THE 15TH EDITION OF THE INTERNATIONAL CONFERENCE
EUROPEAN INTEGRATION
REALITIES AND PERSPECTIVES

The Concept of Computer Crime

Ștefănuț Radu[1]

Abstract: The object of this scientific study is represented by the analysis of the concept of computer crime also called computer-oriented crime, which is not generally acknowledged or accepted.The result of the study consists in analysing the evolution of computer crime.The conclusion is that certain legal provisions shall lead, sooner or later, to an Internet Law.

Keywords: computer crime; Internet Law; illegal action

Computer crime is a phenomenon of our times, frequently reflected in the media. A study even indicates that the fear of cyber attacks far outweighs that of ordinary thefts or frauds. Criminological research on offenses committed through computer systems are still in the exploratory process. Even those achieved so far tend to change the classical way in which crimes are viewed in the current criminal justice systems. (Amza, 2003, p. 14).

The specialists in the field have defined the phenomenon in many ways, not reaching a common point, because of the complexity of this criminal act, and the different ways of regulating the computer crime in each state have led to the impossibility of creating an international legal pattern.

The concept of computer crime has received several definitions, including: any crime in which a computer or computer network is the subject of a crime, or in which a computer or computer network is the instrument or means of committing a crime; any unlawful, unethical or unauthorized behaviour regarding automatic data processing and/or data transmission.

Computer systems currently provide new opportunities, some even sophisticated, for violation of laws and create a high potential for committing types of crimes committed other than in known, traditional ways. Although the society, as a whole, pays for all the economic damage caused by "computer crime", it continues to rely on computerized systems in almost all areas of social life: air traffic, trains and subways control, coordination of medical service or national security. A single breach achieved in the operation of these systems can endanger human lives, which denotes that the society's dependence on information systems has taken on a much deeper dimension than initially anticipated (Dobrinoiu, 2006, p. 59).

A definition on computer crime that seems more eloquent is "any illegal action in which a computer is the instrument or object of the crime, that is to say, any offense whose means or purpose is to influence the function of a computer (Dobrinoiu, 2006, p. 62)".

[1] Assistant Associate Professor, PhD, Danubius University of Galati, Romania, Address: 3 Galati Blvd., 800654 Galati, Romania, Tel.: +40372361102, Fax: +4037236129 0, Corresponding author: stefanut.radu@univ-danubius.ro.

Only a small part of the criminal acts related to the use of information systems are acknowledged by the criminal investigation bodies, so it is very difficult to get an overview on the magnitude and evolution of the phenomenon. If it is possible to make an adequate description of the types of criminal acts encountered, it is very difficult to present a summary based on the extent of the losses caused by them, as well as the actual number of crimes committed, the number of computer crime cases is constantly increasing.

The evolution of organized crime in Romania in recent years is closely linked to the evolution of computer crime and the increasing use of IT&C technology in committing crimes.

The analyzes carried out at the level of the European bodies regarding the tendency of organized crime define computer crime as an important branch of organized crime at the level of the European Union countries.

As a result of this evolution, a series of studies and evaluations have also been carried out in Romania, which have identified some characteristics of this type of criminality that take place in the territory of our country or in which the perpetrators are Romanian citizens.

Thus, these activities aim to obtain financial products, respectively credit and payment systems provided by financial-banking institutions, which the members of these criminogenic networks access fraudulently, causing significant damage to both individuals, but also to corporations or companies. The perpetrators of these crimes are much more difficult to identify and retain due to the fact that they have a high level of intelligence and have sophisticated, state-of-the-art computer resources.

The criminal groups are organized, structured and specialized on different types of activities, depending on the individual abilities of the members and the degree of complexity of the IT operations that those involved are able to make available to the group, in order to access as quickly as possible the technical means, the penetration of workstations, servers and other computing devices used in the financial, banking environment, etc. Another feature of the criminal groups refers to the cross-border character, which means that the members of the networks can be spread both on the territory of Romania and in other areas of the world, from where they can access information and perform criminal operations, without being easily identified.

The evolution of computer crime is motivated by several causes, of which we mention: the sophisticated technology used by the perpetrators, the lack of a reaction plan in case of attacks, by the victims of these offenses, which can lead to the failure to identify the losses caused; the lack of specific training of officers within the criminal investigation bodies; the restraints in reporting the criminal prosecution bodies the commission of the crimes.

