

UNIVERSITATEA BABEȘ-BOLYAI

FACULTATEA DE DREPT

TEZĂ DE DOCTORAT

**Accesul neautorizat la un sistem informatic,
frauda și falsul informatic**

(cuprins și rezumat)

Conducător de doctorat:

Prof. univ. dr. Sergiu BOGDAN

Student-doctorand:

George Michail Rudolf ZLATI

CUPRINS

Abrevieri.....	31
Introducere.....	33

TITLUL I

CONCEPTUL DE CRIMINALITATE INFORMATICĂ ȘI ASPECTE TERMINOLOGICE

Capitolul I. Criminalitate informatică.....	38
§1. Conceptul de criminalitate informatică.....	38
1. Infrațiuni îndreptate împotriva sistemelor ori datelor informatice. Sistemul informatic ca obiect al conduitei infracționale.....	49
2. Infrațiuni unde sistemul informatic este doar un mijloc pentru a comite infracțiunea. Sistemul informatic ca subiect al conduitei infracționale.....	50
3. Conduite infracționale ce sunt incidentale pentru comiterea altor infracțiuni tradiționale.....	51
§2. Statistici privind criminalitatea informatică.....	52
§3. Caracterile și tratamentul juridic al criminalității informatice.....	54
§4. Statele pioner în domeniul criminalității informatice.....	57
Capitolul II. Aspecte terminologice.....	68
§1. Noțiunea de sistem informatic.....	68
§1.1. Definiția sistemului informatic în instrumentele juridice internaționale și europene.....	69
§1.2. Definiția sistemului informatic în dreptul intern.....	77
§1.3. Definiția sistemului informatic în dreptul comparat.....	80
§1.3.1. Sisteme de drept în care noțiunea de sistem informatic beneficiază de o definiție legală.....	80
§1.3.2. Sisteme de drept în care noțiunea de sistem informatic nu beneficiază de o definiție legală.....	85
§1.4. Sistemul informatic în jurisprudența instanțelor naționale și a Curții Constituționale.....	89
§1.4.1. Recursul în interesul legii – decizia ÎCCJ nr. 15/2013.....	89

§1.4.2. Jurisprudența instanțelor naționale.....	90
§1.4.3. Jurisprudența Curții Constituționale.....	92
§1.5. Importanța calificării corecte a unui dispozitiv ca fiind un sistem informatic.....	98
1. Relevanța noțiunii de sistem informatic din perspectiva dreptului penal substanțial.....	98
2. Relevanța noțiunii de sistem informatic din perspectiva dreptului procesual penal.....	98
3. Relevanța noțiunii de sistem informatic din perspectiva tehnicii legislative.....	98
§1.6. Analiza criteriilor legale desprinse din definiția sistemului informatic.....	103
1. Sistemul informatic ca dispozitiv.....	104
2. Prelucrarea automată a datelor informatice.....	108
3. Prelucrarea automată a datelor prin intermediul unui program informatic.....	111
§1.7. Exemple de sisteme informatice și exemple problematice.....	113
1. Servere prin care se furnizează anumite servicii ori pe care sunt găzduite anumite pagini web.....	114
2. Sistemul electronic de tranzacționare pe piața de capital.....	117
3. Bazele de date.....	117
4. Paginile web.....	119
5. Rețelele de socializare.....	119
6. Bancomatele (<i>automated teller machine - ATM</i>).....	120
7. Terminalele POS (<i>point of sale</i>).....	122
8. Dispozitivul tip skimmer.....	123
9. Telefoanele mobile inteligente (<i>smartphones</i>)	124
10. Terminalele de comunicații.....	125
11. Ceasurile inteligente (<i>smartwatch</i>).....	127
12. Televizoarele inteligente (<i>smart-tv</i>).....	128
13. Imprimanta, faxul și scannerul.....	129
14. Reportofoanele digitale.....	130
15. Dispozitivele de distribuire automată a biletelor.....	131

16. Camerele de supraveghere digitale.....	131
17. Aparatele de jocuri de noroc.....	132
18. Dispozitivele din categoria <i>Internet of things</i>	133
19. Cartela SIM (<i>Subscriber Identity Module</i>)	135
20. Instrumentele de plată electronică (cardurile bancare).....	136
21. Autovehiculele moderne.....	137
22. Internetul.....	138
23. Rețeaua de comunicații electronice.....	139
§1.7. O reconceptualizare a noțiunii de sistem informatic?.....	142
§1.7.1. Redefinirea noțiunii de sistem informatic.....	143
1. Simplificarea definiției.....	143
2. Restrângerea definiției prin raportare la funcția principală a dispozitivului.....	143
3. Restrângerea definiției prin raportare la autonomia dispozitivului.....	144
4. Restrângerea definiției prin introducerea unui criteriu negativ..	145
5. Restrângerea definiției prin introducerea unei liste negative.....	146
§1.7.2. O interpretare restrictivă a definiției actuale.....	146
1. Soluționarea controverselor privind utilizarea unor aparate casnice.....	148
2. Soluționarea controverselor privind utilizarea unui televizor inteligent.....	148
3. Soluționarea controverselor privind utilizarea unui mijloc de stocare.....	149
4. Soluționarea controverselor privind utilizarea unei multifuncționale.....	149
§2. Noțiunea de mijloc de stocare a datelor informatice.....	150
§2.1. Definiția noțiunii de mijloc de stocare a datelor informatice.....	150
§2.2. Relevanța noțiunii de sistem informatic din perspectiva dreptului procesual penal și a dreptului substanțial penal.....	151
§2.3. Exemple relevante de mijloace (suporturi) de stocare a datelor informatice....	152
1. Suportii optici (CD, DVD, Blu-Ray etc.).....	152
2. Hard disk, memory card, memory stick.....	152

3. Instrumentele de plată electronică (cardul bancar).....	152
4. Cartela SIM.....	154
§3. Noțiunea de program informatic și date informatice.....	155
§3.1. Definiția datelor informatice și a programelor informatice în instrumentele juridice internaționale și Europene.....	155
§3.2. Definiția programelor și datelor informatice în dreptul intern.....	156
§3.3. Exemple de date informatice.....	158
1. Calificarea unei înregistrări tehnice drept date informatice.....	158
2. Calificarea juridică a informației stocate pe o bandă magnetică.....	158
§3.4. Raportul dintre datele informatice și programele informatice.....	159
§3.4. Importanța identificării unui program informatic.....	161
§4. Noțiunea de instrument de plată electronică.....	161
§4.1. Definiția instrumentelor de plată în dreptul European.....	162
§4.2. Definiția instrumentului de plată electronică în dreptul intern.....	164

TITLUL II

ACCESUL NEAUTORIZAT LA UN SISTEM INFORMATIC (ART. 360 COD PENAL)

Capitolul I. Prezentare generală.....	168
Capitolul II. Raportul dintre reglementarea națională și instrumentele juridice supranaționale.....	169
§1. Sursa de inspirație a legiuitorului național.....	169
§2. Modul de transpunere în dreptul intern.....	176
Capitolul III. Decizii ale Curții Constituționale, recursuri în interesul legii și decizii ale Curții Europene a Drepturilor Omului.....	185
§1. Decizii ale Curții Constituționale.....	185
1. Decizia Curții Constituționale nr. 183/2018 (despre măsurile de securitate).....	186
2. Decizia Curții Constituționale nr. 353/2018 (despre accesul neautorizat).....	187

§2 Recursul în interesul legii – decizia ÎCCJ nr. 15/2013	188
§3. Curtea Europeană a Drepturilor Omului (Bărbulescu c. România)	195
Capitolul IV. Rațiunea și necesitatea incriminării	202
§1. Necesitatea unei incriminări autonome	202
1. Raportul cu violarea de domiciliu.....	202
2. Raportul cu violarea secretului corespondenței.....	204
3. Necesitatea unei incriminări autonome.....	205
§2. Limitele incriminării	206
1. Limitele accesului neautorizat în forma de bază (art. 360 alin. (1) Cod penal).....	206
2. Agravanta accesului neautorizat cu scopul special de a obține date informatice (art. 360 alin. (2) Cod penal).....	208
3. Agravanta accesului neautorizat la un sistem informatic protejat de măsuri de securitate (art. 360 alin. (3) Cod pen).....	209
Capitolul V. Analiza conținutului infracțiunii de acces neautorizat la un sistem informatic	210
§1. Obiectul juridic	210
§2. Natura și forma infracțiunii	213
§3. Subiecții infracțiunii	215
§3.1. Subiectul activ.....	215
§3.2. Subiectul pasiv.....	218
1. Identificarea subiectului pasiv.....	218
2. Teoria titularului sistemului informatic – existența unui drept de folosință consolidat.....	221
3. Existența unui subiect pasiv colectiv?	225
4. Existența unui subiect pasiv secundar?	225
5. Pluralitatea de subiecți pasivi vs. pluralitatea de sisteme informatice accesate.....	226
6. Concluzii.....	229
§4. Latura obiectivă. Cadrul general	230
§4.1. Tipologia accesului ilegal la un sistem informatic în dreptul comparat.....	231
§4.2. Sistemul informatic vs. mijlocul de stocare a datelor informatice.....	235
§5. Conduita comisivă – accesul (la un sistem informatic)	240

§5.1. Cadrul general.....	240
§5.2. Interpretarea noțiunii.....	244
1. Interpretarea gramaticală.....	244
2. Interpretarea legală (în dreptul comparat), doctrinară și jurisprudențială.....	245
3. Decizia ÎCCJ nr. 15/2013 – recurs în interesul legii.....	250
4. Conceptualizarea noțiunii de acces.....	251
4.1. Cadrul general.....	251
4.2. Perspectiva „internă” a accesului.....	251
4.3. Perspectiva „externă” a accesului.....	252
4.4. Identificarea unor trăsături esențiale ale accesului.....	253
§6. Conduita incriminată din perspectiva art. 360 Cod penal.....	255
1. Cadrul general.....	255
2. Accesul propriu-zis – reglementat expres.....	256
3. Depășirea limitelor autorizării – reglementat prin art. 35 alin. (2) din Legea nr. 161/2003?.....	256
4. Menținerea accesului după retragerea ori expirarea autorizării.....	261
5. Accesul nelimitat vs. Accesul limitat (în tot sau doar într-o parte a sistemului informatic).....	263
§7. Ipoteze particulare de acces la un sistem informatic.....	263
§7.1. Accesul propriu-zis la un sistem informatic.....	263
1. Autentificarea în cadrul unui sistem informatic.....	263
2. Folosirea de la distanță [<i>remote access</i>] a unui sistem informatic prin intermediul Team Viewer.....	265
3. Accesarea unui cont bancar online.....	266
4. Autentificarea (accesul) fără drept la interfața de administrare a unei pagini web.....	267
5. Accesarea unui bancomat prin intermediul unui instrument de plată electronică.....	268
6. Alterarea fără drept a unei pagini web prin înlocuirea ori modificarea modului în care aceasta este afișată [în engleză <i>defacing</i>].....	269
§7.2. Depășirea limitelor autorizării ori menținerea neautorizată a accesului.....	269

