Implementing the Provision of the European Council Convention on Cybercrime in the Romanian Legislation

Gheorghe-Iulian IONIȚĂ
Romanian-American University Bucharest
ionita.gheorghe.iulian@profesor.rau.ro

Abstract: The European concerns with respect to preventing and fighting cybercrime materialized in the Council of Europe Convention on Cybercrime. As a reflection of such concerns, the Draft on preventing and fighting cybercrime was included in Title III of Romanian Law no. 161/2003. In the same context, most recommendations which incriminate cybercrimes were also entered in the future Romanian Criminal Code as well. As in other countries, the implementation in the Romanian legislation of the convention provisions generated a number of problems which have been more or less noted and solved. This study attempts to pinpoint such problems.

Keywords: crimes; incrimination; harmonization

1 Introduction

Although it only sets certain standards and allows them to be adjusted according to the needs of each state, the CoE's Convention on Cybercrime (CETS no: 185)[1] still remains the most important international instrument used in fighting cybercrime. For this reason, there is not a global consensus with respect to the implementation of the convention provisions.

Romania has been among the first countries to sign[2] the convention and, through Title III of Romanian Law no. 161/2003[3], it regulated (in Article 34) „the prevention of and fight against cybercrime through specific measures, in order to prevent, discover and sanction the crimes committed by means of computer systems, ensuring the observance of human rights and personal data protection" by adopting (to a considerable extent) the convention provisions. Romanian Law no. 8/1996[4] and the new Romanian Criminal Code (Romanian Criminal Code 2009)[1]

[1] European Council Convention on Cybercrime (CETS no: 185), adopted in Budapest on November 23, 2001.
[2] Romania signed the Convention on November 23, 2001 and implemented it in on May 12, 2004.
[3] Romanian Law no. 161/2003 published in the Official Gazette no. 279/21.04.2003.
[4] Romanian Law no. 8/1996 published in the Official Gazette no. 60/26.03.1996.

also adopted (more or less faithfully) such incrimination recommendations (Ioniţă, 2009).

2 Comparative Analysis of the Manner to Define the Terms Used

We have to specify that the parties do not have to adopt in their internal legislation the same definitions as presented in the CoE's Cybercrime Convention, having the authority to decide on how to implement these concepts. Nevertheless, the concepts formulated in the internal legislations have to be consistent with the principles set through this article 1 of the CoE's Cybercrime Convention.

The Romanian lawgiver went beyond the convention provisions, presenting the meaning of certain terms such as „automatic data processing", „software", „user data", „security measures", „acts illegally".

Unfortunately, the convention also uses other terms whose meaning is not specified and which already generate problems both to experts and to law enforcing authorities: „security measures", „access", „unauthorized", „illegal", „unjustified", etc.

In order to eliminate such problems, **it is necessary,** *as the Romanian lawgiver did*, ***to identify and explain the meaning of the terms used,*** since each national legislation system has its own traditions and certain terms may be interpreted and applied differently.

3 Comparative Analysis of the Manner to Incriminate Crimes Against Data Confidentiality, Integrity and Availability

3.1 Illegal Access

We can note that Article 2, thesis I of the CoE's Cybercrime Convention presents the recommendation to incriminate the illegal access, and the second thesis of the same article indicates the possibility that national lawgivers condition the incrimination for the „infringing security measures", „the intent of obtaining computer data or other dishonest intent", or „in relation to a computer system that is connected to another computer system".

The internal legislation exceeded the convention recommendations, incriminating as aggravated variants the situations where the act is committed „with the intent of obtaining computer data" or „by infringing the security measures".

[1] Romanian Law no. 286/2009 published in the Official Gazette no. 510/24.07.2009.

It is desirable that such ***means to commit the act*** („by infringing the security measures", „with the intent of obtaining computer data or other dishonest intent", „in relation to a computer system connected to another computer system") ***represent*** *aggravating situations*, and not requirement of the material/subjective element.

The final paragraph of Article 360 in the future Romanian Criminal Code no longer uses the term „security measures" (whose meaning is not specified in the title „The meaning of terms and expressions in the criminal legislation" either). But it takes over (to a considerable extent) meaning it has in Article 35 paragraph (1) letter h) of Romanian Law no. 161/2003. The limits of the punishment stipulated (in Article 360) for this method to commit the crime (imprisonment for 2 to 7 years) are under those stipulated in the special law (Article 42) for the same manner to commit the crime (imprisonment for 3 to 12 years).

3.2 Illegal Interception

By ***analyzing the texts*** we can observe that Article 3, thesis I of the CoE's Cybercrime Convention stipulates the recommendation to incriminate illegal interception, and the second thesis of the same article indicates that national lawgivers may condition the incrimination on committing „with dishonest intent" or „in relation to a computer system that is connected to another computer system".

This time, the Romanian lawgiver did not incriminate as aggravated variants the situations where the act is committed „with dishonest intent" or „in relation to a computer system that is connected to another computer system".

As in the case of the previous article, **it is recommendable** that such means to commit the crime („with dishonest intent" or „in relation to a computer system that is connected to another computer system") ***represent aggravating situations***, and not requirements of the material/subjective element.

For this crime, the limits of the punishment stipulated in Article 361 in the future Romanian Criminal Code (imprisonment for 2 to 7 years) are under those stipulated in the Romanian special law (Article 43) for the same crime (imprisonment for 3 to 12 years).

3.3 Data Interference

The Article 4, paragraph 1 of the CoE's Cybercrime Convention presents the recommendation to incriminate data integrity damage, paragraph 2 indicates the possibility that national lawgivers may condition the incrimination of the described behavior on the committing of „serious harm", having the possibility to define

autonomously the extent to which the incurred damage can be deemed „serious", based on the own criteria of the internal legislation.

