CYBERCRIME OFFENCES. TRENDS IN OF THE EVOLUTION, FORMS OF MANIFESTATION AND INCRIMINATION OF THIS PHENOMENON

Gheorghe-Iulian Ioniță[1]
Ștefania-Diana Ioniță-Burda[2]

ABSTRACT

This study refers to the evolution and forms of manifestation of cybercrime offences, as well as the efforts of the law giver and organisms of law enforcement to prevent and fight this phenomenon.

Keywords: cybercrime offences, evolution, forms of manifestation, incrimination.

1. CYBERCRIME OFFENCES

Before any further analysis and for the accurate understanding of the issue it is necessary to delineate cybercrime offences.

Starting from the typology stipulated in the Council of Europe Convention on Cybercrime (Cybercrime Convention)[i] and in the completion thereof, depending on the phenomenon manifestations, *the offences included in the field of cybercrime* can be grouped into[ii]:

A. Offences against the confidentiality, integrity and availability of computer data and systems: illegal access; illegal interception; data interference; system interference.
B. Computer-related offences: computer-related forgery; computer-related fraud; identity theft; misuse of devices.
C. Offences related to content: interaction with the erotic and pornographic material (in the countries where this is incriminated as an offence); child pornography; violent, racist or xenophobic acts; acts referring to religious convictions; illegal gambling and online games; attacks with unrequested messages of the "spam" type; providing information on crimes.
D. Offences related to infringements of copyright and related rights: infringements copyright and related rights; infringements industrial property rights.
E. Complex Offences: cyber terrorism; cyber war; money laundering through computer systems; attacks of the "phishing" type.

2. RENDS IN THE EVOLUTION AND FORMS OF MANIFESTATION OF

[1] PhD., Lecturer of Criminal Law at the Romanian American University in Bucharest. E-mail: ionita.gheorghe.iulian@profesor.rau.ro
[2] PhD., Asistant Professor of Labor Law at the Romanian American University in Bucharest. E-mail: ionitaburda.stefania.diana@profesor.rau.ro

CYBERCRIME OFFENCES

According to Directorate for Investigating Organized Crime and Terrorism (DIOCT)[iii], last year (2011), Romania registered an increasing trend of crimes against computer systems/data or crimes committed with the help of information technology.

Statistically, in 2011, 873 cases were solved (rising by 62.87 % as compared to last year when 536 cases were solved); from among these, 133 cases were completed through court reference (as compared to 103 cases in 2010, representing a 29.13 % rise); 333 defendants were sent to court, out of which 105 in detention under remand (a 22.42 % increase as compared to last year when 272 defendants were indictment, out of which 148 were kept in detention under remand).

From among the increasing forms of cybercrime manifestation, the following were emphasized:

- corrupting access accounts belonging to users of e-trade sites, financial institutions or social networks
- unauthorized accessing of information systems followed by blackmailing or fraudulent use of confidential data obtained (data of electronic payment instruments)
- credit card frauds (ATM corruption, capturing information from the magnetic strips of credit cards, forging electronic payment instruments).

There is an increasing technical micro-specialization of defendants and their gathering in independent cells meant to carry out the specific criminal activity, namely fragmenting general criminal activity into activities at the limit of preparatory acts, in some cases unsanctioned by the law.

The following acts were noted[iv]:

- using “specialists” in plastics, molds, electronics and even workshops with mainly legal activities to execute some of the component items necessary to produce “skimming” devices;
- automating means to commit classic cybercrimes (tenders) to optimize profits by using computer programs and fraud schemes (phishing activities, infestation with various forms of malware in order to obtain data);
- using cells (made of 2 or 3 persons) specialized in the identification of goods, the download of fraudulent notices, corrupting accounts of legitimate users or communicating with the victims, whereas others are specialized in the intermediation, reception, withdrawal of the financial benefit (most of the times from the territory of other states);
- the inefficiency of criminal prosecution due to failure to identify component cells or to relate them to the criminal activity;

In the year 2011, there was also a trend which has been noted for the last years referring to the migration of persons from organized crime towards cybercrime, mainly in the area of fraudulent operations with electronic payment instruments.

