

Cuprins

Prefață	5
Abrevieri	7
Argument	9

CAPITOLUL I. ASPECTE INTRODUCATIVE PRIVIND FENOMENUL DE CRIMINALITATE INFORMATICĂ

1.1. Introducere	11
1.2. Definiția noțiunii de criminalitate informatică	14
1.3. Clasificarea infracțiunilor informatice	20
1.4. Rolul computerului în comiterea infracțiunilor	33
1.5. Analiza juridică generală a infracțiunilor informatice	38
1.5.1. Conținutul infracțiunilor informatice	38
1.5.1.1. Obiectul infracțiunii	40
1.5.1.2. Subiecții infracțiunii	40
1.5.1.3. Latura obiectivă	41
1.5.1.4. Latura subiectivă	41
1.5.2. Autorul infracțiunilor informatice	42
1.6. Caracteristicile infracțiunilor informatice	45
1.7. Principalele organizații internaționale și regionale implicate în studiul fenomenului de criminalitate informatică	46
1.7.1. Organizații internaționale	46
1.7.1.1. Consiliul Europei	46
1.7.1.2. Organizația Națiunilor Unite	49
1.7.1.3. Grupul G8	50
1.7.1.4. Uniunea Internațională a Telecomunicațiilor	51
1.7.1.5. Interpol	52
1.7.2. Organizații regionale	53
1.7.2.1. Uniunea Europeană	54
1.7.2.2. Organizația pentru Cooperare și Dezvoltare Economică	58
1.7.2.3. Grupul APEC	60
1.7.2.4. Commonwealth	61
1.7.2.5. Liga Arabă și Consiliul de Cooperare din Golf	62
1.7.2.6. Organizația Statelor Americane	62
1.7.3. Organisme științifice	63
1.7.4. Concluzii	64

CAPITOLUL II. REGLEMENTAREA JURIDICĂ NAȚIONALĂ ȘI INTERNAȚIONALĂ A CRIMINALITĂȚII INFORMATICE

	67
2.1. Cadrul general privind infracțiunile informatice în sistemul juridic românesc	67
2.1.1. Considerații introductive.....	67
2.1.2. Analiza infracțiunilor incriminate în Legea nr. 161/2003	69
2.1.2.1. Infracțiuni contra confidențialității și integrității datelor și sistemelor informatice	69
2.1.2.1.1. Accesul ilegal la un sistem informatic	69
2.1.2.1.2. Interceptarea ilegală a unei transmisii de date informatice	74
2.1.2.1.3. Alterarea integrității datelor informatice.....	79
2.1.2.1.4. Infracțiunea de perturbare a funcționării sistemelor informatice	83
2.1.2.1.5. Operațiuni ilegale cu dispozitive sau programe informatice	86
2.1.2.2. Infracțiuni informatice.....	89
2.1.2.2.1. Infracțiunea de fals informatic	89
2.1.2.2.2. Infracțiunea de fraudă informatică.....	91
2.1.2.3. Pornografia infantilă prin intermediul sistemelor informatice	94
2.1.2.3.1. Infracțiunea de pornografie infantilă prin intermediul sistemelor informatice.....	94
2.1.3. Aspecte de drept procesual penal privind infracțiunile informatice.....	97
2.1.3.1. Considerații privind desfășurarea urmăririi penale în cazul infracțiunilor informatice	97
2.1.3.2. Dispoziții procedurale prevăzute în Legea nr. 161/2003	100
2.1.3.2.1. Conservarea datelor informatice	101
2.1.3.2.2. Ridicarea obiectelor care conțin date informatice ...	103
2.1.3.2.3. Percheziția informatică	104
2.1.3.2.4. Accesul într-un sistem informatic și interceptarea și înregistrarea comunicărilor desfășurate prin intermediul sistemelor informatice	106
2.1.4. Infracțiunile informatice în reglementarea Noului Cod penal.....	109
2.2. Reglementarea infracțiunilor informatice în Convenția Consiliului Europei privind criminalitatea informatică	115
2.2.1. Considerații preliminare	115

