RSP • No. 45 • 2015: 186-199

ORIGINAL PAPER

Modernization of Romanian Legislation on Preventing and Combating Cybercrime and Implementation Gap at European level

Adrian Cristian Moise*

Abstract
This study presents an analysis of the Romanian legislation on preventing and combating cybercrime within the context of harmonisation of law at European level. Before analysing the offences committed in cyberspace, it has been highlighted that the Romanian legislation has adapted to the provisions of cybercrime at the level of the European Union firstly under the aspect of the used terminology. Romanian legislation on cybercrime is included in the Criminal Code, as well as in Law no.161/2003 on some measures to ensure transparency to exercise public dignities, public office and business environment, prevention and to sanction corruption, specifically in Title III Preventing and combating cybercrime. The main purpose of this study is to establish whetther the Romanian legislation on cybercrime adapted to the provisions of the most important legal instruments at the level of the European Union, such as the Council of Europe Convention on cybercrime, Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and the Council Framework Decision 2001/413/JAI of 28 May 2001 regarding combating fraud and counterfeiting of non-cash means of payment.

***Keywords*:** cybercrime, Criminal Code, information system, computer data, cyberspace.

* Postdoctoral Researcher, Titu Maiorescu University of Bucharest, Faculty of Law, Phone: 0040722524040, E-mail: adriancristian.moise@gmail.com.

Introduction

Romanian legislation on cybercrime is provided in the Criminal Code as well as in Law no. 161/2003 on certain measures to ensure transparency to exercise public dignities, public office and in the business environment, and to prevent and punish corruption, specifically in Title III Preventing and combating cybercrime.

Before analysing the offences committed in cyberspace, it must be highlighted that the Romanian legislation has adapted to the provisions of cybercrime at the level of the European Union firstly under the aspect of the used terminology (Simion, 2010: 1-3). Thus, at Article 181 of the Criminal Code are defined the notions of *information system* and *computer data*. Information system means "any device or set of devices interconnected or in functional relation, of which one or more ensure the automatic processing of data, with the help of an information program". Computer data means „any representation of acts, information or concepts in a form which may be processed through an information system". At the same time, according to Article 35 (1) (d) of Law no. 161/2003, in this category is also included any computer program which can determine the achieving a function by an information system.

Other important definitions are provided by Law no.161/2003 in Title III Preventing and combating cybercrime, Chapter I General provisions, Article 35. Therefore, in Article 35(1) are defined the following terms: *data related to information traffic* means "any computer data related to a communication carried out through an information system and produced by it, which is a part of the communication chain, indicating the origin, the destination, the route, the hour, the date, the size, the volume and the duration of communication, as well as the type of the service used for communication"; *the service provider* means "any natural or legal person providing the users the possibility to communicate through information systems; or any other natural or legal person processing or storing computer data for the persons mentioned above and for the users of the services provided by them".

Moreover, according to the provisions of Article 35 (1) (h) of Law no. 161/2003, by *security measures* it is understood the "use of some specialized procedures, devices or computer programs, with the help of which the access to an information system is restricted or forbidden for some categories of users". For example: access system (LOGIN) based on password and username, infrastructure to encrypt communications, of type PKI-Public Key Infrastructure, with public or private keys, digital signature applications, access equipments through Smart Card, reader/interpreter of fingerprints or retina (Hotca and Dobrinoiu, 2008: 575).

According to Article 35 (1) (i) of Law no.161/2003, by *pornographic material with minors* it is understood "any material depicting a minor having a sexually explicit conduct or an adult who is presented as a minor having a sexually explicit conduct or images which, although do not present a real person, simulate, in a credible manner, a minor having a sexually explicit conduct".

At the same time, for the purpose of this text of Law no.161/2003, pursuant to the provisions of Article 35 (2) it acts, without right, the person who is in one of the following situations: "is not authorized, under the law or a contract; exceeds the limits of authorization; does not have the permission, from the competent natural or legal person, under the law, to give, to use, to administer or to control an information system or to carry out scientific researches or to carry out any other operation in an information system".

Therefore, we noticed that it has been fully transposed the definition of the notion *without right* in Article 2(d) of Directive 2013/40/EU on attacks against information systems (Directive 2013/40/EU/ of the European Parliament and of the Council of 12 august 2013 on attacks against information systems, which was published in the Official Journal of the European Union, 14.08.2013, L218/8) in Article 35 (2) of Law no. 161/2003.

Analysis of the legislation on cybercrime in Romania

Offences committed in cyberspace are stipulated in the Special Part of the Criminal Code as it follows: in Chapter IV of Title II *Offences against the patrimony* were included the *frauds committed through information systems and electronic means of payment* (Articles 249-252) specifying that the "input, alteration or deletion of computer data, restriction of access to such data or any interference with the functioning of a computer system, with the purpose of procuring an economic benefit for oneself or for another person, if loss has been caused to a person, shall be punishable with imprisonment from 2 to 7 years" (Article 249 - Computer-related fraud).

