor și a contrafacerii în legătură cu mijloace de plată fără numerar [în vigoare]	481
Secțiunea a 2-a. Modul de transpunere în dreptul intern	482
§1. Legiuitorul național a folosit noțiunea de „modificare”, și nu pe cea de „alterare”	482
§2. Legiuitorul a făcut trimitere la modalitatea restricționării accesului la datele informatice, și nu la suprimarea datelor informatice	483
§3. „Datele neautentice” din textul convenției au fost transpuse în dreptul intern ca „date necorespunzătoare adevărului”	484
§4. Aparenta lipsă de consecvență terminologică în ceea ce privește scopul special	484
Capitolul II. Rațiunea și necesitatea incriminării	485
Capitolul III. Analiza conținutului infracțiunii de fals informatic	487
Secțiunea 1. Obiectul infracțiunii	487
§1. Obiectul juridic	487
§2. Obiectul material	490
Secțiunea a 2-a. Natura infracțiunii de fals informatic	491
Secțiunea a 3-a. Subiecții infracțiunii	492
§1. Subiectul activ	492
1.1. Aspecte generale	492
1.2. Relația dintre scopul special și participația penală	493
1.3. Participația în cazul contrafacerii (clonării) de pagini web	494
1.4. Aplicabilitatea instituției poziției de garant (art. 17 C.pen.)	495
§2. Subiectul pasiv	496
2.1. Subiectul pasiv principal	496
2.2. Subiectul pasiv secundar	497
Secțiunea a 4-a. Latura obiectivă a falsului informatic	497
§1. Înscrierile tradiționale și documentele electronice	499
1.1. Observații generale	499
1.2. Trăsăturile esențiale și funcțiile unui înscris tradițional	501
1.3. Înscrișul în formă electronică (documentul electronic)	503
1.4. Înscrierile tradiționale vs. înscrisurile în formă electronică (documentele electronice)	505
1.5. Trăsăturile și funcțiile datelor informatice ce fac obiectul falsului informatic	507
1.6. Exemple de date informatice relevante din perspectiva falsului informatic	509
1.6.1. Bazele de date	509
1.6.2. Cataloagele online	509
1.6.3. Documente electronice individuale	509
1.6.4. Paginile web	510
1.6.5. Conturile create pe rețelele de socializare	510
1.6.6. Semnătura electronică	510

§2. Modalități de comitere a falsului informatic.....	513
2.1. Modalitatea introducerii de date informatice	513
2.1.1. Cadrul general.....	513
2.1.2. Ipoteze de comitere a falsului informatic prin introducerea de date informatice	515
A) Contrafacerea (clonarea) unor pagini web [<i>web spoofing</i>].....	515
B) Simularea poștei electronice [<i>e-mail spoofing</i>] prin uzurparea identității.....	523
C) Transmiterea de corespondență electronică folosind un cont accesat fără drept.....	526
D) Utilizarea (aplicarea) fără drept a unei semnături electronice	527
E) Introducerea de date informatice (informații) false în sistemul informatic ECRIS.....	528
F) Introducere de date informatice în programul Revisal	529
G) Emiterea frauduloasă a unui instrument de plată electronică.....	530
H) Crearea unui cont (profil) fals pe o rețea de socializare.....	530
I) Contrafacerea [clonarea] unei cartele SIM.....	536
2.1.3. Ipoteze privind introducerea de date informatice, problematice din perspectiva reținerii falsului informatic	537
A) Introducerea [publicarea] de anunțuri de vânzare fictive pe platformele online	537
B) Publicarea pe Internet a unui model [tipar] pentru crearea unui document electronic fals	540
C) Introducerea unui program malițios în codul sursă al unei pagini web	541
D) Crearea unui duplicat după un document electronic.....	542
E) Transferul de documente electronice într-un sistem informatic	542
2.2. Modalitatea modificării de date informatice.....	543
2.2.1. Cadrul general.....	543
2.2.2. Ipoteze de comitere a falsului informatic prin modificarea de date informatice	544
A) Modificarea notei într-un catalog digital	544
B) Modificarea numărului de copii aflați în întreținere în baza de date a autorității, în vederea obținerii unei alte indemnizații.....	545
C) Modificarea numărului de telefon asociat unui cont bancar.....	546
D) Alterarea unor imagini ce ar putea fi folosite drept probe într-un proces.....	546
E) Alterarea unei înregistrări audio-video folosite într-o procedură penală	547
F) Modificarea denumirii și prețului unui produs la momentul vânzării acestuia	548
G) Modificarea valorii <i>hash</i> stocate pe mijlocul de stocare pe care a fost salvată copia efectuată în condițiile art. 168 alin. (9) C.proc.pen.	549
2.2.3. Ipoteze de modificare a datelor informatice, problematice din perspectiva reținerii falsului informatic.....	550
A) Crearea unui cont [profil] fictiv pe o rețea de socializare	550
B) Modificarea numărului de telefon (<i>caller ID spoofing</i>)	551