2.2.2. Dreptul penal material în reglementarea Convenției Consiliului Europei privind criminalitatea informatică.....	116
2.2.2.1. Art. 2 – Accesarea ilegală.....	116
2.2.2.2. Art. 3 – Interceptarea ilegală	117
2.2.2.3. Art. 4 – Afectarea integrității datelor	118
2.2.2.4. Art. 5 – Afectarea integrității sistemului	119
2.2.2.5. Art. 6 – Abuzurile asupra dispozitivelor	119
2.2.2.6. Art. 7 – Falsificarea informatică	120
2.2.2.7. Art. 8 – Frauda informatică	120
2.2.2.8. Art. 9 – Infracțiuni referitoare la pornografia infantilă	121
2.2.2.9. Art. 10 – Infracțiuni referitoare la atingerile aduse proprietății intelectuale și drepturilor conexe	122
2.2.2.10. Concluzii	123
2.3. Aspecte de drept comparat privind criminalitatea informatică	125
2.3.1. Statele Unite ale Americii.....	125
2.3.2. Marea Britanie.....	129
2.3.3. Australia	132
2.3.4. Germania	134
2.3.5. Franța.....	137
2.3.6. Concluzii.....	140

CAPITOLUL III. MODURI DE OPERARE FRECVENTE ÎNTÂLNITE ÎN CRIMINALITATEA INFORMATICĂ.....

3.1. Considerații preliminare.....	141
3.2. Atacuri asupra sistemelor informatice bazate pe software	142
3.2.1. Programe malițioase	142
3.2.1.1. Programe malițioase care au ca scop infectarea sistemului informatic	143
3.2.1.2. Programe malițioase care au ca scop ascunderea acțiunilor lor.....	144
3.2.1.3. Programe malițioase care aduc profit prin intermediul acțiunilor pe care le efectuează	145
3.3. Atacuri asupra rețelelor și sistemelor informatice	148
3.3.1. Refuzul serviciului – DOS	148
3.3.2. Backdoor	149
3.3.3. Sniffer-ul.....	149
3.3.4. Spoofing-ul	150
3.3.5. Man-in-the-Middle Attack	150
3.3.6. Spargerea parolelor	151
3.3.7. Phishing-ul	152
3.3.7.1. Amenințări de tip phishing	152
3.3.7.1.1. Factorii de inginerie socială.....	152

3.3.7.1.2. Distribuirea mesajelor phishing	153
3.3.7.1.2.1. Distribuirea mesajelor phishing bazate pe e-mail și spam	153
3.3.7.1.2.2. Distribuirea mesajelor phishing bazate pe Web... ..	153
3.3.7.1.2.3. Distribuirea mesajelor phishing bazate pe IRC și Mesageria Instantanee	154
3.3.8. Furtul de identitate referitor la Internet.....	154
3.4. Metode de ascundere a datelor informatice	156
3.4.1. Aplicațiile steganografiei	156
3.4.1.1. Aplicațiile steganografiei la imagini.....	156
3.4.1.2. Aplicațiile steganografiei la fișierele video	157
3.4.1.3. Aplicațiile steganografiei la fișierele text.....	157
3.4.1.4. Aplicațiile steganografiei la fișierele de sistem	157
3.4.1.5. Aplicațiile steganografiei la ascunderea datelor în spațiul hard-discului	158
3.5. Concluzii	158

CAPITOLUL IV. ASPECTE METODOLOGICE PRIVIND INVESTIGAREA CRIMINALISTICĂ A INFRAȚIUNILOR INFORMATICE

4.1. Definiția noțiunii de investigare.....	159
4.2. Considerații privind noțiunea de Științe Forensic	160
4.3. Certificarea, Standardizarea și Acreditarea în domeniul investigării criminalistice a infracțiunilor informatice.....	161
4.3.1. Considerații preliminare	161
4.3.2. Organizații care certifică investigarea criminalistică a infracțiunilor informatice	163
4.3.3. Standardizarea în domeniul investigării infracțiunilor informatice.....	165
4.3.3.1. Standardizarea la nivel internațional	165
4.3.3.2. Standardizarea la nivel european.....	166
4.3.3.3. Standardizarea în Statele Unite ale Americii	167
4.3.3.4. Standardizarea în România	167
4.3.4. Acreditarea în domeniul investigării infracțiunilor informatice.....	168
4.3.4.1. Acreditarea la nivel internațional	168
4.3.4.2. Acreditarea la nivel european	168
4.3.4.3. Acreditarea în Statele Unite ale Americii	169
4.3.4.4. Acreditarea în România	169
4.4. Organisme cu atribuții în prevenirea și combaterea criminalității informatice	170

