Illegal interception of computer data transmission in the regulation of the New Romanian Criminal Code

Assistant Professor Liviu-Cosmin VASILESCU, PhD.
University "Valahia" Târgoviste, ROMANIA
lvvasilescu@yahoo.com

Abstract

The recent explosive development of information technology has triggered new methods of committing crimes, others than those included in the so-called traditional template. As in the text of the new Criminal Code of Romania the legislator pays special attention in the field of computer crime, this paper aims at treating in detail, several specific issues related to the offense of illegal interception of computer data transmission, that has constantly grown to be a substantial threat for the current economic and social reality.

Keywords: *crime, illegal interception, computer data, the new Romanian Criminal Code.*

1. Introductory remarks

The offenses in the field of computers is a rather new domain because the very substance of criminal legislation has appeared only in recent years, due to the astounding advances that have occurred in the theory of systems, in cybernetics, as well as in the manufacturing of computer technology. [1]

Computers have penetrated the progress of all countries, becoming indispensable tools for various activities. They have had a global impact on daily life, on the way of doing business, on communication and on information management. This new technology has brought a sum of great benefits for administration, business and even on individuals themselves. However, this rapid and radical evolution raises a number of problems both of socio-economic nature with the concerns about jobs, but also of legal nature, for example in the protection of computer programs and data security. [2]

As only a small proportion of criminal offenses related to the use of computer systems can come to the knowledge of criminal investigation bodies, at this point it is very difficult to achieve an overview of the extent and evolution of the phenomenon. Even though it is possible to perform an adequate description of the types of offenses encountered, it can hardly be easy to present a synthesis related to the extent of losses caused by them and to the actual number of crimes committed. [3]

The offense of illegal interception of computer data transmission is seen as complementary criminality in relation to the access, without right, to a computer

system; actually, in many cases, both offenses may exist in a consequential relation. [4] In what follows, a thorough approach to the main elements and modifications of the offense of the illegal interception of computer data transmission is performed, according to the new rules in the Romanian Criminal Code.

2. Legal content

The previous Romanian Criminal Code did not contain specific regulation on the offense of illegal interception of computer data transmission, which does not mean that the crime had not been sanctioned by the Romanian law before the entry into force of the new Criminal Code. The offense of illegal interception of computer data transmission was regulated in a special law, namely the article 43 of Law no. 161/2003 on certain measures to ensure transparency in exercising public dignities, public functions and in business environment, on preventing and punishing corruption, which read:

"*1) The interception, without right, of a transmission of non-public electronic data that is intended for a particular computer system, comes from such a system or is carried out within a computer system, is a crime punishable by imprisonment from 2 to 7 years.*

(2) The interception, without right, of electromagnetic emissions from a computer system, which contains information that is not public, is sanctioned with the same punishment." [5]

The entry into force of the new Romanian Criminal Code meant special focus on cybercrime by regulating in the content of the new legal act, more precisely in Title VII, Chapter VI, the offence of illegal interception of computer data transmission. Thus, the article 361 of the new Romanian Criminal Code defines the crime of illegal interception of computer data transmission that is in its formulation, very similar to the previous legal text, namely:

" *(1) The interception, without right, of a transmission of non-public electronic data that is intended for a particular computer system, comes from such a system or is carried out within a computer system, is a crime punishable by imprisonment from 1 to 5 years.*

(2) The interception, without right, of electromagnetic emissions from a computer system, which contains information that is not public, is sanctioned with the same punishment." [6]

It can be easily noticed that almost the entire new text of law only is identical with the previous regulation, being different only in the modification related to the legal sanction on committing such a crime, namely the reduction of its limits. Whereas the Law 161/2003 provided imprisonment from 2 to 7 years for the party found guilty of the crime of illegal interception of computer data transmission, the new Romanian Criminal Code imposes a penalty of one to five years for the same offense.

3. The structure of offense

3.1. *The object of offense*

The legal object consists of all social relations regarding information privacy (the right to data secrecy). [7] The criminalisation of illegal interception in the new Romanian Criminal Code is a measure, both technical and legal, that eventually aims at the protection of the right to privacy of communications. Moreover, the right to protection of correspondence is formulated in Article 8 of the European Convention on Human Rights, the text focusing on covering any forms of data transmission (by mail, fax, telephone, etc.)

The material object is represented by the stream of the information packets (the sequence of “0” and “1” bits, i.e. the sequence of electrical impulses resulted from the controlled fluctuation of voltage), which are transported from one computing device to another or within the same system of information, and towards which the offender’s interest is focused. [8]

Specifically, in the case of paragraph 1, the material object is the material support through which communication is performed, especially the data transfer via public or private telecommunications and on which the intercepted computer data are stored.