The following can be mentioned from among important cases solved by DIOCT last year[v]:

A. Prosecutors of DIOCT - Central Structure ordered the indictment of defendants A.A.A. (34 years old), A.E.L. (30 years old) and N.C.A. (20 years old), for crimes related to the creation of an organized criminal group, illegal accessing of an information system, unauthorized data transfer from an information system, serious illegal perturbation of a computer system, information fraud and blackmailing.

In fact, it was noted that the defendants created an organized criminal group with the aim to obtain a considerable amount by corrupting the computer system belonging to a medical clinic in Bucharest, followed by threats to publish confidential data on the patients.

To this end, A.A.A. illegally accessed the e-mail addresses used by persons from the clinic management, as well as the clinic information system and copied the databases of the information application which manages marital status data, medical treatments and other confidential data on patients.

Subsequently, through the electronic mail, A.A.A. contacted the representatives of the clinic and claimed EURO 300,000 threatening that, if his request is not satisfied, he would publish on the Internet the patients' confidential data, a situation likely to seriously affect the activity of the clinic.

The case was submitted for settlement to the Court of Bucharest.

B. Prosecutors of DIOCT - Central Structure ordered the indictment of defendants D.P.A. (29 years old), O.O. (33 years old), N.A. (30 years old) and G.V. (22 years old), for crimes related to the creation of an organized criminal group, cybercrime offences, false of identity, and traffic of high risk drugs.

In fact, it was noted that the defendants D.P.A. and O.O. created an organized criminal group, to which other persons also adhered in order to obtain substantial financial benefits from fraud through acts of electronic trade, through the fraudulent use of www.eBay.com signs.

Prosecutors identified approximately 200 damaged parties which delivered the goods to the addresses communicated by defendants, without receiving the set price.

The damage caused by the criminal activity is approximately USD 1 million.

Upon the search carried out at the house of D.P.A., 500 grams of cannabis were discovered, drugs that came from Holland and were meant to be sold in Bucharest and the surroundings.

The case was submitted for settlement to the Court of Bucharest.

C. Prosecutors of DIOCT - Territorial Service of Bucharest ordered the indictment of 30 defendants (aged 19 to 42 years), following the destruction of an organized criminal group, specialized in cybercrime.

In fact, it was noted that the defendants Z.C. and C.C. created an organized criminal group, to which other 40 persons also adhered, in order to perform cybercrime, through attacks on information systems and the fraudulent use of information data, obtaining thus substantial material benefits.

The defendants illegally accessed computer systems belonging to the providers of phone services via the Internet in countries such as Romania, Russia, China, Australia, Peru, through the use of a scanner program in order to obtain data (user and password for the Voip account) and made calls from the VoIP accounts to surcharge numbers in countries such as Austria, Zimbabwe, Bulgaria, Somalia.

In calling surcharge numbers, the group members obtained bonuses depending on the number of minutes and amount of the call per minute (for instance, at a fee of EUR 1/minute, the benefit was EUR 0.10).

The damage caused by the criminal activity is approximately USD 11 millions.

The case was submitted for settlement to the Court of Bucharest.

D. Prosecutors of DIOCT - Territorial Service of Oradea ordered the indictment of 19 defendants, of which 8 legal entities, following the destruction of an organized criminal group with the aim to commit offences related to e-commerce, tax evasion and money laundering.

In fact, it was noted that the defendant C.I.I. (35 years old), as leader of the organized criminal group, together with other persons, forged electronic payment instruments issued by foreign banking institutions (especially AMERICAN EXPRESS) and made fraudulent financial operations by using false cards.

The damage caused by the criminal activity is approximately USD 850.000.

In order to recover this damage, an attachment was decided on several amounts of money, buildings and cars belonging to the defendants.

In processing this case, prosecutors collaborated with national representatives of AMERICAN EXPRESS.

The case was submitted for settlement to the Court of Bihar.