Romanian legislator criminalised in Article 249 of the Criminal Code the offence of computer-related fraud as being the act of causing a patrimonial prejudice to a person by input, alteration or deletion of computer data, by restricting the access to computer data or by any interference with the functioning of a computer system, in order to obtain an economic benefit for oneself or for another person (Schjolberg and Ghernaouti-Helie, 2011: 5). With the development of information and communication technology, also increased the opportunities to commit offences against the patrimony. Therefore, the purpose of this Article is to criminalise any act of manipulation without right in processing data with the intent to operate an illegal transfer of property (Dobrinoiu et al., 2014: 313).

We notice the fact that the text of the offence of computer-related fraud comprised in Article 249 of the Criminal Code was adapted to the provisions of Article 8 (computer-related fraud) of the Convention of the European Council on cybercrime (Convention of the European Council on cybercrime). According to Article 250, *Carrying out of financial operations fraudulently*, carrying out of operations of cash withdrawal, uploading and downloading of an instrument of digital currency or transfer of funds, by use, without the consent of the holder, of an electronic payment instrument or the identification data which allows its use, shall be punishable by imprisonment from 2 to 7 years. paragraph (2) specifies that with the same punishment is sanctioned the carrying out of one of the operations stipulated at paragraph (1), by unauthorized use of any of the identification data or by use of fictional identification data. Moreover, according to paragraph (3), unauthorized transmission to other person of any identification data, with a view to carrying out one of the operations stipulated at paragraph (1), shall be punishable by imprisonment from one to 5 years.

The offence of carrying out financial operations fraudulently is part of the category of offences against patrimony which is based on fraud. This type of offence consists in the use of an electronic payment instrument, including also the identification data which allows its use with a view to carrying out the transfer of funds, other than those ordered and executed by financial institutions, cash withdrawals, as well as uploading and downloading of digital currency instrument (Sauca, 2005: 48). This act creates a state of danger for the trust which has to be given for the possession and use of electronic payment instruments.

In Article 180 of Criminal Code is defined the electronic payment instrument, as "an instrument which allows the holder to carry out cash withdrawals, uploading and

downloading of a digital currency instrument, as well as transfers of funds, other than those ordered and executed by financial institutions". Taking into consideration this definition, we have to notice that the notion of *digital currency instrument* is not defined anymore in the current criminal legislation, and the new definition of the *electronic payment instrument* is more comprehensive, covering also the notions of *payment instrument with access at distance,* as well as *instrument of digital currency* which were comprised in the old criminal legislation, specifically in Law no. 365/2002 on electronic commerce.

The offence of carrying out financial operations fraudulently, referred to in Article 250 of the Criminal Code transposed the provisions of Article 2 letter (d) (offences related to payments instruments) of the Council Framework Decision 2001/413/JAI of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment (Council Framework Decision 2001/413/JHA was published in the Official Journal of the European Communities, 02.06.2011, L149/1).

Under the provisions, of Article 251, *Acceptance of financial operations carried out fraudulently*, *paragraph* (1), the acceptance of an operation of cash withdrawal, uploading and downloading of a digital currency instrument or transfer of funds, knowing that is carried out by using a digital payment instrument or is used without the consent of holder, shall be punishable by imprisonment from one to 5 years. paragraph (2) argues that by the same punishment is sanctioned the acceptance of one of the operations stipulated at paragraph (1), knowing that is carried out by the unauthorized use of any of the identification data or by use of fictional identification data.

Like the offence of carrying out financial operations fraudulently, the offence of acceptance of financial operations carried out fraudulently is meant to protect the integrity and security of electronic payments means (Trancă and Trancă, 2014: 30). This offence is correlative to the offence of carrying out financial operations fraudulently, so that operations carried out under the conditions of Article 250 of the Criminal Code are within the offence stipulated at Article 251 of Criminal Code accepted by the beneficiaries of payments made in this way or by institutions - issuers of electronic payment instruments (Dobrinoiu and Neagu, 2011: 278). Romanian legislator intended, by criminalisation of this act, to discourage traders willing to accept to make fraudulent payments, therefore contributing to the decrease of the phenomenon of counterfeiting of electronic payment instruments.

At the end of Chapter IV *Frauds committed through information systems and electronic payment means*, we noticed the fact that in Article 252 of Criminal Code, the Romanian legislator opted for the criminalisation of the attempt at all the offences in this chapter.

The offence of acceptance of financial operations carried out fraudulently, stipulated at Article 251 of Criminal Code transposed the provisions of Article 2 letter (d) (offences related to payment instruments) of the Council Framework Decision 2001/413/JAI of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment.