In the latter situation, even if the crime was noticed, the victims do not notify the criminal prosecution bodies in order to discover and sanction the perpetrator. There are multiple motivations for this behaviour. Of these, we mention concerns about the public image, which could be affected by the publicity around the crime; the desire not to bear the costs of any investigation, given the complexity of such investigation; last but not least, the lack of the possibility of recovering the losses suffered, even in the case of identification of the perpetrator.

Only a small part of the criminal facts related to the use of information systems is acknowledged by the criminal investigation bodies, so it is very difficult to get an overview on the extent and evolution of the phenomenon.

The law of the states of the world is constantly changing due to the increasingly accelerated development of the information technology, and the international cooperation is faced with a continuous challenge

caused by the increase of the computer crime, and the international cooperation is faced with the continuous challenge caused by the increase of the transnational computer crime. More and more states have proceeded to harmonize their legislation in order to combat the phenomenon in question, but the results are only satisfactory, and it will not be possible to speak of an eradication of the phenomenon.

The issues raised at international meetings on combating computer crime are as follows:

a) the lack of a global consensus on the definition of *"computer crime";*

b) the lack of a global consensus regarding the motivation of these offenses;

c) the lack of expertise from authorized persons belonging to institutions with control powers in the field;

d) the absence of adequate legal norms regarding the access and investigation of the information systems, including the lack of the norms by which the computerized databases can be seized;

e) the lack of legislative harmonization regarding investigations in the field;

f) the transnational character of this type of crime;

g) the existence of a small number of international treaties on extradition and mutual assistance in the field.

The Organization for Economic Cooperation and Development (OECD) was one of the first international organizations to carry out a study on harmonizing legislation in this field.

In 1983, the OECD published a report proposing various legislative recommendations to the Member States of the European Union, as well as a minimum list of activities to be punished: computer fraud and forgery, alteration of computer programs and data, copyright, interception of communications or other functions of a computer, unauthorized access and use of a computer (Dobrinoiu, 2006, p. 61).

In Romania, the specialized services investigated only 200 computer-oriented crimes, of which 50% were fraudulent electronic auctions, 30% were fraudulent online ordered goods, 10% were unauthorized access to information systems and 10% were referring to Nigerian letters, transmission of viruses, child pornography and the use of false identities (Vasiu, 1998).

In the US, 18 USC 1030 (a) (4) defines *"computer fraud"* as unauthorized access or access that exceeds the authorization granted to a protected computer, with the intention of fraud, subsequently obtaining any value gain *(anything of value)*, except where the object of the fraud and its result consisted solely in the use of the computer and the value of such use does not exceed $5,000 in a period of one year.

The black figure is motivated by several causes, of which we mention:

- sophisticated technology used by the perpetrators;
- lack of specific training of officers within the criminal investigation bodies;
- the lack of a reaction plan in case of attacks of the victims of these criminal acts, a situation that can lead to the failure to identify the caused losses;
- the retraints in reporting to the criminal investigation bodies the commission of the crimes.

In the latter situation, even if the crime was noticed, the victims do not notify the criminal prosecution bodies in order to discover and sanction the perpetrator. There are multiple motivations for this behaviour:

- concerns about the public image, which could be affected by the publicity around the crime;

- the desire not to bear the costs of any investigation, given the complexity of such investigation;
- the impossibility of recovering the losses suffered, even in the case of identification of the perpetrator.

At the same time, investigations in the field of computer crime are, by their nature, complex and involve the use of sophisticated equipment, at high costs. Also, the training of specialized personnel is a long-term process and involves high costs. Such investigations are time consuming.

In international studies, the term *"computer-oriented crime"* or *"computer crime"* is used, which is not generally ackowledged or accepted.

The content of the notion of criminal offense of computer nature is very varied, being approached from different perspectives within the specialized works.

Thus, in the report of the European Committee for Criminal Problems, computer crimes are systematized into the following categories:

- the crime of computer fraud;
- the crime of forgery in computer science;
- the crime of prejudice to data or computer programs;
- the crime of computer sabotage;
- the crime of unauthorized access to a computer;
- the crime of unauthorized interception;
- the crime of unauthorized reproduction of a computer program protected by law;
- the crime of unauthorized reproduction of a topography;
- the crime of unauthorized alteration of data or computer programs;
- the crime of computer espionage;
- the crime of unauthorized use of a computer;
- the crime of unauthorized use of a computer program protected by law.