In the case of paragraph 2, the material object is made of the electromagnetic energy (emission), that radiates or is identified in residual form or in uncontrolled/uncontrollable form in the vicinity of the electronic equipment that make up the target computer system. Thus, the electromagnetic emission around a device (printer, monitor, cable, etc.) will not be considered as material object if, at the moment of interception (capture), this was not connected to a computer system according to paragraph 2. [9]

3.2. *The subjects of the offense*

3.2.1. The active subject

The new Romanian Criminal Code does not require in the wording of article 361 that the offender of the illegal interception of computer data transmission should meet any special quality. Therefore, the active subject of this crime can be any natural or legal person responsible to criminal law.

For the offense formulation, the offender must necessarily use (directly) certain electronic equipment specially designed for interceptions in the IT environment, the possession of specific knowledge in the field being irrelevant [10]; yet, one statement should be added in this case, namely the fact that this type of crime is most often committed by people who possess expertise in this area or have access to computer systems.

With respect to the prosecution, all the known forms are possible, more precisely, other persons may participate as instigators, accomplices and co-authors in the offense of illegal interception of computer data transmission.

3.2.2. The passive subject

The passive subject is mainly represented by any person or entity, legally holding the information system or the components of transmission between two or more computer systems. [11]

In a secondary plan, the passive subject is the rightful owner of the intercepted computer data or the person concerned directly envisaged by the computerised procession of these data. [12]

4. The content of incorporation

4.1. *The objective side*

4.1.1. The material element

The material element of the crime of illegal interception of computer data transmission is characterised by the action of interception, by any means, of data or electromagnetic emission (the programme submitted by the interaction of electric currents and magnetic fields. [13] The interception (in the technical sense) is the action of capturing by using an electronic device specifically made for this purpose or by a computer, the electrical impulses, the variations in voltage or the electromagnetic emissions transiting the inside of a computer system or manifesting

as a result of its operation time or existing on the route connecting two or more communicating systems. [14]

In order to achieve the material element of the objective side, the action of interception must cumulatively meet the following requirements:

- The interception takes place without right, a condition provided by both paragraph 1 and paragraph 2 for the offense;
- In the first normative variant (paragraph 1), the interception must concern a transmission of non-public electronic data that is intended for a computer system, comes from such a system or is carried out within a computer system. [15] In the case of paragraph 2, the transmission is related to an electromagnetic emission generated by a computer system containing data that are not public.

The European Convention on Cybercrime [16] expressly provides that interception must be carried out by technical means. The Romanian criminal legislator in the text of Article 361 has not expressly provided for it, probably considering that such a provision would be irrelevant, given the fact that interceptions in the digital environment can be achieved exclusively by using technical means.

The technical means include technical devices fixed on the transmission lines to collect or record communications or computer software that facilitates data interception. [17]

The term “non-public” used by the criminal legislator is related to the former normative variant (paragraph 1), namely to the nature of the transmission (communication), and not to the nature of the transmitted data. There is irrelevant whether the transmitted or communicated data are public or not, as long as the parties involved in the transmission process understand the necessity of performing this operation under the condition of confidentiality (privacy). There are also situations when the data are kept secret (protected) until, for example, the access to them (the service) is paid for. In other words, the concept of “non-public” established by the legislature does not exclude *per se* the communications made via public networks.

The investigation must be concerned with the entities that are involved in the data transmission: between the computer systems, between the components of different systems or between the components of the same system and also with the identification of the material support by which the access is done, regardless of the fact that the data transfer is performed through networks by cable or WLAN or that

the cables and issued signs (wiretapping, Eavesdropping on Emanations) are intercepted. [18]

In the latter normative variant, contained in Article 361, paragraph 2 of the new Romanian Criminal Code, the interception of electromagnetic emissions without right is criminalised. This takes the form of capturing the present radiations or electromagnetic fields (on a scientifically determined distance) around any device subject to the transit of electrical or electromagnetic pulses. For example, by using a special device, people with certain interests can capture electromagnetic radiations around the target computer monitor and "translate" them, that is turning them into electrical impulses and then in alphanumeric characters.