In Chapter I of Title VI *Fraud offences* are included the following offences: Article 311 *Forgery of debt securities or payment instruments* stipulating that: forgery of debt securities, titles or instruments to make payments or any other titles or similar values shall be punishable by imprisonment from de 2 to 7 years and the interdiction to exercise some rights (paragraph 1). Moreover, paragraph (2) and (3) consider that should the offence stipulated at paragraph (1) concerns an electronic payment instrument, the

punishment is by imprisonment from 3 to 10 years and the interdiction to exercise some rights and he attempt is punishable.

The provisions of Article 311 (2) of the Criminal Code criminalises an aggravating variant of forgery of debt securities or payment instruments, specifically when forgery targets an electronic payment instrument. In the literature (Trancă and Trancă, 2014: 33) it was considered that the offence of forgery of electronic payment instruments represents a means-offence, intended, finally, to commit the act of carrying out financial operations fraudulently. Considering the minimum and maximum limits of punishment of the offence of forgery of electronic payment instruments as well as of the object-offence, stipulated by Article 250 of Criminal Code, we think that the Romanian legislator considered more serious the offence stipulated at Article 311(2) of the Criminal Code (Truichici, 2008: 8). We also have to notice the fact that the provisions of Article 2 letter (a) (offences related to payment instruments) of the Council Framework Decision 2001/413/JAI of 28 May 2001 combating fraud and counterfeiting of payment means were transposed in the text of Article 311 (2) of Criminal Code. According to *Article 313. Putting into circulation of falsified values, paragraph (1), (2) and (3),* putting into circulation of falsified values stipulated at Article310-312, as well as the receipt, possession or transmission, in order to put them into circulation, is sanctioned with the punishment stipulated by law for the offence of falsification through which they were produced; putting into circulation of falsified values stipulated at Articles 310-312, committed by an author or participant in the offence of falsification, is sanctioned with the punishment stipulated by law for the offence of falsification through which were produced; putting back into circulation of one of the values stipulated at Articles 310-312, by a person who found out, subsequent to the entry into its possession, that is falsified, is sanctioned with the punishment stipulated by law for the offence of falsification through which were produced, of which special limits are reduced to half and the attempt is punishable".

Romanian legislator created for the offence of putting into circulation of falsified values, a distinct incriminatory text and stipulated that also the perpetrator of the offence of falsification may be active subject of this act, but not of the act of possessing in order to put into circulation or of other modalities introduced in the text. The act of putting into circulation of falsified electronic payment instruments represents the correlative criminalisation of the act of falsifying these categories of values. Pursuant to Article 313 (1) of the Criminal Code, it constitutes offence of putting into circulation of falsified electronic payment instruments only in the case when the material object of the offence of putting into circulation is constituted by the falsified electronic payment instruments.

Therefore, the Romanian legislator criminalised all the possible modalities of committing this offence, including the act of putting back into circulation of electronic payment instruments by a person who found out the false character of electronic payment instruments exactly following its entry into possession.

Finally, we noticed that the provisions of Article313 of Criminal Code were adapted to the provisions of Article 2 letters (c) and (d) (offences related to payment instruments) of the Council Framework Decision 2001/413/JAI of 28 May 2001 combating fraud and counterfeiting of non-cash payment means. Article 314, paragraph (1)-(3) entitled *Possession of instruments in order to falsify values appreciated that: m*aking, receiving, possession or transmission of instruments or materials in order to serve for falsifying values or titles stipulated at Article 310, Article 311 (1) and Article 312 shall be punishable by imprisonment from one to 5 years; making, receiving, possession or transmission of equipments, including hardware or software, in order to serve for

falsifying electronic payment instruments shall be punishable by imprisonment from 2 to 7 years. Moreover, according to paragraph (3), it is not punished the person that, after committing one of the acts stipulated at paragraph (1) or paragraph (2), before discovering them and before preceding to the commitment of the act of falsification, gives the instruments or the materials held to judiciary authorities or informs these authorities about their existence".

The offence to possess instruments in order to falsify electronic payment instruments is regulated as a distinct offence in Article 314 of Criminal Code. Moreover, the offence to possess instruments in order to falsify electronic payment instruments represents a means-offence intended, in the end, to commit the act of falsifying electronic payment instruments. Besides the act of possession, in Article 314 (2) of Criminal Code are also criminalised the actions of making, receiving and transmitting equipments, including hardware and software, in order to falsify electronic payment instruments.

However, in Article 314 (3) of Criminal Code is stipulated a non-punishment clause, incident when the perpetrator gives these instruments to authorities or informs the authorities of their existence, before committing the act of falsification.

The provisions of the offence of possession of instruments in order to falsify electronic payment instruments comprised in Article 314 of Criminal Code were adapted to the provisions of Article 4 (offences related to specifically adapted devices) of the Council Framework Decision 2001/413/JAI of 28 May 2001 combating fraud and counterfeiting non-cash means of payment.