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.....	269
2. Accesarea unei baze de date în mod autorizat, continuată de cereri SQL [<i>SQL queries</i>] în vederea accesării unor informații privilegiate.....	270
3. Continuarea accesului la un sistem informatic fără plata redevenței.....	271
4. Primirea datelor de autentificare într-un cont de e-mail pentru o verificare punctuală și omisiunea cu intenție a delogării.....	272
§7.3. Ipoteze particulare ce nu vizează un acces la un sistem informatic.....	272
1. Transmiterea unui e-mail.....	272
2. Transmiterea unui program informatic.....	273
3. Atacurile de tip denial-of-service [<i>DoS attack</i>]	274
4. Scanarea porturilor [<i>port scanning</i>]	274
5. Citirea informației afișate pe monitorul sistemului informatic.....	275
6. Obținerea de date informatice prin <i>phishing</i>	275
7. Conțurfacerea de pagini web	276
8. Punerea în vânzare pe Internet a unor bunuri fictive.....	277
9. Captarea informației lizibile pe monitor.....	277
10. Interacțiunea fizică cu un bancomat.....	278
11. Efectuarea de plăți la un terminal POS.....	279
12. Efectuarea de plăți online.....	280
§7.4. Ipoteze particulare ce impun o analiză atentă.....	282
1. Accesarea unor adrese URL (nepublice) ale unor pagini web (publice).....	282
2. Copierea fără drept de date informatice din sistemul informatic aparținând unei terțe persoane.....	283
3. Copierea fără drept de date informatice într-un sistem informatic aparținând unei terțe persoane.....	284
4. Utilizarea unui program informatic tip <i>keylogger</i> pentru a intercepta datele introduse de la tastatură de către victimă.....	285
5. Restricționarea accesului la anumite date informatice de către administratorul sistemului informatic.....	286
6. Infectarea unor sisteme informatice cu un program malițios (virus).....	287
§8 Lipsa autorizării – noțiunea „fără drept”	288

1. Cadrul general.....	288
2. Noțiunea „fără drept” și alte noțiuni interschimbabile.....	290
§8.1. Ipoteze particulare ale accesului „fără drept” în doctrină și jurisprudență.....	291
1. Lipsa autorizării exprese a administratorului de rețea.....	291
2. Utilizarea fără drept a unui card de carburant.....	291
3. Introducerea de anunțuri fictive pe platforma eBay.....	292
4. Crearea de conturi fictive pe platforma eBay.....	292
5. Accesarea de către un funcționar bancar a aplicației „CARD PIN” și „CARD FORM” prin utilizarea fără drept a unui cod de acces.....	293
6. Accesarea de către un funcționar bancar a unei componente a sistemului informatic care era restricționată pentru categoria de angajați din care făcea aceasta parte.....	293
7. Accesarea unei pagini web restricționate de către angajat cu un scop fraudulos.....	293
8. Utilizarea unui laptop bun comun al soților.....	294
9. Accesarea contului de Internet banking de către unul dintre soți.....	295
10. Accesarea unui cont de e-mail ori de Facebook de către unul dintre soți.....	295
11. Accesarea contului de Skype al soției.....	295
12. Accesarea unui cont de e-mail prin folosirea unui parole primite anterior.....	296
13. Verificarea situației fiscale a unor contribuabili din altă jurisdicție.....	297
14. Transferul de materiale pornografice cu minori.....	298
§8.2. Orientări jurisprudențiale relevante în dreptul comparat.....	297
1. Jurisprudența Curții de Casație italiene.....	298
2. Teorii ale accesului fără drept în dreptul american.....	300
§8.3. Identificarea unui <i>framework</i> rezonabil pentru noțiunea „fără drept”.....	311
1. Stabilirea unor puncte de reper.....	311
2. Soluționarea limitelor autorizării pentru accesul între soți.....	315
3. Accesul la sistemul informatic al copilului.....	316
§9. Urmarea.....	316

§10. Vinovăția (latura subiectivă)	317
§11. Momentul consumării și tentativa	318
1. Cadrul general.....	318
2. Momentul consumării infracțiunii.....	319
3. Ipoteze ce se situează în sfera tentativei.....	320
3.1. Simpla pornire a unui sistem informatic.....	320
3.2. Inițializarea [<i>bootarea</i>] unui sistem de operare de pe un CD.....	322
3.3. Depășirea parțială a măsurilor de securitate ce împiedică cu totul accesul la sistemul informatic.....	323
4. Ipoteze care se situează în sfera actelor preparatorii.....	323
5. Teoria tentativei neidonee – o soluție de compromis.....	325
6. Desistarea și împiedicarea producerii rezultatului.....	327
6.1. Desistarea.....	327
6.2. Împiedicarea producerii rezultatului.....	328
§12. Formele agravate ale accesului ilegal la un sistem informatic	328
§12.1. Scopul obținerii de date informatice.....	328
1. Cadrul general.....	328
2. Conținutul scopului special.....	329
3. Relația cu alte infracțiuni.....	330
§12.2. Încălcarea măsurilor de securitate.....	330
1. Cadrul general.....	330
2. Rațiunea agravantei.....	333
3. Natura măsurilor de securitate – fizice, organizaționale ori doar logice?.....	336
4. Caracteristicile măsurilor de securitate.....	339
4.1. Natura și specificul măsurilor de securitate.....	339
4.2. Controlul accesului.....	340
4.3. Scopul controlului accesului.....	342
4.4. Efectivitatea măsurilor de securitate.....	342
4.5. Fiabilitatea (eficacitatea) măsurilor de securitate.....	343
5. Proceduri de interzicere ori de restricționare a accesului.....	345
5.1. Parole sau coduri de acces.....	345
5.2. Criptarea datelor informatice.....	345

5.3. Utilizarea unor elemente biometrice.....	346
5.4. Setarea adreselor MAC [<i>media access control adress</i>].....	346
5.5. Securizarea unui browser web.....	346
6. Dispozitive de interzicere ori restricționare a accesului.....	346
7. Programe informatice ce interzic ori restricționează accesul.....	347
8. Modalitățile prin care sunt „încălcate” măsurile de securitate.....	347
8.1. Obținerea frauduloasă a datelor de la victimă.....	348
8.2. Folosirea datelor de autentificare după pierderea autorizării.....	348
8.3. Utilizarea unor date reale în vederea autentificării.....	350
9. Consecințele inexistenței unor măsuri de securitate.....	350
Capitolul VI. Raportul dintre accesul neautorizat la un sistem informatic și alte infracțiuni.....	351
§1. Relația cu alte infracțiuni informatice.....	351
1. Relația cu falsul informatic (art. 325 Cod pen.)	351
2. Relația cu fraudă informatică (art. 249 Cod pen.).....	351
3. Relația cu alterarea integrității datelor informatice (art. 362 Cod pen.).....	352
4. Relația cu operațiuni ilegale cu dispozitive sau programe informatice (art. 365 Cod pen.).....	353
§2. Relația cu alte infracțiuni din codul penal.....	354
1. Relația cu infracțiunea de violare a vieții private (art. 226 Cod penal).....	354
2. Relația cu infracțiunea de furt (art. 228 Cod pen.).....	354
2.1. Accesarea sistemului informatic ulterior momentului sustragerii acestuia.....	355
2.2. Sustragerea unor componente din diferite sisteme informatice și accesarea sistemului informatic alcătuit din acestea.....	357
3. Relația cu infracțiunea de furt de folosință - art. 230 alin. (2) Cod pen.....	358
4. Relația cu infracțiunea de tănuire – art. 270 Cod penal.....	359
5. Relația cu infracțiunea de violare a secretului corespondenței (art. 302 alin. (1) Cod penal).....	359

5.1. Aplicabilitatea art. 360 Cod pen. – accesarea serverului de mail.....	362
5.3. Aplicabilitatea art. 302 alin. (1) Cod pen. – deschiderea unei corespondențe sau comunicări?	366
5.4. Concurs de infracțiuni sau de calificări?.....	367
6. Relația cu infracțiunea privind efectuarea de operațiuni financiare în mod fraudulos (art. 250 alin. (1) Cod penal).....	368
7. Relația cu infracțiunea privind fraudă la votul electronic (art. 388 Cod pen.).....	369
§3. Relația cu alte infracțiuni din legislația specială.....	370
1. Relația cu infracțiunile privind drepturile de autor (Legea nr. 8/1996).....	370
2. Relația cu infracțiunile privind concurența neloială (Legea nr. 11/1991).....	371
3. Relația cu infracțiunea (infracțiunile) de terorism (Legea nr. 535/2004).....	373
4. Relația cu infracțiunea privind supravegherea tehnică neautorizată (Legea nr. 51/1991)	375
Capitolul VII. Reformarea art. 360 cod penal.....	376
§1. O reformă conceptuală?	376
§2. Propuneri referitoare la modificarea art. 360 Cod penal.....	378
1. Introducerea „încălcării măsurilor de securitate” ca element constitutiv al formei de bază.....	378
2. Clarificarea noțiunii de acces și introducerea unor teze alternative de comitere a faptei.....	379
3. Extinderea accesului la mijloacele de stocare a datelor informatice.....	379
4. Abrogarea art. 360 alin. (2) Cod penal.....	379
5. Introducerea unei clauze de subsidiaritate.....	380
§3. Intervenții de lege ferenda ce ar trebui evitate.....	381
1. Introducerea plângerii prealabile.....	381
2. Introducerea unor cauze de atipicitate.....	381
§4. Alte intervenții de lege ferenda.....	382

TITLUL III
FRAUDA INFORMATICĂ
(ART. 249 COD PENAL)