C) Falsificarea unei adrese IP (<i>IP spoofing</i>)	552
D) Generarea unui nou cod PIN aferent unui instrument de plată electronică.....	554
E) Alterarea modului de funcționare a jocurilor de noroc electronice.....	554
2.3. Modalitatea ștergerii de date informatice	555
2.3.1. Cadrul general.....	555
2.3.2. Ipoteze de comitere a falsului informatic prin ștergerea de date informatice.....	555
2.4. Modalitatea restricționării accesului la date informatice	557
2.4.1. Cadrul general	557
2.4.2. Ipoteze de comitere a falsului informatic prin restricționarea accesului la datele informatice	557
2.4.3. Ipoteze de restricționare a accesului la datele informatice, problematice din perspectiva reținerii falsului informatic.....	557
§3. Lipsa autorizării – noțiunea „fără drept”	558
§4. Urmarea – rezultarea unor date necorespunzătoare adevărului	561
4.1. Cadrul general.....	561
4.2. Urmarea din perspectiva consecințelor juridice.....	564
4.3. Înțelesul sintagmei „rezultând date necorespunzătoare adevărului”	564
Secțiunea a 5-a. Vinovăția (latura subiectivă)	565
§1. Forma de vinovăție	565
§2. Scopul special – utilizarea în vederea producerii de consecințe juridice	565
2.1. Considerente generale.....	565
2.2. Natura juridică a scopului special	567
2.3. Efectele scopului special asupra formei de vinovăție	569
2.4. Conținutul scopului special.....	569
Secțiunea a 6-a. Momentul consumării falsului informatic și tentativa	574
§1. Cadrul general.....	574
§2. Momentul consumării falsului informatic	575
§3. Falsul informatic în formă tentată.....	576
§4. Tentativa neidonee (absurdă).....	577
Capitolul IV. Raportul dintre falsul informatic și falsurile tradiționale	578
Secțiunea 1. Precizări generale.....	578
Secțiunea a 2-a. Analiza raportului dintre falsul informatic și falsurile tradiționale.....	578
Secțiunea a 3-a. Diferențele existente la nivelul celor două categorii de infracțiuni	579
§1. Sub aspectul limitelor de pedeapsă.....	579
§2. Sub aspectul sancționării tentativei.....	580
§3. Sub aspectul incriminării uzului de fals și al neincriminării uzului de fals informatic	580
§4. Condiția folosirii ori încredințării documentului falsificat	581
§5. Distincția dintre documentele oficiale și cele private	581
Secțiunea a 4-a. Ipoteze concrete din care rezultă raportul dificil de soluționat dintre falsul informatic și falsurile tradiționale	581
§1. Contrafacerea sau alterarea unui înscris tradițional pe un sistem informatic.....	582
§2. Continuarea acțiunii de alterare după tipărirea conținutului documentului electronic pe suport hârtie.....	583

§3. Contrafacerea sau alterarea unei facturi electronice.....	583
§4. Contrafacerea ori alterarea unei corespondențe electronice și depunerea acesteia la dosarul cauzei în formă tipărită	584
§5. Contrafacerea unei cereri adresate instanței, introducerea în documentul electronic a unei semnături olografe și transmiterea cererii la dosarul cauzei, prin e-mail	585
§6. Modificarea datei privind crearea documentului prin alterarea informațiilor metadata și tipărirea pe suport hârtie a conținutului fals al respectivului document electronic.....	585
Secțiunea a 5-a. Identificarea problemelor de drept relevante din perspectiva raportului dintre falsul informatic și falsurile tradiționale	586
§1. Momentul în care putem discuta despre un înscris tradițional.....	586
§2. Identificarea actului de executare	586
§3. Reținerea tentativei.....	587
§4. Identificarea autoratului și a formelor de participare penală.....	587
§5. O eventuală încălcare a principiului ne bis in idem.....	587
§6. Problema metamorfozei falsului informatic într-un fals tradițional, din perspectiva regimului sancționator	587
Secțiunea a 6-a. Posibile soluții pentru rezolvarea raportului dintre falsul informatic și falsul tradițional	588
§1. Caracterul special al falsului informatic în raport cu falsurile tradiționale.....	589
§2. Excluderea falsului tradițional prin raportare la valoarea probatorie a unei copii improprii.....	589
§3. Funcția probatorie și funcția de garanție a datelor informatice asupra cărora se intervine	589
§4. Delimitarea între falsul informatic și falsul tradițional, prin raportare la scopul agentului.....	590
Capitolul V. Furtul (uzurparea) de identitate. O formă a falsului informatic.....	592
Secțiunea 1. Aspecte introductive.....	592
Secțiunea a 2-a. Conceptul de „furt de identitate”	593
§1. Fazele furtului de identitate.....	595
1.1. Faza întâi. Obținerea datelor personale	595
1.2. Faza a doua. Interacțiunea cu datele personale obținute în faza întâi	596
1.3. Faza a treia. Folosirea efectivă a datelor personale.....	597
§2. Concluzii cu privire la furtul de identitate	598
2.1. O incriminare autonomă ar trebui să acopere toate fazele furtului de identitate	598
2.2. „Furtul de identitate” este un concept impropriu.....	598
2.3. Identitate falsă vs. identitate fictivă	599
2.4. Furtul de identitate vs. uzurparea identității.....	599
Secțiunea a 3-a. Furtul de identitate ca fals informatic.....	600
§1. Activitatea de <i>phishing</i>	600
§2. Activitatea de <i>pharming</i>	602