In Chapter III of Title VI *Offences of forgery* is stipulated at Article 325 the *computer-related forgery offence* (Article 325 *Computer-related forgery*, the act of inputting, altering or deleting, without right, of computer data or restricting, without right, the access to this data, resulting data not compliant with truth, in order to be used to produce a legal consequence, constitutes offence and shall be punishable by imprisonment from one to 5 years". This regulation intends to protect legal security by criminalising all the actions which may, by alteration of some data on a computer support, draw unwanted legal consequences for the persons who conceived, carried out, implemented or over whom the altered information manifests its effects (Corlățeanu and Căşuneanu, 2004: 216). Thus, the purpose of this criminalisation is to create a legal protection for documents in electronic format similar to documents on material support (i.e. on paper). Taking into consideration the form of computer data and the possibilities more and more advanced to process it in any state of existence, we appreciate that it would have been more appropriate, in the continuation of the dispositions of criminalisation rule in Romanian law, to be added the sentence *regardless whether or not the data is directly readable and intelligible*, which is part of Article 7 of the European Council Convention on cybercrime (Spiridon, 2008: 243) which is the equivalent text for Article 325 of Criminal Code. Therefore, we notice that the provisions of Article 7 (computer-related forgery) of the Council of Europe Convention of cybercrime were transposed in Article 325 of the Criminal Code.

The offence of computer-related forgery is an object-offence from the point of view of modality of commitment, having an illicit purpose of patrimonial nature (Savin, 2013: 238-239). Taking into consideration the new occurred offences, such as spam and identity theft which are not criminalised or are not criminalised expressly in the main legal instruments at the level of the European Union, we consider that these acts may be criminalised in Article 325 of Criminal Code. The acts of spam and identity theft consist in the creation of false Internet pages or addresses de which are transmitted to possible

victims, and once they are accessed, they allow the transmission of personal data (Trancă and Trancă, 2014: 44).

In Chapter VI of Title VII *Offences against public safety* are included *Offences against safety and integrity of information systems and computer data* (Articles 360-366), Article *360. Illegal access to information systems: a*ccess, without right, to an information system, shall be punishable by imprisonment from 3 months to 3 years or by fine; the act referred to in paragraph (1), committed in order to get computer data, shall be punishable by imprisonment from 6 months to 5 years. Moreover, should the act referred to in paragraph (1) was committed in relation to an information system to which, through some procedures, devices or specialised programs, the access is restricted or forbidden for certain categories of users, the punishment is imprisonment from 2 to 7 years".

The offence of illegal access to an information system is stipulated in a simple form, which prohibits the access without right to an information system (paragraph1) and two aggravating variants, consisting in committing the act referred to in paragraph 1 in order to obtain computer data (paragraph 2), as well as in committing the act referred to in paragraph 1 in relation to an information system to which, through some procedures, devices or specialised programs, the access is restricted or forbidden for certain categories of users (paragraph 3).

By "access" it is understood any successful interaction with an information system, computer or mobile phone, entering the whole or just a part of the information system (Spiridon, 2008: 238). Access without right to an information system means, for the purpose of Article 35 (2) of Law no.161/2003, that such person is in one of the following situations: is not authorized, under a law or a contract; exceeds the limits of authorization; does not have the permission, from the competent natural or legal person, pursuant to law, to give, use, administer or control an information system or to carry out scientific researches or to carry out any other operation in an information system.

Access means an "interaction of the perpetrator with concerned computer technology, through the equipments or different components of the concerned system" (Dobrinoiu, 2006: 149). Thus, the modality of illegal access of information system may be carried out closely, directly by the person in front of the information system, but it may also be carried out from distance, through communication public networks (Vasiu and Vasiu, 2011: 145).

Illegal access to an information system is a means-offence which is aimed at affecting the patrimony of natural or legal persons (Reed and Angel, 2007: 565-567). We consider that Romanian legislators should modify both the title and the content of Article 360 of Criminal Code (illegal access to an information system), as from the technical point of view illegal access is carried out within an information system, not to an information system.

We noticed that the provisions of Article 2 (illegal access) of the Council of Europe Convention on cybercrime, as well as the provisions of Article 3 (illegal access to information systems) of Directive 2013/40/EU on attacks against information systems were transposed in Article 360 of the Criminal Code (Gercke, 2012: 179). According to Article 361, *Illegal interception of a transmission of computer data, i*nterception, without right, of a transmission of computer data which is not public and which is intended to an information system, coming from such system or carried out within an information system, shall be punishable by imprisonment from one to 5 years. paragraph (2) stipulates also that by the same punishment is sanctioned the interception, without right, of an electromagnetic

emission coming from an information system, containing computer data which is not public".

By the criminalisation of this type of act it is intended to be protected the confidentiality of computer data which is in progress to be transmitted against their interception, without right. The offence is referred to in two legal variants: the first consists in the interception without right of a transmission of computer data which is not public and which is intended to an information system, comes from such system and is carried out within an information system (paragraph 1), and in interception without right of an electromagnetic emissions which contain non-public computer data, respectively (paragraph 2). This legal regulation protects transmissions of computer data within or between information systems, regardless how these are carried out (Picotti and Salvadori, 2008: 18-19).

