

**BABEȘ-BOLYAI UNIVERSITY**

**FACULTY OF LAW**

# **DOCTORAL THESIS**

**Unauthorized Access to a Computer System,  
Computer Fraud, and Computer-related  
Forgery**

*(table of contents and summary)*

**Doctoral Thesis Coordinator:**

**Professor Sergiu BOGDAN**

**PhD Student:**

**George Michail Rudolf ZLATI**

# TABLE OF CONTENTS

<b>Abbreviations.....</b>	<b>31</b>
<b>Introduction.....</b>	<b>33</b>

## SECTION I THE CONCEPT OF CYBERCRIME AND TERMINOLOGY MATTERS

<b>Chapter I. Cybercrime.....</b>	<b>38</b>
<b>§1. The Concept of Cybercrime.....</b>	<b>38</b>
1. Crimes Directed Against Information Systems or Data. The Computer System as an Object of Criminal Conduct .....	49
2. Crimes Where the Information System Is Just a Means of Committing the Offense. The Computer System as a Subject of Criminal Conduct .....	50
3. Types of Criminal Conduct Which Are Incidental to the Perpetration of Other Traditional Crimes.....	51
<b>§2. Statistics Relevant to Cybercrime.....</b>	<b>52</b>
<b>§3. The Nature and Legal Treatment of Cybercrimes.....</b>	<b>54</b>
<b>§4. Pioneer-States in the Field of Cybercrime.....</b>	<b>57</b>
<b>Chapter II. Terminology Matters.....</b>	<b>68</b>
<b>§1. The Concept of Information System.....</b>	<b>68</b>
§1.1. The Definition of an Information System in International Legal Instruments And European Legal Instruments.....	69
§1.2. The Definition of an Information System as Construed by National Legislation.....	77
§1.3. The Definition of an Information System as Construed by comparative Law.....	77
§1.3.1. Legal Systems Where the Concept of Information System Benefits From a Legal Definition.....	80
§1.3.2. Legal Systems Where the Concept of Information System Does Not Benefit from a Legal Definition.....	85

§1.4. The Information System in the Case Law of National Courts and That of the Constitutional Court.....	89
§1.4.1. The Appeal In The Interest Of the Law - Decision No 15/2013 of the High Court of Cassation and Justice.....	89
§1.4.2. The Case Law of National Courts.....	90
§1.4.3. The Case Law of the Constitutional Court.....	92
§1.5. The Importance of the Proper Qualification of A Device As An Information System.....	98
1. The Relevance of the Information System Concept from the Perspective Of Substantive Criminal Law .....	98
2. The Relevance of the Information System Concept from the Perspective Of Procedural Criminal Law.....	98
3. The Relevance of the Information System Concept from the Perspective Of Legislative Technique.....	98
§1.6. The Analysis of Legal Criteria Arising From the Definition of the Information System.....	103
1. The Computer System as a Device.....	104
2. Automatic Processing Of Computerized Data.....	108
3. The Automatic Processing Of Data Via A Computer Program.....	111
§1.7. Examples of Information Systems and Problematic Examples.....	113
1. Servers Which Provide Certain Services or Where Certain Web Pages Are Hosted.....	114
2. The Electronic Trading System on the Capital Market.....	117
3. Databases.....	117
4. Web Pages.....	119
5. Social Networks.....	119
6. ATMs ( <i>automated teller machines</i> ).....	120
7. POS Terminals ( <i>Point Of Sale Terminals</i> ).....	122
8. Skimmer Devices.....	123
9. Smart Mobile Phones ( <i>smartphones</i> ) .....	124
10. Communications Terminals .....	125
11. Smartwatches.....	127

12. Smart-TVs.....	128
13. Printers, Fax Machines and Scanners.....	129
14. Digital Voice Recorders.....	130
15. Automatic Ticket Distribution Devices.....	131
16. Digital Surveillance Cameras.....	131
17. Gambling Machines.....	132
18. Devices in the <i>Internet of Things</i> Category.....	133
19. SIM ( <i>Subscriber Identity Module</i> ) Cards.....	135
20. Electronic Payment Instruments (Banking Cards).....	136
21. Modern Vehicles.....	137
22. The Internet.....	138
23. The Electronic Communications Network.....	139
§1.7. A Reconceptualization of the Concept of Information System?.....	142
§1.7.1. Redefining the Concept of Information System.....	143
1. Simplifying the Definition.....	143
2. Restricting the Definition by Reference to the Main Function of the Device.....	143
3. Restricting the Definition by Reference To The Autonomy of the Device.....	144
4. Restricting the Definition by Introducing A Negative Criterion.....	145
5. Restricting the Definition by Introducing a Negative List.....	146
§1.7.2. A Restrictive Interpretation of the Current Definition.....	146
1. The Settlement of Controversies Regarding the Use of Certain Household Appliances.....	148
2. The Settlement of Controversies Regarding the Use Of A Smart TV.....	148
3. The Settlement of Controversies Regarding the Use Of A Storage Device.....	149
4. The Settlement of Controversies Regarding the Use Of A Multi-function Printers.....	149
<b>§2. The concept of computerised data storage device.....</b>	<b>150</b>
§2.1. The definition of the concept of computerised data storage device.....	150

§2.2. The Relevance of the Information System Concept from the Perspective Of Procedural Criminal Law and Substantive Criminal Law.....	151
§2.3. Relevant Examples of Means (Media) For the Storage of Computerized Data.....	152
1. Optical Data Media (CD, DVD, Blu-Ray, Etc.).....	152
2. Hard Disk, Memory Card, Memory Stick.....	152
3. Electronic Payment Instruments (Banking Cards).....	152
4. SIM cards.....	154
<b>§3. The concept of a computer program and computerized data.....</b>	<b>155</b>
§3.1. The Definition of Computerized Data and Computer Programs In International and European Legal Instruments.....	155
§3.2. The Definition of Computerized Programs and Data in National Legislation.....	156
§3.3. Examples of Computerised Data.....	158
1. The Qualification of a Technical Record as Computerised Data.....	158
2. The Legal Qualification of Information Stored On A Magnetic Strip.....	158
§3.4. The Relationship between Computerized Data and Computer Programs.....	159
§3.4. The Importance of Identifying a Computer Program.....	161
<b>§4. The Concept of Electronic Payment Instrument.....</b>	<b>161</b>
§4.1. The Definition of Payment Instruments in the European Legislation.....	162
§4.2. The Definition of Electronic Payment Instruments In the Internal Legislation.....	162

## SECTION II

### UNAUTHORIZED ACCESS TO A COMPUTER SYSTEM

#### (ARTICLE 360 CRIMINAL CODE)

<b>Chapter I.</b> Overview.....	168
<b>Chapter II.</b> The Relationship between the National Regulations And Supranational Legal Instruments.....	169

<b>§1. The Inspiration Source for the National Legislator</b> .....	169
<b>§2. The Means of Transposition into National Law</b> .....	176
<b>Chapter III. Decisions of the Constitutional Court, Appeals In The Interest Of the Law and Decisions</b>	
Of The European Court of Human Rights.....	185
<b>§1. Decisions of the Constitutional Court</b> .....	185
1. Decision No 183/2018 of the Constitutional Court (About The Security Measures).....	186
2. Decision No 353/2018 of the Constitutional Court (About Unauthorized Access).....	187
<b>§2 The Appeal in The Interest of the Law - Decision No 15/2013 of the High Court Of Cassation and Justice</b> .....	188
<b>§3. The European Court of Human Rights (Bărbulescu c. Romania)</b> .....	195
<b>Chapter IV. The Reason and Necessity of Criminalization</b> .....	202
<b>§1. The Need for Autonomous Criminalization</b> .....	202
1. The Relationship with Trespassing.....	202
2. The Relationship with the Violation of the Confidentiality of Correspondence.....	204
3. The Need for Autonomous Criminalization.....	205
<b>§2. The Limits of Criminalization</b> .....	206
1. The Limits of Unauthorized Access In Its Basic Form (Article 360 Paragraph (1) of the Criminal Code).....	206
2. Aggravating Circumstances to Unauthorized Access with the Particular Purpose of Obtaining Computerised Data (Article 360 Paragraph (2) Of the Criminal Code).....	208
3. Aggravating Circumstances to Unauthorized Access to an Information System Protected By Security Measures (Article 360 Paragraph (3) Of the Criminal Code).....	209
<b>Chapter V. Analysis of the Contents of the Crime of Unauthorized Access To A Computerised System</b> .....	210
<b>§1. The Legal Object</b> .....	210
<b>§2. The Nature and Form of the Crime</b> .....	213
<b>§3. The Subjects of the Crime</b> .....	215

§3.1. The Active Subject .....	215
§3.2. The Passive Subject.....	218
1. Identification of the Passive Subject.....	218
2. The Theory of the Holder of an Information System - The Existence of a Consolidated Right of Use.....	221
3. Does A Collective Passive Subject Exist? .....	225
4. Does A Secondary Passive Subject Exist? .....	225
5. The Plurality of Passive Subjects Vs. The Plurality of Accessed Information Systems.....	226
6. Conclusions.....	229
<b>§4. The Objective Side. General Framework .....</b>	<b>230</b>
§4.1. The Typology of Illegal Access to an Information System in Comparative Law.....	231
§4.2. The Information System Vs. The Means of Computer Data Storage.....	235
<b>§5. The Commissive Conduct - Access (To an Information System).....</b>	<b>240</b>
§5.1. The General Framework.....	240
§5.2. The Interpretation of the Concept.....	244
1. The Grammatical Interpretation.....	244
2. The Legal Interpretation (In Comparative Law), the Doctrinal Interpretation, And the Interpretation in Accordance with the Case Law.....	245
3. Decision No 15/2013 of the High Court of Cassation and Justice - Appeal In the Interests of the Law.....	250
4. The Conceptualization of the Notion of Access.....	251
4.1. The General Framework.....	251
4.2. The “Internal” Perspective of Access.....	251
4.3. The “External” Perspective of Access.....	252
4.4. Identification of Essential Features of Access.....	253
<b>§6. The Incriminating Conduct from the Perspective of Article 360 of the Criminal Code.....</b>	<b>255</b>
1. The General Framework.....	255
2. Access Itself - Expressly Regulated.....	256
3. Authorization Violations - Governed By Article 35 Paragraph (2)	

