

George Zlati

# Tratat de criminalitate informatică



# Cuprins

<b>Prefață</b> .....	<b>XXV</b>
<b>Listă de abrevieri</b> .....	<b>XXVII</b>
<b>Introducere</b> .....	<b>1</b>
<b>Titlul I. Conceptul de „criminalitate informatică” și aspecte terminologice</b> .....	<b>5</b>
<b>Capitolul I. Criminalitatea informatică</b> .....	<b>5</b>
Secțiunea 1. Conceptul de „criminalitate informatică” .....	5
§1. Infrațiuni îndreptate împotriva sistemelor ori datelor informatice. Sistemul informatic ca obiect al conduitei infracționale .....	15
§2. Infrațiuni unde sistemul informatic este doar un mijloc pentru a comite infracțiunea. Sistemul informatic ca subiect al conduitei infracționale .....	15
§3. Conduite infracționale ce sunt incidentale pentru comiterea altor infracțiuni tradiționale .....	16
Secțiunea a 2-a. Caracterile 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
<b>Capitolul II. Aspecte terminologice</b> .....	<b>29</b>
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 (automated teller machine – ATM) .....	72
7.7. Terminalele POS (point of sale).....	73
7.8. Dispozitivul tip skimmer .....	74
7.9. Telefoanele mobile inteligente (smartphones) .....	75
7.10. Terminalele de comunicații.....	76
7.11. Ceasurile inteligente (smartwatch).....	78
7.12. Televizoarele inteligente (smart tv) .....	79
7.13. Imprimanta, faxul și scannerul .....	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 Internet of Things (IoT) .....	83
7.19. Cartela SIM (Subscriber Identity Module).....	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 (suporturi) 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 banda 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
<b>Titlul II. Accesul neautorizat la un sistem informatic (art. 360 C.pen.).....</b>	<b>111</b>
<b>Prezentare generală .....</b>	<b>111</b>
<b>Capitolul I. Raportul dintre reglementarea națională și instrumentele juridice     supranaționale .....</b>	<b>112</b>
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
<b>Capitolul II. Decizii ale Curții Constituționale, Recursuri în interesul legii și Decizii     ale Curții Europene a Drepturilor Omului .....</b>	<b>125</b>
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 skimmer-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 (Bărbulescu c. României) .....	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 Bărbulescu cu privire la incidența art. 360 C.pen. ....	137
<b>Capitolul III. Rațiunea și necesitatea incriminării.....</b>	<b>139</b>
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
<b>Capitolul IV. Analiza conținutului infracțiunii de acces neautorizat la un sistem informatic.....</b>	<b>147</b>
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 (in 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 [remote access] 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. defacing].....	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 (trial access) a expirat.....	200
2.2. Accesarea unei baze de date în mod autorizat, continuată de cereri SQL [SQL queries], 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 denial-of-service [DoS attack] .....	203
3.4. Scanarea porturilor [port scanning] .....	203
3.5. Obținerea de date informatice prin phishing.....	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 keylogger, 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 aceasta 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
§2. Orientări jurisprudențiale relevante în dreptul comparat.....	222
2.1. Jurisprudența Curții de Casație italiene.....	222
2.2. Teorii ale accesului „fără drept” în dreptul american .....	225
2.2.1. Teoria contractuală [contract-based approach] .....	226
2.2.2. Teoria încălcării unei obligații de loialitate ori fiduciare [agency-based approach].....	230
2.2.3. Teoria depășirii unor măsuri de securitate [code-based approach] .....	231
2.2.4. Teoria revocării autorizării.....	232
§3. Identificarea unui framework rezonabil pentru noțiunea „fără drept” .....	234
3.1. Stabilirea unor puncte de reper.....	234
3.2. Soluționarea limitelor autorizării pentru accesul între soți.....	236
3.3. 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 [boot-area] 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 interzicere 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 [media access control adress] .....	261
2.5.5. Securizarea unui browser web .....	262
2.6. Dispozitive de interzicere 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**