Also, the group of experts gathered within the OECD adopted a working definition in the form: "*computer abuse* is any illegal or unethical or unauthorized behaviour that concerns automatic data processing and/or data transmission".

It can be seen that these experts did not find it useful to explicitly define the term "*computer crime*" but retained a functional classification as a basis of study (Vasiu, 1998, p. 27).

At the same time, the term *computer crime* is defined as "any illegal action in which a computer constitutes an instrument or the object of the offense, that is to say, any crime whose means or purpose is to influence the function of a computer".

Computer abuse could be defined, in turn, by "any incident related to the computer technique in which a person suffered or could have suffered a prejudice and from which the perpetrator obtained or could have intentionally obtained a profit (Vasiu, 1998, p.29)" or by "all the acts committed in the area of new technologies, in a certain period of time and on a certain well-defined territory (Amza, 2003, p.13)".

According to the European Committee for Criminal Issues, all these attempts to define *computer crime* have some drawbacks that are not easily reconciled with the aim of conciseness of the formulation and that of leaving no doubt about the importance or use of the definition.

Thus, more specifically, a computer crime means *any crime in which a computer or computer network is the object of a crime, or where a computer or computer network is the instrument or means of committing a crime.* (Banciu & Vlăduţ, 2001)

By computer crime in the restricted sense is meant *any crime in which the perpetrator interferes, without authorization, with the processes of automatic data processing.*

The content of the notion of criminal act of computer nature is very varied, being approached from different perspectives in the specialized works.

Computer crimes can be classified according to various criteria. We will use for the classification of computer crimes the criterion of the role played by the computer systems in committing the crime. From this perspective, computer crimes are classified into:

- *crimes committed with the help of information systems*, in which information systems are a tool to facilitate the commission of crimes. These are "traditional" crimes, perfected by the use of computer systems;

- *crimes committed through and on the computer systems*, in which the computer systems, including the data stored therein, are the target of the crime. These crimes can only be committed through computer systems. They have become the obbject of legal regulations in recent years.

We also hereby mention another role that information systems can play in the forensic investigation: the role medium for storage and retrieving clues or evidence regarding the way of committing a crime. These crimes can only be committed through computer systems. They have been regulated in recent years.

Awareness of the existence of the social danger of the criminal facts of computer nature has led to their incrimination in many states of the world. Thus, the concept of "criminal law with computer specificity" came into being, as a reflection of the many novelty elements introduced in the field of criminal law by the new forms of criminality based on modern technology.

To begin with, a definition of the instruments or concepts with which the legislator has understood to operate in this field is necessary. This is even done by the legislator in the provisions of art. 35 of *Law no. 161/2003*, as follows:

a) "*computer system*" means any device or set of devices interconnected or in functional relationship, of which one or more ensure the automatic processing of data, by means of a computer program; Examples: personal computer (PC), two or more computers connected by cable or wireless (wireless), computer network, computer-peripheral assembly (printer, external storage media, scanner, etc.);

b) "*automatic processing*" of data means the process by which the data in a computer system are processed through an informatics program. Example: following a logical algorithm, the instructions for the computer are written in a high-level programming language (Pascal, C ++, Visual Basic, Java, etc.), introduced from the keyboard and interpreted by the Central Processing Union, and then translated into machine-code language and implemented by the Execution Union, each component of the informatics system performing a certain operation;

c) "*computer programme*" means a set of instructions that can be executed by a computer system in order to obtain a certain result. Examples of programs: operating systems (MS-DOS, MS, Windows, UNIX etc.), standard application packages (MS OFFICE which includes a text editor, MS Word, a database management software, MS Access, a tabular computer program, MS Excel, a presentation program, MS Powerpoint, a mail management program and current activities, MS Outlook etc), antivirus programs (Bit Defender, Norton System Works, RAV etc.), Internet access programs (browsers - Explorer, Netscape etc., e-mail - Outlook, Webmail, Eudora etc.), various applications created for a particular purpose (viruses, Trojans, logic bombs, keylogger, spyware etc.) and many more;

d) "*computer data*" means any representation of facts, information or concepts in a form that can be processed through a computer system. This category includes any computer program that can determine the performance of a function by a computer system. At the user level, the data are represented in alphanumeric form - numbers, letters, special characters, as they appear on the computer screen, and at the computer system level they are presented in the form of rows ordered by 8, 16, 32, 64 or 128 bit (elements "0" and "1" which, at the level of the electronic components of the computing system, are equivalent to controlled variations of the supply voltage);

e) "*service provider*" means:

- any natural or legal person that provides users the opportunity to communicate through computer systems;
- any other natural or legal person that processes or stores computer data for the persons mentioned in point 1 and for the users of the services provided by them;

f) "*data related to information traffic*" means any computer data related to a communication made through an information system and produced by it, which is part of the communication chain, indicating the origin, destination, route, time, date, size, volume and duration of the communication, as well as the type of service used for the communication;

g) "*user data*" means any information that can lead to the identification of a user, including the type of communication and the service used, the postal address, the geographical address, telephone numbers or other access numbers and the payment method of the respective service, as well as any other data that may lead to user identification;

h) "*security measures*" means the use of specialized procedures, devices or software by which access to a computer system is restricted or prohibited for certain categories of users. Example: access system (LOGIN) based on password and username, PKI type - Public Key Infrastructure, with public or private keys, electronic signature applications, Smart Card access equipment, reader/interpreter fingerprints or retina etc.;

i) "*child pornographic material*" means any material that presents a minor having explicit sexual behaviour or a major person who is presented as a minor having explicit sexual behavior or images that, although they do not present a real person, simulate, in a credible way, a minor having explicit sexual behaviour.

The categories of computer crimes provided by the Romanian legislation are:

Crimes committed using computer systems

A series of offenses provided by the criminal law have particularities that allow them to improve their enforcement by resorting to the help given by the information systems. They are those crimes in which "modus operandi" is not directed against the proper functioning of a computer system, or on the

information contained therein, but the result of the data processing is used for the commission of some classic crimes. The perpetrators thus appeal to non-traditional means for committing crimes of a "traditional" character. (Vasiu, 2002, p. 166).

Crimes committed by computer systems

Law no. 21/1999, for the prevention and sanctioning of money laundering introduced for the first time in the Romanian legislation the notion of "crimes committed through computers".

According to the text of art. 23, lit. a, the crime of money laundering (…] is *the change or transfer of values, knowing that they come from the commission of crimes*: (…] *crimes committed through computers,* (…] *for the purpose of hiding or concealing their illicit origin, as well as in purpose of concealing or favoring the persons involved in such activities or supposed to evade the legal consequences of their actions.*

Currently, the Romanian criminal law regulates a number of 10 crimes that correspond to the definition above. They are provided in Title III (Prevention and Fight against Computer Crime) of the Law on certain measures to ensure transparency in the exercise of public dignities, public functions and in the business environment, preventing and sanctioning of corruption, as well as in the Law on copyright and related rights.

As I mentioned, this offense, incriminated in art. 249 Criminal Code, had a similar regulation through the provisions of art. 49, Title III of Book I of Law no. 161/2003. If, with regard to the conditions of incrimination, there are no differences, with regard to the sanctioning regime, the new Criminal Code represents the more favorable criminal law (see the prison sentence from 2 to 7 years provided for by the new Criminal Code compared with the prison sentence from 3 to 12 years established by Article 49 of Law 161/2003) (Vasiu, 2015, p. 604).

Thus, in the contents of the Law no. 161/2003 we find defined three categories of crimes, namely:

1. Crimes against the confidentiality and integrity of data and information systems:

- the crime of *illegal access to a computer system*;
- the crime of *illegal interception of a transmission of computer data*;
- the crime of *altering the integrity of computer data*;
- the o crime of *disrupting the functioning of the information systems*;
- the crime of *carrying out illegal operations with devices or software*.

2. Computer crimes:

- the crime of *computer forgery;*
- the crime of computer fraud.

3. Child pornography through computer systems while the copyright law incriminates:

- allowing public access to computer databases containing or constituting protected works;
- making available to the public the technical means of neutralizing the protection of computer programs.

The concepts of *cybercrime*, "computer abuse" and "misuse of the computer" are also used, the expressions having different meanings. A distinction must be made between the intention of fraud and the misuse of information system or between the unauthorized entry into a network and the wrong action

of computer keys. As an example, if an employee receives a password to access a database from another employee, he should not be charged with a crime if he enters that database. Otherwise, it is judged the situation in which an employee steals the access password to that database, knowing that he has no access authorization to that database. The situation in which an employee steals password access to the database, knowing that he does not have authorized access to the base is judged in a completely different way.