E. Prosecutors of DIOCT - Territorial Service of Cluj ordered to retain the defendant for 24 hours for crimes of illegal accessing of a computer system, breaching security measures,

serious disturbance of a computer system by entering, modifying and corrupting information data and by restricting access to such data and illegal possession of a computer system in order to commit the crimes stipulated at articles 42 paragraphs 1 and 3, article 45 and 46 paragraph 2 of Law no. 161/2003.

It was discovered that, on 12.12.2010, the defendant illegally accessed, through breach of the security means, several NSA servers, thus seriously affecting the server operation by entering, modifying and damaging information data and restricting access to such data.

The damage caused by the criminal activity is approximately USD 500.000.

The case was submitted for settlement to the Court of Cluj.

3. TRENDS IN THE INCRIMINATION OF CYBERCRIME OFFENCES

The (still) valid regulation on the prevention and fight of cybercrime is Law no. 161/2003[vi] (Title III).

The new Penal Code (Penal Code 2009)[vii] takes over, more or less faithfully, the incrimination provisions in the above-mentioned regulation[viii].

It is also worth mentioning that, at present, Law no. 187/2012[ix] was adopted which (except for Article 121 point 8 and Article 249) shall enter into force on 01.02.2014 (the same date when the new Penal Code enters into force).

According to article 130 point 1-4 of Law no. 187/2012, Law no. 161/2003, chapter III of title III *"Preventing and fighting cybercrime"* of book I, section 1 *"Offences against the confidentiality and integrity of data and computer systems"*, containing articles 42-47, section 2 *"Cybercrimes*, containing articles 48-50, section 3 *"Child pornography through computer systems"*, containing article 51 are abrogated; article 59 of chapter IV *"Procedural provisions"* of the same title is also abrogated.

In other words, the provisions of material and procedural law stipulated in the regulation on the prevention and fight of cybercrime shall be abrogated, and the incrimination provisions of the new Penal Code shall apply.

The above-mentioned regulation (Law no. 187/2012, article 54) also modified the incrimination provision of Law 8/1996 on copyright and related rights[x].

Under these circumstances, we hereby mention these provisions:

A. Illegal access

According to Article 42 of the Law no. 161/2003,

(1) The access without right to a computer system is a criminal offence (is punished with imprisonment from 6 months to 3 years or a fine).

(2) Where the act provided in paragraph (1) is committed with the intent of obtaining computer data the punishment (is imprisonment for 6 months to 5 years).

(3) Where the act provided in paragraph (1) or (2) is performed by infringing the security measures (the punishment is imprisonment from 3 to 12 years).

According to Article 360 of the new Penal Code, is considered a criminal offence of **illegal access to a computer system**,

(1) Access, without right, to a computer system (is punished with imprisonment from 3 months to 3 years or with fine).

(2) The fact mentioned at item (1), committed for the purpose of obtaining computer data (is punished with imprisonment from 6 months to 5 years).

(3) If the fact mentioned at item (1) was committed on a computer system that, through certain procedures, devices or programs, the access is restricted or prohibited for certain categories of users, the punishment is imprisonment from 2 to 7 years).

B. Illegal interception

According to Article 43 of the Law no. 161/2003,

(1) The interception without right of an transmission of computer data which is not public and which is meant for a computer system, emanates from such a system or is executed on a computer system is a criminal offence (and is punished with imprisonment from 2 to 7 years).

(2) (The same punishment shell sanction) the interception, without right, of electromagnetic emission from a computer system, which contains electronic data that are not public.

According to Article 361 of the new Penal Code, is considered a criminal offence of **illegal interception of a transmission of computer data**,

(1) The interception, without right, of any transmission of computer data which is not public and is meant to a computer system, comes from such a system or is performed in a computer system (is punished from one to 5 years).

(2) The interception, without right, of any electromagnetic emission from a computer system, which contains non-public data (is sanctioned with similar punishment).

C. Data interference

According to Article 44 of the Law no. 161/2003,

(1) The act of altering, deleting or damaging computer data or restricting access to such data, without right is a criminal offence (and is punished with imprisonment from 2 to 7 years).