Of Law No. 161/2003?.....	256
4. Maintaining Access after the Withdrawal or Expiry of the Authorization.....	261
5. Unlimited Access vs. Limited Access (In Whole or Only In Part of the Information System).....	263
<b>§7. Particular Hypotheses Regarding the Access to an Information System.....</b>	<b>263</b>
§7.1. Actual Access to an Information System.....	263
1. Authentication within an Information System.....	263
2. Remote Access to an Information System Through Team Viewer.....	265
3. Accessing a Bank Account Online.....	266
4. Unauthorized Authentication (Access) To the Management Interface Of A Web Page.....	267
5. Accessing an ATM Via an Electronic Payment Instrument.....	268
6. The Unauthorized Alteration of a Web Page by Replacing or Changing the Way in Which It Is Displayed [ <i>Defacing</i> ].....	269
§7.2. Authorization Violations or Maintaining Unauthorized Access.....	269
1. Continued Use of a Database Via an Access Code, Although the Trial Access Period Has Expired.....	269
2. Unauthorized Access to A Database, followed by SQL Queries Aiming to Access Privileged Information.....	270
3. Continued Access to an Information System without Payment of the Royalty.....	271
4. Receipt of Authentication Data to an E-Mail Account for Spot Checking and the Intentional Omission of Signing Out.....	272
§7.3. Special Hypotheses Which Do Not Concern Access to an Information System.....	272
1. The Transmission of an Email.....	272
2. The Transmission of a Computer Program.....	273
3. DoS (Denial-of-Service) Attacks.....	274
4. Port Scanning.....	274

5. Reading the Information Displayed On the Screen of the Computer System.....	275
6. Obtaining Computerized Data via <i>Phishing</i> .....	275
7. Counterfeiting Web Pages.....	276
8. Offering Non-Existent Goods for Sale on the Internet.....	277
9. Capturing Legible Information on the Screen.....	277
10. Physical Interaction with an ATM.....	278
11. Making Payments at a POS Terminal.....	279
12. Making Online Payments.....	280
§7.4. Special Hypotheses Requiring Careful Analysis.....	282
1. Accessing Certain (Non-Public) URLs of (Public) Web Pages.....	282
2. Unauthorized Copying Of Computerized Data from the Information System Belonging To a Third Party.....	283
3. Unauthorized Copying Of Computerised Data in an Information System Belonging To a Third Party.....	284
4. The Use of a <i>Keylogger</i> -Type Computer Program To Intercept the Data Entered Via the Keyboard by the Victim.....	285
5. Restricting Access to Certain Computerized Data By The Administrator of the Information System.....	286
6. The Infection of Information Systems with A Malicious Program (Virus).....	287
<b>§8 Lack of Authorisation - The “Unauthorized” Concept.....</b>	<b>288</b>
1. General Framework.....	288
2. The “Unauthorized” Concept and Other Interchangeable Concepts.....	290
§8.1. Special Hypotheses of “Unauthorized” Access within the Doctrine And Case-Law.....	291
1. Lack of Express Permission from the Network Administrator.....	291
2. The Unauthorized Use of a Fuel Card.....	291
3. Adding Fictitious Ads On The eBay Platform.....	292
4. Creating Fictitious Accounts On The eBay Platform.....	292
5. Accessing the Application “CARD PIN” And “CARD FORM” Via Unauthorized Use of an Access Code by an Employee of the Bank.....	293

6. Access by an Employee of the Bank to A Component of the Information System Which Was Restricted To Employees in Their Category.....	293
7. Accessing a Restricted Web Page Performed By an Employee With A Fraudulent Purpose.....	293
8. The Use of a Laptop Which Is a Joint Asset of the Spouses.....	294
9. Accessing the Internet Banking Account by One of the Spouses.....	295
10. Accessing an Email Account or a Facebook Account by One Of The Spouses.....	295
11. Accessing the Skype Account of the Wife.....	295
12. Accessing an Email Account Using A Previously Received Password.....	296
13. Checking the Fiscal Situation of Tax Payers in another Jurisdiction.....	297
14. The Transfer of Child Pornography Materials.....	298
§8.2. Legal Guidance Relevant To Comparative Law.....	297
1. The Case-Law of the Italian Supreme Court of Cassation.....	298
2. Unauthorized Access Theories in American Law.....	300
§8.3. Identification of A Reasonable <i>Framework</i> for the “Unauthorized” Concept.....	311
1. Establishing Benchmarks.....	311
2. Settlement of the Clearance Limit for Access between Spouses.....	315
3. Access to the Information System of the Child.....	316
<b>§9. Consequences.....</b>	<b>316</b>
<b>§10. Guilt (Subjective Aspect) .....</b>	<b>317</b>
<b>§11. The Moment of Perpetration of the Offense and Attempts.....</b>	<b>318</b>
1. The General Framework.....	318
2. The Moment of Perpetration of the Offense.....	319
3. Hypotheses Which Pertain To the Sphere of Attempts.....	320
3.1. The Simple Start-Up of an Information System.....	320
3.2. Initialization ( <i>Booting</i> ) Of an Operating System from a CD...322	
3.3. Partially Overcoming the Security Measures Completely Preventing Access to the Computer System.....	323
4. Hypotheses Pertaining to Preparatory Acts.....	323

5. The Theory of Factual Impossibility - A Compromise Solution.....	325
6. Desistance and Prevention of the Outcome.....	327
6.1. Desistance.....	327
6.2. Prevention of the Outcome.....	328
<b>§12. Aggravated Forms of Illegal Access to an Information System.....</b>	<b>328</b>
§12.1. The Purpose of Obtaining Computerized Data.....	328
1. The General Framework.....	328
2. The Contents of the Special Purpose.....	329
3. The Relationship with Other Crimes.....	330
§12.2. Breaching the Safety Measures.....	330
1. The General Framework.....	330
2. The Reason for the Aggravation.....	333
3. The Nature of Security Measures - Physical, Organizational, Or Just Logical?.....	336
4. The Characteristics of Security Measures.....	339
4.1. The Nature and Specificity of Security Measures.....	339
4.2. Access Control.....	340
4.3. The Purpose of Access Control.....	342
4.4. The Effectiveness of Security Measures.....	342
4.5. The Reliability (Efficiency) Of Security Measures.....	343
5. Procedures for Forbidding or Restricting Access.....	345
5.1. Passwords or Access Codes.....	345
5.2. The Encryption of Computerized Data.....	345
5.3. The Use of Biometric Identifiers.....	346
5.4. Setting the MAC Addresses ( <i>Media Access Control Addresses</i> ).....	346
5.5. Securing a Web Browser.....	346
6. Devices Used To Forbid or Restrict Access.....	346
7. Computer Programs Which Forbid or Restrict Access.....	347
8. Manners in Which Security Measures Are “Broken”.....	347
8.1. Fraudulent Means of Obtaining Data from the Victim.....	348
8.2. The Use of Authentication Data After the Loss of Authorization.....	348

8.3. The Use of Actuals In Order To Authenticate.....	350
9. The Consequences of the Non-Existence of Security Measures.....	350
<b>Chapter VI. The Relationship between Unauthorized Access to A Computer System And Other Crimes.....</b>	<b>351</b>
<b>§1. The Relationship with Other Cybercrimes.....</b>	<b>351</b>
1. The Relationship with Computer Forgery (Article 325 of the Criminal Code).....	351
2. The Relationship with Computer Fraud (Article 249 of the Criminal Code).....	351
3. The Relationship with the Alteration of the Integrity of the Computerized Data (Article 362 of The Criminal Code).....	352
4. The Relationship with Illegal Operations with Devices or Software (Article 365 of the Criminal Code).....	353
<b>§2. The Relationship with Other Offenses in the Criminal Code.....</b>	<b>354</b>
1. The Relationship with the Breach of Privacy Offense (Article 226 of The Criminal Code).....	354
2. The Relationship with the Offense of Theft (Article 228 of the Criminal Code).....	354
2.1. Accessing the Information System after the Moment Of Breaching It.....	355
2.2. The Theft of Components of Different Information Systems And Accessing the Computer System Composed of These.....	357
3. The Relationship with the Offense of Identity Theft - Article 230 Paragraph (2) of the Criminal Code.....	358
4. The Relationship with the Offense of Concealment - Article 270 of the Criminal Code.....	359
5. The Relationship with the Offense of Violation of Confidentiality of Correspondence (Article 302 Paragraph (1) Of the Criminal Code).....	359
5.1. The Applicability of Article 360 of the Criminal Code - Accessing the Email Server.....	362
5.3. The Applicability of Article 302 Paragraph (1) Of the Criminal Code - Opening Mail or Communications?.....	366