4.4.1. Direcția de Investigare a Infrațunilor de Criminalitate Organizată și Terorism din cadrul Parchetului de pe lângă Înalta Curte de Casație și Justiție	170
4.4.2. Direcția de Combatare a Criminalității Organizate	171
4.5. Probele digitale	172
4.5.1. Considerații preliminare privind definiția probelor	172
4.5.2. Noțiunea de probe digitale	173
4.5.3. Principii și standarde în domeniul probelor digitale	175
4.5.4. Caracteristicile probelor digitale	177
4.5.5. Potențiale probe digitale în sistemele informatice	179
4.5.6. Principii de examinare a unui sistem informatic pentru a se obține probele digitale	180
4.6. Metodologii de investigare a infrațunilor informatice	180
4.6.1. Definiția noțiunii de „metodologie de investigare a infrațunilor informatice”	180
4.6.2. Metodologii de investigare a infrațunilor informatice în literatura de specialitate	181
4.6.2.1. Séamus Ó Ciardhuáin. Un model extins de investigare a infrațunilor informatice	182
4.6.2.1.1. Fluxurile de informații existente în metodologia prezentată	184
4.6.2.2. Brian Carrier, Eugene H. Spafford. Un proces integrat de investigare digitală	185
4.6.2.3. Mark Reith, Clint Carr, Gregg Gunsch. Un model Criminalistic Digital Abstract	190
4.6.2.4. Hai-Cheng Chu, Der-Jiunn Deng, Han-Chieh Chao. Model pentru investigații criminalistice digitale	191
4.6.2.5. George Mohay, Alison Anderson, Byron Collie, Olivier De Vel, Rod McKemmish. Model de investigare criminalistică a infrațunilor informatice (CFSAP – Computer Forensic Secure Analyze Present Model)	192
4.6.2.6. Gary R. Gordon, Chet D. Hosmer, Christine Siedsma, Don Rebovich. Investigarea criminalistică a infrațunilor informatice	193
4.6.3. Metodologii de investigare a infrațunilor informatice în cadrul unor instituții și organizații	194
4.6.3.1. Institutul Național pentru Standarde și Tehnologie din cadrul Departamentului de Comerț al Statelor Unite ale Americii	194
4.6.3.2. Romanian Information Technology Initiative și Guvernul României	196

4.6.3.3. Institutul Național de Justiție din cadrul Departamentului de Justiție al Statelor Unite ale Americii.....	197
4.6.3.4. Grupul de lucru „Digital Forensic Research Workshop”	198
4.6.4. Concluzii.....	200
4.6.4.1. Analiza modelelor de investigare a infracțiunilor informatic prezentate	200
4.6.4.2. Propunere de model de investigare a infracțiunilor informatic	202

CAPITOLUL V. PARTICULARITĂȚI PRIVIND PERCHEZIȚIA CALCULATORULUI ȘI CERCETAREA LA FAȚA LOCULUI ÎN CAZUL INFRACTIUNILOR INFORMATICE.....

5.1. Particularități tactice de efectuare a percheziției sistemelor informatic	204
5.1.1. Aspecte generale	204
5.1.1.1. Noțiunea și importanța percheziției	204
5.1.1.2. Reguli tactice generale aplicate în efectuarea percheziției.....	205
5.1.2. Efectuarea percheziției informatice.....	205
5.2. Particularități privind cercetarea la fața locului în cazul infracțiunilor informatice	208
5.2.1. Noțiunea, obiectivele și importanța cercetării la fața locului ..	208
5.2.1.1. Noțiunea de cercetare la fața locului	208
5.2.1.2. Considerații privind reglementarea procesual penală	209
5.2.1.3. Importanța cercetării la fața locului.....	211
5.2.2. Fazele cercetării la fața locului în cazul infracțiunilor informatic.....	212
5.2.3. Fixarea rezultatelor cercetării la fața locului în cazul infracțiunilor informatice	213
5.3. Etapele procesului de investigare a infracțiunilor informatice	213
5.3.1. Pregătirea investigării.....	214
5.3.1.1. Pregătirea echipei de investigare	214
5.3.1.1.1. Rolul primelor organe judiciare sosite la fața locului	214
5.3.1.1.2. Rolul investigatorilor.....	216
5.3.1.1.3. Rolul tehnicienilor de la fața locului.....	217
5.3.1.2. Pregătirea instrumentelor de investigare.....	221
5.3.1.3. Obținerea documentelor necesare desfășurării procesului de investigare	224
5.3.2. Colectarea probelor.....	225