Capitolul I. Aspecte introductive.....	384
Capitolul II. Raportul dintre reglementarea națională și instrumentele juridice supranaționale.....	386
§1. Sursa de inspirație a legiuitorului național	386
§2. Modul de transpunere în dreptul intern	399
Capitolul III. Rațiunea și necesitatea incriminării fraudei informatice.....	405
Capitolul IV. Analiza conținutului infracțiunii de fraudă informatică.....	414
§1. Obiectul infracțiunii	414
§1.1. Obiectul juridic	414
§1.2. Obiectul material.....	420
§2. Subiecții infracțiunii	422
§2.1. Subiectul activ.....	422
§2.2. Subiectul pasiv.....	424
§3. Latura obiectivă a fraudei informatice	428
§3.1. Sistemul informatic și datele informatice.....	429
§3.2. Modalități de comitere a fraudei informatice.....	430
§3.2.1. Aspecte generale.....	430
1. Infracțiune cu conținut alternativ.....	431
2. Infracțiune comisivă și omisivă.	431
§3.2.2. Analiza conduitei comise.....	433
§3.2.3. Modalitatea introducerii de date informatice.....	434
1. Cadrul general.....	434
2. Situația premisă.....	436
3. Ipoteze de comitere a fraudei informatice prin introducerea de date informatice	437
3.1. Furtul [transferul fără drept] de monede virtuale.....	437
3.2. Achiziționarea de telefoane mobile la valoare zero prin activarea în sistemul informatic a unor discount-uri...	439

3.3. Folosirea fără drept a unui tichet pentru reîncărcarea cartelei <i>prepay</i>	439
3.4. Transferul de credit pe o cartelă telefonică <i>prepay</i>	440
3.5. Mărirea „artificială” a soldului contului bancar.....	442
3.6. Obținerea frauduloasă a unui bilet de transport în comun de la un automat de bilete.....	443
3.7. Introducerea mențiunii „plătit” cu privire la un anumit debit stocat într-o bază de date.	443
3.8. Folosirea frauduloasă a unui fotocopiator prin utilizarea unei cartele falsificate.....	444
4. Ipoteze privind introducerea de date informatice problematice din perspectiva reținerii fraudei informatice.....	445
4.1. Licitațiile online frauduloase.....	445
4.2. Frauda prin trimiterea de mesaje prin mijloace de comunicare electronică.	449
4.3. Activitatea de <i>phishing</i> și <i>pharming</i>	451
4.4. Trimiterea de corespondență electronică nesolicitată (spam).	454
4.5. Folosirea datelor de identificare ale unui instrument de plată electronică.....	454
4.6. Efectuarea de tranzacții offline.....	455
4.7. Retragera de numerar de la bancomat imediat după retragerea sumei de la ghișeu al băncii.....	457
4.8. Crearea frauduloasă de credite bancare în sistemul informatic al băncii.	458
4.9. Folosirea unui <i>spyware dialer</i>	458
4.10. Comandarea frauduloasă de produse în calitate de agent de vânzări.	460
4.11. Folosirea unor coduri <i>paysafecard</i> pentru efectuarea de plăți online.	461
4.12. „minarea” de monede virtuale (<i>crypto-jacking</i>).....	461
4.13. Tipărirea unor bancnote falsificate.....	466
§3.2.4. Modalitatea modificării de date informatice.....	467

1. Cadrul general.....	467
2. Ipoteze de comitere a fraudei informatice prin modificarea de date informatice.....	468
2.1. Efectuarea unui transferuri de fonduri.....	468
2.2. Modificarea soldului dintr-un cont bancar printr-o intervenție asupra bazei de date.....	469
2.3. Menținerea ca activat a unui anumit serviciu în vederea facturării suplimentare.....	469
2.4. Modificarea „creditului” disponibil la un joc de poker online.....	470
2.5. Rotunjirea sumelor la momentul efectuării unui transfer de fonduri.....	471
2.6. Modificarea programului informatic al unui aparat de joc de noroc pentru a nu mai fi necesară plata de credite suplimentare.....	471
3. Ipoteze privind modificarea de date informatice problematice din perspectiva reținerii fraudei informatice	471
3.1. Alterarea conținutului unui pagini web.....	471
3.2. Modificarea sumei ce apare afișată pe ecranul terminalului POS.....	472
§3.2.5. Modalitatea ștergerii de date informatice.....	475
1. Cadrul general.....	475
2. Ipoteze de ștergere a datelor informatice relevante din perspectiva art. 249 cod pen.....	476
3. Ipoteze privind ștergerea de date informatice problematice din perspectiva reținerii fraudei informatice.....	478
3.1. Ștergerea datelor informatice prin utilizarea unui magnet.....	478
3.2. Ștergerea unor debite ori a unor debitori din baza de date.....	478
§3.2.6. Modalitatea restricționării accesului la datele informatice.....	479
1. Cadrul general.....	479

2. Ipoteze de restricționare a accesului la datele informatice ce se pliază pe art. 249 cod pen.....	480
3. Ipoteze privind restricționarea accesului la datele informatice problematice din perspectiva reținerii fraudei informatice	480
3.1. Restricționarea accesului la anumite conturi prin schimbarea parolei de acces.....	480
3.2. Nerestituirea unor sume de bani ajunse din eroare în contul agentului.....	481
3.3. Conduita tip <i>ransomware</i>	482
§3.2.7. Modalitatea împiedicării în orice mod a funcționării unui sistem informatic	483
1. Cadrul general.	483
2. Ipoteze de împiedicare a funcționării unui sistem informatic posibil relevante din perspectiva art. 249 Cod pen.....	484
2.1. Manipularea jocurilor electronice de noroc.....	484
2.2. Interacțiunea logică cu un bancomat.....	487
3. Ipoteze privind împiedicarea în orice mod a funcționării unui sistem informatic problematice din perspectiva reținerii fraudei informatice.....	487
3.1. Interacțiunea fizică cu un bancomat (metoda „furculița”).....	487
3.2. Dezactivarea unor dispozitive electronice de protecție în vedere sustragerii bunului.....	491
3.3. Obținerea fără drept a unui bun de la un automat.....	491
3.4. Atacuri informatice tip dos (<i>denial-of-service</i>).....	491
§3.2.8. Conduita omisivă improprie (comisiva prin omisiune).....	492
§3.3. Lipsa autorizării – noțiunea „fără drept”	493
§3.4. Urmarea.....	493
1. Cadrul general.....	494
2. Cauzarea unei pagube.....	496
§3.5. Obținerea unui beneficiu material.....	501
1. Clarificarea noțiunii.....	501
2. Beneficiu material just vs. Beneficiu material injust.....	502

§3.6. Raportul de cauzalitate.....	503
§4. Vinovăția (latura subiectivă)	504
§4.1. Elementul subiectiv.....	504
§4.2. Scopul special.....	504
§5. Unitatea naturală sau legală a infracțiunii.....	507
§6. Momentul consumării și tentativa	508
§6.1. Momentul consumării infracțiunii.....	508
§6.2. Tentativa.....	509
1. Cadrul general.....	509
2. Ipoteze care se situează în sfera tentativei.....	509
3. Ipoteze care se situează în sfera actelor preparatorii.....	510
3.1. Accesul neautorizat la un sistem informatic.....	510
3.2. Activitatea de phishing.....	510
§6.3. Desistarea și împiedicarea producerii rezultatului.....	511
1. Desistarea.....	511
2. Împiedicarea producerii rezultatului.....	514
3. Consecințele desistării ori ale împiedicării producerii rezultatului.....	514
§7. Sancțiunea.....	515
§8. Frauda informatică în formă agravată.....	516
Capitolul V. Raportul dintre infracțiunea de fraudă informatică și alte infracțiuni.....	520
§1. Relația cu alte infracțiuni informatice.....	520
§1.1. Relația cu accesul la un sistem informatic (art. 360 Cod penal).....	520
§1.2. Relația cu falsul informatic (art. 325 Cod penal).....	526
§1.3. Relația cu alterarea datelor informatice (art. 362 Cod penal).....	529
§1.4. Relația cu perturbarea funcționării sistemelor informatice (art. 363 Cod penal).....	539
§1.5. Relația cu efectuarea de operațiuni financiare în mod fraudulos (art. 250 Cod penal)	541
1. Cadrul general.....	541
2. Concurs de infracțiuni sau concurs de calificări.....	542
3. Ipoteze problematice.....	544
3.1. Utilizarea unui instrument de plată electronică falsificat (card bancar clonat).....	544

3.2. Frauda prin metoda „salam”	545
3.3. Interacțiunea logică și de la distanță cu un bancomat.....	546
3.4. Folosirea frauduloasă a cardurilor de comerciant.....	549
3.5. Efectuarea de plăți online.	552
3.6. Retragera de numerar de către funcționarul bancar de la casieria băncii, prin debitarea contului unui client.....	552
§2. Relația cu alte infracțiuni din codul penal	553
§2.1. Relația cu infracțiunea de înșelăciune (art. 244 Cod penal).....	553
1. Cadrul general.....	553
2. Frauda informatică vs. Înșelăciunea tradițională prin mijloace informatic.....	554
3. Analiza conceptuală a fraudei informatice în raport cu înșelăciunea.....	555
4. Criterii pentru delimitarea fraudei informatice înșelăciunea tradițională.....	558
4.1. Lipsa conduitei autoprejudiciate.....	558
4.2. Sistemul informatic – instrument sau obiectul acțiunii.....	558
4.3. Lipsa unei legături subiective.....	558
4.4. Irelevanța conduitei victimei.....	559
4.5. Caracterul voluntar sau nevoluntar al transferului de active...560	
5. Existența unor conduite care se pliază atât pe înșelăciunea tradițională cât și pe fraudă informatică.....	560
§2.2. Relația cu infracțiunea de furt de folosință [art. 230 alin. (2) Cod penal].....	562
§2.3. Relația cu infracțiunea de abuz de încredere (art. 238 Cod penal).....	564
§2.4. Relația cu infracțiunea de distrugere (art. 253 Cod penal)	565
§2.5. Relația cu infracțiunea de delapidare (art. 295 Cod penal).....	566
§3. Relația cu infracțiunea prevăzută de art. 25 lit. c) din O.U.G. 77/2009....	567
Capitolul VI. Reformarea art. 249 cod penal.....	569
§1. O reformă radicală?.....	569
1. Cadrul general.....	569
2. Modificarea art. 244 alin. (1) cod pen. Prin introducerea unei teze distincte de incriminare.....	569
2. Modificarea art. 244 alin. (1) cod pen. Prin lărgirea sferei de aplicabilitate.....	570

§2. Propuneri referitoare la modificarea art. 249 cod penal.....	571
1. Cu privire la beneficiul material.	571
2. Cu privire la caracterul injust.....	571
3. Referitor la modalitatea împiedicării în orice mod a funcționării unui sistem informatic.	571
4. Referitor la modalitatea deteriorării.....	572
§3. Alte intervenții de lege ferenda.....	572

TITLUL IV
FALSUL INFORMATIC
(ART. 325 COD PENAL)