5.4. A Contest of Offenses or Of Qualifications?.....	367
6. The Relationship with the Offense Concerning Carrying Out Financial Transactions in A Fraudulent Way (Article 250 Paragraph (1) Of the Criminal Code).....	368
7. The Relationship with the Offense of Electronic Vote Fraud (Article 388 Of the Criminal Code).....	369
<b>§3. The Relationship with Other Crimes Regulated by Special Legislation..</b>	<b>370</b>
1. The Relationship with Offenses Concerning Copyright (Law no. 8/1996).....	370
2. The Relationship with Offenses Concerning Unfair Competition (Law no. 11/1991).....	371
3. The Relationship with the Offense (Offenses) Of Terrorism (Law no. 535/2004).....	373
4. The Relationship with the Offense Concerning Unauthorized Technical Surveillance (Law no. 51/1991).....	375
<b>Chapter VII. The Reformation of Article 360 of the Criminal Code.....</b>	<b>376</b>
<b>§1. A Conceptual Reform? .....</b>	<b>376</b>
<b>§2. Proposals Relating To the Amendment of Article 360 of the Criminal Code.....</b>	<b>378</b>
1. The Introduction of “The Breach of Security Measures” As Constituent For the Basic Form.....	378
2. The Clarification of the Concept of Access, And the Introduction of Alternative Theses For Perpetrating the Deed.....	379
3. Extending Access to the Means of Storage of Computerized Data.....	379
4. The Repeal of Article 360 Paragraph (2) Of the Criminal Code.....	379
5. The Introduction of a Subsidiarity Clause.....	380
<b>§3. <i>Lex Ferenda</i> Interventions That Should Be Avoided.....</b>	<b>381</b>
1. The Introduction of Prior Complaint.....	381
2. The Introduction of Atypicality Causes.....	381
<b>§4. Other <i>Lex Ferenda</i> Interventions.....</b>	<b>382</b>

**SECTION III**  
**COMPUTER FRAUD**  
**(ARTICLE 249 OF THE CRIMINAL CODE)**

<b>Chapter I.</b> Introductory Matters.....	384
<b>Chapter II.</b> The Relationship between the National Regulations And Supranational Legal Instruments.....	386
<b>§1. The Inspiration Source for the National Legislator</b> .....	386
<b>§2. The Means of Transposition into National Law</b> .....	399
<b>Chapter III.</b> The Reason and Necessity of the Criminalization of Computer Fraud.....	405
<b>Chapter IV.</b> The Analysis of the Contents of the Offense of Computer Fraud.....	414
<b>§1. The Object of the Offense</b> .....	414
§1.1. The Legal Object .....	414
§1.2. The Material Object.....	420
<b>§2. The Subjects of the Crime</b> .....	422
§2.1. The Active Subject.....	422
§2.2. The Passive Subject.....	424
<b>§3. The Objective Aspect in Computer Fraud</b> .....	428
§3.1. The Information System and Data.....	429
§3.2. Ways of Perpetrating Computer Fraud.....	430
§3.2.1. General Aspects.....	430
1. Crimes with Alternative Content.....	431
2. Commissive Offenses and Omissive Offenses. ....	431
§3.2.2. The Analysis of Commissive Conduct.....	433
§3.2.3. The Means of Computerized Data Entry.....	434
1. The General Framework.....	434
2. The Premise.....	436
3. Hypotheses of Perpetrating Computer Fraud via Entry Of Computerized Data.....	437
3.1. The Theft [Unauthorized Transfer] Of Virtual Coins..	437
3.2. The Purchase of Mobile Phones with Zero Value By Activating Discounts in the Information System.....	439

3.3. The Unauthorized Use of a Ticket To Top-Up the Prepaid Card.....	439
3.4. The Transfer of Credit onto a <i>Prepaid</i> Phone Card....	440
3.5. The “Artificial” Increase of the Bank Account Balance.....	442
3.6. Fraudulently Obtaining a Public Transportation Ticket From A Ticket Vending Machine.....	443
3.7. The Introduction of the Mention “Paid” With Respect to a Certain Debit Stored in A Database.....	443
3.8. Fraudulent Use of a Photocopier by The Use of a Forged Card.....	444
4. Hypotheses Regarding the Introduction of Computerized Data Which Is Problematic from The Perspective of the Retention of Computer Fraud.....	445
4.1. Fraudulent Online Auctions.....	445
4.2. Fraud Committed By Sending Messages Through Electronic Communications Means. ....	449
4.3. The Activities of <i>Phishing</i> and <i>Pharming</i> .....	451
4.4. The Sending of Unsolicited Electronic Mail (spam)....	454
4.5. The Use of the Identification Details Of An Electronic Payment Instrument.....	454
4.6. Offline Trading.....	455
4.7. Cash Withdrawals from an ATM Immediately After the Withdrawal of the Sum from the Bank Teller....	457
4.8. The Fraudulent Creation of Bank Loans In The Information System of the Bank. ....	458
4.9. The Use of a <i>Spyware Dialer</i> . ....	458
4.10. The Fraudulent Ordering of Products As Salesperson. ....	460
4.11. The Use of <i>Paysafecard</i> Codes to Carry Out Online Payments. ....	461
4.12. Cryptojacking.....	461
4.13. The Printing of Forged Banknotes.....	466

§3.2.4. Means of Altering Computerized Data.....	467
1. The General Framework.....	467
2. Hypotheses of Committing Computer Fraud by Altering Computerized Data.....	468
2.1. Performing a Transfer of Funds.....	468
2.2. Changing the Balance of a Bank Account Through An Intervention on the Database.....	469
2.3. Maintaining a Certain Service Active for The Purpose of Additional Billing.....	469
2.4. Changing the Available “Credit” At an Online Poker Game.....	470
2.5. Rounding of Amounts at the Time of a Transfer of Funds.....	471
2.6. Changing the Computer Program of a Gambling Device So That the Payment of Additional Credits Is No Longer Necessary.....	471
3. Hypotheses Concerning the Alteration of Computerized Data Problematic from The Perspective of the Retention of Computer Fraud.....	471
3.1. Alteration of the Contents of a Web Page.....	471
3.2. Changing the Sum Displayed on the POS Terminal Screen.....	472
§3.2.5. The Means of Erasing Computerised Data.....	475
1. The General Framework.....	475
2. Hypotheses of Computerized Data Erasure Relevant From The Perspective of Article 249 of the Criminal Code.....	476
3. Hypotheses Regarding the Deletion of Computerized Data Problematic From the Point Of View of Retention of Computer Fraud.....	478
3.1. Deleting Computerized Data Through The Use Of A Magnet.....	478
3.2. Erasure of Debits or Of Debtors from the Database.....	478

§3.2.6. The Means to Restrict Access to Computerized Data.....	479
1. The General Framework.....	479
2. Hypotheses of Restricting Access to Computerized Data Relevant To Article 249 of the Criminal Code.....	480
3. Hypotheses on Restricting Access to Computerized Data Problematic from the Point of View of Retention of Computer Fraud.....	480
3.1. Restricting Access to Certain Accounts by Changing the Password.....	480
3.2. Failure to Repay Money Which Was Transferred in Error into the Account of the Agent.....	481
3.3. Ransomware-Type Conduct.....	482
§3.2.7. Means to Prevent the Functioning of a Computer System in Any Way.....	483
1. General Framework. ....	483
2. Hypotheses of Preventing the Functioning of a Computer System Which May Be Relevant from the Perspective of Article 249 of the Criminal Code.....	484
2.1. The Manipulation of Electronic Games of Chance.....	484
2.2. The Logical Interaction with an ATM.....	487
3. Hypotheses on Preventing in Any Way the Functioning of a Computer System Problematic from the Point of View of Retention of Computer Fraud.....	487
3.1. The Physical Interaction with an ATM (“Forking” Technique).....	487
3.2. Disabling of Protective Electronic Devices With a View to Stealing the Good.....	491
3.3. The Unlawful Obtainment of a Good from a Vending Machine.....	491
3.4. DoS-Type ( <i>Denial-of-Service</i> ) Attacks.....	491
§3.2.8. Improper Omissive Conduct (Commissive By Omission).....	492
§3.3. Lack of Authorization - The “Unauthorized” Concept.....	493
§3.4. Consequences.....	493

1. The General Framework.....	494
2. Causing Damages.....	496
§3.5. Obtaining a Material Benefit.....	501
1. The Clarification of the Concept.....	501
2. Fair Material Benefit Vs. Unfair Material Benefit.....	502
§3.6. The Causal Relation.....	503
<b>§4. Guilt (The Subjective Aspect).....</b>	<b>504</b>
§4.1. The Subjective Element.....	504
§4.2. The Special Purpose.....	504
<b>§5. The Natural or Legal Unity of the Offense.....</b>	<b>507</b>
<b>§6. The Moment of Perpetration and the Attempt .....</b>	<b>508</b>
§6.1. The Moment of Perpetration of the Offense.....	508
§6.2. The Attempt.....	509
1. The General Framework.....	509
2. Hypotheses Which Fall Within the Scope of the Attempt.....	509
3. Hypotheses Which Fall Within the Scope of Preparatory Acts.....	510
3.1. Unauthorized Access to an Information System.....	510
3.2. The Phishing Activity.....	510
§6.3. Desistance and Prevention of the Occurrence of the Outcome.....	511
1. Desistance.....	511
2. Prevention of the Outcome.....	514
3. The Consequences of Desistance or Prevention of the Outcome.....	514
<b>§7. The Sanction.....</b>	<b>515</b>
<b>§8. Computer Fraud in Aggravated Form.....</b>	<b>516</b>
<b>Chapter V. The Relationship between the Offense of Cyber-Fraud and Other Crimes...520</b>	
<b>§1. The Relationship with Other Cybercrimes.....</b>	<b>520</b>
§1.1. The Relationship with the Access to A Computer System (Article 360 of the Criminal Code).....	520
§1.2. The Relationship with Computer Forgery (Article 325 of the Criminal Code).....	526
§1.3. The Relationship with the Alteration of Computerized Data (Article 362 of the Criminal Code).....	529