5.3.2.1. Securizarea, evaluarea și înregistrarea locului infrațiunii.....	225
5.3.2.2. Căutarea de probe.....	231
5.3.2.3. Ascultarea persoanelor implicate	232
5.3.2.4. Conservarea probelor	233
5.3.2.4.1. Conservarea probelor volatile	235
5.3.2.4.2. Conservarea probelor nevolatile	237
5.3.2.5. Particularități ale colectării probelor în cazul computerelor legate în rețea.....	240
5.3.3. Examinarea probelor.....	241
5.3.4. Analiza probelor	243
5.3.4.1. Analiza intervalului de timp.....	243
5.3.4.2. Analiza datelor ascunse	243
5.3.4.3. Analiza aplicațiilor și a fișierelor.....	245
5.3.4.4. Analiza datelor criptate	245
5.3.4.5. Analiza informațiilor despre site-urile Web vizitate	245
5.3.4.6. Analiza fișierelor temporare.....	246
5.3.4.7. Analiza fișierelor de schimb	247
5.3.5. Raportarea	248

CAPITOLUL VI. INVESTIGAREA TRAFICULUI DE REȚEA ȘI A APLICAȚIILOR DE INTERNET.....

6.1. Investigarea traficului de rețea	252
6.1.1. Aspecte introductive.....	252
6.1.2. Surse de date legate de traficul de rețea	254
6.1.2.1. Firewall-uri și Router-e.....	254
6.1.2.2. Detectoarele de pachete și analizatorii de protocol.....	254
6.1.2.3. Sistemele de detectare a intruziunii.....	255
6.1.2.4. Accesul de la distanță.....	255
6.1.2.5. Software-ul de management al securității evenimentului.....	256
6.1.2.6. Instrumente de analiză criminalistică a rețelei.....	256
6.1.3. Alte tipuri de surse de date legate de traficul de rețea:	256
6.1.4. Colectarea datelor referitoare la traficul de rețea	257
6.1.5. Examinarea și analiza datelor referitoare la traficul de rețea	258
6.1.5.1. Valoarea sursei de date.....	258
6.1.5.2. Instrumente de examinare și analiză a traficului de rețea	260
6.2. Investigarea aplicațiilor de Internet.....	260
6.2.1. Investigarea unei adrese IP sau a unei adrese de Internet ...	260
6.2.2. Investigarea e-mail-ului.....	266

6.2.3. Investigarea paginilor Web	270
6.2.3.1. Identificarea sursei HTML la o pagina Web	272
6.2.3.2. Identificarea datelor din pagina Web	272
6.2.3.3. Localizarea și sechestrarea server-ului Web	272
6.2.4. Investigarea Mesageriei Instantanee, Grupurilor de discuții și Dialogului on-line	273
6.2.4.1. Investigarea Mesageriei Instantanee	273
6.2.4.2. Investigarea Grupurilor de discuții	274
6.2.4.3. Investigarea Dialogului on-line	275

CAPITOLUL VII. INVESTIGAREA INFRAACȚIUNILOR INFORMATICE SĂVÂRȘITE PRIN UTILIZAREA FRAUDULOASĂ A INSTRUMENTELOR DE PLATĂ ELECTRONICĂ

