Present regulations regarding cyberrime within the Romanian and European Union law system

Adriana Iuliana MUSCĂ
Titu Maiorescu University, Bucharest, ROMANIA
psihologie@utm.ro

Abstract:
The number of cybercrimes is increasing and this is due to the fact that more and more people own a computer and internet connection, in order to benefit from real-time information, apply modern ways of work or other various reasons. Such crimes can be practically committed by any person who owns minimum informatics knowledge although it is clear that the level of intelligence of the ones who commit them is above average. Committing such deeds can prejudice a great number of people because, although at the beginning, informatics systems were found in scientific, governmental or military sights, today they are available to the masses as a result of increasing performance and lower costs of such systems. There are several obstacles in from of efficient investigations as far as informatics crimes and prosecution are concerned, on a European level. Among these obstacles we may mention jurisdictional boundaries, insufficient capacities regarding information exchange, technical difficulties regarding locating the origin of the informatics crime authors, lack of personnel qualified for such activity but also the lack of cooperation with other interested parts, responsible for the informatics security.
Within this context, law regulations regarding cybercrime need a uniform modeling within the entire community space.
Keywords: *cybercrime, online crime, informatics system, investigation, act of cybercrime, sanction.*

"This work was supported by the strategic grant POSDRU/159/1.5/S/141699, Project ID 141699, co-financed by the European Social Fund within the Sectorial Operational Program Human Resourses Development 2007-2013"

1. INTRODUCTION: GENERAL PHRAME OF NATIONAL AND INTERNATIONAL CRIMINAL REGULATION REGARDING CYBERCRIME

The evolution of information technology and informatics systems has taken place mostly during the second half of the XXth century and is still in continuous expansion, affecting all domains of social, economic, political and civic life, among other aspects. Informatics decisively impacts the evolution of humanity due to the speed with which the information is moving and the possibility of rapid communication which it provides. It is legitimate to assert that"the informatics revolution – especially conducted via the Internet – is the third (and probably the last) industrial revolution" .

Cybercrime includes, among the classic infractions (such as fraud, prostitution, forgery), other deeds inherent to the cybernetic domain such as falsifying electronic pay

instruments, card steeling, infecting networks, electronic terrorism, harassing, etc. We may therefore say that informatics technology offers diverse and particular possibilities of breaking the law, in any domain which utilizes informatics systems (road, air, navy traffic, national safety, military, education, social, medical and financier services, etc.) .

2. REGULATIONS WHICH SIGHT CYBERCRIME WITHIN THE ROMANIAN LEGAL SYSTEM

As a result of increasing number of cybercrimes registered in Romania as in other countries, legal actions have been approached in order to punish the deeds which are considered infractions specific to the informatics domain (Boroi, Nistoreanu, 2004). Such dispositions are met in the following laws:

2.1. Infractions sighted in Law no. 365/2002, replicated in the year 2006 regarding electronic commerce:

The main acts presented and incriminated by the present law are:

Falsifying electronic pay instruments (par.24)

Within this deed we may find, along the falsification itself, the utilization of the falsified electronic pay instruments. The active subject of the qualified forms of this infraction is the person who, based on work obligations, makes technical operation of emitting falsified pay instruments, has access to identification data of security mechanisms – par. 24, (3), lit. a, b, c.

The ownership of equipment destined for falsification (par.25). The incrimination sights the use and ownership of equipment for the purpose of falsifying both hardware and software.

False declarations regarding emitting or utilizing electronic pay instruments (par.26). Such declarations may be done within a bank institution – of credits or financier, in the presence of their legal representative or in the presence of an authorized law representative in order to emit foreign pay instruments.

Conducting fraudently financier operations (par.27). Such incrimination sights operations conducted through utilizing electronic pay instruments and of identification data without owning the consent of the instrument's legal owner. Other forms of this infraction interfere in the case of utilizing fictional identification data or unauthorized

transmission of identification data, qualified variant sighting the person who commits the infraction in accomplishing service duty (par.27, point 2-3 and 4).

Accepting financial operations illegally conducted (par.28). The section refers to the unauthorized access to an informatics system, the unauthorized transfer of data within an informatics system and modifying, total or partial, unauthorized destruction of information stocked within an informatics system.

2.2. Infractions provided in Law no.161/2003

The law distinguishes three categories of infractions:

2.2.1. Infractions against the confidentiality and integrity of data and systems

- Access without permission to an informatics system with aggravated forms respectively obtaining informatics data and breaking security measures (par. 42, align 2 and 3);
- Intercepting without permission of an informatics data transmission which cannot be published (par. 43);
- Modifying, deleting or damaging informatics data or restraining access to such data, without permission, including unauthorized data transfer from an informatics system (par. 44, align 1-3);
- The deed of gravely perturbing, without permission, the functioning of an informatics system by introducing, transmitting, modifying, deleting or damaging informatics data (par.45);
- The deeds of producing, selling, importing, distributing dispositive or informatics programs, conceived or adapted to committing the infractions from par.42 to 45 refer also to similar deeds which are connected to access codes or passwords (par. 46, align. 1 and 2).