Another requirement for the existence of the crime, present in both normative paragraphs, is that the offender should have acted without right. The act will be legitimate if the party who shall intercept data has the right to benefit from the communicated data, if they act under the disposition or authorisation of the participants or of the recipient of the transmission, if the data are intended for their own use or for public use, or if, due to a specific legal provision, the supervision is authorised in the interest of national security or in order to allow the authorities to uncover certain crimes that were committed. [19]

4.1.2. The immediate result

The immediate result is in the detrimental effect on the interests of the persons legally performing the transmissions of information. The text of the law does not expressly require the production of a particular injury. It is sufficient to intercept transmissions without the requirement that the data thus obtained be disclosed to others. [20]

4.1.3. Causation

With regard to causality, we are of the opinion that it results precisely from the materiality of the offense ex re. The crime of illegal interception of computer data transmission is one of danger (formal), a reason for which causation simply results from unauthorised interception of data transmission.

Even if effective results are not produced, in the cases of social danger offenses, the created state of danger can have the ability to produce a socially dangerous result. Within this category of crime, the social danger, more precisely, the harmful consequence, results from the materiality of the act, i.e. from the forbidden act of behaviour.

In formal offenses or those of social risk, the socially dangerous result and thus, the hurtful immediate consequence is presumed. In terms of probation, it should not be proved. [21]

4.2 *The subjective aspect*

As far as the mental attitude of the offender at the time of committing the crime is concerned, we should notice that the offense of illegal interception of computer data transmission can only be committed intentionally and not by negligence.

The question is whether it can be committed only with direct intention, excluding the possibility of the indirect intention. There are interpretations that the crime of illegal interception of computer data transmission can be committed only with direct intention (qualified intention). The explanation may be found under the grounds of the analysis of the material element of the objective side, hence it is impossible for the offender, foreseeing the result of its action, to capture (and possibly to record) the communication data packets in a computer system or between two such systems, without pursuing this possibility, accepting instead only the possibility of producing the result. [22]

In other authors' opinions, [23] it is considered that the subjective element of the offense is represented by the intention, in its both direct and indirect forms.

As for us, we shall rally the latter opinions expressed in practice, due to the fact that the Article 361 of the new Romanian Criminal Code does not require that the offender should pursue a qualified aim in order to commit the offense, an aspect for which we consider that the crime of illegal interception of computer data transmission can be committed with both direct and indirect intention.

5. The forms of the offense. Sanctions and procedural aspects

5.1 *The forms of the offense*

The preparatory acts, although possible and sometimes even necessary, are not covered by the legal text of the new Romanian Criminal Code. However, they may be the object of an autonomous offense if all the constitutive elements of the offense in question are present.

Regarding the attempt to commit the offense of illegal interception of computer data transmission, we must highlight the fact that it is penalised and punished by criminal legislature. The new Romanian Criminal Code, under Article 366 provides

that the attempt to all the offenses under Title VII, Chapter VI, is sanctioned, the illegal interception of computer data transmission being found in this category. [24]

The consumption of this offense occurs at the moment when the socially dangerous consequence is produced, that is the breach of confidentiality on the content of electronic data transmission, thereby creating a state of danger to the social values protected by law. The exhaustion of the offense of illegal interception of computer data transmission takes place at the time of the last act criminalised by law in any of the normative variants.

The offense can be performed both in simple and continuously repeated forms. [25]

5.2. *Sanctions and procedural aspects*

Before the entry into force of the new Romanian Criminal Code, the offense of illegal interception of computer data transmission was sanctioned by criminal imprisonment from 2 to 7 years.

The new Criminal Code has opted for a reduction of the sentence limits for this crime, so that at present, the illegal interception of computer data transmission is punished with imprisonment from one to five years. [26]

Criminal proceedings shall be initiated *ex officio*.

Conclusions

Romania, as well as the entire world need cyberspace – this intense and frequent phenomenon of our times – to be safe, free and open. The new Romanian Criminal Code brings important changes in the category of cybercrimes, treating them with great stringency, managing to correlate the legal provisions on such offences with the current technology and the new methods of committing crimes.

"This paper was funded by the contract HRD / 159 / 1.5 / S / 141 699, the strategic project with the ID 141 699, co-funded by the European Social Fund through Human Resources Development Sector Operational Programme 2007-2013"

References:

[1] Maxim Dobrinoiu, ,,*Interceptarea ilegală a unei transmisii de date informatice",* p. 1 - http://ecrime. Ro / ecrime/site/files/57341236022318interceptareadatelorinformaticeCHIP.pdf
[2] http://www.juspedia.ro/13161/infractiuni-informatice/