§1.4. The Relationship with the Disruption of the Performance of Information Systems (Article 363 Of the Criminal Code.....	539
§1.5. The Relationship with the Fraudulent Carrying Out of Financial Transactions (Article 250 Of the Criminal Code.....	541
1. The General Framework.....	541
2. Contest of Offenses or Contest of Qualifications.....	542
3. Problematic Hypotheses.....	544
3.1. The Use of A Forged Electronic Payment Instrument (Cloned Bank Card).....	544
3.2. Fraud via the “Salami” Technique.....	545
3.3. The Logical and Remote Interaction with an ATM.....	546
3.4. The Fraudulent Use of Merchant Cards.....	549
3.5. Performing Online Payments. ....	552
3.6. Withdrawal of Cash by the Bank Clerk from the Bank Cashier’s Office, by Debiting the Account of a Customer.....	552
<b>§2. The Relationship with Other Offenses in the Criminal Code.....</b>	<b>553</b>
§2.1. The Relationship with the Offense of Fraud (Article 244 of the Criminal Code).....	553
1. The General Framework.....	553
2. Computer Fraud vs. Traditional Fraud by Computerized Means.....	554
3. The Conceptual Analysis of Computer Fraud In Relation To Fraud.....	555
4. Criteria for the Delimitation of Computer Fraud from Traditional Fraud.....	558
4.1. The Lack of Self-Harming Behaviour.....	558
4.2. The Information System - Instrument or the Object of the Action.....	558
4.3. The Lack of a Subjective Connection.....	558
4.4. Irrelevancy of the Victim’s Conduct.....	559
4.5. The Voluntary or Involuntary Nature of the Transfer of Assets.....	560
5. The Existence of a Conduct Which Draws On Both Traditional Fraud As Well As On Computer Fraud.....	560

§2.2. The Relationship with the Offense of Identity Theft [Article 230 Paragraph (2) Of the Criminal Code].....	562
§2.3. The Relationship with the Offense of Breach of Trust (Article 238 of the Criminal Code).....	564
§2.4. The Relationship with the Offense of Destruction (Article 253 of the Criminal Code).....	565
§2.5. The Relationship with the Offense of Embezzlement (Article 295 of the Criminal Code).....	566
<b>§3. The Relationship with the Offense Referred to In Article 25 letter (c) of the Government Emergency Order No 77/2009.....</b>	<b>567</b>
<b>Chapter VI. Reformation of Article 249 of the Criminal Code.....</b>	<b>569</b>
<b>§1. A Radical Reform?.....</b>	<b>569</b>
1. The General Framework.....	569
2. The Amendment of Article 244 Paragraph (1) Of the Criminal Code through the Introduction of a Distinct Sentence for Criminalization.....	569
3. The Amendment of Article 244 Paragraph (1) Of the Criminal Code by Broadening the Scope of Applicability.....	570
<b>§2. Proposals Relating to the Amendment of Article 249 of the Criminal Code.....</b>	<b>571</b>
1. With Regard to the Material Benefit. ....	571
2. With Regard to the Unjust Nature.....	571
3. With Regard to Preventing, In Any Way, the Operation of an Information System. ....	571
4. With Regard to the Manner of Producing the Damages.....	572
<b>§3. Other <i>lex ferenda</i> interventions.....</b>	<b>572</b>

**SECTION IV**  
**COMPUTER FORGERY**  
**(ARTICLE 325 OF THE CRIMINAL CODE)**

<b>Chapter I. Introductory Matters.....</b>	<b>575</b>
<b>Chapter II. The Relationship between the National Regulations and Supranational Legal Instruments.....</b>	<b>576</b>

<b>§1. The Inspiration Source for the National Legislator</b> .....	576
<b>§2. The Means of Transposition into National Law</b> .....	583
<b>Chapter III. The Reason and Necessity of Criminalization</b> .....	586
<b>Chapter IV. The Analysis of the Contents of the Offense of Computer Forgery</b> .....	589
<b>§1. The Object of the Offense</b> .....	589
§1.1. The Legal Object.....	589
§1.2. The Material Object.....	591
<b>§2. The Nature of the Offense</b> .....	591
<b>§3. The Subjects of the Crime</b> .....	592
§3.1. The Active Subject.....	592
1. The Relationship between the Special Purpose and the Participation in Crime.....	592
2. Participation In The Case Of Counterfeiting Web Pages.....	593
3. The Applicability of the Institution of the Position of Guarantor (Article 17 of the Criminal Code).....	594
§3.2. The Passive Subject.....	594
<b>§4. The Objective Aspect of Computer Forgery</b> .....	596
§4.1. The Concept of Writ.....	599
§4.2. Electronic Documents.....	601
§4.3. Traditional Writs vs. Computerised Data [Electronic Documents].....	602
1. The General Framework.....	602
2. The Features and Functions of Computerized Data Which Is the Object of Computer Forgery.....	604
3. Examples of Computerized Data Relevant from the Point of View of Computer Forgery.....	606
3.1. Databases. ....	606
3.2. Online Catalogues. ....	606
3.3. Individual Electronic Documents. ....	607
§4.4. Electronic Signature.....	607
§4.5. Means of committing computerized forgery.....	608
§4.5.1. Computerized Data Input Means.....	608
1. The General Framework.....	608

2. Hypotheses of Perpetration of Computer Forgery by Inputting Computerized Data.....	610
2.1. Counterfeiting (Cloning) Of Web Pages - <i>Web Spoofing</i> .....	610
2.2. The Simulation of Electronic Mail (Email <i>Spoofing</i> ) Through Usurpation of Identity.....	617
2.3. The Transmission of Electronic Mail Using an Account Accessed Without Authorization.....	619
2.4. The Unauthorized Use (Application) Of an Electronic Signature.....	620
2.5. The Introduction of False Computerized Data (Information) In the ECRIS System.....	620
2.6. Computerised Data Entry in the “Revisal” Program.....	621
2.7. The Fraudulent Issuance of an Electronic Payment Instrument. ....	621
2.8. Creating a Fake Account (Profile) On a Social Network.....	622
2.9. Counterfeiting [Cloning] A SIM Card.....	625
3. Hypotheses Regarding the Introduction of Computerized Data Which Is Problematic from The Perspective of the Retention of Computer Forgery.....	626
3.1. The Introduction (Publication) Of Fictitious Ads on Online Platforms.....	626
3.2. Publication on the Internet of a Model [Sample] For the Creation of a False Electronic Document.....	629
3.3. The Introduction of a Malicious Program into the Source Code of a Web Page.....	630
3.4. The Creation of a Duplicate of an Electronic Document.....	630
3.5. The Transfer of Electronic Documents Into An Information System.....	631
§4.5.2. The Means of Altering Computerized Data.....	632

1. General Framework. ....	632
2. Hypotheses of Perpetration of Computer Forgery by Altering Computerized Data.....	632
2.1. Changing the Baccalaureate Grade from the Digital Catalogue.....	632
2.2. Changing the Number of Dependent Children on The Basis Of The Database of the Authority With A View To Obtaining More Benefits.....	634
2.3. Changing the Phone Number Associated With A Bank Account.....	635
2.4. Alteration of Images That Could Be Used As Evidence In A Court Trial. ....	636
2.5. Alteration of an Audio-Video Recording Used In A Criminal Procedure.....	636
2.6. Changing the Name and the Price of a Product At The Moment of Sale.....	637
2.7. Changing the Hash Value Stored On the Storage Device On Which the Copy Made Under the Conditions Laid Down in Article 168 Paragraph (9) Criminal Procedure Code Was Saved.....	638
3. Hypotheses of Alteration of Computerized Data Problematic From The Perspective of the Retention of Computer Forgery.....	639
3.1. Creating a Fake Account [Profile] On a Social Network.....	639
3.2. Changing the Phone Number ( <i>Caller ID Spoofing</i> ).....	640
3.3. Forging an IP Address ( <i>IP spoofing</i> ).....	640
3.4. Regeneration of A PIN Code Corresponding To An Electronic Payment Instrument.....	641
§4.5.3. Means of Erasing Computerized Data.....	642
1. The General Framework.....	642
2. Hypotheses of Perpetration of Computer Forgery by Erasing Computerized Data.....	643
3. Hypotheses of Erasure of Computerized Data Problematic From The Perspective of the Retention of Computer Forgery.....	644

§4.5.4. The Means to Restrict Access to Computerized Data.....	644
1. The General Framework.....	644
2. Hypotheses of Perpetration of Computer Forgery by Restricting Access To Computerized Data.....	645
3. Hypotheses of Restricting Access to Computerized Data from The Perspective of the Retention of Computer Forgery.....	645
§4.6. Lack of Authorization - The “Unauthorized” Concept.....	646
§4.7. The Consequences - Returning Inaccurate Data.....	648
1. The General Framework.....	648
2. The Legal Consequences of This Consequence.....	650
3. Examples of Inaccurate Data.....	650
<b>§5. Guilt (The Subjective Aspect).....</b>	<b>651</b>
§5.1. The Type of Guilt.....	651
§5.2. Special Purpose - Usage With A View To Generating Legal Consequences.....	651
1. The Legal Nature of the Special Purpose.....	651
2. The Effects of the Special Purpose on the Form of the Intention.....	651
3. The Contents of the Special Purpose.....	652
<b>§6. The Moment of Perpetration and the Attempt .....</b>	<b>653</b>
1. The General Framework.....	653
2. The Moment of Perpetration of Computer Forgery.....	654
3. Computer Forgery in Attempted Form.....	655
<b>Chapter V. The Relationship between Computer Forgery and Traditional Forgery .....</b>	<b>656</b>
<b>§1. General Specifications.....</b>	<b>656</b>
<b>§2. The Analysis of the Relationship between Computer Forgery and     Traditional Forgery.....</b>	<b>656</b>
<b>§3. The Differences between the Two Categories of Offenses.....</b>	<b>657</b>
1. Matters Regarding Penalty Limits.....	658
2. Matters Regarding the Penalty for Attempt.....	658
3. The Criminalization of the Use of Forgery.....	658
4. The Condition of Using or Entrusting the Forged Document.....	659
5. The Distinction between Official and Private Documents.....	660