2.2.2. Cybercrime (par. 48-49):

- the deed of introducing, modifying or deleting, without permission, informatics data or restraining, also without permission, the access to such data, resulting to other data inconsistent with the truth (par.48). The law states that: the deed of introducing, modifying or deleting, without permission, or restricting, without permission, the access to such data resulting in data inconsistent with the truth in order to be utilized for

producing a juridical consequence, represents and infraction and is punished through 2 to 7 years of imprisoning.

The regulation sights protecting law security by incriminating all those actions which may, by modifying data found on informatics support, to attack unwanted consequences by/to the persons which conceived, made and implemented or upon those who manifest the effects of modified information.

The specific juridical object is represented by social relationships included in the protection of legal circuit security.

The objective side. The material element is given by the action of: introducing, modifying, deleting or restricting the access of informatics data in order to produce legal effects.

The subjective component is characterized by direct intention.

Sanction. The infraction of informatics false is punished with 2 to 7 years of jail.

2.2.3. Child pornography through informatics system

This type of criminality is frequent and aggressively encountered, especially online.

According to this law, child pornography consists in producing in order to spread, offer or provide, spreading or transmitting, buying for one's self or for others of pornographic materials involving underage persons through informatics systems. Also, the owning without permission of child pornography materials on an informatics system, is punished.

Such an infraction is placed on the line between crimes committed with the help of informatics systems and the ones which sight information systems. The infraction of child pornography is regulated by the Romanian criminal legislation in force.

Child pornography is regulated by two laws, namely:

1. Law 678/2001, regarding preventing and combating human trafficking which at par.18 states that: (1) The deed of exposing, selling or spreading, renting, distributing, making or owning in order to spread objects, movies, photographs, diaphragms, emblems or other visual supports which represent sexual acts or positions with pornographic nature, which present or involve underage persons – namely who have not reached the age of 18 years old, or importing or transmitting such objects to a

shipping or distribution agent in order to be commercialized or distributed represents a child pornography infraction and is punished by jail from 2 to 7 years; (2) the deeds described at par. (1) Committed by a person who is part of an organized group is punished with 3 to 10 years of prison.

2. Law 196/2003, regarding preventing and combating pornography, which within par. 12 states that: (1) distribution of materials of obscene nature which present images with underage persons showing explicit sexual behavior is punished by 1 to 5 years of prison; (2) The same punishment is also applied in the case of owning materials presented within par. (1) With the intent of sharing.

The specific juridical object is constituted by social relationships which follow protecting the underage persons.

Sanction. The infraction of child pornography through informatics systems is punished by 3 to 12 years of prison and suspending of several rights.

Other regulations available in Romania regarding informatics crime:

Normative acts which contain norms which sight this type of crime are:

- Law no. 285/2004 regarding copyright and connected rights.
- Law no. 445/2001 regarding electronic signature.
- Law no. 51/2003 regarding the juridical system of afar contracts.
- Law no. 506/2004 regarding processing data with personal character and protecting the private life within electronic communications, with ulterior modifications.
- Law no. 677/2001 regarding the protection of people regarding processing data with personal character and free circulation of these data.
- Law no. 64/2004 for ratifying the Convention regarding informatics criminality from Budapest, 2001.

3. REGULATIONS REGARDING CYBERCRIME WITHIN THE EUROPEAN UNION

On November 23rd 2001 the Convention of Cybercrime has been signed.

The convention proposes to prevent acts against confidentiality, integrity and availability of informatics systems, networks and data along with illegal use of such systems, networks and data by assuring the incrimination of such conducts and by encouraging the adoption of measures of nature to allow the effective combat of such

infractions, meant to facilitate the discovery, investigation and prosecution both on a national level and international and also by applying material dispositions necessary to assuring a rapid and safe international cooperation.

The convention has been ratified by Romania by Law 64/2004 (in order to ratify the European Council's Convention of Cybercrime, adopted at Budapest on November 23rd, 2001). After the ratifying, in March 2004, by the fifth state, the convention has taken effect on July 4th, 2004.

In the year 2012, the European Commission has sent notice to the European Council and the European Parliament regarding the necessity of instituting a European Center of combating informatics crime. Within this notice, The Commission specified that the value of world commercial exchanges conducted annually through electronic trade reaches approximately 8 trillion dollars and that because the numbers of commercial transactions are made online, the number of informatics crimes also increases.

Such deeds of criminal nature include infractions from „selling stolen credit cards for a modest sum of 1 Euro, identity theft and sexual abuse of children to severe informatics attacks upon institutions and infrastructure".

The European Union informs upon the fact that there are numerous obstacles in the way of effective applying of investigations as far as informatics crime and prosecution are concerned, on a European level, of authorities which sight such infractions. Among these obstacles we may encounter jurisdictional boundaries, insufficient capacities regarding information exchange, technical difficulties regarding locating the origin of authors of informatics crime acts, differences of investigation and legal expertise capacities, lack of the personnel qualified for such activity but also the lack of cooperation with other interested parties, responsible for the informatics security (Paraschiv & Damaschin, 2004).