(2) The unauthorized transfer of data from a computer system (is punished with imprisonment from 3 to 12 years).

(3) (The penalty under paragraph 2 shall sanction) the unauthorized transfer of data from the computer data storage medium.

According to Article 362 of the new Penal Code, is considered a criminal offence of ***alteration of computer data integrity***, the illegal alteration, deletion or deterioration of computer data of the access restriction to such data (is punished with imprisonment from one to 5 years).

According to Article 364 of the new Penal Code, is considered a criminal offence of ***unauthorized computer data transfer***, the unauthorized data transfer from a computer system or from any means of an information data storing (is punish with imprisonment from one to 5 years).

D. System interference

According to Article 45 of the Law no. 161/2003, the act of seriously affecting, without right, of a computer system operation, by the introducing, transmitting, altering, deleting or deteriorating computer data or by restricting the access to computer data is a criminal offence (and is punished with imprisonment from 3 to 15 years).

According to Article 363 of the new Penal Code, is considered a criminal offence of ***hindering of functioning system***, the serious hindering, without right, of a computer system operation, by the introducing, transmitting, altering, deleting or deteriorating computer data or by restricting the access to these data (is punished with imprisonment from 2 to 7 years).

E. Misuse of devices

According to Article 46 of the Law no. 161/2003,

(1) It is criminal offences (and shall be punished with imprisonment from 1 to 6 years):

a) the act of producing, selling, importing, distributing or making available, in any other form, without right, of a device or a computer program designed or adapted from the purpose of committing any of the offences established in accordance with Articles 42-45;

b) the act of producing, selling, importing, distributing or making available, in any other form, without right, of a password, access code or other such computer data allowing total or partial access to a computer system for the purpose of committing any of the offences established in accordance with Articles 42-45;

(2) (The same penalty shall sanction) the possession, without right, of a device, computer program, password, access code or computer data referred to at paragraph (1) for the purpose of committing any of the offences established in accordance with Articles 42-45.

According to Article 365 of the new Penal Code, is considered a criminal offence of illegal operations with devices or computer programs,

(1) Act of production, sale, import, distribution or making available, in any other form, without right, of:

a) device or a computer program designed or adapted for the purpose of committing one of the offences established in accordance with articles 360-364;

b) password, access codes or other such computer data allowing total or partial access to a computer system for the purpose of one of the offences established in accordance with articles 360-364,

(is punished with imprisonment from 6 months to 3 years or with fine).

(2) The possession, without right, of a device, computer program, password, access code or computer data referred to at paragraph (1) for the purpose of one of the offences established in accordance with articles 360-364 (is punished with imprisonment from 3 months to 2 years or with fine).

F. Computer-related forgery

According to Article 48 of the Law no. 161/2003, the act of inputting, modifying or deleting, without right, computer data or of restricting, without right, the access to such data, resulting data which are incompliant with reality, with the intent to be used for legal purpose, is a criminal offence (and shall be punished with imprisonment for 2 to 7 years).

According to Article 325 of the new Penal Code, is considered a criminal offence of ***computer forgery***, the act of inputting, modifying or deleting, without right, of computer data or the restriction, without right, of the access to these data, resulting in inauthentic data, with the intent to be used for legal purposes (is punished with imprisonment from one to 5 years).

G. Computer-related fraud

According to Article 35 of the Law no. 161/2003, the act of causing a loss of property to another person by inputting, altering or deleting of computer data, by restricting the access to such data or by any interference with the functioning of a computer system with the intent of procuring an economic benefit for oneself or for another (shall be punished with imprisonment from 3 to 12 years).

According to Article 249 of the new Penal Code, is considered a criminal offence of ***computer fraud***, the input, alteration or deletion of computer data, access restriction to these data or prevent in any way the operation of a computer system, in order to obtain a economic benefit for himself or for other, if caused a damage to a person (is punished with imprisonment from 2 to 7 years).