<b>§4. Specific Hypotheses Illustrating the Problematic Relationship Between Computer Forgery and Traditional Forgery.....</b>	<b>660</b>
1. Counterfeiting or Alteration of A Traditional Writ On An Information System.....	660
2. Continuation of the Action of Alteration after Printing the Contents Of the Electronic Document on Paper.....	662
3. Counterfeiting or Alteration of Electronic Invoices.....	662
4. Counterfeiting or Alteration of Electronic Mail and Filing It to the Case File in Printed Form.....	663
5. Counterfeiting of A Request Addressed to The Court, The Introduction into The Electronic Document of a Handwritten Signature, And the Transmission of The Application Via Email.....	664
6. Changing the Date Regarding the Creation of a Document by Altering the <i>Metadata</i> Information and Printing the Forged Contents of That Electronic Document.....	665
<b>§5. The Identification of the Legal Problems Relevant From the Perspective Of The Relationship between Computer Forgery and Traditional Forgery.....</b>	<b>666</b>
1. The Moment When We Can Deem a Writ to Be Traditional.....	666
2. The Identification of the Act of Execution.....	666
3. The Retention of the Attempt.....	667
4. The Identification of Authorship and Forms of Criminal Participation.....	667
5. A Possible Breach of the Principle of Non Bis In Idem.....	667
6. The Problem of the Metamorphosis of Computer Forgery into Traditional Forgery from The Perspective of the Sanctioning Regime.....	667
<b>§6. Possible Solutions for Solving the Relationship between Computer Forgeries and Traditional Forgery.....</b>	<b>668</b>
1. The Special Character of Computer Forgery in Relation With Traditional Forgery.....	668
2. The Exclusion of Traditional Forgery by Reference to the Probative Value of an Inadequate Copy.....	669
3. The Probative Function and The Function of Warranty for Computerized Data on Which an Intervention Is Made.....	669

4. The Delineation between Computer Forgery and Traditional Forgery by Reference to The Purpose of the Agent.....	670
<b>Chapter VI. Identity Theft. A form of computer forgery.....</b>	<b>672</b>
<b>§1. Introductory Matters.....</b>	<b>672</b>
<b>§2. The Concept of Identity Theft.....</b>	<b>673</b>
1. The Phases of Identity Theft.....	675
1.1. Stage One. Obtaining the Personal Data.....	675
1.2. Stage Two: Interaction with the Personal Data Obtained In Stage One.....	677
1.3. Stage Three: The Actual Use of the Personal Data.....	678
2. Conclusions with Regard to Identity Theft.....	678
2.1. An Autonomous Criminalization Should Cover All the Phases of Identity Theft. ....	678
2.2. Identity Theft Is An Improper Concept. ....	679
2.3. False Identity vs. Fictitious Identity. ....	679
2.4. Identity Theft vs. Usurpation of Identity. ....	680
<b>§3. Identity Theft as Computer Forgery .....</b>	<b>681</b>
1. The <i>Phishing</i> Activity. ....	681
2. The <i>Pharming</i> Activity. ....	683
<b>Chapter VII. The Relationship between the Offense of Computer Forgery and Other Crimes.....</b>	<b>685</b>
<b>§1. The Relationship with Other Cybercrimes.....</b>	<b>685</b>
1. The Relationship with the Alteration of the Integrity of the Computerized Data (Article 362 of the Criminal Code).....	685
2. The Relationship with the Disruption of the Performance of Information Systems (Article 363 Of the Criminal Code).....	686
4. The Relationship with the Unauthorized Transfer of Data (Article 364 of the Criminal Code).....	687
5. The Relationship with Illegal Operations with Devices or Software (Article 365 of the Criminal Code) .....	687
6. The Relationship with the Forgery of Electronic Payment Instruments (Article 311 Paragraph (2) of the Criminal Code).....	688

7. The Relationship with the Fraudulent Carrying Out of Financial Transactions (Article 250 of the Criminal Code).....	689
<b>§2. The Relationship with Other Crimes.....</b>	<b>690</b>
1. The Relationship with the Offense of Fraud.....	690
2. The Relationship with the Offense of Forgery of Technical Records.....	690
3. The Relationship with the Offense of Tax Evasion (Article 9 Letter (c) of Law no. 241/2005).....	691
<b>Chapter VIII. The Reformation of Article 325 of the Criminal Code.....</b>	<b>693</b>
<b>§1. The Repeal of Article 325 of the Criminal Code and the Extension of the Applicability of Traditional Forgery.....</b>	<b>693</b>
<b>§2. The Amendment of Article 325 of the Criminal Code.....</b>	<b>695</b>
<b>§3. Amendments with Regard to Other Criminalization Texts.....</b>	<b>696</b>
1. The Criminalisation of the Use of Computer Forgery.....	696
2. The Repeal of Article 311 Paragraph (2) Of the Criminal Code [The Forgery of Electronic Payment Instruments].....	696
3. The Repeal of Article 324 of the Criminal Code [Forgery of a Technical Record].....	697
4. The Amendment of Article 311 Paragraph (2) Of the Criminal Code in Accordance with Directive (EU) 2019/713.....	697
<b>Conclusions.....</b>	<b>699</b>
<b>Bibliography.....</b>	<b>702</b>

## KEYWORDS

Unauthorized Access; Computer Fraud; Computer Forgery; Information System; Storage Device; Computer Data; Electronic Payment Instrument; Web Page Cloning, Phishing; Identity Theft; Internet Fraud.

## SUMMARY

In this paper we analyse three cybercrimes: unauthorized access to an information system [Article 360 of the Criminal Code], Computer Fraud [Article 249 of the Criminal Code], and Computer Forgery [Article 325 of the Criminal Code]. In addition to these three offenses, we analyse the concept of cybercrime and relevant terminological matters, such as the concept of information system, electronic payment instrument, etc.

Cybercrimes **have been the subject of at least a few monographs**,<sup>1</sup> even when they were only regulated by special legislation (Law no. 161/2003<sup>2</sup>, and Law no. 365/2003<sup>3</sup>). At the present moment, the literature analysing the special part of the new Criminal Code automatically also addresses the offenses which are the subject of this Thesis, because they have been taken over from the special legislation into the contents of

---

<sup>1</sup> **By Way Of Example We List The Following Works:** I. VasIU, *Criminalitatea informatică, (Cybercrime)* Ed. Nemira, Bucharest, 1998; I. VasIU, L. VasIU, *Totul despre hackeri, (All About Hackers)*, Ed. Nemira, Bucharest, 2001; I. VasIU, L. VasIU, *Informatica juridică și Drept informatic, (Legal Informatics And Informatics Law)*, Ed. Albastră, Cluj, 2002; T. Amza, C.-P. Amza, *Criminalitatea informatică, (Cybercrime)*, Ed. Lumina Lex, București, 2003; I. VasIU, L. VasIU, *Prevenirea criminalității informatică, (The Prevention Of Cybercrime)*, Ed. Hamangiu, București, 2006; M. Dobrinou, *Infracțiuni în domeniul informatic, (Crimes In The Field Of Informatics)*, Ed. C.H. Beck, Bucharest, 2006; Ș. I. VasIU, *Criminalitatea informatică, (Cybercrime)*, Ed. Sitech, 2008; M. Dobrinou, *Criminalitatea informatică, (Cybercrime)*, Ed. Academiei Naționale de Informații, București 2009; A. Trancă, I. VasIU, L. VasIU, *Criminalitatea în cyberspațiu, (Criminality In Cyberspace)*, Ed. Universul Juridic, 2011; D.C. Trancă, *Infracțiunile informatică în noul Cod penal, (Cybercrimes In The New Criminal Code)*, Ed. Universul Juridic, Bucharest, 2014. **At the level of comparative law we could list the following works:** 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.

<sup>2</sup> Regarding certain measures meant to ensure transparency in the exercise of public dignities, public positions, as well as in business, and to prevent and sanction corruption, (published in The Official Journal of Romania no. 279 of 21 April 2003).

<sup>3</sup> Regarding electronic trade, republished (published in the Official Journal Of Romania no. 403 of 10 May 2006).

the Criminal Code – Article 249 [Computer Fraud], Article 250 [carrying out fraudulent financial operations], Article 325 [Computer Forgery], Articles 360-365, Article 374 [Child pornography], etc. of the Criminal Code.

Despite the existence of these doctrinal analyses, the national literature **still requires an in-depth analysis** in the field. From a critical perspective, we might argue that, as regards cybercrime, we do not lack literature, but the literature currently in existence highlights the need for additions. Here we refer to an in-depth analysis of certain problems relevant from the point of view of legal practice, and not just a general and schematic overview of the contents of criminalization texts.