Capitolul VI. Raportul dintre infracțiunea de fals informatic și alte infracțiuni	604
Secțiunea 1. Relația cu alte infracțiuni informatice	604
§1. Relația cu alterarea integrității datelor informatice (art. 362 C.pen.)	604
§2. Relația cu perturbarea funcționării sistemelor informatice (art. 363 C.pen.)	605
§3. Relația cu transferul neautorizat de date (art. 364 C.pen.)	606
§4. Relația cu operațiuni ilegale cu dispozitive sau programe informatice (art. 365 C.pen.)	607
§5. Relația cu falsificarea instrumentelor de plată electronică [art. 311 alin. (2) C.pen.]	607
§6. Relația cu efectuarea de operațiuni financiare în mod fraudulos (art. 250 C.pen.)	608
Secțiunea a 2-a. Relația cu alte infracțiuni	609
§1. Relația cu infracțiunea de înșelăciune	609
§2. Relația cu infracțiunea de falsificare a unei înregistrări tehnice (art. 324 C.pen.)	609
§3. Relația cu infracțiunea de evaziune fiscală [art. 9 alin. (1) lit. c) din Legea nr. 241/2005]	610
Capitolul VII. Reformarea art. 325 C.pen.	612
Secțiunea 1. Abrogarea art. 325 C.pen. și extinderea aplicabilității falsurilor tradiționale	612
Secțiunea a 2-a. Modificarea art. 325 C.pen.	613
Secțiunea a 3-a. Modificări cu privire la alte texte de incriminare.....	614
§1. Incriminarea uzului de fals informatic	614
§2. Abrogarea art. 311 alin. (2) C.pen. [falsificarea instrumentelor de plată electronică]	615
§3. Abrogarea art. 324 C.pen. [falsificarea unei înregistrări tehnice]	615
§4. Modificarea art. 311 alin. (2) C.pen. în acord cu Directiva (UE) 2019/713.....	616
Ultimul cuvânt	617
Bibliografie	619
Index tematic.....	645

Titlul I

Conceptul de „criminalitate informatică” și aspecte terminologice

Capitolul I Criminalitatea informatică

Secțiunea 1. Conceptul de „criminalitate informatică”

Menționăm *ab initio* că nu ne propunem o analiză *in extenso* cu privire la ce este criminalitatea informatică⁹, ce nu este și cum este înțeles acest concept în doctrină, jurisprudență ori diferitele instrumente juridice la nivel internațional sau european. Despre acest concept se pot scrie, s-au scris și se vor scrie monografii întregi, în care analiza *in extenso* să surprindă toate particularitățile, dezbaterile doctrinare și consecințele juridice ce derivă din modalitatea în care acest concept este definit.

Ceea ce ne propunem este doar a evidenția câteva chestiuni punctuale, care să scoată în evidență ceea ce apreciem noi ca fiind esențial de reținut cu privire la conceptul de „criminalitate informatică”. Ar putea părea că acest concept este cu vechime, dar, în realitate, până în anul 1970, în SUA nu se discuta cu adevărat despre criminalitatea informatică, infracțiuni prin intermediul calculatorului ori altele asemenea¹⁰.

Începând cu această perioadă, conceptul de „criminalitate informatică” – indiferent de terminologia folosită – a început să câștige tot mai mult teren, iar progresele tehnologice și îndeosebi apariția Internetului nu au făcut decât ca interesul pentru criminalitatea informatică și importanța acesteia să crească exponențial. Totuși, 50 de ani în domeniul juridic nu reprezintă o perioadă de timp semnificativă. Nu este o perioadă scurtă de timp, dar, având în vedere că despre răspunderea penală a persoanei juridice se discută în *common law* de sute de ani¹¹ și, cu toate acestea, discuțiile în plan juridic nu sunt încă definitiv tranșate,

⁹ Și ne vom rezuma la a folosi această noțiune, deși în literatura de specialitate întâlnim o terminologie cât se poate de variată precum: *e-crime*, *high-tech crime*, *IT crime*, *ICT crime*, *computer crime* etc. Vom evita traducerea acestor termeni în limba română, pentru a nu ajunge la descoperirea de noi noțiuni. În legătură cu diversitatea acestor termeni, apreciați ca fiind interschimbabili, se poate vedea J. CLOUGH, *Principles of Cybercrime*, ed. a II-a, Cambridge University Press, UK, 2015, pp. 9-10; I. VASIU, L. VASIU, *Criminalitatea în Cyberspațiu*, op. cit., p. 119, n.s. nr. 5. Așa cum bine s-a evidențiat, oricare dintre acești termeni ar fi analizați gramatical, s-ar ajunge la concluzia că sunt deficitari, deoarece aduc limitări ce ar părea nejustificate – în acest sens, J. CLOUGH, *Principles of Cybercrime*, op. cit., p. 10. Astfel, noțiunea de „computer” – cel puțin în sens tradițional – exclude alte dispozitive ce ar intra însă în accepțiunea noțiunii de „sistem informatic”.