Capitolul I. Aspecte introductive.....	575
Capitolul II. Raportul dintre reglementarea națională și instrumentele juridice supranaționale.....	576
§1. Sursa de inspirație a legiuitorului național.....	576
§2. Modul de transpunere în dreptul intern.....	583
Capitolul III. Rațiunea și necesitatea incriminării.....	586
Capitolul IV. Analiza conținutului infracțiunii de fals informatic.....	589
§1. Obiectul infracțiunii.....	589
§1.1. Obiectul juridic.....	589
§1.2. Obiectul material.....	591
§2. Natura infracțiunii.....	591
§3. Subiecții infracțiunii.....	592
§3.1. Subiectul activ.....	592
1. Relația dintre scopul special și participația penală.....	592
2. Participația în cazul contrafacerii de pagini web.....	593
3. Aplicabilitatea instituției poziției de garant (art. 17 Cod pen.).....	594
§3.2. Subiectul pasiv.....	594
§4. Latura obiectivă a falsului informatic.....	596
§4.1. Conceptul de înscris.....	599
§4.2. Documentul electronic.....	601

§4.3. Înscrierile tradiționale vs. Datele informatice [documentele electronice].....	602
1. Cadrul general.....	602
2. Trăsăturile și funcțiile datelor informatice ce fac obiectul falsului informatic.....	604
3. Exemple de date informatice relevante din perspectiva falsului informatic.....	606
3.1. Bazele de date.	606
3.2. Cataloagele online.	606
3.3. Documente electronice individuale.	607
§4.4. Semnătura electronică.....	607
§4.5. Modalități de comitere a falsului informatic.....	608
§4.5.1. Modalitatea introducerii de date informatice.....	608
1. Cadrul general.....	608
2. Ipoteze de comitere a falsului informatic prin introducerea de date informatice.....	610
2.1. Contrafacerea (clonarea) unor pagini web – <i>web spoofing</i>	610
2.2. Simularea poștei electronice [<i>e-mail spoofing</i>] prin uzurparea identității.....	617
2.3. Transmiterea de corespondență electronică folosind un cont accesat fără drept.....	619
2.4. Utilizarea (aplicarea) fără drept a unei semnături electronice.....	620
2.5. Introducerea de date informatice (informații) false în sistemul ECRIS.....	620
2.6. Introducere de date informatice în programul „Revisal”.....	621
2.7. Emiterea frauduloasă a unui instrument de plată electronică.	621
2.8. Crearea unui cont (profil) fals pe o rețea de socializare.....	622
2.9. Contrafacerea [clonarea] unei cartele SIM.....	625

3. Ipoteze privind introducerea de date informatice problematice din perspectiva reținerii falsului informatic.....	626
3.1. Introducerea (publicarea) de anunțuri fictive pe platformele online.....	626
3.2. Publicarea pe Internet a unui model [tipar] pentru crearea unui document electronic fals.....	629
3.3. Introducerea unui program malițios în codul sursă al unei pagini web.....	630
3.4. Crearea unui duplicat după un document electronic.....	630
3.5. Transferul de documente electronice într-un sistem informatic.....	631
§4.5.2. Modalitatea modificării de date informatice.....	632
1. Cadrul general.	632
2. Ipoteze de comitere a falsului informatic prin modificarea de date informatice.....	632
2.1. Modificarea notei de la BAC în catalogul digital.....	632
2.2. Modificarea numărului de copii aflați în întreținere în baza de date a autorității în vederea obținerii unei alte indemnizații.....	634
2.3. Modificarea numărului de telefon asociat unui cont bancar.....	635
2.4. Alterarea unor imagini ce ar putea fi folosite drept probe într-un proces.	636
2.5. Alterarea unei înregistrări audio-video folosite într-o procedură penală.....	636
2.6. Modificarea denumirii și prețului unui produs la momentul vânzării acestuia.....	637
2.7. Modificarea valorii hash stocate pe mijlocul de stocare pe care a fost salvată copia efectuată în condițiile art. 168 alin. (9) Cod proc. pen.....	638
3. Ipoteze de modificare a datelor informatice problematice din perspectiva reținerii falsului informatic.....	639
3.1. Crearea unui cont [profil] fictiv pe o rețea de socializare.....	639
3.2. Modificarea numărului de telefon (<i>caller ID spoofing</i>).....	640

3.3. Falsificarea unei adrese IP (<i>IP spoofing</i>).....	640
3.4. Regenerarea codului PIN aferent unui instrument de plată electronică.....	641
§4.5.3. Modalitatea ștergerii de date informatice.....	642
1. Cadrul general.....	642
2. Ipoteze de comitere a falsului informatic prin ștergerea de date informatice.....	643
3. Ipoteze de ștergere a datelor informatice problematice din perspectiva reținerii falsului informatic.....	644
§4.5.4. Modalitatea restricționării accesului la date informatice.....	644
1. Cadrul general.....	644
2. Ipoteze de comitere a falsului informatic prin restricționarea accesului la datele informatice.....	645
3. Ipoteze de restricționare a accesului la datele informatice problematice din perspectiva reținerii falsului informatic.....	645
§4.6. Lipsa autorizării – noțiunea „fără drept”.....	646
§4.7. Urmarea – rezultarea unor date necorespunzătoare adevărului.....	648
1. Cadrul legal.....	648
2. Consecințele juridice ale acestei urmări.....	650
3. Exemple de date necorespunzătoare adevărului.....	650
§5. Vinovăția (latura subiectivă)	651
§5.1. Forma de vinovăție.....	651
§5.2. Scopul special – utilizarea în vederea producerii de consecințe juridice.....	651
1. Natura juridică a scopului special.....	651
2. Efectele scopului special asupra formei intenției.....	651
3. Conținutul scopului special.....	652
§6. Momentul consumării și tentativa.....	653
1. Cadrul general.....	653
2. Momentul consumării falsului informatic.....	654
3. Falsul informatic în formă tentată.....	655
Capitolul V. Raportul dintre falsul informatic și falsurile tradiționale.....	656
§1. Precizări generale.....	656
§2. Analiza raportului dintre falsul informatic și falsurile tradiționale.....	656

§3. Diferențele existente la nivelul celor două categorii de infracțiuni.....	657
1. Sub aspectul limitelor de pedeapsă.....	658
2. Sub aspectul sancționării tentativei.....	658
3. Incriminarea uzului de fals.....	658
4. Condiția folosirii ori încredințării documentului falsificat.....	659
5. Distincția între documentele oficiale și cele private.....	660
§4. Ipoteze punctuale din care rezultă raportul problematic dintre falsul informatic și cel tradițional.....	660
1. Contrafacerea sau alterarea unui înscris tradițional pe un sistem informatic.....	660
2. Continuarea acțiunii de alterare după tipărirea conținutului documentului electronic pe suport hârtie.....	662
3. Contrafacerea sau alterarea unei facturi electronice.....	662
4. Contrafacerea ori alterarea unei corespondențe electronice și depunerea acesteia la dosarul cauzei în formă tipărită.....	663
5. Contrafacerea unei cereri adresate instanței, introducerea în documentul electronic a unei semnături olografe și transmiterea la dosar a cererii, prin e-mail.....	664
6. Modificarea datei privind crearea documentului prin alterarea informațiilor <i>metadata</i> și tipărirea pe suport hârtie a conținutului fals a respectivului document electronic.....	665
§5. Identificarea problemelor de drept relevante din perspectiva raportului dintre falsul informatic și falsurile tradiționale.....	666
1. Momentul în care putem discuta despre un înscris tradițional.....	666
2. Identificarea actului de executare.....	666
3. Reținerea tentativei.....	667
4. Identificarea autoratului și a formelor de participare penală.....	667
5. O eventuală încălcare a principiului <i>ne bis in idem</i>	667
6. Problema metamorfozei falsului informatic într-un fals tradițional din perspectiva regimului sancționator.....	667
§6. Posibile soluții pentru rezolvarea raportului dintre falsul informatic și falsurile tradiționale.....	668

1. Caracterul special al falsului informatic în raport cu falsurile tradiționale.....	668
2. Excluderea falsului tradițional prin raportare la valoarea probatorie a unei copii improprie.....	669
3. Funcția probatorie și funcția de garanție a datelor informatice	
4. asupra cărora se intervine.....	669
4. Delimitarea între falsul informatic și falsul tradițional prin raportare la scopul agentului.....	670
Capitolul VI. Furtul de identitate. O formă a falsului informatic.....	672
§1. Aspecte introductive.....	672
§2. Conceptul de furt de identitate.....	673
1. Fazele furtului de identitate.....	675
1.1. Faza unu. Obținerea datelor personale.....	675
1.2. Faza a doua. Interacțiunea cu datele personale obținute în faza unu.....	677
1.3. Faza a treia. Folosirea efectivă a datelor personale.....	678
2. Concluzii cu privire la furtul de identitate.....	678
2.1. O incriminare autonomă ar trebui să acopere toate fazele furtului de identitate.	678
2.2. Furtul de identitate este un concept impropriu.	679
2.3. Identitate falsă vs. identitate fictivă.	679
2.4. Furtul de identitate vs. uzurparea identității.	680
§3. Furtul de identitate ca fals informatic	681
1. Activitatea de <i>phishing</i>	681
2. Activitatea de <i>pharming</i>	683
Capitolul VII. Raportul dintre infracțiunea de fals informatic și alte infracțiuni.....	685
§1. Relația cu alte infracțiuni informatice.....	685
1. Relația cu alterarea integrității datelor informatice (art. 362 Cod penal).....	685
2. Relația cu perturbarea funcționării sistemelor informatice (art. 363 Cod penal).....	686
4. Relația cu transferul neautorizat de date (art. 364 Cod pen.).....	687

5. Relația cu operațiuni ilegale cu dispozitive sau programe informatice (art. 365 Cod pen.)	687
6. Relația cu falsificarea instrumentelor de plată electronică (art. 311 alin. (2) Cod penal).....	688
7. Relația cu efectuarea de operațiuni financiare în mod fraudulos (art. 250 Cod penal).....	689
§2. Relația cu alte infracțiuni.....	690
1. Relația cu infracțiune de înșelăciune.....	690
2. Relația cu infracțiunea de falsificare a unei înregistrări tehnice.....	690
3. Relația cu infracțiunea de evaziune fiscală (art. 9 lit. c) din Legea nr. 241/2005)	691
Capitolul VIII. Reformarea art. 325 cod penal.....	693
§1. Abrogarea art. 325 cod penal și extinderea aplicabilității falsurilor tradiționale	693
§2. Modificarea art. 325 cod penal.....	695
§3. Modificări cu privire la alte texte de incriminare.....	696
1. Incriminarea uzului de fals informatic.....	696
2. Abrogarea art. 311 alin. (2) Cod pen. [falsificarea instrumentelor de Plată electronică].....	696
3. Abrogarea art. 324 Cod pen. [falsificarea unei înregistrări tehnice].....	697
4. Modificarea art. 311 alin. (2) Cod pen. în acord cu Directiva (UE) 2019/713.....	697
Concluzii.....	699
Bibliografie.....	702

CUVINTE CHEIE

Acces neautorizat, fraudă informatică, fals informatic, sistem informatic, mijloc de stocare, date informatice, instrument de plată electronică, clonare pagini web, phishing, furt de identitate, fraude pe Internet.