**A first argument** targets the problems revealed by legal practice. In this respect, within the legal practice we often note how cybercrimes pose **major problems at the level of interpretation**, and the legal relationships between these (for instance, the relationship between computer forgery and computer fraud), as well as the relationships between cybercrimes and other offenses considered to be traditional (for instance, the relationships between computer fraud and the offense of fraud), have generated an **inconsistent legal practice**.

However, an analysis of the critiques which can be made to the many solutions used in legal practice allows us to conclude that these rarely, if ever, find an answer in literature. This is precisely why we decided to perform, within this Thesis, an ample analysis of the legal practice and to identify practical legal solutions for each problem which generated controversy or difficulties at the level of interpretation and application of the criminalization texts.

**A second argument** is that, too often, doctrinal analyses – particularly domestic ones – target general matters or matters that have already been clarified, and too few times do they focus on truly controversial matters which already generate issues or which may do so in the future. Taking into account that the role of literature is not just to offer an answer to current problems, but also to preclude discussions with a view to avoiding an inconsistent future legal practice, we believe this Thesis to be necessary and opportune.

In this context, we believe that even **an in-depth analysis at the level of comparative law** becomes a necessity. Indeed, a review of the national literature reveals that the comparative method is rarely used, and when it is used, the references are usually to American law.

As far as we are concerned, we have no reservations in arguing that American law represents a point of reference in the field of cybercrime. However, in relation to the provisions of national legislation which are the object of this Thesis, American law becomes truly relevant only from the point of view of the offense of unauthorized access to an information system [Article 360 of the Criminal Code], where the literature<sup>4</sup> and case-law is vast and has a remarkable scientific standard.<sup>5</sup> We therefore believe that, in order to clarify the concepts of “access” and “unauthorized”<sup>6</sup> an incursion in American law is an important step in any scientific research carried out in this field.

Instead, from the point of view of computer fraud and computer forgery we believe that this legal system is not truly a model for the national legislator. Beyond an ample analysis with regard to identity theft in general and *phishing*<sup>7</sup> in particular, we do not believe that American literature or case-law can offer relevant answers to the problems which can be identified in the national legislation with regard to these two offenses.

This is why we believe that we should also direct our attention to other legal systems, such as the Spanish, Italian, German ones, etc. Within the literature originating in these countries, or referring to these legal systems, can be identified ample analyses at conceptual level meant to delineate the offense of computer fraud (Article 248.2 of the Spanish Criminal Code, Article 640-ter Italian Criminal Code, and section 263a of the German Criminal Code) from traditional fraud.

Taking into account that, within the national body of case-law, the overwhelming majority of cases regarding the offense of computer fraud highlight a regrettable confusion between this offense and traditional fraud,<sup>8</sup> such an incursion in Comparative Law

---

<sup>4</sup> Here we refer particularly to the work of Professor Orin Samuel Kerr, which represents a reference point at international level in the field of cybercrime. For example, see O.S., Kerr, *Cybercrime's scope: interpreting "access" and "authorization" in Computer Misuse Statutes*, in “New York University Law Review”, vol. 78, 2003; O.S. Kerr, *Norms of Computer Trespass*, in “Columbia Law Review”, vol. 116, 2016; O.S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, in “Minnesota Law Review”, vol. 94, 2010.

<sup>5</sup> Remarkable not due to the fact that it determined us to acquiesce to the legal practice solutions, which it did not; but due to that fact that any conclusion which was reached had a complex logical and legal reasoning behind it, which we often find to be missing from the justification of the decisions of Courts.

<sup>6</sup> American law mentioning “lack of authorization”.

<sup>7</sup> For example, see L.L. Sullins, *“Phishing for a solution”: domestic and international approaches to decreasing online identity theft*, in „Emory International Law Review”, vol. 20, 2006.

<sup>8</sup> Thus, in hypotheses of fraud through cyber-means (online auctions or online sales of goods) **some Courts retain the offense of fraud:** The Bucharest Court of Appeal, II-nd Criminal Section, dec. no. 421/2015; Pitești Court of Appeal, Criminal Section, dec. no. 689/R/2008; Ploiești Court of Appeal, Criminal Section, dec. no. 1084/2016; Ploiești Court of Appeal, Criminal Section, dec. no. 804/2015. Still, **other Courts retain the offense of computer fraud:** The Bacău Court of Appeal, Criminal Section, dec. no. 128/2011; Pitești Court of Appeal, Criminal Section, dec. no. 496/2014; Pitești Court of Appeal, Criminal

represents a useful and necessary endeavour. Precisely for this reason, as shall become evident during this Thesis, the references made to other legal systems are numerous. Besides Spanish, Italian, or German law, we have made references to Swiss, French, Dutch law etc.

The study of computer forgery from the point of view of Comparative Law is problematic to an extent. This is because, despite the provisions of Article 7 of the Convention on Cybercrime, legal systems of a particular relevance to the national legal system (Italian, Spanish, German, or French Law) did not criminalize computer forgery as an autonomous crime, or had an approach which was completely different from that of the Romanian legislator.

**Additionally**, it is noticeable that the literature generally hesitates to propose practical solutions for solving certain real problems at the level of the interpretation or application of criminalization texts.

In this context, we consider that following an in-depth analysis of national legislation, by reference to elements of Comparative Law, and taking into account the relevant European legislation, **it is possible to formulate definite proposals of reformation of the cybercrimes** under analysis or of other crimes with which these are in a problematic relationship from a legal point of view. The role of literature is not only to clarify or to bring controversial discussions to an end, but also to propose **solutions to simplify criminal law** in the context of the continuous quantitative and qualitative expansions of criminal law which we are undergoing, which tends to become worrisome from the point of view of general legal principles.

As regards its contents, the Thesis shall focus on **the analysis of three cybercrimes**, namely unauthorized access to an information system (*Section II*), computer fraud (*Section III*) and computer forgery (*Section IV*), and each crime shall have a **distinct section within the Thesis** for a better systematization of the subject matter. These three sections shall have certain similarities, namely: the existence of a chapter referring to the

---

Section, dec. no. 672/2013; Craiova Court of Appeal, Criminal Section, dec. no. 1113/2015; Bucharest Court of Appeal, IInd Criminal Section, dec. no. 637/2017; Alba Iulia Court of Appeal, Criminal Section, dec. no. 171/2015; Bacău Court of Appeal, Criminal Section, dec. no. 128/2011; Cluj Court of Appeal, Criminal Section, dec. no. 1801/2011; Bucharest Court of Appeal, Ist Criminal Section, dec. no. 938/2016; Bucharest Court of Appeal, Ist Criminal Section, dec. no. 1189/2016; Bucharest Court of Appeal, IInd Criminal Section, dec. no. 1472/2017; Craiova Court of Appeal, Criminal Section, dec. no. 279/2017. There are some **Courts which retain a combination of offenses of fraud and computer fraud**: The High Court of Cassation And Justice, Criminal Section, dec. no. 3764/2013; Bacău Court of Appeal, Criminal Section, dec. no. 1012/2014; Bacău Court of Appeal, Criminal Section, dec. no. 1170/2015; Bucharest Court of Appeal, IInd Criminal Section, dec. no. 854/2016; Pitești Court of Appeal, Criminal Section, dec. no. 295/2011.

relationship between the national legislation and the provisions of certain supranational legal instruments; the analysis of the reasons and necessity of criminalization; and the discussion, within a distinct chapter, of the relationship between the crime which is the object of the analysis and other traditional cybercrimes provided for in the Criminal Code or in special legislation.

Additionally, taking into account that all cybercrimes which have been analysed shall be subordinated to the concept of “cybercrime” and shall represent a transposition in internal legislation of certain European legal instruments (The Framework Decision 2005/222/JAI on attacks against information systems<sup>9</sup> or Directive 2013/40/EU on attacks against information systems and replacing Council Framework Decision 2005/222/JAI<sup>10</sup>) or international ones (The Council Of Europe Convention On Cybercrime<sup>11</sup>), an introductory section was dedicated to analysing **the concept of cybercrime** (Section I, Chapter I) and **the terminology used** within the contents of criminalization texts which shall be the object of the analysis (Section I, Chapter II).

**The first section** (titled “Introductory Matters”) was structured in two chapters. The first chapter was dedicated to the concept of “cybercrime”, and the second one to the terminology used by the legislator within the contents of criminalization texts.

In **Chapter I** (titled “Cybercrime”) we aimed to highlight the difficulty of defining the concept of “cybercrime”<sup>12</sup> and the risks of using such a concept in the legislation. Firstly, we have identified examples of national or European normative acts where references are made to the concept of “cybercrime” (for example, Law no. 302/2004<sup>13</sup>, Directive 2018/1673/EU<sup>14</sup>, etc.).

In context, we have tried to point out that the use of a vague concept in the contents of legal instruments which should excel in clarity and predictability might make us question the observance of the principle of legality. Similarly, we have highlighted the risk of abusive interpretations through an unjustified expansion of the applicability sphere of criminal law, with the risk of violating the proportionality principle.

---

<sup>9</sup> Published in JOUE L 069/67.

<sup>10</sup> Published in JOUE L 218/8 of 14.08.2013.

<sup>11</sup> Ratified by Law no. 64/2004 for the ratification of the European Convention on Cybercrime, adopted in Budapest on 23 November 2001 (published in the Official Journal of Romania no. 343 of 20 April 2004).

<sup>12</sup> See, with respect to this, S. Gordon, R. Ford, *On the definition and classification of cybercrime*, in „Journal of Computer Virology”, nr. 2/2006, p. 13.

<sup>13</sup> Regarding international legal cooperation in criminal matters, republished (Official Journal of Romania no. 707 of 21 September 2015).

<sup>14</sup> Regarding combating money laundering by criminal law (JOUE L 284 of 12 November 2018).