H. Child pornography

According to Article 35 of the Law no. 161/2003,

(1) It is a criminal offence (and shall be punished with imprisonment from 3 to 12 years and denial of certain rights) the production for the purpose of distribution, offering or making available, distributing or transmitting, procuring for oneself or another of child pornography material through a computer system, or possession, without right, child pornography material in a computer or computer data storage medium.

(2) The attempt shall be punished.

According to Article 374 of the new Penal Code, is considered a criminal offence of child pornography,

(1) Producing, possession for the purpose of exposing or distributing, procuring, storage, exposure, promotion, distribution and making available, in any way of child pornography materials (is punished with imprisonment from one to 5 years).

(2) If the facts set up in paragraph (1) have been made through a computer system or other data mean storage (the punishment is imprisonment from 2 to 7 years).

(3) Accessing child pornography materials, without right, through computer systems or other means of electronic communications (is punished with imprisonment from 3 months to 3 years or with fine).

(4) By child pornography materials we mean any material which presents a child with a explicit sexual behavior or which, although is not representing a real person, is simulating, in a credible way, a child with such a behavior.

(5) Attempt is punished.

I. Infringements of copyright and related rights

According to Article 139[6] of the Law no. 8/1996,

(1) The following acts are criminal offence (and are punished with imprisonment for 2 to 5 years or with a fine):

a) producing pirate goods for distribution purposes, without directly or indirectly pursuing a material advantage, by any means and in any manner;

b) placing pirate goods under a final customs regime of import or export, under a suspensive customs regime or in free areas;

c) any other means to introduce pirate goods on the domestic market.

(2) The distribution, possession or storage or transport of pirate goods for distribution purposes, as well as their possession for the purpose of being used through public communication at the working points of legal entities are crimes (and are punished with imprisonment for 1 to 5 years or a fine).

(3) If the acts stipulated in paragraphs (1) and (2) are committed for commercial purposes (they are punished with imprisonment for 3 to 12 years).

(4) The rental or offering for rental of pirate goods (is also punished as stipulated in paragraph 3).

(5) Promoting pirate goods by any means and in any manner, including by using public ads or electronic communication means or by display or presentation of product lists or catalogues to the public are crimes (and are punished with imprisonment for 6 months to 3 years of with a fine).

(6) If any of the facts stipulated in paragraphs (1)-(4) has particularly serious consequences (they are punished with imprisonment for 5 to 15 years). In order to assess the seriousness of the consequences, the material damages are calculated considering the pirate goods identified under the conditions stipulated in paragraphs (1)-(4) and the unit price of original products, cumulated with the amounts that have been illegally cashed by the offender.

(7) The acts stipulated in paragraphs (1)-(5) committed by an organized crime group (are punished as stipulated in paragraph 6).

(8) In the meaning of this law, pirate goods means: all copies, regardless of media, including covers, produced without the consent of the rights owner or of the person duly authorized by him/her and which are executed, directly or indirectly, in full or in part, after a product which bears copyright or related rights or after the packages or covers thereof.

(9) In the meaning of this law, commercial purpose means the aim to obtain, directly or indirectly, an economic or material advantage.

(10) The commercial purpose is presumed if the pirate goods are identified at the headquarters, working points, in their surroundings or in the transportation means used by the economic operators who have as their object of activity the reproduction, distribution, rental, storage or transport of products bearing copyright or related rights.

According to Article 139[8] of the Law no. 8/1996, it is a criminal offence (and shall be punished with imprisonment for 1 to 4 years or with a fine) the act of making available to the public, including through the Internet or other computer networks, without the consent of the rights owner of the copyright of protected works, or products bearing related rights or sui-generis rights of database manufacturers or copies of such protected work, regardless of the form of storage thereof, so that the public may access them in any place or at any moment chosen individually.

According to Article 139[9] of the Law no. 8/1996, it is a criminal offence (and shall be punished with imprisonment for 1 to 4 years or with a fine) the unauthorized reproduction of computer software on calculation systems under any of the following ways: installation, storage, running or execution, display or transmission in the internal network.