REZUMAT

În această teză sunt analizate trei infracțiuni informatice: accesul neautorizat la un sistem informatic [art. 360 Cod pen.], fraudă informatică [art. 249 Cod pen.] și falsul informatic [art. 325 Cod pen.]. În afara acestor trei infracțiuni, este analizat conceptul de criminalitate informatică și aspecte terminologice relevante, precum noțiunea de sistem informatic, instrument de plată electronică etc.

Infracțiunile informatice **au făcut obiectul a cel puțin câtorva monografii**,¹ inclusiv la momentul în care acestea erau cuprinse doar în legislația specială (Legea nr. 161/2003² și Legea nr. 365/2003³). În prezent, lucrările de specialitate ce analizează partea specială a noului Cod penal abordează automat și infracțiunile ce fac obiectul prezentei teze deoarece acestea au fost preluate din legislația specială în conținutului Codului penal – art. 249 [frauda informatică], art. 250 [efectuarea de operațiuni financiare în mod

¹ **Cu titlu de exemplu enumerăm următoarele lucrări:** I. VasIU, *Criminalitatea informatică*, Ed. Nemira, București, 1998; I. VasIU, L. VasIU, *Totul despre hackeri*, Ed. Nemira, București, 2001; I. VasIU, L. VasIU, *Informatica juridică și Drept informatic*, Ed. Alabastră, Cluj, 2002; T. Amza, C.-P. Amza, *Criminalitatea informatică*, Ed. Lumina Lex, București, 2003; I. VasIU, L. VasIU, *Prevenirea criminalității informatice*, Ed. Hamangiu, București, 2006; M. Dobrinou, *Infracțiuni în domeniul informatic*, Ed. C.H. Beck, București, 2006; Ș. Prună, I.-C. Mihai, *Criminalitatea informatică*, Ed. Sitech, 2008; M. Dobrinou, *Criminalitatea informatică*, Ed. Academiei Naționale de Informații, București 2009; A. Trancă, I. VasIU, L. VasIU, *Criminalitatea în cyberspațiu*, Ed. Universul Juridic, 2011; D.C. Trancă, *Infracțiunile informatice în noul Cod penal*, Ed. Universul Juridic, București, 2014. **La nivel de drept comparat am putea enumera următoarele lucrări:** P.F., Cabana, *Las nuevas tecnologías en los delitos contra el patrimonio y el orden socioeconómico*, Ed. Tirant lo Blanch, Valencia, 2009; L. Cuomo, E. Razzante, *La nuova disciplina dei reati informatici*, Ed. Giappichelli, Torino, 2009; M. Quéméner, Y. Charpenel, *Cybercriminalité. Droit pénal appliqué*, Ed. Economica, Paris, 2010; A. Amato G. Saraceni, *I reati informatici. Elementi di teoria generali e principali figure criminose*, Ed. Giappichelli, Torino, 2015; G.B. Hoyos, *El delito de estafa informática*, Ed. Leyer, Bogotá, 2009; A. Cadoppi, S. Canestrari, A. Manna, M. Papa M. (dir.), *Cybercrime* [Kindle], Ed. UTET Giuridica, Milano, 2019; J. Clough, *Principles of Cybercrime*, second edition, Cambridge University Press, UK, 2015.

² Privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice și în mediul de afaceri, prevenirea și sancționarea corupției (publicată în M.Of. nr. 279 din 21 aprilie 2003).

³ Privind comerțul electronic republicată (publicată în M.Of. nr. 403 din 10 mai 2006).

fraudulos], art. 325 [falsul informatic], art. 360-365, art. 374 [pornografia infantilă] ș.a. Cod pen.

În ciuda existenței acestor analize doctrinare, în literatura de specialitate autohtonă **se simte în continuare nevoia unei analize aprofundate** în domeniu. Într-o abordare critică, s-ar putea susține că în ceea ce privește criminalitatea informatică nu ducem lipsă de literatură de specialitate, dar literatura de specialitate existentă până în momentul de față evidențiază nevoia unor completări. Iar aici ne referim la o analiză în profunzime asupra unor probleme relevante din perspectiva practicii judiciare și nu doar o prezentare generală și schematică a conținutului textelor de incriminare.

Un prim argument vizează problemele evidențiate în practica judiciară. În acest sens, în practica judiciară se observă adesea cum infracțiunile informatice ridică **probleme majore la nivel de interpretare** iar atât raporturile juridice dintre acestea (de exemplu, relația dintre falsul informatic și fraudă informatică), cât și raporturile dintre infracțiunile informatice și alte infracțiuni considerate ca fiind tradiționale (de exemplu, relația dintre fraudă informatică și infracțiunea de înșelăciune), au generat o **practică judiciară neunitară**.

Or, o analiză a criticilor ce pot fi aduse numeroaselor soluții de practică judiciară ne determină să concluzionăm că acestea își găsesc de mult prea puține ori răspunsul în literatura de specialitate. Tocmai de aceea ne-am propus ca în prezenta teză să efectuăm o analiză amplă a practicii judiciare și identificarea unor soluții juridice concrete pentru fiecare problemă în parte ce a generat controverse ori dificultăți la nivel de interpretare și aplicare a textelor de incriminare.

Un alt doilea argument este acela că de prea multe ori analizele doctrinare – îndeosebi cele autohtone – vizează aspecte generale ori deja clarificate și de prea puține ori se concentrează pe chestiuni cu adevărat controversate ce ridică deja probleme ori care ar putea să apară în viitor. Având în vedere că rolul literaturii de specialitate nu este doar de a oferi răspuns la probleme actuale, ci și acela de a preîntâmpina discuții în vederea evitării unei viitoare practici judiciare neunitare, apreciem că prezenta teză este necesară și oportună.

În acest context, credem că inclusiv **o analiză aprofundată la nivel de drept comparat** devine o necesitate. Or, o recenzie a literaturii de specialitate autohtone ne arată că metoda abordării comparative este de prea puține ori folosită, iar atunci când este folosită trimiterile sunt făcute îndeosebi la dreptul american.

În ceea ce ne privește, nu avem vreo rezervă în a susține că dreptul american reprezintă un punct de referință în domeniul criminalității informatice. Totuși, raportat la prevederile naționale ce fac obiectul prezentei teze, dreptul american devine cu adevărat relevant doar din perspectiva infracțiunii de acces neautorizat la un sistem informatic [art. 360 Cod pen.], acolo unde literatura de specialitate⁴ și jurisprudența este vastă și de o ținută științifică remarcabilă.⁵ Credem așadar că pentru clarificarea noțiunilor de „acces” și „fără drept”⁶ o incursiune în dreptul american este un pas important în orice cercetare științifică în domeniu.

În schimb, din perspectiva fraudei informatice și a falsului informatic credem că acest sistem de drept nu reprezintă cu adevărat un model pentru legiuitorul național. Dincolo de o analiză amplă cu privire la furtul de folosință [în engleză, *identity theft*] în general și conduitele tip *phishing*⁷ în particular, nu credem că literatura de specialitate ori jurisprudența americană este în măsură să ofere răspunsuri relevante pentru problemele ce pot fi identificate în dreptul național în legătură cu aceste două infracțiuni.

De aceea, credem că atenția trebuie îndreptată și înspre alte sisteme de drept, precum cel spaniol, italian, german etc. În literatura de specialitate din aceste țări ori referitoare la aceste sisteme de drept, pot fi identificate analize ample la nivel conceptual pentru a delimita infracțiunea de fraudă informatică (art. 248.2 Cod pen. spaniol, art. 640-ter Cod pen. italian și secțiunea 263a Cod pen. german) de înșelăciunea tradițională.

Având în vedere că în jurisprudența națională majoritatea covârșitoare a cauzelor privind infracțiunea de fraudă informatică evidențiază o regretabilă confuzie între această infracțiune și înșelăciunea tradițională,⁸ o asemenea incursiune în dreptul comparat

⁴ Ne referim aici îndeosebi la materialele profesorului Orin Samuel Kerr ce reprezintă un punct de referință la nivel internațional în materia criminalității informatice. A se vedea cu titlu de exemplu, O.S., Kerr, *Cybercrime's scope: interpreting „access” and „authorization” in Computer Misuse Statutes*, în „New York University Law Review”, vol. 78, 2003; O.S. Kerr, *Norms of Computer Trespass*, în „Columbia Law Review”, vol. 116, 2016; O.S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, în „Minnesota Law Review”, vol. 94, 2010.

⁵ Remarcabilă nu datorită faptului că ne-a determinat să achiesăm soluțiilor de practică judiciară, ceea ce nu a fost cazul, ci datorită faptului că orice concluzie la care s-a ajuns a avut în spate un întreg raționament logico-juridic ce de multe ori lipsește în motivarea instanțelor.

⁶ În dreptul american făcându-se vorbire despre „lipsa autorizării”.

⁷ A se vedea cu titlu de exemplu L.L. Sullins, „*Phishing for a solution*”: *domestic and international approaches to decreasing online identity theft*, în „Emory International Law Review”, vol. 20, 2006.

⁸ Astfel, în ipoteze de înșelăciuni prin mijloace informatice (licitații online ori vânzări de bunuri online) **unele instanțe rețin infracțiunea de înșelăciune**: C. Ap. București, secția a II-a penală, dec. nr. 421/2015; C. Ap. Pitești, secția penală, dec. nr. 689/R/2008; C. Ap. Ploiești, secția penală, dec. nr. 1084/2016; C. Ap. Ploiești, secția penală, dec. nr. 804/2015. În schimb, **alte instanțe rețin infracțiunea de fraudă informatică**: C. Ap. Bacău, secția penală, dec. nr. 128/2011; C. Ap. Pitești, secția penală, dec. nr. 496/2014; C. Ap. Pitești, secția penală, dec. nr. 672/2013, C. Ap. Craiova, secția penală, dec. nr. 1113/2015; C. Ap.

reprezintă un demers util și necesar. Tocmai de aceea, așa cum urmează a se vedea pe parcursul tezei, trimiterile făcute la alte sisteme de drept sunt numeroase. Pe lângă dreptul spaniol, italian ori german s-au făcut trimiteri inclusiv la dreptul elvețian, francez, olandez etc.