7.1. Comerțul electronic	277
7.1.1. Definiția comerțului electronic	277
7.1.2. Sisteme electronice de plată	277
7.1.3. Reglementarea juridică a comerțului electronic	278
7.1.3.1. Reglementarea juridică a comerțului electronic în Uniunea Europeană	278
7.1.3.2. Reglementarea juridică a comerțului electronic în România	279
7.2. Semnătura electronică ca mijloc de probă	281
7.2.1. Definiția și structura semnăturii electronice	282
7.2.2. Reglementarea juridică a semnăturii electronice	284
7.2.2.1. Reglementarea juridică a semnăturii electronice în Uniunea Europeană	284
7.2.2.2. Reglementarea juridică a semnăturii electronice în România	285
7.3. Considerații generale privind cardurile ca sisteme electronice de plăți	286
7.3.1. Definiția noțiunii de card și tipuri de carduri	286
7.3.2. Caracteristicile cardurilor bancare	288
7.4. Tipuri de fraude în legătură cu cardurile bancare	290
7.4.1. Contrafacerea cardurilor bancare	290
7.4.1.1. Obținerea detaliilor bancare ale unui cont de card	290
7.4.1.2. Falsificarea propriu-zisă	294
7.4.2. Carduri pierdute sau furate	294
7.4.3. Cardurile obținute prin aplicații false	295
7.4.4. Preluarea contului	295
7.4.5. Fraude la comerciant	295

7.5. Particularități privind investigarea infracțiunilor informatice săvârșite prin utilizarea frauduloasă a instrumentelor de plată electronică	296
7.5.1. Analiza fizică a cardurilor bancare	298
7.5.2. Analiza logică a cardurilor bancare	299
7.5.3. Prezentarea unui raport de constatare tehnico-științifică	299

CAPITOLUL VIII. PARTICULARITĂȚI ALE INVESTIGĂRII INFRAȚIUNILOR INFORMATICE SĂVÂRȘITE PRIN INTERMEDIUL TELEFONIEI MOBILE

8.1. Aspecte legale privind comunicațiile electronice în România	301
8.2. Interceptările și înregistrările audio-video	302
8.3. Noțiuni introductive privind telefonía mobilă	306
8.3.1. Comunicațiile celulare	307
8.3.2. Structura unei rețele GSM	308
8.3.3. Componenta unui telefon celular	310
8.4. Etapele de investigare a infracțiunilor informatice săvârșite prin intermediul telefoniei mobile	313
8.4.1. Conservarea datelor	313
8.4.1.1. Securizarea și evaluarea locului infracțiunii	313
8.4.1.2. Înregistrarea scenei infracțiunii	314
8.4.1.3. Colectarea probelor	314
8.4.1.4. Împachetarea, transportul și stocarea probelor	315
8.4.2. Achiziția datelor	316
8.4.2.1. Identificarea telefonului mobil	316
8.4.2.1.1. Caracteristicile telefonului mobil	316
8.4.2.1.2. Interfața telefonului mobil	316
8.4.2.1.3. Eticheta telefonului mobil	317
8.4.2.2. Considerații privind memoria telefonului mobil și memoria cardului SIM	317
8.4.2.3. Obținerea datelor din telefonul mobil	318
8.4.2.3.1. Considerații privind telefoanele mobile GSM	319
8.4.2.3.2. Considerații privind cardul SIM	320
8.4.2.4. Metode de recuperare a datelor din telefoanele mobile blocate	321
8.4.2.4.1. Metode bazate pe investigare	321
8.4.2.4.2. Metode bazate pe software	321
8.4.2.4.3. Metode bazate pe hardware	322
8.4.2.5. Dispozitive care conțin memorie și sunt asociate cu telefonul mobil	323
8.4.3. Examinarea și analiza datelor	323
8.4.3.1. Potențiale probe aflate în telefonul mobil	324

8.4.3.2. Potențiale probe aflate în cardul SIM	324
8.4.3.3. Potențiale probe aflate în rețeaua de telefonie mobilă ...	325
8.4.3.4. Instrumente de investigare pentru analiza probelor	327
8.4.3.4.1. Instrumente de investigare care extrag datele din cardul SIM	328
8.4.3.4.2. Instrumente de investigare care extrag datele din telefonul mobil	328
8.4.3.4.3. Kit-uri cu instrumente de investigare	329
8.4.4. Raportarea rezultatelor obținute	329
8.5. Atacuri des întâlnite în telefonia mobilă	330
8.5.1. Atacuri asupra cardului SIM	330
8.5.2. Atacuri asupra telefonului mobil	331
8.5.3. Atacuri asupra rețelei GSM	332