According to Article 140 of the Romanian Law no. 8/1996,

(1) The following acts committed without the authorization or consent of the owner of rights acknowledged by this law are crimes (and are punished with imprisonment for 1 month to 2 years or with a fine):

a) the reproduction of works or products bearing related rights;
b) the distribution, rental or import on the domestic market of works or products bearing related rights, other than pirate goods;
c) the public communication of works or products bearing related rights;
d) the broadcasting of works or products bearing related rights;
e) the re-transmission by cable of works or products bearing related rights;
f) the execution of derivative works;
g) the fixing of artistic interpretations or performances or of radio or television broadcasts for commercial purposes;
h) the breach of the provisions of Article 134.

(2) Products bearing related rights means fixed artistic interpretations or performances, phonograms, videograms or the own shows or program services of radio and television bodies.

According to Article 143 of the Law no. 8/1996,

(1) It is a crime (and is punished with imprisonment for 6 months to 3 years or with a fine) the act of the person who, without right, produces, imports, distributes or rents, offers by any means, for sale or rental, or who holds, for selling purposes, devices or components which allow the neutralization of technical protection measures or who provides services leading to the neutralization of technical protection measures or who neutralizes such technical protection measures, including in the digital environment.

(2) It is a crime (and is punished with imprisonment for 6 months to 3 years or with a fine) the act of the person who, without having the consent of the rights owners and knowing that this way s/he allows, facilitates, causes or hides a breach of any right stipulated in this law:

a) removes for commercial purposes from works or other protected products or modifies on these any electronic information applying to the regime of copyright or related rights;

b) distributes, imports for distribution purposes, broadcasts or communicates publicly or makes available to the public, so as to be accessed, in any place and at any moment chosen individually, illegally and by means of digital technology, works or other protected products for which the existing electronic information on the regime of copyright or related rights has been removed or modified without any authorization.

4. CONCLUSIONS

Cybercrime registers an alarming incidence and a diversification of methods, although efforts are being made both by the law giver and by organisms for the application of the law on the prevention and fight of this phenomenon.

During these last years, a new trend has been noted related to the migration of persons from organized crimes towards cybercrime.

Under the circumstances, it is not a surprise to discover the technical micro-specialization and grouping of defendants in independent cells, which makes their detection and punishment all the more difficult.

---

i European Council Convention on Cybercrime (CETS no: 185), adopted in Budapest on November 23, 2001.
ii Ioniță G.-I., Infracțiunile din sfera criminalității informatice: incriminare, investigare, prevenire și combatere, Ed. Universul Juridic, București, 2011, p. 49-51; Ioniță G.-I., Ioniță Gheorghe-Iulian, Criminalitatea informatică şi investigarea criminalistică digitală - controverse terminologice şi de conţinut, în Revista „Criminalistica", iunie 2010, vol. XI, nr. 3, Editura Asociaţiei Criminaliştilor din România, Bucureşti, 2010, p. 395-398.
iii Directorate for Investigating Organized Crime and Terrorism, Activity Report 2011, p. 40-46, available at http://www.diicot.ro/images/documents/rapoarte_activitate/raport2011.pdf.
iv idem.
v idem p. 46-51.
vi Law no. 161/2003 published in the Official Gazette no. 279/21.04.2003.
vii Law no. 286/2009 published in the Official Gazette no. 510/25.07.2009.
viii for a detailed analysis, see Ioniță G.-I., Infracțiunile din sfera criminalității informatice: incriminare, investigare, prevenire și combatere, op. cit., p. 193-215; Ioniță G.-I., O scurtă analiză a infracţiunilor din sfera criminalităţii informatice incriminate în Legea nr. 161/2003 şi în noul Cod penal al României, în Revista „Criminalistica", aprilie 2011, vol. XI, nr. 2, Editura Asociaţiei Criminaliştilor din România, Bucureşti, 2011, p. 673-681.
ix Law no. 187/2012 published in the Official Gazette no. 757/12.11.2012.
x Law no. 8/1996 published in the Official Gazette no. 60/26.03.1996.