Studiul falsului informatic din perspectiva dreptului comparat se dovedește într-o bună măsură problematic. Aceasta întrucât, în ciuda art. 7 din Convenția privind criminalitatea informatică, sistemele de drept de referință pentru dreptul național (dreptul italian, spaniol, german sau francez) nu au incriminat falsul informatic ca o infracțiune autonomă ori au avut o abordare cu totul diferită față de cea a legiuitorului român.

De asemenea, se observă că literatura de specialitate ezită în general să propună soluții concrete pentru soluționarea unor probleme reale la nivel de interpretare ori aplicare a textelor de incriminare.

În context, apreciem că în urma unei analize aprofundate a legislației naționale, prin raportare la elemente de drept comparat și ținând cont de dreptul european în materie, **se pot formula propuneri concrete de reformare a infracțiunilor informatice** supuse analizei ori a altor infracțiuni cu care acestea se află într-un raport problematic din punct de vedere juridic. Rolul literaturii de specialitate nu este doar acela de a aduce clarificări ori de a tranșa discuții controversate, ci și acela de a propune **soluții pentru simplificarea legislației penale** în contextul în care ne aflăm într-o continuă expansiune cantitativă și calitativă a dreptului penal, ce tinde să devină îngrijorătoare din perspectiva principiilor generale de drept.

La nivel de conținut, teza se va axa pe **analiza a trei infracțiuni informatice** și anume accesul neautorizat la un sistem informatic (*Titlul II*), fraudă informatică (*Titlul III*) și falsul informatic (*Titlul IV*), fiecare infracțiune în parte urmând a beneficia de un **titlu distinct în cadrul tezei** pentru o mai bună sistematizare a materiei. Aceste trei titluri vor prezenta unele asemănări și anume: existența unui capitol referitor la raportul dintre reglementarea națională și prevederile anumitor instrumente juridice supranaționale, analizarea rațiunii și necesității incriminării și tratarea într-un capitol distinct a relației

București, secția a II-a penală, dec. nr. 637/2017; C. Ap. Alba Iulia, secția penală, dec. nr. 171/2015; C. Ap. Bacău, secția penală, dec. nr. 128/2011; C. Ap. Cluj, secția penală, dec. nr. 1801/2011; C. Ap. București, secția I penală, dec. nr. 938/2016; C. Ap. București, secția I penală, dec. nr. 1189/2016; C. Ap. București, secția a II-a penală, dec. nr. 1472/2017; C. Ap. Craiova, secția penală, dec. nr. 279/2017. Există chiar **instanțe chiar rețin un concurs de infracțiuni între înșelăciune și fraudă informatică**: ÎCCJ, secția penală, dec. nr. 3764/2013; C. Ap. Bacău, secția penală, dec. nr. 1012/2014, C. Ap. Bacău, secția penală, dec. nr. 1170/2015; C. Ap. București, secția a II-a penală, dec. 854/2016; C. Ap. Pitești, secția penală, dec. nr. 295/2011.

dintre infracțiunea ce face obiectul analizei și alte infracțiuni informatice, tradiționale, prevăzute în Codul penal sau în legislația specială.

De asemenea, având în vedere că toate infracțiunile informatice ce au făcut obiectul analizei se subsumează noțiunii de “criminalitate informatică” și reprezintă o transpunere în dreptul intern a unor instrumente juridice europene (Decizia-cadru 2005/222/JAI privind atacurile împotriva sistemelor informatice⁹ ori Directiva 2013/40/EU privind atacurile împotriva sistemelor informatice și de înlocuire a Deciziei-cadru 2005/222/JAI a Consiliului¹⁰) ori internaționale (Convenția Consiliului Europei privind criminalitatea informatică¹¹), a fost dedicat un titlu introductiv prin care s-a analizat **conceptul de criminalitate informatică** (Titlul I, Capitolul I) și **terminologia folosită** în cuprinsul textelor de incriminare ce vor face obiectul analizei (Titlul I, Capitolul II).

Primul titlu (intitulat „Aspecte introductive”) a fost structurat în două capitole. Primul capitol a fost dedicat conceptului de „criminalitate informatică”, iar cel de al doilea terminologiei folosite de legiuitor în cuprinsul unor texte de incriminare.

În **Capitolul I** (intitulat „Criminalitatea informatică”) ne-am propus să evidențiem dificultatea definirii conceptului de „criminalitate informatică”¹² și riscurile utilizării unui asemenea concept în legislație. În primul rând, au fost identificate exemple de acte normative naționale ori europene în care se face trimitere la conceptul de „criminalitate informatică” (spre exemplu, Legea nr. 302/2004¹³, Directiva 2018/1673/UE¹⁴ etc.).

În context, s-a încercat a se puncta că utilizarea unui concept vag în conținutul unor instrumente juridice care ar trebui să exceleze la nivel de claritate și previzibilitate ar putea pune în discuție respectarea principiului legalității. De asemenea, s-a evidențiat riscul unor interpretări abuzive printr-o extindere nejustificată a sferei de aplicabilitate a normei penale, cu riscul încălcării principiului proporționalității.

În continuare, s-a procedat la o prezentare succintă a principalelor orientări legate de definirea conceptului de „criminalitate informatică”. În acest sens, s-a insistat asupra

⁹ Publicată în JOUE L 069/67.

¹⁰ Publicată în JOUE L 218/8 din 14.08.2013.

¹¹ Ratificată prin Legea nr. 64/2004 pentru ratificarea Convenției Europei privind criminalitatea informatică, adoptată la Budapesta la 23 noiembrie 2001 (publicată în M.Of. nr. 343 din 20 aprilie 2004).

¹² În acest sens și S. Gordon, R. Ford, *On the definition and classification of cybercrime*, în „Journal of Computer Virology”, nr. 2/2006, p. 13.

¹³ Privind cooperarea judiciară internațională în materie penală republicată (M.Of. nr. 707 din 21 septembrie 2015).

¹⁴ Privind combaterea prin măsuri de drept penal a spălării banilor (JOUE L 284 din 12 noiembrie 2018).

definiției larg răspândite¹⁵ ce stabilește conținutul criminalității informatice prin raportare la trei categorii de infracțiuni: **(1)** infracțiuni îndreptate împotriva sistemelor ori datelor informatice – acestea fiind „ținta” conduitei infracționale; **(2)** infracțiuni unde sistemul informatic este doar un mijloc pentru a comite infracțiunea – caz în care sistemul informatic este doar o „unealtă” pentru realizarea conduitei infracționale; **(3)** activități infracționale ce sunt incidentale pentru comiterea altor infracțiuni tradiționale.

Tot cu privire la conținutul conceptului de criminalitate informatică a fost identificată practică judiciară națională la nivelul Înaltei Curți de Casație și Justiție,¹⁶ în care fie s-a încercat definirea conceptului fie au fost incluse anumite infracțiuni ori conduite infracționale în acest concept.

În **Capitolul II** (intitulat „Aspecte terminologice”) ne-am propus să analizăm *in extenso* noțiunea de „sistem informatic”. Analiza a avut ca premisă instrumentele juridice supranaționale ce au reprezentat un izvor de drept pentru legiuitorul național. Ne referim în acest sens la Convenția Consiliului Europei privind criminalitatea informatică, Decizia-cadru 2005/222/JAI privind atacurile împotriva sistemelor informatice și Directiva 2013/40/UE privind atacurile împotriva sistemelor informatice.

În continuare, s-a analizat definiția sistemului informatic în dreptul intern [art. 181 alin. (1) Cod pen.] în încercarea de a identifica și explica criteriile legale pentru calificarea unui anumit dispozitiv drept sistem informatic. Ne-am referit în acest sens la sistemul informatic ca dispozitiv [componenta hardware] și la prelucrarea automată a datelor informatice prin intermediul unui program informatic [componenta software]. S-au făcut trimitere inclusiv la elemente de drept comparat, încercând a se evidenția două modele de abordare: cel în care sistemul informatic beneficiază de o definiție legală (SUA, Canada,

¹⁵ A se vedea în acest sens J. Clough, *Principles of Cybercrime...*, precit., p. 10-11; S. Fafinski, *Computer Misuse. Response, regulation and the law*, Willian Publishing, UK, 2009, p. 5; J. Clough, *Cybercrime*, în „Commonwealth Law Bulletin”, vol. 37, nr. 4/2011, p. 672; S.W. Brenner, *U.S. Cybercrime Law: Defining Offenses*, în „Information Systems Frontiers”, vol. 6, nr. 2/2004, p. 117; J. Müller, *La cybercriminalité économique au sens étroit. Analyse approfondie du droit suisse et aperçu de quelques droits étrangers*, Ed. Schulthees Médias Juridiques, Zurich, 2012, p. 12; H. Lu, B. Liang, M. Taylor, *A Comparative Analysis of Cybercrimes and Governmental Law Enforcement in China and the United States*, în „Asian Criminology”, vol. 5, 2010, p. 126; I. Vasiiu, L. Vasiiu, *The Cybercrime Challenge: Does the Romanian Legislation Answer Adequately*, în „Law Review”, vol. III, nr. 2/2013, p. 45-46; D. Chilstein, *Législation sur la cybercriminalité en France*, în „Revue internationale de droit comparé”, nr. 2/2010, p. 553; S.W. Brenner, *Cybercrime. Criminal Threats from Cyberspace*, Ed. Praeger, SUA, 2010, p. 39-47.

¹⁶ A se vedea în acest sens, ÎCCJ, secția penală, dec. nr. 1415/2014 (despre definirea conceptului); ÎCCJ, secția penală, dec. nr. 1396/2013 (despre apartenența conduitelor tip phishing la conceptul de criminalitate informatică); ÎCCJ, secția penală, dec. nr. 2346/2012 (despre infracțiunile ce fac parte din conceptul de criminalitate informatică).

Olanda, Austria etc.) și cel în care interpretarea noțiunii a fost lăsată în sarcina literaturii de specialitate și a jurisprudenței (Regatul Unit, Italia, Franța, Spania etc.).