¹⁰ A se vedea, în acest sens, un istoric al criminalității informatice, pe faze „de dezvoltare”, în J.B. HILL, N.E. MARION, *Introduction to Cybercrime. Computer Crimes, Laws, and Policing in the 21st Century* [Kindle], Ed. Praeger, SUA, 2016, la Capitolul II – History of Cybercrime, *passim*.

¹¹ A se vedea, în acest sens, H.W. EDGERTON, *Corporate criminal responsibility*, în *Yale Law Journal*, nr. 5/1927, p. 827. Autorul citează cauze din *common law* din anul 1864 [Statul c. *Ohio R.R.*], 1841 [Statul c. *Great Works Co.*] etc. A se vedea, de asemenea, o analiză doctrinară din 1899, în C.J. LINDLEY, *Criminal acts of corporations and their punishment*, în *American Lawyer*, nr. 7/1899, p. 564 și urm.

creдем că studiul criminalității informatice se află, momentan, doar într-o etapă adolescen-tină. Acest lucru înseamnă că mai avem multe de învățat, iar dezbaterile juridice ar trebui să fie considerate ca fiind într-o fază incipientă.

Cert este faptul că, deși acest concept a intrat deja în limbajul curent, este folosit extrem de des, a devenit deja un subiect de o importanță deosebită, acesta rămâne **un concept deosebit de vag¹² și dificil de definit¹³**. La întrebarea „Ce este criminalitatea informatică?” răspunsul nu poate fi decât unul complicat și plin de nuanțe.

Tocmai de aceea încă nu există o definiție legală¹⁴. În loc să se accepte faptul că acesta reprezintă un „concept-umbrelă” ce își schimbă sensul și conținutul în funcție de perspectivă, teoreticienii și decidenții politici încearcă în continuare să îl umple de conținut. În acest sens, au fost elaborate și vor fi elaborate în continuare definiții, clasificări și analize în legătură cu acest concept, însă, din punctul de nostru de vedere, este imposibil a se ajunge în viitorul apropiat la un consens. Explicația o regăsim în gama deosebit de variată de conduite infracționale, unele dintre acestea aflate, din perspectiva clasificării, la limita dintre infracțiunile tradiționale și cele informatice. Ne-am putea referi aici la infracțiunea de hărțuire prin mijloace de transmitere la distanță (art. 208 C.pen.) sau violarea vieții private (art. 226 C.pen.), prin raportare la o eventuală supraveghere tehnică. Sunt acestea niște infracțiuni tradiționale ce pot fi comise inclusiv prin mijloace tehnice sau intră în accepțiunea conceptului de „criminalitate informatică”? Un răspuns tranșant la o asemenea întrebare l-am aprecia ca fiind unul hazardat, existând argumente pentru a susține oricare dintre aceste teze.

O primă problemă ar putea fi chiar aceea dacă ar trebui să ne referim la „criminalitate informatică” sau la „criminalitatea în cyberspațiu”. Aceasta deoarece, dacă termenul de criminalitate informatică pare a fi mai apropiat de ceea ce înțelegem prin „computer crime”, criminalitatea în cyberspațiu ar fi mai apropiată de noțiunea de „cybercrime”. Unii autori susțin că există o trecere de la categoria conceptuală a criminalității informatice [în engleză, *computer crime* / în italiană *reati informatici*] la criminalitatea în cyberspațiu [în engleză, *cybercrime* / în italiană, *reati cibernetici*]¹⁵.

Preferăm să nu polemizăm pe marginea acestui subiect, folosind în continuare noțiunea de „criminalitate informatică”, care este oricum la fel de vagă precum noțiunea de „criminalitate în cyberspațiu”. În opinia noastră, aceste noțiuni sunt interschimbabile. Apreciem, de asemenea, că infracțiunile care intră în accepțiunea acestor noțiuni ridică ele însele atât de

¹² În acest sens, S. GORDON, R. FORD, On the definition and classification of cybercrime, în *Journal of Computer Virology*, nr. 2/2006, p. 13; A. ZAVRŠNIK, Cybercrime definitional challenges and criminological particularities, în *Masaryk University Journal of Law and Technology*, nr. 2/2008, p. 2; V. CIOCLEI, A.-R. ILIE, Impactul dreptului penal european asupra noului Cod penal român. Privire asupra traficului de persoane și a criminalității informatice, în AUB (seria Drept), partea III-IV, 2012, p. 337.