Like any social phenomenon, *computer crime* is a system of own properties and functions, qualitatively distinct from those of the component elements (Nistoreanu & Păun, 1996, p. 23).

It is known that, in criminological research, criminality as a social phenomenon comprises: *real criminality* - which implies the totality of criminal acts committed in a certain territory and in a certain period of time; *apparent criminality* - which includes the entire set of crimes reported to the state's authorized bodies and registration as such; legal criminality - seen as the totality of the criminal acts committed in the informatics space and for which judgments are decretory.

Each of these segments also has its correspondent in *computer crime* (Amza, 2003, p. 13). The difference between *real computer crime* and apparent *computer crime* is the "black figure" of this new type of crime and it includes all those offenses sanctioned by the legislator, but which, for some reason, remain undiscovered by the authorized bodies (Amza, 1998, pp. 31-32).

Illegal access to a computer system

The legal regulation aims to protect the computer systems and data stored on them from unauthorized access thereto. *The computer system* is defined by law as any device or set of devices interconnected or in functional relation, of which one or more ensure the automatic processing of data, by means of a computer program.

A computer program is also defined by the law as a set of instructions that can be executed by a computer system in order to obtain a certain result. By *security measures*, the law means the use of specialized procedures, devices or software with which access to a computer system is restricted or prohibited for certain categories of users (Dobrinoiu, 2006, p. 147).

Illegal interception of a computer data transmission

The legal regulation protects the transmissions of computer data within or between computer systems, regardless of how they are performed. Computer data is defined as any representation of facts, information or concepts in a form that can be processed by a computer system, in the same category being included any computer program that can determine the performance of a function by a computer system.

Alteration of the integrity of computer data

The legal regulation aims to protect the computer data stored within the computer systems, aiming to prevent the alteration, deletion or deterioration of the computer data, restricting the access thereto, the unauthorized transfer of data from a computer system or a means of storing the computer data.

Disruption of the functioning of computer systems

The legal regulation aims to protect the computer data stored within the computer systems. We observe that, unlike the offense regulated in article 44, the emphasis is placed here on the effect that the actions on the computer data have on the affected computer systems (introduction, transmission, alteration, deletion, deterioration, restriction of access).

Computer forgery

The regulation aims to protect the legal security by incriminating all those actions that can, by modifying data on computer media, entail unintended legal consequences by or for the people who have designed, carried out, implemented or on which the effects of the modified information are manifested.

Child pornography through computer systems

This crime is on the border between the crimes committed with the help of computer systems and those targeting the computer systems. The crime of child pornography is regulated by the Romanian criminal law in force.

The introduction of these provisions in the law of computer crime gives rise to a new crime, different from the one previously regulated. This is on the line of child protection through different legislative instruments at European Union level.

Allowing public access to computer databases containing or constituting protected works

The legal regulation aims to protect the copyright of some computer databases, databases that constitute protected works themselves, or contain such protected works.

By *author*, the law means the natural person or natural persons who created the work. By *protected work*, the law means the original work of intellectual creation in the literary, artistic or scientific field, whatever the method of creation, the way or the concrete form of expression and regardless of its value and purpose.

The law does not define the notion of database. *Database* means a collection of data organized according to a conceptual structure that describes the characteristics of these data and the relationships between their corresponding entities, destined to one or more fields of application (Vasiu, 2006, p. 78).

In Romania, not the lack of legal definition, but its faulty interpretation in the cases in practice led to different or faulty solutions given by the courts, in similar situations, which led to the promotion and acceptance on October 14, 2013 of an appeal in the interest of the law[1].

The solutions recommended by the supreme court for defining key terms (such as "*computer system*" or "*access to a computer system*"), respectively the interpretation of the factual situations and the accomplishment of the legal frameworks, maintain their validity even after the entry into force of the *new Criminal Code* (February 1, 2014) and repealing the special provisions of *Law no. 161/2003* and *Law no. 365/2002*, and the corresponding articles of the new Criminal Code shall be applicable.

The new Criminal Code, in art. 181 paragraph (1) and (2), took over the legal definitions of the key terms *computer system* and *computer data*, used by the legislator in this chapter, from the European Convention on *computer crime* (Vasiu, 2015; p. 604).

[1] See Decision no. 15/2003 of the High Court of Cassation and Justice, on the judgment of the appeal in the interest of the law that forms the object of File no. 12/2013, published in the Official Monitor no. 760 of December 6, 2013.