In what follows, we proceeded with a succinct presentation of the main guidelines related to the definition of the concept of “cybercrime”. In this respect, we have insisted on the widespread definition<sup>15</sup> which establishes the contents of cybercrime by relating to three categories of crimes: **(1)** crimes against information systems or data – these being the “target” of criminal conduct; **(2)** crimes where the information system is only a means for the perpetration of the crime – in which case the information system is only a “tool” to the perpetration of the criminal act; **(3)** criminal activities which are incidental to the perpetration of other traditional crimes.

Also with regard to the contents of the concept of cybercrime we have identified, as national legal practice at the level of the High Court of Cassation and Justice,<sup>16</sup> that either an attempt was made to define the concept, or certain crimes or criminal conducts were included in this concept.

In **Chapter II** (titled “Terminological Aspects”) our aim was to analyse *in extenso* the concept of “information system”. The analysis had as its premise the supranational legal instruments which represented the sources of law for the national legislator. We refer, to that effect, to the Council of Europe Convention on Cybercrime, the Framework Decision 2005/222/JAI on attacks against information systems and to Directive 2013/40/EU on attacks against information systems.

In continuation, we have analysed the definition of the information system in the internal legislation [Article 181 Paragraph (1) of the Criminal Code] in an attempt to identify and explain the legal criteria to qualify a certain device as information system. We have referred, to this effect, to the information system as a device [the hardware component] and to the automatic processing of data via computer software [the software

---

<sup>15</sup> See, to that effect, 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*, in “Commonwealth Law Bulletin”, vol. 37, nr. 4/2011, p. 672; S.W. Brenner, *U.S. Cybercrime Law: Defining Offenses*, in “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*, in “Asian Criminology”, vol. 5, 2010, p. 126; I. VasIU, L. VasIU, *The Cybercrime Challenge: Does the Romanian Legislation Answer Adequately*, in “Law Review”, vol. III, nr. 2/2013, p. 45-46; D. Chilstein, *Législation sur la cybercriminalité en France*, in “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.

<sup>16</sup> See, in this respect, The High Court of Cassation and Justice, Criminal Section, dec. no. 1415/2014 (on the definition of the concept); The High Court of Cassation and Justice, Criminal Section, dec. no. 1396/2013 (on the inclusion of phishing-type conducts to the concept of cybercrime); The High Court of Cassation and Justice, Criminal Section, dec. no. 2346/2012 (on crimes which are included in the concept of cybercrime).

component]. We have even made references to elements of comparative law, attempting to highlight two types of approaches: the one in which the information system benefits from a legal definition (USA, Canada, the Netherlands, Austria, etc.) and the one in which the interpretation of the concept was left to the literature and case-law (the United Kingdom, Italy, France, Spain, etc.).

The centre of gravity of the analysis of the concept of “information system” targets an *in concreto* analysis of numerous examples of information systems or problematic examples from the point of view of the legal qualification, including through reporting to the legal practice. As an example, we have taken into account the following devices: servers offering certain services or where certain web pages are hosted; the electronic trading system for the capital market; ATMs, POS terminals, smartwatches, smart TVs, gambling machines, devices in the category of the *Internet of Things*, skimmer-type devices, modern vehicles, etc. Besides these devices we have analysed databases, web pages, the Internet, the electronic communications network, SIM cards, electronic payment instruments, etc. All this to try to clarify the sphere of applicability of the concept of “information system” and to highlight the possible controversies which may occur in connection to this concept.

Upon identification of all these problems, we have also taken into account a possible reconceptualization of the notion, starting with redefining it. We have analysed, in this respect, the possibility of introducing additional elements to the definition, such as the main function of an information system, its autonomous nature, or certain negative criteria to provide reasonable limitations to the sphere of applicability of the concept. Not least, we have proposed a restrictive interpretation of the current definition in an attempt to solve the possible controversies which may arise in connection with the use of certain household appliances, of a smart TV, of a multi-function printer, etc.

Besides the concept of “information system” we have analysed the concepts of “computer software”, “computerized data”, and “electronic payment instrument”. All of these analyses have aimed to eventually clarify certain concepts which are included in the constituent elements of certain crimes, or which have special relevance from the point of view of criminal procedural law.

As regards the electronic payment instrument, we have even analysed Directive (EU) 2019/713 on combating fraud and counterfeiting of non-cash means of payment and

replacing Council Framework Decision 2001/413/JAI.<sup>17</sup> Even though the electronic payment instrument is expressly taken into account only by Article 250 of the Criminal Code [carrying out fraudulent financial operations], Directive (EU) 2019/713 refers even to virtual coins. However, these are not included by *lege lata* in the concept of electronic payment instrument, which implies the necessity of testing the applicability of the crime provided for by Article 249 of the Criminal Code [computer fraud] with a view to covering this apparent “legal vacuum”.

**The second section of the Thesis** (titled “Unauthorized Access to an Information System”) represents an ample analysis of the crime provided for by Article 360 of the Criminal Code, with repeated references to elements of comparative law and vast national and comparative law bodies of case-law.

Starting with the inspiration source of the national legislator and continuing with the means of transposition within the internal legislation of the Convention on Cybercrime and of Directive 2013/40/EU, interpretation problems and controversies have been highlighted which may arise in legal practice in relation with the current regulation. We have also analysed both decisions of the Constitutional Court identified in connection with the crime of unauthorized access to an information system,<sup>18</sup> as well as the appeal in the interests of the law settled by the High Court of Cassation and Justice by Decision no. 15/2013.<sup>19</sup>

Before actually analysing the contents of the crime an attempt was made to clarify the reasons for criminalization. Through this activity, we did not just aim to justify the introduction of an autonomous criminalization text which would cover unauthorized access to an information system, but we also aimed to highlight certain possible similarities to the crime of trespassing on private property [Article 224 of the Criminal Code]. The purpose of such an activity was to identify certain connections which, despite the difference at conceptual level, may help to clear certain matters in connection with the crime of unauthorized access to an information system. Here we refer to the identification of the passive subject, the delegation of authorization from the owner of the information system,

---

<sup>17</sup> JOUE L 123/18 of 10 May 2019.

<sup>18</sup> See, in this respect, Decision no. 183/2018 of the Constitutional Court (published in the Official Journal of Romania no. 486 of 13.06.2018) and Decision no. 353/2018 of the Constitutional Court (published in the Official Journal of Romania no. 650 of 26.07.2018).

<sup>19</sup> See, in this respect, The High Court of Cassation and Justice, the Panel competent to hear the appeal in the interests of the law, dec. no. 15/2013 (published in the Official Journal of Romania no. 760 of 6.12.2013).

the relationship between unauthorized access and exceeding the limits of the authorization or the unauthorized maintenance of access, etc.

From the perspective of the contents of the crime the analysis was done *in extenso*, attempting to clarify all problematic matters which may arise in connection with this criminalization text. For example, as regards the passive subject, we aimed to elaborate a theory for the identification of the owner of the information system, by reference to the existence of a consolidated right of usage, also attempting to clear the relationship between the plurality of passive subjects and the plurality of information systems accessed.

The analysis of the objective aspect has as its starting point the typology of unauthorized access to an information system in comparative law in order to highlight major discrepancies with regard to the regulation of this crime. In what follows, we have firstly attempted to clarify the relationship between access to an information system and access to a storage device for computerized data, by relating it to various problematic hypotheses. This was done in order to highlight a possible problem connected to the sphere of applicability of the crime, taking into account that the omission of the legislator to criminalize not just access to an information system, but also the access to a storage device for computerized data.

The analysis of the criminalized conduct (access) was also based on a vast body of literature and case law relevant with regard to the meaning of the concept of access. Through such an activity we have attempted to identify clear examples of access and examples liable to generate controversies.

We have taken into account in this respect a large range of hypotheses, such as: remote use of an information system by means of *Team Viewer*; accessing an online bank account; unauthorized authentication (access) to the control panel of a web page; accessing an ATM via an electronic payment instrument; unauthorized alteration of a web page by replacing or changing the way in which it is displayed; the transmission of an email; *denial-of-service* attacks [*DoS attack*]; *port scanning*; obtaining computerized data via *phishing*; *web spoofing*; offering fictitious goods for sale on the Internet; the physical interaction with an ATM; the making of payments at a POS terminal; the making of online payments; accessing certain URL addresses (non-public) of certain web pages (public); unauthorized copying of computerized data from an information system belonging to a third party; the use of *keylogger* software in order to intercept data input via the keyboard by the victim; infecting of certain information systems with malicious software (virus), etc.

The conclusion with regard to the concept of “access” was that it should take into account an interaction at logical level through which the agent can benefit from the resources or / and functions of that information system.

Lack of authorization, by reference to the “unauthorized” concept, was also examined *in extenso*, in an attempt to settle certain controversies. Similarly, the analysis of the notion of access has taken into account numerous hypotheses identified in the legal practice. By way of example, we make reference to the following: lack of express authorization from the network administrator; unauthorized use of a fuel card; the introduction of fictitious ads on the eBay platform; the creation of fictitious accounts on the eBay platform; accessing a restricted web page by an employee having a fraudulent purpose; use of a laptop which is a joint asset of the spouses; accessing the Internet banking account by one of the spouses; accessing an email account using a password previously received; checking the fiscal situation of tax payers in another jurisdiction, etc.

To better highlight the complexity of the analysis of this concept, we even analysed the case-law of the Italian Court of Cassation which excessively extended the scope of the offense of unauthorized access [abusive access in Italian law], as well as the theories proposed by American law regarding the lack of authorization (contractual theory, the theory of breaching an obligation of loyalty, the theory of overrunning security measures, and the theory of revoking authorization). Subsequently to all of these analyses, we have attempted to identify a *reasonable framework* through the establishment of limits to the “unauthorized” concept in relation to a series of objective adjunctive criteria.