¹³ Recomandarea R (89) 9 privind criminalitatea informatică, p. 13; P. KLEVE, R. DE MULDER, K. VAN NOORTWIJK, The definition of ICT Crime, în *Computer Law & Security Review*, vol. 27, 2011, p. 162; M.D. GOODMAN, Why the Police don't care about computer crime, în *Harvard Journal of Law & Technology*, vol. 10, nr. 3, 1997, p. 468; E. STANCU, A.C. MOISE, Considerații privind fenomenul de criminalitate informatică, în AUB (seria Drept), nr. 1/2010, p. 42; I. SLABU, Considerații generale cu privire la criminalitatea informatică, în *Studii de Securitate Publică*, vol. II, nr. 4(8)/2013, p. 105.

¹⁴ I. WALDEN, Harmonizing Computer Crime Laws in Europe, în *European Journal of Crime, Criminal Law and Criminal Justice*, vol. 12, nr. 4/2004, p. 321.

¹⁵ A se vedea, în acest sens, L. PICOTTI, Diritto penale e tecnologie informatiche: Una visione d'insieme, în A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA (dir.), *Cybercrime* [Kindle], Ed. UTET Giuridica, Milano, 2019, la secțiunea a 3-a, *passim*.

multe probleme, încât aceste debateri juridice la nivel terminologic nu sunt decât o „perdea de fum”, fără relevanță practică deosebită. Sau cel puțin așa ar trebui să fie, chiar dacă, uneori, legiuitorul național ori cel european ne demonstrează că în legislație se poate face trimitere și la astfel de noțiuni cu un conținut imprecis.

Revenind, apariția conceptului de „criminalitate informatică” – sau cum își dorește cititorul să îl numească – ține și de tendința de a grupa infracțiunile în funcție de specificul acestora. Așa este cazul, de exemplu, cu infracțiunile de criminalitate organizată (unde pot intra inclusiv cele privind criminalitatea informatică¹⁶), infracțiunile economice (unde nu vedem de ce nu s-ar încadra și anumite infracțiuni informatice precum fraudă informatică)¹⁷ etc. Observăm, de asemenea, că această încercare de a grupa anumite infracțiuni generează însă riscuri în plan juridic, deoarece nu tot timpul sintagmele folosite sunt cele mai fericite.

În acest sens, un exemplu potrivit ar fi sintagma „infracțiuni economice prevăzute în legi speciale”, care a fost apreciată ca fiind neconstituțională – a se vedea, în acest sens, **Decizia CCR nr. 573/2011**¹⁸, în legătură cu neconstituționalitatea art. 74¹ C.pen. anterior¹⁹. Nu putem decât să precizăm că atât fraudă informatică, cât și efectuarea de operațiuni financiare în mod fraudulos erau prevăzute, anterior intrării în vigoare a noului Cod penal, în legislația specială – fraudă informatică, în Legea nr. 161/2003, iar efectuarea de operațiuni, în Legea nr. 365/2002. Din punctul nostru de vedere, nu există niciun argument pentru a susține că aceste două infracțiuni nu intrau în categoria infracțiunilor economice²⁰ prevăzute în legi speciale la care făcea trimitere art. 74¹ C.pen. anterior. Prin urmare, raportat la aplicarea în timp a legii penale [aplicarea legii penale mai favorabile], art. 74¹ C.pen. anterior ar trebui să își găsească aplicabilitate în ceea ce privește infracțiunea de fraudă informatică și efectuarea de operațiuni financiare în mod fraudulos. Ambele infracțiuni sunt contra patrimoniului, infracțiunea de efectuare de operațiuni financiare în mod fraudulos privind chiar sistemul bancar, ce reprezintă un argument suplimentar în susținerea concluziei învederate anterior.

Practică judiciară. Înalta Curte de Casație și Justiție²¹: „(...) infracțiunile reținute în sarcina inculpaților, respectiv art. 48 din Legea nr. 161/2003 [*falsul informatic* – n.n.], ce constă în introducerea, modificarea și ștergerea fără drept de date informatice care au fost utilizate în scopul producerii de consecințe juridice, și art. 49 din Legea nr. 161/2003

¹⁶ A se vedea, în acest sens, și L.C. KÖVESI, S. FINTA, Încadrarea juridică a unor fapte de fraudă informatică, în Dreptul, nr. 12/2006, p. 187.

¹⁷ Există autori ce plasează falsul informatic în sfera criminalității economice, fapt ce ne pune pe gânduri referitor la înțelegerea corespunzătoare a acestei infracțiuni și raportul acesteia cu infracțiunea de fraudă informatică – a se vedea E. STANCU, A.C. MOISE, op. cit., p. 48.