[3] Internews Network, RITI dot-GOV. (2004). *Ghid introductiv pentru aplicarea dispoziţiilor legale referitoare la criminalitatea informatică*, Bucureşti, p. 50 - http://www.riti-internews.ro/Capitolul%2005%20-%20Reglementarea%20criminalitatii%20informatice.pdf
[4] Anamaria Trancă, Dumitru Cristian Trancă (2014), *,,Infracţiunile informatice în noul Cod penal"*, Editura Universul Juridic, Bucureşti, p. 50
[5] Legea nr.161 din 19 aprilie 2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice și în mediul de afaceri, prevenirea și sancționarea corupției. Articolul 43 - www.legi-internet.ro
[6] Noul Cod Penal actualizat 2014 - Legea 286/2009. Articolul 361 - http://legeaz.net/noul-cod-penal
[7] Ioana Vasiu, Lucian Vasiu (2011), *,,Criminalitatea în cyberspaţiu",* Editura Universul Juridic, Bucureşti, p. 150
[8] http://www.rasfoiesc.com/legal/criminalistica/ASPECTE-DE-DREPT-PENAL-IN-MATE96.php
[9] Ibidem
[10] Maxim Dobrinoiu, ,,*Interceptarea ilegală a unei transmisii de date informatice",* p. 2 - http://e-crime.ro/ecrime/site/files/57341236022318interceptareadatelorinformaticeCHIP.pdf
[11] Florescu Valentin, Florescu Gabriela, *,,Analiza infracţiunilor informatice incriminate în legislaţia în vigoare şi din perspectiva noului Cod penal"* – Institutul Naţional de Cercetare Dezvoltare în Informatică – ICI Bucureşti, Revista Română de Informatică şi Automatică, vol.22, nr. 2, p.27 - http://rria.ici.ro/ria2012_2/art03.pdf
[12] Florescu Valentin, Florescu Gabriela, *,,Analiza infracţiunilor informatice incriminate în legislaţia în vigoare şi din perspectiva noului Cod penal"* – Institutul Naţional de Cercetare Dezvoltare în Informatică – ICI Bucureşti, Revista Română de Informatică şi Automatică, vol.22, nr. 2, p.27 - http://rria.ici.ro/ria2012_2/art03.pdf
[13] http://www.juspedia.ro/13161/infractiuni-informatice/
[14] http://e-crime.ro/ecrime/site/index.php/acasa/materiale_documentare/interceptarea_informatica/
[15] Ioana Vasiu, Lucian Vasiu (2011), *,,Criminalitatea în cyberspaţiu",* Editura Universul Juridic, Bucureşti, p.151
[16] Consiliul Europei, *,,Convenţia privind criminalitatea informatică",* Budapesta, 23 noiembrie 2001
[17] Ioana Vasiu, Lucian Vasiu (2011), *,,Criminalitatea în cyberspaţiu",* Editura Universul Juridic, Bucureşti, p.151
[18] Academia de Poliţie A.I. Cuza, *,,Metodologie criminalistică - Structurile infracţionale şi activităţile ilicite desfăşurate de către acestea*" (2008), Editura AIT Laboratories s.r.l., Bucureşti, p. 330
[19] http://www.creeaza.com/legislatie/drept/Analiza-contintului-juridic-a-893.php
[20] *Analiza conţinutului juridic al infracţiunii de interceptare ilegală a unei transmii de date informatice* - http://www.creeaza.com/legislatie/drept/Analiza-contintului-juridic-a-893.php
[21] Vasile Sorin Curpăn, Cosmin Ștefan Burleanu (2012), *,,Infracţiunea – faptă ilicită socialmente periculoasă"*, Articole științifice publicate. Bucureşti, p.5 - www.sorincurpan.ro/carti/enciclopedie_vol2.pdf
[22] Maxim Dobrinoiu, ,,*Interceptarea ilegală a unei transmisii de date informatice",* p. 8 - http://e-crime.ro/ecrime/site/files/57341236022318jinterceptareadatelorinformaticeCHIP.pdf
[23] Gheorghe Iulian Ioniță (2013), *,,Infracţiuni din sfera criminalităţii informatice – incriminare, investigare, prevenire şi combatere"*, Editura PRO Universitaria, Bucureşti, p. 203
[24] Noul Cod Penal actualizat 2014 - Legea 286/2009. Articolul 366 - http://legeaz.net/noul-cod-penal
[25] Ioana Vasiu, Lucian Vasiu (2011), *,,Criminalitatea în cyberspaţiu",* Editura Universul Juridic, Bucureşti, p. 153
[26] Noul Cod Penal actualizat 2014 - Legea 286/2009. Articolul 361 - http://legeaz.net/noul-cod-penal