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

SECTION II

UNAUTHORIZED ACCESS TO A COMPUTER SYSTEM

(ARTICLE 360 CRIMINAL CODE)

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

SECTION IV

COMPUTER FORGERY

(ARTICLE 325 OF THE CRIMINAL CODE)

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**,[1] even when they were only regulated by special legislation (Law no. 161/2003[2], and Law no. 365/2003[3]). 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

[1] **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 şi Drept informatic*, (*Legal Informatics And Informatics Law*), Ed. Albastră, Cluj, 2002; T. Amza, C.-P. Amza, *Criminalitatea informatică*, (*Cybercrime*), Ed. Lumina Lex, Bucureşti, 2003; I. Vasiu, L. Vasiu, *Prevenirea criminalităţii informatice*, (*The Prevention Of Cybercrime*), Ed. Hamangiu, Bucureşti, 2006; M. Dobrinoiu, *Infracţiuni în domeniul informatic*, (*Crimes In The Field Of Informatics*), Ed. C.H. Beck, Bucharest, 2006; Ş. I. Vasiu, *Criminalitatea informatică*, (*Cybercrime*), Ed. Sitech, 2008; M. Dobrinoiu, *Criminalitatea informatică,* (*Cybercrime*), Ed. Academiei Naţionale de Informaţii, Bucureşti 2009; A. Trancă**,** I. Vasiu, L. Vasiu, *Criminalitatea în cyberspaţiu*, (*Criminality In Cyberspace*), Ed. Universul Juridic, 2011; D.C. Trancă, *Infracţiunile informatice 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 informatice*, Ed. Giappichelli, Torino, 2009; M. Quéméner, Y. Charpenel, *Cybercriminalité. Droit pénal appliqué,* Ed. Economica, Paris, 2010; A. Amato G. Saraceni, *I reati informatici. Elementi di teoria generali e principali figure criminose*, Ed. Giappichelli, Torino, 2015; G.B. Hoyos, *El delito de estafa informática*, Ed. Leyer, Bogotá, 2009; A. Cadoppi, S. Canestrari, A. Manna, M. Papa M. (dir.), *Cybercrime* [Kindle], Ed. UTET Giuridica, Milano, 2019; J. Clough, *Principles of Cybercrime*, second edition, Cambridge University Press, UK, 2015.

[2] 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).

[3] 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[4] and case-law is vast and has a remarkable scientific standard.[5] We therefore believe that, in order to clarify the concepts of "access" and "unauthorized"[6] 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*[7] 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,[8] such an incursion in Comparative Law

---

[4] 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 Statues*, 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.

[5] 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.

[6] American law mentioning "lack of authorization".

[7] 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.

[8] 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; Piteşti Court of Appeal, Criminal Section, dec. no. 689/R/2008; Ploieşti Court of Appeal, Criminal Section, dec. no. 1084/2016; Ploieşti 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; Piteşti Court of Appeal, Criminal Section, dec. no. 496/2014; Piteşti 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[9] or Directive 2013/40/EU on attacks against information systems and replacing Council Framework Decision 2005/222/JAI[10]) or international ones (The Council Of Europe Convention On Cybercrime[11]), 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"[12] 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[13], Directive 2018/1673/EU[14], 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.

---

[9] Published in JOUE L 069/67.

[10] Published in JOUE L 218/8 of 14.08.2013.

[11] 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).

[12] 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.

[13] Regarding international legal cooperation in criminal matters, republished (Official Journal of Romania no. 707 of 21 September 2015).

[14] 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[15] 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,[16] 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

[15] 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 droi suisse et aperçu de quelqyes 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.

[16] 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.[17] 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,[18] 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.[19]

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,

[17] JOUE L 123/18 of 10 May 2019.

[18] 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).

[19] 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[20], 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

[20] 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.