CAPITOLUL IX. PARTICULARITĂȚI ALE INVESTIGĂRII INFRAȚIUNILOR INFORMATICE DIN CATEGORIA PORNOGRAFIEI INFANTILE

9.1. Introducere	333
9.2. Reglementarea juridică a pornografiei infantile	335
9.2.1. Reglementarea juridică a pornografiei infantile la nivel internațional	335
9.2.2. Reglementarea juridică a pornografiei infantile în România ..	339
9.3. Localizarea probelor digitale în cazul infracțiunilor informatice din categoria pornografiei infantile	340
9.4. Urma electronică pe Internet ca mijloc de probă	344
9.4.1. Atribuirea și continuitatea infracțiunii	344
9.4.2. Determinarea fizică a contactelor și locațiilor	345
9.4.3. Utilizarea fișierelor de evidență ale furnizorilor de servicii de Internet	346
9.4.4. Descoperirea activităților ilegale pe Internet	347
9.4.4.1. World Wide Web	347
9.4.4.2. E-mail	347
9.4.4.3. Partajarea fișierelor	348

CAPITOLUL X. COOPERAREA INTERNAȚIONALĂ ȘI EUROPEANĂ ÎN DOMENIUL COMBATERII CRIMINALITĂȚII INFORMATICE

10.1. Caracterul transfrontalier al infracțiunilor informatice	349
10.2. Cooperarea judiciară internațională în domeniul combaterii criminalității informatice	350
10.2.1. Convenția Consiliului Europei privind criminalitatea informatică	350

10.2.1.1. Jurisdicția penală	350
10.2.1.2. Principiile generale referitoare la cooperarea internațională	352
10.2.1.3. Principii referitoare la extrădare.....	353
10.2.1.4. Principii generale referitoare la asistența juridică reciprocă	354
10.2.1.5. Informarea spontană.....	354
10.2.1.6. Procedurile referitoare la cererile de asistență juridică reciprocă în absența acordurilor internaționale aplicabile	354
10.2.1.7. Asistența judiciară reciprocă în materie de măsuri provizorii.....	355
10.2.1.8. Accesarea transfrontalieră a datelor stocate	356
10.2.1.9. Rețeaua de contacte 24/7	357
10.2.2. Convenția Națiunilor Unite împotriva criminalității organizate transfrontaliere	359
10.2.3. Convenția europeană de asistență judiciară în materie penală.....	360
10.2.4. Interpol	361
10.3. Cooperarea judiciară europeană în domeniul combaterii criminalității informatice	362
10.3.1. Decizia-Cadru a Consiliului Uniunii Europene 2002/584/JAI privind mandatul european de arestare și procedurile de predare între statele membre.....	362
10.3.2. Decizia-Cadru 2008/978/JAI a Consiliului Uniunii Europene privind mandatul european de obținere a probelor în scopul obținerii de obiecte, documente și date în vederea utilizării acestora în cadrul procedurilor în materie penală	364
10.3.3. Convenția privind asistența judiciară reciprocă în materie penală între statele membre ale Uniunii Europene.....	365
10.3.4. Eurojust	365
10.3.5. Rețeaua Judiciară Europeană în materie penală	366
10.3.6. Europol.....	368
10.4. Legislația din România privind cooperarea internațională în domeniul combaterii criminalității informatice.....	368

CONCLUZII ȘI PROPUNERI DE LEGE FERENDA.....	371
---	-----

ANEXA I

LEGISLAȚIA DIN ROMÂNIA ÎN DOMENIUL TEHNOLOGIEI INFORMAȚIEI ȘI COMUNICAȚIILOR.....	382
--	-----

ANEXA II

Organigrama pașilor efectuați în procesul de colectare a probelor digitale	390
---	-----

ANEXA III

Structura rețelei GSM	391
-----------------------------	-----

ANEXA IV

Organigrama procedurii de conservare a probelor în cazul infrapecuniilor informatice săvârșite prin intermediul telefoniei mobile	392
--	-----

BIBLIOGRAFIE	393
--------------------	-----