Centrul de greutate al analizei noțiunii de „sistem informatic” vizează o analiză *in concreto* a numeroase exemple de sisteme informatice ori exemple problematice din perspectiva calificării juridice, inclusiv prin raportare la practica judiciară. Cu titlu exemplificativ, au fost avute în acest sens următoarele dispozitive: servere prin care se furnizează anumite servicii ori pe care sunt găzduite anumite pagini web; sistemul electronic de tranzacționare pe piața de capital; bancomatele, terminalele POS, ceasurile inteligente, televizoarele inteligente, aparatele de jocuri de noroc, dispozitivele din categoria *Internet of Things*, dispozitivele tip skimmer, autovehicule moderne etc. În afara acestor dispozitive au fost mai analizate bazele de date, paginile web, Internetul, rețeaua de comunicații electronice, cartelele SIM, instrumentele de plată electronică etc. Toate acestea în încercarea de a clarifica sfera de aplicabilitate a noțiunii „sistem informatic” și de a evidenția eventualele controverse ce pot apărea în legătură cu această noțiune.

După identificarea tuturor acestor probleme a fost avută în vedere inclusiv o posibilă reconceptualizare a noțiunii, începând de la o redefinire a acesteia. S-a analizat în acest sens posibilitatea de a introduce elemente suplimentare în conținutul definiției precum funcția principală a sistemului informatic, caracterul autonom ori anumite criterii negative care să limiteze în mod rezonabil sfera de aplicabilitate a noțiunii. Nu în ultimul rând, s-a propus o interpretare restrictivă a definiției actuale în încercarea de a rezolva posibilele controverse ce ar putea apărea în legătură cu utilizarea unor aparate casnice, a unui televizor inteligent, a unei multifuncționale etc.

În afara noțiunii „sistem informatic” au fost analizate noțiunile „program informatic”, „date informatice” și „instrument de plată electronică”. Toate aceste analize au urmărit în cele din urmă clarificarea unor noțiuni ce fac parte din elementele constitutive ale unor infracțiuni sau prezintă o relevanță aparte din perspectiva dreptului procesual penal.

În ceea ce privește instrumentul de plată electronică a fost analizată inclusiv 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.¹⁷ Cu toate că instrumentul de plată electronică este avut în vedere în mod expres doar de art. 250 Cod pen. [efectuarea de operațiuni financiare în mod fraudulos],

¹⁷ JOUE L 123/18 din 10 mai 2019.

Directiva (UE) 2019/713 se referă inclusiv la monedele virtuale. Or, acestea nu sunt incluse de *lege lata* în noțiunea de instrument de plată electronică ceea ce implică necesitatea de a testa aplicabilitatea infracțiunii prevăzute de art. 249 Cod pen. [frauda informatică] în vederea acoperirii acestui aparent „vid legislativ”.

Al doilea titlu al tezei (intitulat „Accesul neautorizat la un sistem informatic”) reprezintă o analiză amplă a infracțiunii prevăzute la art. 360 Cod pen., cu trimiteri repetate la elemente de drept comparat și la o vastă jurisprudență națională și din dreptul comparat.

Pornind de la sursa de inspirație a legiuitorului național și continuând cu modul de transpunere în dreptul intern a Convenției privind criminalitatea informatică și a Directivei 2013/40/UE, au fost evidențiate probleme de interpretare și controverse ce ar putea apărea în practica judiciară raportat la reglementarea actuală. Au fost analizate de asemenea atât decizii ale Curții Constituționale identificate în legătură cu infracțiunea de acces neautorizat la un sistem informatic,¹⁸ cât și recursul în interesul legii soluționat de către Înalta Curte de Casație și Justiție prin decizia nr. 15/2013.¹⁹

Înainte de a se analiza propriu-zis conținutul infracțiunii s-a încercat clarificarea rațiunii incriminării. Prin acest demers nu ne-am propus doar justificarea introducerii unui text de incriminare autonom care să acopere accesul neautorizat la un sistem informatic, ci s-a urmărit inclusiv evidențierea unor posibile asemănări cu infracțiunea de violare de domiciliu [art. 224 Cod pen.]. Scopul unui asemenea demers a fost acela de a identifica anumite puncte de legătură care, în ciuda diferenței la nivel conceptual, să ajute la tranșarea unor aspecte în legătură cu infracțiunea de acces neautorizat la un sistem informatic. Ne referim aici la identificarea subiectului pasiv, delegarea autorizării din partea titularului sistemului informatic, raportul dintre accesul neautorizat și depășirea limitărilor autorizării ori păstrarea neautorizată a accesului etc.

Din perspectiva conținutului infracțiunii analiza a fost una *in extenso*, încercându-se clarificarea tuturor aspectelor problematice ce ar putea să apară în legătură cu acest text de incriminare. Spre exemplu, în ceea ce privește subiectul pasiv ne-am propus elaborarea unei teorii pentru identificarea titularului sistemului informatic, prin raportare la existența unui drept de folosință consolidat, încercând de asemenea lămurirea raportului dintre pluralitatea de subiecți pasivi și pluralitatea de sisteme informatice accesate.

¹⁸ A se vedea în acest sens, decizia Curții Constituționale nr. 183/2018 (publicată în M.Of. nr. 486 din 13.06.2018) și decizia Curții Constituționale nr. 353/2018 (publicată în M.Of. nr. 650 din 26.07.2018).

¹⁹ A se vedea în acest sens, ÎCCJ, Completul competent să judece recursul în interesul legii, dec. nr. 15/2013 (publicată în M.Of. nr. 760 din 6.12.2013).

Analiza laturii obiective a avut ca premisă tipologia accesului neautorizat la un sistem informatic în dreptul comparat pentru a se evidenția discrepanțele majore cu privire la reglementarea acestei infracțiuni. În continuare, s-a încercat în primul rând clarificarea raportului dintre accesul la un sistem informatic și accesul la un mijloc de stocare a datelor informatice, prin raportare la diverse ipoteze problematice. Aceasta pentru a evidenția o posibilă problemă legată de sfera de aplicabilitate a infracțiunii având în vedere omisiunea legiuitorului de a incrimina nu doar accesul la un sistem informatic, ci și accesul la un mijloc de stocare a datelor informatice.

Analiza conduitei incriminate (accesul) s-a bazat inclusiv pe o vastă literatură de specialitate și jurisprudență relevantă cu privire la semnificația noțiunii de acces. Printr-un asemenea demers s-a încercat identificarea unor exemple clare de acces și exemple susceptibile să genereze controverse.

Au fost avute în vedere în acest sens o gamă largă de ipoteze precum: folosirea de la distanță a unui sistem informatic prin intermediul *Team Viewer*; accesarea unui cont bancar online; autentificarea (accesul) fără drept la interfața de administrare a unei pagini web; accesarea unui bancomat prin intermediul unui instrument de plată electronică; alterarea fără drept a unei pagini web prin înlocuirea ori modificarea modului în care aceasta este afișată; transmiterea unui e-mail; atacurile de tip *denial-of-service* [*DoS attack*]; scanarea porturilor [*port scanning*]; obținerea de date informatice prin *phishing*; contrafacerea de pagini web [*web spoofing*]; punerea în vânzare pe Internet a unor bunuri fictive; interacțiunea fizică cu un bancomat; efectuarea de plăți la un terminal POS; efectuarea de plăți online; accesarea unor adrese URL (nepublice) ale unor pagini web (publice); copierea fără drept de date informatice din sistemul informatic aparținând unei terțe persoane; utilizarea unui program informatic tip *keylogger* pentru a intercepta datele introduse de la tastatură de către victimă; infectarea unor sisteme informatice cu un program malițios (virus) etc.

Concluzia cu privire la noțiunea de „acces” a fost aceea că aceasta trebuie să aibă în vedere o interacțiune la nivel logic prin intermediul căreia agentul să poată beneficia de resursele ori/și funcțiile respectivului sistem informatic.

Lipsa autorizării, prin raportare la noțiunea „fără drept”, a făcut de asemenea obiectul unei analize *in extenso* în încercarea de a tranșa anumite controverse. Similar analiza noțiunii de acces au fost avute în vedere numeroase ipoteze identificate în practică judiciară. Cu titlu de exemplu, facem trimitere la următoarele: lipsa autorizării exprese a

administratorului de rețea; utilizarea fără drept a unui card de carburant; introducerea de anunțuri fictive pe platforma eBay; crearea de conturi fictive pe platforma eBay; accesarea unei pagini web restricționate de către angajat cu un scop fraudulos; utilizarea unui laptop bun comun al soților; accesarea contului de Internet banking de către unul dintre soți; accesarea unui cont de e-mail prin folosirea unui parole primite anterior; verificarea situației fiscale a unor contribuabili din altă jurisdicție etc.

Pentru a evidenția cât mai bine complexitatea analizei acestei noțiuni a fost analizată inclusiv jurisprudența Curții de Casație italiene care a extins în mod excesiv sfera de aplicabilitate a infracțiunii de acces neautorizat [acces abuziv în dreptul italian] și teoriile apărute în dreptul american cu privire la lipsa autorizării (teoria contractuală, teoria încălcării unei obligații de loialitate, teoria depășirii unor măsuri de securitate și teoria revocării autorizării). Ulterior tuturor acestor analize s-a încercat identificarea unui *framework* rezonabil prin stabilirea limitelor noțiunii „fără drept” raportat la o serie de criterii obiective adjuvante.

Momentul consumării infracțiunii și delimitarea dintre tentativă și simplele acte de pregătire fără semnificație penală au făcut de asemenea obiectul unei analize detaliate. În context, dincolo de încercarea de a identifica momentul consumării infracțiunii și de a analiza desistarea și împiedicarea producerii rezultatului, au fost avute în vedere ipoteze concrete care ar putea ridica probleme din perspectiva calificării juridice a acestora drept acte de executare ori acte pregătitoare.

Formele agravate ale infracțiunii de acces neautorizat la un sistem informatic (în scopul obținerii de date informatice [art. 360 alin. (2) Cod pen.] și prin depășirea măsurilor de securitate [art. 360 alin. (3) Cod pen.]) beneficiază de o secțiune distinctă. În ceea ce privește agravanta prevăzută la art. 360 alin. (2) Cod pen. s-a analizat conținutul scopului special și relația cu alte infracțiuni. În schimb, agravanta prevăzută la art. 360 alin. (3) Cod pen. a beneficiat de o analiză mai detaliată, fiind atinse aspecte precum: rațiunea incriminării formei agravate, natura măsurilor de securitate (fizice, organizaționale ori logice) ori caracteristici ale acestora.

Cu privire la caracteristicile măsurilor de securitate s-a punctat inclusiv pe diferențierea dintre efectivitatea și fiabilitatea (eficacitatea) măsurilor de securitate, în încercarea de a oferi criterii adjuvante pentru stabilirea unor limite rezonabile de aplicabilitate a acestei agravante. De asemenea, au fost descrise anumite proceduri specifice de interdicere ori de restricționare a accesului (spre exemplu, utilizarea unor

elemente biometrice ori setarea adreselor MAC), împreună cu clarificarea dispozitivelor ori a programelor informatice prin intermediul cărora se poate atinge același scop.