The text of the criminal legislator referred to in Article 361 of the Criminal Code is a transposition of Article 3 (illegal interception) of the Council of Europe Convention on cybercrime. Unlike the text in the Council of Europe Convention on cybercrime (Article 3 – Illegal interception), Article 361 of Criminal Code does not expressly stipulate that the interception be made by technical means. In the literature it was considered that in digital environment interceptions can be made only by using such means (Vasiu and Vasiu, 2011: 151).

We also noticed that the provisions of Article 6 (illegal interception) within Directive 2013/40/EU on attacks against information systems were transposed in Article 361 of the Criminal Code. Moreover, the act of altering, deleting or deteriorating computer data or restricting the access to such data, without right, shall be punishable by imprisonment from one to 5 years (*Article 362. Alteration of integrity of computer data*). The legal regulation in Article 362 intends to protect computer data stored within information systems, intending to prevent alteration, deletion or deterioration of computer data or restriction of access to such data.

Taking into consideration what was presented above, we notice that the Romanian criminal law does not specify as alternative modalities the *destruction* or *suppression* of computer data like in the text of the Council of Europe Convention on cybercrime, but introduces a new modality of committing an offence, namely the *restriction of access* to computer data within an information system or within a computer data storage medium. Probably it was considered that *destruction* or *suppression* are operations similar to those of *deletion* and *deterioration* or are comprised in the broad sense of these terms (Spiridon, 2008: 241).

Thus, Romania transposed the provisions of Article 4 (data interference) of the Council of Europe Convention on cybercrime, as well as the provisions of Article 5 (illegal data interference) of Directive 2013/40/EU on attacks against information systems in the text of Article 362 of the Criminal Code. Also, Article *363 Hindering of the functioning of computer systems stipulates that* "the act of seriously hindering, without right, of the functioning of a computer system, by inputting, transmitting, altering, deleting or deteriorating computer data or by restricting the access to information data shall be punishable by imprisonment from 2 to 7 years". The offence of hindering of the functioning of computer systems intends to protect computer data stored within information systems against attacks of computer piracy or other malicious activities which have as objective to bring into non-functioning information systems. Unlike the offence regulated in Article 362 of the Criminal Code, the focus is here on the effect the actions on computer data have for affected information systems (input, transmission, alteration,

deletion, deterioration, restriction of access) (Romanian Information Technology Initiative and Romanian Government, 2004: 61).

The authors of the Council of Europe Convention on cybercrime left to the discretion of each Member State to acquire and interpret the notion of *serious hindering* (Vasiu and Vasiu, 2011: 159). However, the Romanian legislator does not provide any criterion to be able to appreciate if hindering was serious or not. Thus, in these circumstances, we consider that the task of appreciating if the hindering is serious or not will be left for the law courts.

Serious hindering must be committed *without right*, so that it will not exist when the interference into an information system is allowed or authorised (e.g. testing of the security of information system). The provisions of Article 363 of Criminal Code are inspired from the provisions of Article 5 of the Council of Europe Convention on cybercrime. Thus, unlike the text of the Council of Europe Convention on cybercrime, we notice that the Romanian law does not retain as alternative modalities the *endangering*, *alteration* or *suppression* of computer data and introduces a new modality, that of *restriction* of access to this computer data. We consider that the action of *suppression* of computer data, which is the equivalent of a destruction of computer data, should have been retained as alternative modality to commit the offence along with the *endangering*.

Besides the provisions of Article 5 (system interference) of the Council of Europe Convention on cybercrime, which were transposed in Article 363 of the Criminal Code, the Romanian legislator also transposed in Article 363 the provisions of Article 4 (illegal system interference) of Directive 2013/40/EU on attacks against information systems. Article *364. Unauthorised transfer of computer data stipulates that u*nauthorised transfer from an information system or from a computer data storage medium shall be punishable by imprisonment from one to 5 years.

The offence of unauthorised transfer of computer data is regulated in a variant-type with two assumptions, consisting in the unauthorised transfer of computer data from an information system or from a computer data storage medium. In the literature (Trancă and Trancă, 2014: 55) it was considered that the unauthorised transfer of computer data is a criminalisation which complements those of access without right from an information system and interception without right of a transmission of computer data.

The provisions of Article 364 of Criminal Code were adapted to the provisions of Article 3 (computer-related offences) of the Council Framework Decision 2001/413/JAI of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment. Article *365. Illegal operations with computer devices or programmes* provides that the act of the person that, without right, makes, imports, distribute or makes available, under any form: computer devices or programmes conceived or adapted in order to commit one of the offences referred to in Articles 360-364; passwords, access codes or other similar computer data allowing total or partial access to an information system, in order to commit one of the offences referred to in Articles 360-364, shall be punishable by imprisonment from 6 months to 3 years or by fine.