¹⁸ Publicată în M. Of. nr. 363 din 25 mai 2011. Extras din Decizia CCR nr. 573/2011: „din redactarea aceluiași alineat nu se desprinde cu suficientă claritate și precizie care pot fi acele «unor infracțiuni economice prevăzute în legi speciale» [s.n.], putându-se ajunge la o înțelegere deficitară a conceptului de «infracțiuni economice» (cum ar fi, de pildă, infracțiunile împotriva intereselor financiare ale Comunităților Europene ori infracțiunile în legătură directă cu infracțiunile de corupție prevăzute în Legea nr. 78/2000 pentru prevenirea, descoperirea și sancționarea faptelor de corupție). Prin urmare, textul de lege criticat este deficitar din perspectiva lipsei de corelare atât cu alte prevederi similare din Codul penal, cât și cu cele reglementate în legi speciale la care se face trimitere, ceea ce este de natură să genereze confuzii, incertitudine și dificultăți în ceea ce privește interpretarea și aplicarea acestuia”.

¹⁹ Normă legală ce permitea reducerea limitelor de pedeapsă, aplicarea unei amenzi penale ori a unei sancțiuni administrative în funcție de cuantumul prejudiciului cauzat și recuperat.

²⁰ Detalii despre semnificația infracțiunilor economice se pot vedea în M.K. GURU, Criteriul infracțiunilor economice, în Dreptul, nr. 12/2008, p. 173 și urm.

²¹ ICCJ, s. pen., dec. nr. 749/2013.

[*frauda informatică* – n.n.], constând în introducerea, modificarea sau ștergerea de date informatice, restricționarea accesului la aceste date ori împiedicarea în orice mod a funcționării unui sistem informatic în scopul de a obține un beneficiu material, nu au caracterul unor infracțiuni economice de natură să atragă incidența dispozițiilor art. 74¹ C.pen. [anterior – n.n.]. Faptul că prin comiterea acestor infracțiuni se urmărește producerea unui prejudiciu în dauna părților vătămate le clasifică ca fiind infracțiuni de rezultat, însă *în niciun caz nu pot fi clasificate ca infracțiuni economice* [s.n.].” Credem că această soluție este în parte discutabilă, fiind de asemenea regretabilă omisiunea instanței de a explica motivele pentru care a ajuns la această concluzie. Simpla precizare că nu este suficient să se urmărească producerea unui prejudiciu nu reprezintă un argument pentru lipsirea de efecte a art. 74¹ C.pen. anterior. Dacă în ceea ce privește infracțiunea de fals informatic achiesăm opiniei instanței, credem că există argumente solide pentru respingerea tezei potrivit căreia *frauda informatică este o infracțiune economică*. De altfel, paralela făcută, de multe ori, între *frauda informatică* și *înselăciunea tradițională* reprezintă un argument pentru aplicabilitatea art. 74¹ C.pen. anterior.

Revenind, dacă în ceea ce privește infracțiunea de acces ilegal la un sistem informatic [art. 360 C.pen.] nu ar exista dificultăți în a susține că face parte din conceptul de „criminalitate informatică”, fiind chiar o infracțiune definitorie pentru acesta, analiza se complică atunci când discutăm despre *frauda informatică*, *falsul informatic*, *pornografia infantilă*, *hărțuirea prin mijloace de transmitere la distanță*, *racolarea de minori prin mijloace de transmitere la distanță* etc.

Prin urmare, înainte de a explora puțin acest concept al „criminalității informatice”, credem că s-ar impune o concluzie tranșantă, și anume aceea că **trimiterea la criminalitatea informatică este deosebit de periculoasă atunci când ne propunem să atingem standardul impus de principiul legalității**²². Cu toate că am mai folosit – și vom folosi în continuare – trimeri la acest concept, pentru a ne raporta în mod generic la anumite infracțiuni informatice, credem că, din perspectiva tehnicii legislative, este de evitat să se folosească această terminologie. Din punctul nostru de vedere, este de evitat a se folosi inclusiv trimiterea la „infracțiuni informatice” [sintagmă ce putea fi identificată în Legea nr. 21/1999]²³ ori la „infracțiuni care se săvârșesc prin sisteme informatice sau mijloace de comunicare electronică” [sintagmă regăsită în cuprinsul art. 139 alin. (2) C.proc.pen.].

Găsim, așadar, ca fiind problematică prevederea din art. 139 alin. (2) C.proc.pen. în materia supravegherii tehnice, ce face trimitere la sintagma „**infracțiuni care se săvârșesc prin sisteme informatice sau mijloace de comunicare electronică**”. Aceasta este preluată prin intermediul unei norme de trimitere inclusiv în conținutul art. 152 alin. (1) lit. a) C.proc.pen. [Obținerea datelor de trafic și de localizare]. Sintagma devine **problematică din perspectiva respectării principiului legalității** prevăzut de art. 1 alin. (5) din Constituție, ridicând, implicit, serioase semne de întrebare din perspectiva constituționalității. Nimeni nu

²² Pentru exemple de instrumente juridice supranaționale în care este folosită noțiunea de „criminalitate informatică”, se poate vedea și R. FLOR, Lotta alla „criminità” e tutela di „tradizionali” e „nuovi” diritti fondamentali neelera di Internet, în *Diritto Penale Contemporaneo*, 2012, pp. 3-4.