<b>cu alte infracțiuni.....</b>	<b>266</b>
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 neloyală (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
<b>Capitolul VI. Reformarea art. 360 C.pen.</b> .....	<b>286</b>
Secțiunea 1. O reformă conceptuală? .....	286
Secțiunea a 2-a. Propuneri referitoare la modificarea art. 360 C.pen. ....	287
§1. Introducerea „încălării 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 de lege ferenda ce ar trebui evitate.....	289
§1. Introducerea plângerii prealabile.....	289
§2. Introducerea unor cauze de atipicitate.....	289
§3. Alte intervenții de lege ferenda .....	290
<b>Titlul III. Frauda informatică (art. 249 C.pen.) .....</b>	<b>291</b>
<b>Aspecte introductive .....</b>	<b>291</b>
<b>Capitolul I. Raportul dintre reglementarea națională și instrumentele juridice supranaționale .....</b>	<b>293</b>
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
<b>Capitolul II. Rațiunea și necesitatea incriminării fraudei informatice .....</b>	<b>308</b>
<b>Capitolul III. Analiza conținutului infracțiunii de fraudă informatică .....</b>	<b>316</b>
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 comisive .....	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 phishing și pharming.....	358
D) Trimiterea de corespondență electronică nesolicitată (spam) .....	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 ghișeul băncii.....	364
H) Folosirea unui spyware dialer/utilizarea frauduloasă a serviciului VoIP (Voice over IP) .....	365
I) Comandarea frauduloasă de produse în calitate de agent de vânzări .....	367
J) Folosirea unor coduri paysafecard pentru efectuarea de plăți online .....	368
K) „Minarea” de monede virtuale (crypto-jacking).....	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 transferuri 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, problematică 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 ransomware .....	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, problematică 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 (denial-of-service) .....	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 phishing .....	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. 2561 C.pen. ....	421
§2. Aplicarea legii penale mai favorabile, prin raportare la art. 2561 C.pen. și Decizia CCR nr. 368/2017 .....	423
<b>Capitolul IV. Raportul dintre infracțiunea de fraudă informatică și alte infracțiuni .....</b>	<b>425</b>
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
3.4. 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, rounding-down fraud] .....	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 autoperjudiciante 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 frauda 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
<b>Capitolul V. Reformarea art. 249 C.pen.....</b>	<b>468</b>
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 de lege ferenda 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 de lege ferenda.....	472
<b>Titlul IV. Falsul informatic (art. 325 C.pen.).....</b>	<b>475</b>
<b>Aspecte introductive .....</b>	<b>475</b>
<b>Capitolul I. Raportul dintre reglementarea națională și instrumentele juridice supranaționale .....</b>	<b>476</b>
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
<b>Capitolul II. Rațiunea și necesitatea incriminării .....</b>	<b>485</b>
<b>Capitolul III. Analiza conținutului infracțiunii de fals informatic .....</b>	<b>487</b>
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. Înscrisul 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 [web spoofing].....	515
B) Simularea poștei electronice [e-mail spoofing] 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 hash 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 (caller ID spoofing) .....	551

C) Falsificarea unei adrese IP (IP spoofing).....	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
1. Cadrul general .....	557
2. Ipoteze de comitere a falsului informatic prin restricționarea accesului la datele informatice .....	557
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
<b>Capitolul IV. Raportul dintre falsul informatic și falsurile tradiționale .....</b>	<b>578</b>
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 improprie.....	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
<b>Capitolul V. Furtul (uzurparea) de identitate. ....</b>	<b>592</b>
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 phishing.....	600
§2. Activitatea de pharming.....	602

<b>Capitolul VI. Raportul dintre infracțiunea de fals informatic și alte infracțiuni .....</b>	<b>604</b>
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
<b>Capitolul VII. Reformarea art. 325 C.pen. ....</b>	<b>612</b>
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
<b>Ultimul cuvânt .....</b>	<b>617</b>
<b>Bibliografie .....</b>	<b>619</b>
<b>Monografii .....</b>	<b>619</b>
<b>Articole / studii / rapoarte .....</b>	<b>625</b>
<b>Index .....</b>	<b>643</b>