By Article 365 of the Criminal Code, the Romanian legislator intends to limit the access to the tools (computer devices, programmes, passwords, access codes) allowing to commit the offences regulated by Articles 360-364 of the Criminal Code.

The offence of illegal operations with computer devices or programmes criminalises acts similar to those referred to in Article 314 (2) of the Criminal Code. Due to the overlap of activities in the field of new technologies developed with a view to falsifying electronic payment instruments, in judicial practice was identified a

concurrence of several offences in one action between the offence stipulated at Article 314 (2) of the Criminal Code in the modality of transmission of hardware and software equipments and the offence stipulated at Article 365 (1) letters (a) and (b) of the Criminal Code (Trancă and Trancă, 2014: 59).

The text of Article 4 (offences related to specifically adapted devices) of the Council Framework Decision 2001/413/JAI of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment, as well as the texts of Article6 (misuse of devices) of the Council of Europe Convention on cybercrime and Article 7 (tools used for committing offences) of Directive 2013/40/EU on attacks against information systems were transposed in Article 365 of the Criminal Code. Pursuant to the provisions of Article 366 of the Criminal Code, the attempt to the offences comprised in Articles 360-365 is punishable.

In Chapter I of Title VIII *Offences affecting some relations regarding social cohabitation* was also included the *offence of child pornography* (Article 374) arguing that producing, possessing in order to expose or distribute, procuring, storing, exposing, promoting, distributing, as well as making available, in any way, pornographic materials with minors, shall be punishable by imprisonment from one to 5 years. According to the same author, should the acts referred to in paragraph (1) were committed through a computer system or a computer-data storage medium, the punishment is from 2 to 7 years and accessing, without right, of pornographic material with minors, through computer systems or other means of electronic communications, shall be punishable by imprisonment from 3 months to 3 years or by fine.

Increased danger of acts of child pornography, as well as the necessity to ensure a maximum protection of social relations concerning principles of morality determined the Romanian legislator to establish a special regime of criminalisation and sanctioning of these infringements (Dobrinoiu and Neagu, 2011: 748). The offence is referred to in Article 374 of the Criminal Code in a variant-type, an aggravating variant and an attenuated variant.

It is considered variant-type, pursuant to paragraph 1 of Article 374 "Producing, possessing in order to expose or distribute, procuring, storing, exposing, promoting, distributing, as well as making available, in any way, of pornographic materials with minors". It constitutes aggravating variant, pursuant to Article 374 (2) "should the acts referred to in paragraph (1) were committed through a computer system or a computer-data storage medium". It constitutes attenuated variant, pursuant to Article 374 (4) "accessing, without right, pornographic materials with minors, through computer systems or other means of electronic communications".

I noticed that the provisions of Article 374 of Criminal Code appear in the text of Article 9 (offences related to child pornography) of the Council of Europe Convention on cybercrime. The offence referred to in Article 374 of Criminal Code is at the limit between the offences committed with the help of information systems and those committed through information systems (Féral-Schuhl, 2010: 980-981).

The text of Article 374 of Criminal Code was also adapted to the provisions of Article 5 (offences concerning child pornography, in paragraph 3 being stipulated the offence to obtain, intentionally, through information and communication technology, the access to child pornography) of Directive 2011/92/EU on combating the sexual abuse and sexual exploitation of children and child pornography (Directive 2011/92/EU was published in the Official Journal of the European Union, 17.12.2011, L335/1), as well as to the provisions of Article 20 (offences concerning child pornography, at paragraph (1)

letter (f) being stipulated the offence of knowingly obtaining access, through information and communication technologies, to child pornography) of the Council of Europe Convention on protection of children against sexual exploitation and sexual abuse (Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse) of the year 2007.

In Chapter VIII of Title I *Offences against the person* was also included the *offence of corruption of children for sexual purposes* (Article 222): the proposal, by an adult, to meet a minor who has not reached the age of 13, for the purpose of committing one of the offences established in accordance with Article 220 or Article 221, including when the proposal was made by means of transmission at distance, shall be punishable by imprisonment from one month to one year or by fine.

The offence provided for in Article 222 of the Criminal Code in one variant-type consists in the act of an adult to propose to a minor who has not reached the age of 13 to meet, for the purpose of committing one of the offences referred to in Article 220 (sexual act with a minor) or Article 221 (sexual corruption of minors), including when the proposal was made through means of transmission at distance (Sheldon and Howitt, 2007: 142-143). This criminalisation also occurred in Romanian legislation because of the increase of the phenomenon of sexual abuse on minors, following their meeting with adults in the offline environment whom they knew in the cyberspace. Thus, this new criminalisation in the Romanian legislation refers to the preparation of minor to have sexual acts of any nature for the purpose of obtaining sexual satisfactions. The perpetrator, for the purpose of reaching his aim, first tries to befriend with the minor, by drawing the minor into discussing intimate matters, and gradually exposing the child to sexually explicit materials in order to reduce inhibition about sex (Dobrinoiu et al., 2014: 185). Moreover, the text of Article 222 of the Criminal Code stipulates that the proposal of perpetrator with a view to corrupting minors for sexual purposes be also achieved through information and communication technology.