²³ A se vedea, în acest sens, art. 23 alin. (1) lit. a) din Legea nr. 21/1999 pentru prevenirea și sancționarea spălării banilor (publicată în M. Of. nr. 18 din 21 ianuarie 1999 și abrogată prin art. 31 din Legea nr. 656/2002), ce făcea trimitere la „infracțiunile săvârșite prin intermediul calculatoarelor”. În contextul în care infracțiunile despre care vorbim în prezent ca fiind „informatice” au apărut pentru prima dată în legislația națională prin intermediul Legii nr. 161/2003 și al Legii nr. 365/2002, nu putem decât să ne întrebăm ce infracțiuni a avut în vedere legiuitorul și unde a fost controlul de constituționalitate.

ne va putea convinge că infracțiunile ce ar trebui să fie înglobate în această sintagmă sunt determinabile. Cu toate acestea, găsim drept fascinant faptul că, până în prezent, nu s-a ridicat în mod serios o problemă de constituționalitate cu privire la sintagma „infracțiuni care se săvârșesc prin sisteme informatice sau mijloace de comunicare electronică”, în ciuda faptului că aceasta stă la baza unei ingerințe majore în dreptul la viață privată garantat de art. 26 din Constituție. Mai mult, am putea să anticipăm inclusiv concluzia Curții Constituționale pe acest subiect, în sensul că sintagma criticată nu suferă sub aspectul previzibilității. Dacă se va ajunge aici, tot ce ne dorim reprezintă oferirea câtorva criterii obiective în baza cărora se poate concluziona ce infracțiuni intră în accepțiunea sintagmei „infracțiuni care se săvârșesc prin sisteme informatice sau mijloace de comunicare electronică” și să știm de ce în această categorie nu intră orice infracțiune tradițională, de la omor la viol.

În context, nu putem decât să observăm faptul că o asemenea sintagmă pare a se referi la conceptul de „criminalitate informatică” *lato sensu*, în care sistemul informatic nu este obiectul sau subiectul infracțiunii, ci doar o „unealtă” (un mijloc) ce poate fi folosită pentru a comite infracțiuni tradiționale. Or, doar imaginația ne oprește în a oferi exemple în care orice infracțiune prevăzută în Codul penal poate fi comisă – în cel puțin una dintre formele participăției penale – prin intermediul unor sisteme informatice sau prin mijloace de comunicare electronică. Vedem, în acest sens, posibilitatea de a sustrage un autovehicul modern printr-un control exercitat asupra acestuia de la distanță [*remote access*] sau posibilitatea de a ucide o persoană prin dezactivarea de la distanță a unui dispozitiv tip *pacemaker*. În aceste condiții, enumerarea infracțiunilor prevăzute la art. 139 alin. (2) C.pen. nu ar mai fi una limitativă, supravegherea tehnică fiind susceptibilă de a produce o ingerință în dreptul la viață privată indiferent de infracțiunea la care ne raportăm.

Din perspectiva constituționalității acestei sintagme, un punct de plecare ar putea fi chiar **Decizia CCR nr. 553/2015**²⁴, referitoare neconstituționalitatea sintagmei „trafic de stupefiante” din cuprinsul dispozițiilor art. 223 alin. (2) C.proc.pen. Dispoziția legală ar putea ridica probleme inclusiv din perspectiva ingerinței în dreptul la viață privată [art. 8 din Conv. EDO], fiind discutabil în ce măsură sunt îndeplinite condițiile ce țin de calitatea legii, din perspectiva jurisprudenței CEDO – criteriul clarității și previzibilității normei legale²⁵. Aceasta dincolo de faptul că lipsa de claritate poate genera o interpretare abuzivă, cu repercusiuni în ceea ce privește respectarea principiului proporționalității în contextul unei ingerințe în dreptul la viață privată generate de supravegherea tehnică – art. 8 par. 2 din Conv. EDO.

Un alt exemplu relevant se regăsește în cuprinsul art. 280 alin. (1) pct. 11 din Legea nr. 302/2004 privind cooperarea judiciară internațională în materie penală, republicată²⁶. Astfel, într-un articol important referitor la lista infracțiunilor pentru care nu este necesară condiția

²⁴ Publicată în M. Of. nr. 707 din 21 septembrie 2015.