Nu în ultimul rând, au fost analizate modalitățile prin care se poate ajunge la depășirea măsurilor de securitate, aspect ce a generat pe alocuri inclusiv o practică judiciară neunitară. În context, a fost avută în vedere obținerea frauduloasă a datelor de autentificare de la victimă, folosirea acestora după pierderea autorizării sau utilizarea unor date reale în vedere autentificării.

Ultimele două capitole (Capitolul VI și Capitolul VII) ale Titlului II se referă la relația infracțiunii de acces neautorizat la un sistem informatic cu alte infracțiuni prevăzute în Codul penal sau în legislația specială și reformarea art. 360 Cod pen. Cea mai relevantă discuție ține de soluționarea raportului dintre accesul neautorizat la un sistem informatic și violarea secretului corespondenței [art. 302 Cod pen.]. În acest sens, s-a argumentat *in extenso* în sensul reținerii doar a infracțiunii prevăzute de art. 360 Cod pen. în ipoteza accesării corespondenței electronice, în ciuda unor opinii doctrinare și jurisprudențiale în sens contrar.

Al treilea titlu al tezei (intitulat „Frauda informatică”) reprezintă de asemenea o analiză amplă a infracțiunii prevăzute la art. 249 Cod pen., cu trimiteri la elemente de drept comparat.

Dincolo de analiza sursei de inspirație a legiuitorului național, modalitatea de transpunere în dreptul intern a art. 8 din Convenția privind criminalitatea informatică și analiza necesității de a transpune în viitor prevederile Directivei (UE) 2019/713 privind combaterea fraudelor și a contrafacerii în legătură cu mijloacele de plată fără numerar, a fost analizată *in extenso* rațiunea și necesitatea incriminării fraudei informatice. S-a analizat în acest sens posibilul conflict la nivel conceptual între fraudă informatică și înșelăciunea tradițională în încercarea de a concluziona în ce măsură înșelăciunea tradițională poate acoperi conduitele specifice fraudei informatice.

Din perspectiva analizei conținutului infracțiunii de fraudă informatică accentul a fost pus pe o analiză *in concreto* a fiecărei modalități de comitere a faptei, cu trimiteri la ipoteze ce au fost avute în vedere în practica judiciară ori în literatura de specialitate. Astfel, cu privire la fiecare modalitate de comitere în parte, dincolo de a clarifica conținutul respectivei modalități, au fost analizate ipoteze care se pliază pe conceptul de fraudă informatică și ipoteze care ar trebui să se afle sub incidența altor texte de incriminare.

În context, în ceea ce privește **modalitatea introducerii de date informatice** au fost analizate ipoteze precum furtul de monede virtuale, reîncărcarea unei cartele prepay, mărirea „artificială” a soldului contului bancar, licitațiile online frauduloase, activitățile de *phishing* și *pharming*, efectuarea de tranzacții offline, folosirea unui *spyware dialer*, „minarea” de monede virtuale (*crypto-jacking*) etc.

Pentru **modalitatea modificării de date informatice** au fost avute în vedere ipoteze precum efectuarea unui transfer de fonduri, modificarea soldului într-un cont bancar, menținerea ca activat a unui anumit serviciu în vederea facturării suplimentare, alterarea conținutului unei pagini web etc. Cu toate că **modalitatea ștergerii de date informatice** nu este des întâlnită în practica judiciară au fost analizate ipoteze problematice legate de utilizarea unui magnet asupra unui mijloc de stocare a datelor informatice sau ștergerea unor debite din baza de date. În ceea ce privește **modalitatea restricționării accesului la datele informatice** a fost analizată îndeosebi prin raportare la ipoteza restricționării accesului la anumite conturi prin schimbarea parolei de acces la la conduitele de tip *ransomware*. Nu în ultimul rând, **modalitatea împiedicării în orice mod a funcționării unui sistem informatic** a scos în evidență problematica manipulării jocurilor electronice de noroc, a interacțiunii logice cu un bancomat fără a se utiliza un instrument de plată electronică, interacțiunea fizică cu un bancomat (metoda „furculița”), dezactivarea unor dispozitive electronice de protecție pentru sustragerea unui anumit bun etc.

Dincolo de analiza acestor conduite comise ori posibilitatea de a reține comisiunea prin omisiune prin raportare la instituția poziției de garant (art. 17 Cod pen.), a fost analizată urmarea constând în producerea unei pagube și beneficiul material din conținutul scopului special prevăzut de art. 249 Cod pen.

Din perspectiva momentului consumării infracțiunii de fraudă informatică, principala analiză a vizat identificarea actelor preparatorii care nu sunt susceptibile să intre în sfera tentativei. Au fost analizate în acest sens îndeosebi accesul neautorizat la un sistem informatic și activitatea de phishing.

Similar cu infracțiunea de acces neautorizat la un sistem informatic ultimele două capitole sunt dedicate relației infracțiunii de fraudă informatică cu alte infracțiuni prevăzute în Codul penal sau în legislația specială și reformarea art. 249 Cod pen.

Al patrulea titlu al tezei (intitulat „Falsul informatic”), similar cu fraudă informatică și accesul neautorizat la un sistem informatic reprezintă o analiză amplă a

infracțiunii prevăzute la art. 325 Cod pen., cu trimiteri la elemente de drept comparat. Studiul falsului informatic din perspectiva dreptului comparat a fost totuși limitat de faptul că, în ciuda art. 7 din Convenția privind criminalitatea informatică, sistemele de drept de referință pentru dreptul național (dreptul italian, spaniol, german sau francez) nu au incriminat falsul informatic ca o infracțiune autonomă ori au avut o abordare cu totul diferită față de cea a legiuitorului român.

În încercarea de a conceptualiza infracțiunea de fals informatic s-a pornit de la conceptul de înscris tradițional și s-a efectuat o paralelă între funcțiile acestuia și datele informatice relevante din perspectiva falsului informatic. A fost avută așadar în vedere funcția de perpetuare, probatorie și de garanție pentru a încerca efectuarea unei corespondențe între datele informatice asupra cărora intervine agentul și conceptul de document electronic ca echivalent al înscrisului tradițional.

Analiza laturii obiective a infracțiunii de fals informatic a urmat aceeași abordare precum în cazul fraudei informatice și a accesului neautorizat la un sistem informatic. S-a insistat așadar asupra unor ipoteze din practica judiciară, acestea fiind analizate astfel încât să se poată concluziona în ce măsură și-ar putea găsi aplicabilitatea art. 325 Cod pen. ori este incident un alt text de incriminare.

În ceea ce privește **modalitatea introducerii de date informatice** au fost analizate ipoteze precum contrafacerea de pagini web (*web spoofing*), simularea poștei electronice (*e-mail spoofing*), utilizarea fără drept a unei semnături electronice, introducerea de date informatice (informații) false în sistemul ECRIS, crearea de profile (conturi) false sau fictive pe rețelele de socializare, clonarea unei cartele SIM, publicarea de anunțuri fictive pe diverse platforme online, crearea unui duplicat după un document informatic etc. **Modalitatea modificării de date informatice** a fost analizată prin raportare la ipoteze precum modificarea notei de la BAC într-un catalog digital, modificarea numărului de telefon asociat unui cont bancar, modificarea denumirii și prețului unui produs, modificarea numărului de telefon (*caller ID spoofing*), falsificarea unei adrese IP (*IP spoofing*) etc. În ceea ce privește **modalitatea ștergerii de date informatice** a fost avută în vedere în primul rând ștergerea unor debite dintr-o bază de date. Nu în ultimul rând, referitor la **modalitatea restricționării accesului la datele informatice**, a fost analizată situația dezactivării opțiunii de Home Banking sau restricționarea accesului procurorului la anumite documente electronice prin parolarea acestora.

Spre deosebire de fraudă informatică și accesului neautorizat la un sistem informatic, în Titlul IV dedicat infracțiunii de fals informatic se regăsesc două capitole dedicate relației dintre falsul informatic și falsurile tradiționale și relevanța falsului informatic în contextul furtului de identitate.

În ceea ce privește relația dintre falsul informatic și falsul tradițional s-a evidențiat în primul rând paralelismul deficitar din perspectiva limitelor de pedeapsă, sancționării tentativei, incriminării uzului de fals etc. Având drept premisă aceste discrepanțe existente între cele două categorii de infracțiuni au fost analizate diferite ipoteze deosebit de problematice printre care: contrafacerea sau alterarea unui înscris tradițional pe un sistem informatic; continuarea acțiunii de alterare după tipărirea conținutului documentului electronic pe suport hârtie; contrafacerea sau alterarea unei facturi electronice etc.

Toate aceste ipoteze analizate atât din perspectiva falsului informatic cât și a falsului tradițional au avut scopul de a evidenția dificultatea identificării momentului în care putem discuta despre un înscris tradițional ori a actului de executare ori consecințele juridice problematice ale metamorfozei falsului informatic într-un fals tradițional.

În ceea ce privește furtul de identitate, s-a încercat clarificarea acestui concept prin raportare la trei faze acceptate la nivel doctrinar²⁰ și anume: faza obținerii datelor personale; faza interacțiunii cu datele personale obținute în primă fază; faza utilizării efective a datelor personale. Având în vedere aceste trei faze ce înglobează conceptul de furt de identitate s-a analizat relevanța infracțiunii de fals informatic. În context, a fost analizată activitatea de phishing și alte activități conexe susceptibile de a atrage aplicabilitatea art. 325 Cod pen.

Similar cu infracțiunea de acces neautorizat la un sistem informatic ultimele două capitole sunt dedicate relației infracțiunii de fraudă informatică cu alte infracțiuni prevăzute în Codul penal sau în legislația specială și reformarea art. 325 Cod pen.

Summa summarum, prezenta teză reprezintă un studiu aprofundat cu privire la infracțiunea de acces neautorizat la un sistem informatic, fraudă și falsul informatic. Analiza se axează în principal pe analiza unor probleme de drept ignorate în mare parte de

²⁰ A se vedea în acest sens S. Schjolberg, *The History of Cybercrime 1976-2014*, Cybercrime Research Institute, Cologne, 2014 p. 128; M. Gercke, *Internet-related identity theft*, Discussion Paper (Council of Europe), 2007, p. 13; J. Clough, *Principles of Cybercrime, second edition, precit.*, p. 238; A.N. Martín, *Identity theft and international criminal policy: manufacturing consent*, în „Cahiers de défense sociale”, nr. 36/2009-2010, p. 25.

în literatura de specialitate autohtonă, dar care au ridicat probleme deosebite în practica judiciară.