The offence of corruption of minors for sexual purposes or solicitation of minors for sexual purposes (grooming), as it is used in Directive 2011/92/EU on combating the sexual abuse and sexual exploitation of children and child pornography, as well as in the Council of Europe Convention on protection of children against sexual exploitation and sexual abuse of 2007 is a very often committed offence in cyberspace (Clough, 2010: 248-250).

Following the carried out analysis, we noticed that the provisions of Article 6 of Directive 2011/92/UE on combating the sexual abuse and sexual exploitation of children and child pornography, as well as the provisions of Article 23 of the Council of Europe Convention on the protection of children against sexual exploitation and sexual abuse, which regulates the *solicitation of children for sexual purposes through information and communication technology*, were almost entirely transposed in Article 222 of the Criminal Code.

In Chapter VI of Title I *Offence against the person* was also included the *offence of harassment* (Article 208) arguing that: the act of an individual who, repeatedly, stalks, without right or a legitimate interest, a person or mnitors his/her house, workplace or other places where he/she goes, thus causing a state of fear, shall be punishable by imprisonment from 3 to 6 months or with fine; making of phone calls or communications by means of distance communication, who, by frequency or content, causes fear to a person, shall be punishable by imprisonment from one month to 3 months of by fine, if the act does not

constitute a more serious offence; criminal action is initiated upon the prior charge of the injured party".

The offence of harassment is stipulated in a variant-type and an attenuated variant. Thus, the variant-type, pursuant to paragraph 1 of Article 208 of the Criminal Code refers to the act of that individual who, repeatedly, stalks, without right or a legitimate interest, a person, or monitors his/her house, workplace or other places where he/she goes, thus causing a state of fear. At paragraph 2 of Article 208 of the Criminal Code is stipulated the attenuated variant, which refers to making phone calls or communication by means of transmission at distance, which, by frequency and content, cause fear to a person.

Once with the development of Internet and especially with the use of social networking, new forms of harassment occurred: cyberstalking and cyberbulling. Cyberstalking is a form of harassment by information systems of adults through electronic mail, groups of discussions, instant messages, which involve a physical threat which induces to the victim a feeling of fear (Moise, 2011: 26-27). Cyberbulling is a form of harassment through information systems of minors (Vasiu and Vasiu, 2011: 234).

As cyberstalking and cyberbulling are not expressly stipulated within the legal instruments in the field of cyberspace at the level of the European Union, the Member States of the European Union began to elaborate specific regulations to criminalise the two forms of harassment or to elaborate provisions that comprise certain forms of harassment by electronic communications along with the traditional forms of harassment. The last variant is also the choice of Romanian legislators to regulate the offence of harassment in Article 208 of the Criminal Code.

The text of Article 208 of the Criminal Code adapted to the provisions of Article 3 (offences related to sexual abuse) of Directive 2011/92/UE on combating sexual abuse and sexual exploitation of children and child pornography, as well as to the provisions of Article18 (sexual abuses) of the Council of Europe Convention on the protection of children against sexual exploitation and sexual abuse.

Offences related to infringements of copyright related rights (Article 10 of the Council of Europe Convention on cybercrime and Articles 2, 3, 4 and 6 of Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society) are referred to in Article 139 index number 6-Article 143 of Law no. 8/1996 (Law no. 8/1996 regarding copyrights and related rights which was published in the Official Gazette of Romania no. 60 from the 26th of March 1996) on the copyright and related rights.

Conclusions

Taking into consideration the carried out analysis, we notice that the Romanian legislation on cybercrime adapted to the provisions of the most important legal instruments on preventing and combating cybercrime at the European Union, such as the Council of Europe Convention on cybercrime, Directive 2013/40/UE of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and Council Framework Decision 2001/413/JAI of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment.

As for the new offences which are committed in cyberspace and which are not regulated expressly in the Romanian criminal law legislation, we consider them liable to be criminalised by the following existent provisions: spam could be criminalised by the provisions of Article 325 and Article 363 of the Criminal Code; phishing could be criminalised by the provisions of Article 249 of the Criminal Code; data theft could be

criminalised by the provisions of Article 325 and Article 364 of the Criminal Code; cyberstalking could be criminalised by the provisions of Article 208 of the Criminal Code; cyberbulling could be criminalised by the provisions of Article 208 of the Criminal Code; denial of Service -DOS- could be criminalised by the provisions of Article 362 of the Criminal Code.

Romania signed the Council of Europe Convention on cybercrime on 23/11/2001 and ratified it on 12/05/2004 by Law no. 64/2004 (Law no. 64/2004 regarding the ratification of the Convention of the European Council on cybercrime which was published in the Official Gazette of Romania no. 343 of 20th of April 2004) on the ratification of the Council of Europe Convention on cybercrime.