The commission thus proposed to institute a European Cybercrime Center and proposed that it should mostly focus and the following major aspects of the informatics crime:

1. Acts of informatics crime committed by organized crime groups, mostly acts which generate considerable profit obtained by committing infractions such as on-line fraud.

2. Acts of informatics crime which bring sever prejudice to their victims such as sexual exploit of children via the internet.

3. Acts of informatics crime (including informatics attacks) pointed against the critical infrastructure and informatics systems of the Union.

4. PROPER CRIME INVESTIGATION OF CYBERCRIME

The main issues which need clarification within the investigation of cybercrimes which mostly refer to identifying the hardware or other ways of access which have been used of destined to serve to committing the crime, of the obtained information as a result of an illegal action, of the hardware as a result of the crime, identifying the author and possible accomplices, establishing the conditions which favored committing the crime, the deed's consequences, etc (Paraschiv, 1998, 2001).

The criminalistics investigation includes several steps which we will describe as follows: (1). identifying objects which have been used or destined to serve to committing the crime. No matter if they were used in this purpose or were to be used by the criminal in order to commit the deed, such sample material means represent ways of committing the infraction, being part of the „Corpus delicts". These means are a source of proof and with the help of scientific methods and means may reveal informative elements of maximum importance.

Even so, these do not own a priori value of proof and are to be valorized by being added to other samples; (2). The identification of obtained information as a result of the infraction. The software copies owned by these persons by violating the law of copyright are naturally sequestrated, as can be the case with any other documentation obtained by illegal means.

During the criminal investigation, it must be taken into account that since the very beginning the software producer allows the buyer to create a reserve copy which cannot be commercialized or shared as a result of the law which protects individual property; (3). Identifying the hardware as a result of the crime. The legal procedures authorize the issuance of warrants in order to sequestrate the data, product of such

infractions and other similar materials. According to the American definition, „the infraction result" (Donovan, & Bernier, 2008) includes goods obtained through criminal activity (such as cash obtained by using a falsified credit card), and the „contraband" represents having the property of goods which a citizen cannot possess (for instance, drugs).

The criminal investigation body will examine whether the context has conducted for certain to the illicit consequences, thus the investigator can be sure that the respective object is a result of infraction or has been illegally possessed; (4).

The identification of the author and circumstances which favored committing the crime. It will be established the means in which the author had access to secured information, taking into consideration the possibility of unauthorized use of a computer.

5. CONCLUSIONS

Cybercrime is an increasing challenge for investigators, once time passes and implicitly, as technology evolves. It is known that the number of cybercrimes is increasing continuously because more people possess a computer and internet connection from the wish of being informed in real time, to work modernly or for various other reasons (Vasiu, 1998). Such crimes can be practically committed by any person who possesses minimum knowledge regarding the field of informatics although it is clear that the level of intelligence of the people who commit such crimes is above average (Voicu, Dascălu & Stan, 2002).

Committing such deeds may bring prejudice to a great number of people because, if at the beginning, the informatics systems could have been found in scientific, governmental or military sights, today they have become available to the masses, as a result of increased performance and decreased costs of such systems.

The anonymity secured by worldwide computer networks and also methods of message encryption, together with the reduced possibility of the authorities to control the information flux represent immense advantages for the criminals or for the organized crime groups in committing cybercrimes.

Certainly, such data should lead, at a near point in the future, to building a Law system of the Internet, a system extremely necessary for all users of the discussed international network.

Bibliography:

Boroi, A. & Nistoreanu, G. (2004). Drept penal: partea generală. Ed. All Beck, Bucureşti.
Banciu, D., Vlăduţ, I. (2001). Internetul şi Criminalitatea Informatică, Bucureşti.
Donovan, F., & Bernier, K. (2008). Cyber crime fighters: Tales from the trenches. Pearson Education.
Stancu, E. (2000). Terorism şi Internet, în „Pentru Patrie", nr. 12/2000, pag. 27.
Stancu, E. (2010). Tratat de Criminalistică, Ediţia a V-a, revizuită şi adaugită, Editura "Universul Juridic", Bucureşti.
Damian, V. (2000). Frauda pe Internet are sediul în România. Românii conduc detaşat în topul celor mai ingenioşi hoţi din reţeaua mondială, în „Capital", nr. 38, 21 septembrie 2000.
Paraschiv, C.S.; Damaschin, M. (2004). Drept procesual penal, Editura Lumina Lex, Bucureşti.
Vasiu, I. (1998). Criminalitatea informatică, Editura Nemira, Bucureşti.
Voicu, C., Dascălu, I., Stan, E. (2002). Investigarea infracţiunilor digitale, Editura Argument, Bucureşti.
Paraschiv, T.(1998). Informatica dreptului, Editura Augusta, Timişoara.
Paraschiv, T. (2001). Cibernetica juridică, Editura Augusta, Timişoara.