To illustrate contextually and the ways of committing *computer crimes*, the following case is eloquently solved by the High Court of Cassation and Justice - Criminal Section[1], having as fields: electronic commerce, *computer crime* - falsification of electronic payment instruments, access without right to a computer system.

In the motivation of the criminal decision no. 4399/2006, it was acknowledged that: "the offenses of the defendant J.C.F. to unlawfully own equipment for the forgery of electronic payment instruments, to forge such instruments and to own and put them into circulation, as well as to unlawfully access the information systems of R.B. at different time intervals, but based on the same criminal resolution, they meet the constituent elements of the crimes provided by art. 24 paragraph (1) and (2) of Law no. 365/2002 with the application of art. 41 paragraph (2) Criminal Code, art. 25 of the same normative deed and of art. 42 paragraph (1) of Law no. 161/2003 with the application of art. 41 paragraph (2) Criminal Code" and that:

"charged to the defendant CI and AT, who helped the other defendant to forge electronic payment instruments and who put them into circulation, at different time intervals, but based on the same criminal resolution, such forged payment instruments, and who helped the other defendant to unlawfully access the information systems of the injured party, the commission of the offenses provided by art. 26 Criminal Code, referred to in art. 24 paragraph (1) and (2) of Law no. 365/2002 with the application of art. 41 paragraph (2) Criminal Code, and of art. 26 Criminal Code, referred to in art. 42 paragraph (1) of *Law no. 161/2003*, with the application of art. 41 paragraph (2) Criminal Code was acknowledged."

From the analysis of data related to computer crime, we can highlight the following trends in the future:

• *Computer crimes are becoming more and more common*. The information society is increasingly dependent on computers. Important components of social life are coordinated by computer systems. As a consequence, the attacks through and on them will multiply;

• *Computer crimes can be virtually committed nowadays by any person and can virtually reach any person.* If the information systems were, upon their emergence, an attribute of the scientific, military and governmental media, nowadays, due to the increase of the performances correlated with the reduction of the prices, they became available to everyone;

• *Computer crimes have an increasingly mobile and international character*. Electronic data processing is increasingly converging with the telecommunications field. Computer crimes are to a greater extent committed through telecommunications networks;

• *Computer crimes and the Internet are especially attractive for organized crime groups*. The anonymity provided by the global computer networks, as well as the methods of encrypting the transmission of messages through them, correlated with the impossibility of the forces to maintain the public order to control the flow of information, have special advantages for organized crime groups, including those with a transnational character (Banciu & Vlăduţ, 2001).

Therefore, "the knowledge of the different laws governing the Internet and the decision of the international community to cover all the voids of this new world and to harmonize them is a very current one". Or, unquestionably, these concerns will have to lead, sooner or later, to an *Internet Law*, to a law with a cross-border and global character, as this fabulous information network itself is, and finally to a *Cyberspace Law*.

[1] Criminal decision no. 4399/2006 issued by the High Court of Cassation and Justice in file no. 1380/46/3006.

References

Amza, T. (1998). *Criminologie/ Criminology.* Bucharest: Lumina Lex Publishing House.

Amza, T.-P. (2003). *Criminalitatea informatică/Cybercrime.* Bucharest: Lumina Lex Publishing House.

Banciu, D. & Vlăduţ, I. (2001). *Internetul şi Criminalitatea Informatică/ Internet and Cybercrime.* Bucharest.

Dobrinoiu, M. (2006). *Infracţiuni în domeniul informatic/ Computer offenses.* Bucharest: C.H. Beck Publishing House.

Nistoreanu, G. & Păun, C. (1996). *Criminologie/ Criminology.* Bucharest: Europa Nova Publishing House.

Vasiu, I. (1998). *Criminalitatea informatică/ Cybercrime.* Bucharest: Nemira Publishing House.

Vasiu, I. (2002). *Informatică juridică şi dreptul informatic/ Legal informatics and computer law*. Cluj-Napoca: Albastră Publishing House.

Vasiu, I. (2006). *Prevenirea criminalităţii informatice/ Prevention of cybercrime.* Bucharest: Hamangiu Publishing House.

Vasiu, I. (2015). *Explicaţiile noului Cod penal, Vol. III/ Explanations of the new Criminal Code, Vol. III*. Bucharest: Universul Juridic.