Acknowledgement

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 Resources Development 2007-2013".

References:

Clough**,** J. (2010). *Principles of cybercrime*, Cambridge: Cambridge University Press.

Convention of the European Council on cybercrime. Retrieved from: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201), 25 october 2007. Retrieved from: http://conventions.coe.int/Treaty/EN/treaties/Html/201.htm.

Corlățeanu, S., Căşuneanu, C. (2004). Delicte contra datelor şi sistemelor informatice. *Revista Dreptul*, (11).

Council Framework Decision 2001/413/JHA of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment, Official Journal of the European Communities, 02.06.2011, L149/1. Retrieved from: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32001F0413&from=RO.

Directive 2013/40/EU of the European Parliament and of the Council of 12 august 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. Retrieved from: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013L0040&from=EN.

Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JAI, Official Journal of the European Union, 17.12.2011, L335/1, Retrieved from: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32011L0093&from=RO.

Dobrinoiu, V., Hotca, M. A., Gorunescu, M., Dobrinoiu, M., Pascu, I., Chiş, I., Păun, C., Neagu, N., Sinescu, M.C. (2014). *Noul Cod penal comentat. Partea specială*. Second Edition. Bucharest: Universul Juridic Publishing House.

Dobrinoiu, V., Neagu, N. (2011). *Drept penal. Partea specială. Teorie şi practică judiciară*. Bucharest: Universul Juridic Publishing House.

Dobrinoiu, M. (2006). *Infracțiuni în domeniul informatic*. Bucharest: C. H. Beck Publishing House.

Féral-Schuhl, C. (2010). *Cyberdroit. Le droit à l' épreuve de l' Internet*, Sixième Édition. Paris: Dalloz.

Gercke, M. (2012). International Telecommunication Union. *Understanding Cybercrime: Phenomena, Challenges and Legal Response*. Geneva. Retrieved from: www.itu.int/ITU D/cyb/cybersecurity/legislation.html.

Hotca, M. A., Dobrinoiu, M. (2008). *Infracţiuni prevăzute în legi speciale*. Bucharest: C. H. Beck Publishing House.

Law no. 8/1996 regarding copyrights and related rights which was published in the Official Gazette of Romania no. 60 from the 26th of March 1996.

Law no. 64/2004 regarding the ratification of the Convention of the European Council on cybercrime which was published in the Official Gazette of Romania no. 343 from the 20th of April 2004.

Moise, A. C. (2011). *Metodologia investigării criminalistice a infracţiunilor informatice*. Bucharest: Universul Juridic Publishing House.

Picotti, L., Salvadori, I. (2008). Council of Europe. Project of Cybercrime**,** *National legislation implementing the Convention on Cybercrime. Comparative analysis and good practices*, Strasbourg. Retrieved from: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/reports-presentations/567%20study2-d-version8%20_28%20august%2008.pdf.

Reed, C., Angel, J. (2007). *Computer Law. The Law and Regulation of Information Technology*. Sixth Edition. Oxford: Oxford University Press.

Romanian Information Technology Initiative and Romanian Goverment (2004). *Ghid introductiv pentru aplicarea dispoziţiilor legale referitoare la criminalitatea informatică*. Bucharest. Retrieved from: http://www.riti-internews.ro/ro/ghid.htm.

Savin, A. (2013). *EU Internet Law*. Cheltenham, Glos: Edward Elgar Publishing Limited.

Sauca, M. (2005). *Infracţiuni privind comerţul electronic*. Timişoara: Mirton Publishing House.

Schjolberg, S., Ghernaouti-Helie, S. (2011). *A Global Treaty on Cybersecurity and Cybercrime*. Second Edition, Oslo: AIT.

Sheldon, K., Howitt, D. (2007). *Sex Offenders and the Internet*. Chichester, West Sussex: John Wiley & Sons Ltd.

Simion, R. (2010). *Recent developments as regards cybercrime legislation in Romania*. Council of Europe. Octopus Interface Conference – Cooperation against Cybercrime. 23-25 March 2010. Strasbourg.

Spiridon, I. C. (2008). Reflecţii cu privire la legislaţia română în domeniul criminalităţii informatice. *Revista Dreptul*, (6).

Trancă, A. M., Trancă, D.C. (2014). *Infracţiunile informatice în noul Cod penal*. Bucharest: Universul Juridic Publishing House.

Truichici, A. M. (2008). Lupta împotriva fraudei şi falsificării mijloacelor de plată, altele decât lichiditățile la nivelul Uniunii Europene. *Revista de Drept Comercial*, (2).

Vasiu, I., Vasiu, L. (2011). *Criminalitatea în cyberspaţiu*. Bucharest: Universul Juridic Publishing House.

Article Info

Received: February 25 2015
Accepted: March 20 2015