The moment of perpetration of the offense and the delimitation between the attempt and simple preparatory acts without criminal significance were also the subject of detailed analysis. In this context, beyond the attempt to identify the moment of perpetrating the offense, and to analyse the desistance and prevention of the occurrence of the result, we have also taken into account actual hypotheses which could create problems from the perspective of the legal qualification of these as acts of execution or preparatory acts.

Aggravated forms of the offense of unauthorized access to an information system (in order to obtain computerized data [Article 360 Paragraph (2) of the Criminal Code] and by overriding the security measures [Article 360 Paragraph (3) of the Criminal Code]) have a separate section. As regards the aggravating circumstance referred to in Article 360 Paragraph (2) of the Criminal Code we have analysed the special contents and the relationship with other crimes. Instead, the aggravating circumstance referred to in Article

360 Paragraph (3) of the Criminal Code benefited from a more detailed analysis, touching on issues such as: the reason for the criminalization of the aggravated form, the nature of the security measures (physical, organizational, or logical), or characteristics of these.

With regard to the characteristics of the security measures, we even highlighted the differentiation between the effectiveness and reliability (efficiency) of the security measures, in an attempt to provide adjuvant criteria for setting reasonable limits to the applicability of this aggravating circumstance. Additionally, we have described certain specific procedures for prohibiting or restricting access (for example, the use of biometric elements or the setting of MAC addresses), together with the clarification of devices or software by means of which it is possible to achieve the same purpose.

Not least, we analysed the ways in which it is possible to overcome the security measures, a matter which even generated, in places, an inconsistent legal practice. In this context, we have taken into account the fraudulent means of obtaining the authentication data from the victim, using these after the loss of authorization, or the use of actuals for authentication.

The last two chapters (Chapter VI and Chapter VII) of Section II refer to the relationship of the offense of unauthorized access to an information system with other criminal offenses provided for in the Criminal Code or in the special legislation, and the reformation of Article 360 of the Criminal Code. The most relevant discussion is related to the settlement of the relationship between unauthorized access to an information system and violating the confidentiality of correspondence [Article 302 of the Criminal Code]. In this respect, it was argued *in extenso*, within the meaning of only retaining the offense referred to in Article 360 of the Criminal Code, within the hypothesis of accessing electronic mail, despite some doctrinal opinions and case-law stating the contrary.

**The third section of the Thesis** (entitled “Computerized Fraud”) is also a broad analysis of the offense referred to in Article 249 of the Criminal Code, with reference to elements of comparative law.

Beyond the analysis of the source of inspiration of the national legislator, the method of transposition into national law of Article 8 of the Convention on Cybercrime and the analysis of the need to transpose, in the future, the provisions of Directive 2019/713 (EU) on combating fraud and counterfeiting of non-cash means of payment, we have also analysed *in extenso* the reason and the necessity of the criminalization of computer fraud. In this respect, we have analysed the potential conflict occurring at

conceptual level between computer fraud and traditional fraud, in an attempt to conclude to what extent traditional fraud can cover the conduct specific to computer fraud.

From the perspective of the analysis of the contents of the offense of computer fraud, we emphasized an *in concreto* analysis of each way of perpetrating a deed, with reference to hypotheses that have been taken into account in legal practice and in the literature. Thus, with regard to each means of perpetrating, beyond clarifying the contents of each respective means, we have analysed hypotheses complying with the concept of computer fraud, and hypotheses which should be subject to other criminalization texts.

In this context, as regards **the means of introduction of computerized data** we have analysed hypotheses such as theft of virtual currencies, top-ups of prepaid cards, “artificial” increase of the balance of a bank account, fraudulent online auctions, *phishing* and *pharming* activities, offline trading, the use of a *spyware dialer*, *crypto-jacking*, etc.

For **the means of altering computerised data** we have taken into account hypotheses such as carrying out a transfer of funds, altering the balance of a bank account, maintaining a given service as active for the purpose of additional billing, alteration of the contents of a web page, etc. Even though **the means of erasure of computerised data** is not often encountered in legal practice, we analysed problematic hypotheses related to the use of a magnet on a computerized data storage device, or the erasure of debts from the database. As regards **the means of restricting access to computerised data** we analysed in particular by reference to the hypothesis of restricting access to certain accounts by changing the password and ransomware type conducts. Not least, **the means to prevent in any way the functioning of an information system** revealed the problematic of manipulating electronic games of chance, the logical interaction with an ATM without the use of an electronic payment instrument, the physical interaction with an ATM (the “fork” method), the deactivation of electronic protection devices for the theft of a particular good, etc.

Beyond the analysis of such commissive conduct whenever the possibility to retain the commissive act by omission, by reference to the institution of the position of guarantor (Article 17 of the Criminal Code), we have analysed the consequence consisting in the production of material damages and the material benefit from the contents of the special purpose provided for in Article 249 of the Criminal Code.

From the perspective of the moment of perpetration of the offense of computer fraud, the main analysis was focused on the identification of preparatory acts which are not

liable to come within the scope of attempts. To this effect, we have analysed in particular the unauthorized access to an information system and the phishing activity.

Similar to the offense of unauthorized access to a computer system, the last two chapters are dedicated to the relationship between the offense of computer fraud with other criminal offenses provided for in the Criminal Code, or in the special legislation, and the reformation of Article 249 of the Criminal Code.

**The fourth section of the Thesis** (entitled “Computerized Forgery”), similar to Computer Fraud and Unauthorized Access To An Information System, is also an ample analysis of the offense referred to in Article 325 of the Criminal Code, with reference to elements of comparative law. The study of computer forgery from the perspective of comparative law was, however, limited by the fact that, despite the provisions of Article 7 of the Convention on Cybercrime, legal systems of note to the national legal system (Italian, Spanish, German, or French Law) did not criminalize computer forgery as an autonomous crime, or had an approach which was completely different from that of the Romanian legislator.

In an attempt to conceptualize the offense of computer forgery we have started from the concept of traditional writ and we have drawn a parallel between its functions and the computerized data relevant from the perspective of computerized forgery. We have therefore considered the function of perpetuation, probative, and guarantee in order to attempt to establish a correspondence between the computerized data on which the agent intervenes, and the concept of electronic document as equivalent of a traditional writ.

The analysis of the objective aspect of the offense of computer forgery followed the same approach used in the case of computer fraud and unauthorized access to an information system. We have, therefore, insisted on certain hypotheses drawn from legal practice, these being analysed in such a way as to be able to conclude to what extent is Article 325 of the Criminal Code applicable or is another criminalization text incident.

As regards **the means to introduce computerized data** we have analysed hypotheses like *web spoofing*, *email spoofing*, the unauthorized use of electronic signatures, the introduction of false computerized data (information) into the ECRIS system, creating false or fictitious profiles (accounts) on social networks, cloning SIM cards, the publication of fictitious ads on various online platforms, creating a duplicate of an electronic document, etc. **The means of altering computerized data** was analysed by reference to hypotheses such as changing the Baccalaureate grade in a digital catalogue,

changing the phone number associated with a bank account, changing the name and price of a product, *caller ID spoofing*, *IP spoofing*, etc. As regards **the means of erasure of computerized data** we have firstly taken into account the erasure of debts from a database. Not least, in relation with **the means of restricting access to computerized data**, we have analysed the situation of deactivating the option of Home Banking or restricting access to the prosecutor to certain electronic documents by protecting them with a password.

Unlike computer fraud and unauthorized access to an information system, in Section IV, dedicated to the offense of computer forgery, we included two chapters dedicated to the relationship between computer forgery and traditional forgery, and the relevance of computer forgery in the context of identity theft.

As regards the relationship between computer forgery and traditional forgery, we have primarily highlighted the deficient parallel from the point of view of the penalty limits, the sanctioning of the attempt, the criminalization of using forged instruments, etc. Having as a prerequisite these differences existing between the two categories of offenses, we analysed various extremely problematic hypotheses, such as: counterfeiting or alteration of a traditional writ in an information system; continuing the activity of alteration after printing the contents of the electronic document on paper; counterfeiting or alteration of electronic invoices, etc.

All these hypotheses analysed both from the point of view of computer forgery, as well as traditional forgery, were intended to highlight the difficulty of identifying the moment in which we can perceive a traditional writ, or the act of execution, or the problematic legal consequences of the metamorphosis of computer forgery into traditional forgery.

As regards identity theft, we attempted to clarify this concept by reference to three internationally accepted phases<sup>20</sup>, namely: the phase of obtaining the personal data; the phase of interacting with the personal data obtained in the first phase; the phase of the actual use of the personal data. Having regard to these three phases which incorporate the concept of identity theft, we analysed the relevance of the offense of computer forgery. In

---

<sup>20</sup> See, to that effect, 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*, in “Cahiers de défense sociale”, nr. 36/2009-2010, p. 25.

this context, we analysed the activity of phishing and other related activities likely to attract the applicability of Article 325 of the Criminal Code.

Similar to the offense of unauthorized access to a computer system, the last two chapters are dedicated to the relationship between the offense of computer fraud with other criminal offenses provided for in the Criminal Code, or in the special legislation, and the reformation of Article 325 of the Criminal Code.

*Summa summarum*, this Thesis is an in-depth study of the offense of unauthorized access to an information system, computer fraud, and computer forgery. The analysis is mainly focused on the analysis of certain legal issues largely ignored by the national literature, but which have generated particular problems in legal practice.