²⁵ Sub acest aspect, am subliniat cu o altă ocazie [a se vedea, în acest sens, G. ZLATI, Comentariu, în M. UDROIU (coord.), Codul de procedură penală. Comentariu pe articole, ed. a II-a, Ed. C.H. Beck, București, 2017, p. 749, par. 72], faptul că, deși în Capitolul VI al titlului VII din Codul penal, se regăsesc infracțiunile contra siguranței sau integrității sistemelor și datelor informatice, infracțiunile care se săvârșesc prin intermediul unui sistem informatic sau prin mijloace de comunicare electronică sunt extrem de diverse. Astfel, amenințarea [art. 206 C.pen.], hărțuirea [art. 208 alin. (2) C.pen.], racolarea de minori [art. 222 C.pen.], violarea vieții private [art. 226 C.pen.], violarea secretului corespondenței [art. 302 alin. (2) C.pen.] etc. sunt infracțiuni ce pot fi comise prin sisteme informatice sau mijloace de comunicare electronice. Aceasta fără a pune în discuție posibilitatea de a comite un act de violență [art. 193 C.pen.] ori o lipsire de libertate [art. 205 C.pen.] prin intermediul unui sistem informatic (sic!).

²⁶ Republicată în M. Of. nr. 411 din 27 mai 2019.

dublei incriminări, se face trimitere la sintagma „**faptelor legate de criminalitatea informatică**”, trimitere care nu ar trebui să surprindă pe nimeni, având în vedere că sintagma este preluată din cuprinsul art. 2 din Decizia-cadru 2002/584/JAI privind mandatul european de arestare și procedurile de predare între statele membre – cu mențiunea că în instrumentul juridic european se face trimitere doar la criminalitatea informatică, nu și la faptele legate de aceasta²⁷.

Credem că reglementarea europeană este totuși superioară, deoarece sintagma „faptelor legate de”, din dreptul național, poate genera mult mai multe discuții decât o trimitere generică la „criminalitatea informatică”. Probabil cea mai radicală interpretare ar fi cea potrivit căreia faptele legate de criminalitatea informatică sunt altele decât cele ce intră în cuprinsul noțiunii de „criminalitate informatică”. Altfel, dacă faptele la care face trimitere legiuitorul sunt chiar infracțiuni informatice, nu înțelegem de ce acestea ar fi legate de criminalitatea informatică, adică un ansamblu de infracțiuni informatice.

Cu toate acestea, rațiunea din spatele acestei formulări, mai ales dacă ne raportăm la instrumentul juridic european transpus în dreptul intern, pare destul de clară. Identificarea acestei rațiuni ține însă de elemente extrinseci actului normativ, deoarece, în acest caz, pare să existe un conflict între ceea ce și-a dorit legiuitorul național și ceea ce a rezultat din transpunerea deciziei-cadru.

Ar mai trebui poate precizat că inclusiv **Tratatul privind funcționarea Uniunii Europene** [TFUE] face trimitere la conceptul de „criminalitate informatică”, în cuprinsul art. 83 alin. (1), referitor la competența Parlamentului European și a Consiliului de a legifera, prin intermediul directivelor, cu privire la definirea infracțiunilor și sancțiunilor în domenii considerate de o gravitate deosebită și având o dimensiune transfrontalieră. Această trimitere este una deosebit de periculoasă, deoarece poate conduce la o extindere nerezonabilă a competenței Parlamentului European și a Consiliului de a legifera în domeniul dreptului penal. Lipsa unei definiții legale a criminalității informatice poate reprezenta, așadar, un „cec în alb”, fiind doar o chestiune de timp până ce vom putea discuta despre primul act de legiferare discutabil într-un domeniu apreciat ca făcând parte din conceptul „criminalității informatice”.

De asemenea, **Directiva 2018/1673/UE privind combaterea prin măsuri de drept penal a spălării banilor**²⁸ include în gama de activități infracționale relevante și „**criminalitatea informatică** [s.n.], inclusiv orice infracțiune prevăzută în Directiva 2013/40/UE a Parlamentului European și a Consiliului” [art. 2 par. 1 lit. (v) din Directivă]. Din această formulare, pare să reiasă destul de clar faptul că legiuitorul european interpretează extensiv acest concept, fără a-l limita doar la infracțiunile ce fac obiectul art. 360-365 C.pen. Ceea ce rămâne neclar este până unde se întinde acesta din perspectiva conduitelor infracționale pe care le mai poate îngloba. Având în vedere lejeritatea cu care legiuitorul european tinde să se raporteze la acest concept în instrumentele juridice, așteptăm cu interes prima intervenție a Curții de Justiție a Uniunii Europene cu privire la respectarea principiului legalității.

Observăm, de asemenea, ezitarea legiuitorului european de a se raporta doar la „criminalitatea informatică”, acesta simțind nevoia de a clarifica în mod expres că în acest concept ar intra *inclusiv* infracțiunile informatice prevăzute în Directiva 2013/40/UE. Dacă acest concept era unul clar din perspectiva conținutului, trimiterea la infracțiunile prevăzute în directivă nu ar fi fost necesară.

²⁷ Această trimitere din lista infracțiunilor excluse de la condiția dublei incriminări a fost apreciată, inclusiv în literatura de specialitate, ca fiind vagă – a se vedea, în acest sens, M. FLETCHER, R. LÖÖF, B. GILMORE, EU Criminal Law and Justice, Elgar European Law Publisher, 2008, p. 115.

²⁸ Publicat în JOUE L 284 din 12 noiembrie 2018.