Besides the CoE's Cybercrime Convention recommendations, the Romanian lawgiver further incriminated, as a distinct manner to commit this criminal offence, „the restriction access to computer data without right", but failed to stipulate as aggravating variant the occurrence of result, „serious harm".

In this situation also, *such result* („serious harm") should ***represent an aggravating situation***.

The future Romanian Criminal Code incriminates (in Article 362 and 364) two distinct crimes („Altering the computer data integrity" and „Unauthorized transfer of computer data"), but which take over the content of the incrimination in the Romanian special law (Article 44), less the limits of punishment, which are different. Thus, in the Romanian special law, the stipulated limits are imprisonment for 2 to 7 years (in case of the standard variant), imprisonment for 3 to 12 years, respectively (in case of aggravated variants) as compared to imprisonment for 1 to 5 years as stipulated in the future Romanian Criminal Code (in case of altering the computer data integrity and the unauthorized transfer of computer data).

3.4 System Interference

As can be noted in the Article 5, thesis I of the CoE's Cybercrime Convention, it specifies the recommendation to incriminate the system integrity damage, conditioning the incrimination on the status of „serious", „intentional", „without right".

The Romanian lawgiver also maintained these requirements of the material element of the offence specified in the recommendation to incriminate („serious", „without right") and even introduced an additional one, „restricting the access to computer data". However, **it would have been preferable** to ***eliminate the requirement*** „serious", in order to include as well certain forms of manifestation of the phenomenon which are less destructive. The limits of the punishment stipulated in Article 363 in the future Romanian Criminal Code for this crime (imprisonment for 2 to 7 years) are under those stipulated in the Romanian special law (Article 45) for the same crime (imprisonment for 3 to 15 years).

3.5 Misuse of Devices

We can observe that Article 6 in the CoE's Cybercrime Convention, after presenting the recommendation to incriminate (in paragraph 1), it stipulates in paragraph 2 that it „shall not be interpreted as imposing criminal liability" where

the acts recommended for incrimination „is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorized testing or protection of a computer system"

The Romanian lawgiver, *even if it did not incriminate* „procurement for use" as a means to commit the offence, **adopted a clearer solution for all the acts incriminated**: „for the purpose of committing any of the offences established in accordance with Articles …". We have to specify that the limits of the punishment stipulated in Article 365 in the future Romanian Criminal Code for this offences (imprisonment for 6 months to 3 years or a fine, imprisonment for 3 months to 2 years or a fine, respectively) are under those stipulated in the Romanian special law (Article 45) for the same crime (imprisonment for 1 to 6 years).

4 Comparative Analysis of the Manner to Incriminate Computer-Related Offences

4.1 Computer-related Forgery

By ***analyzing the texts***, we can observe that the concept formulated in the CoE's Cybercrime Convention recommendation is distinct from the concept adopted by the Romanian lawgiver.

Article 7 of the CoE's Cybercrime Convention lays emphasis on authenticity, as indicated in the wording of the incrimination recommendation: „*… resulting in inauthentic data … as if it were authentic, regardless whether or not the data is directly readable and intelligible"*.

In exchange, the Romanian lawgiver, as clear from the wording of the incrimination norm, lays emphasis on truthfulness: „*… resulting data which are incompliant with reality"*. In addition to the Convention recommendations, the Romanian lawgiver incriminated as *a distinct manner to commit this crime*, „the act of restricting, without right, the access to computer data". However, the limits of the punishment stipulated in Article 325 in the future Romanian Criminal Code for this crime (imprisonment for 1 to 5 years) are under those stipulated in the Romanian special law (Article 48) for the same crime (imprisonment or 2 to 7 years).

4.2 Computer-related Fraud

As compared to the CoE's Cybercrime Convention recommendations, the incrimination adopted by the Romanian lawgiver eliminated the **„without right" circumstances for causing the damage,** but also the **circumstances of obtaining**

the benefit *„with criminal or fraudulent intention”*, circumstances which have significant legal consequences.

The incrimination provisions adopted by the Romanian lawgiver **should be provided with circumstances** both objectively and subjectively, by ***introducing the expressions „without right” and „unjust”* and thus**

(a) *Article 49* of the Romanian Law no. *161/2003* should have the following wording: *„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, **without right**, with the intent of procuring an **unjust** economic benefit for oneself or for another, shall be punisher with imprisonment …”*.

(b) *Article 249* in the future Romanian Criminal Code („Computer fraud”) should have the following wording: *„The input, alteration or deletion of computer data, the restriction of access to such data or the interference with the functioning of a computer system, **without right**, with the intent of procuring an **unjust** economic benefit for oneself or for another shall be, if damage was caused to a person, punished with imprisonment …”*.

The limits of the punishment stipulated in Article 249 of the future Romanian Criminal Code for this crime (imprisonment for 2 to 7 years) are under those stipulated in the Romanian special law (Article 49) for the same crime (imprisonment for 3 to 12 years).

5 Comparative Analysis of the Manner to Incriminate Offences Relating to Child Pornography

As can be noted by ***analyzing the texts***, the Romanian lawgiver incriminated (in Article 374 paragraph 3 of the future Romanian Criminal Code), besides the CoE's Cybercrime Convention recommendations, as a *distinct manner to commit this crime*, „the illegal accessing of pornographic child materials by means of computer systems or other computer data storage medium”. However, in paragraph (4) of the same article (which explains the meaning of the term „pornographic child materials”), it did not include the situation of „a person of age who is presented as an underage child having an explicit sexual behavior”, a situation included in Article 35 paragraph (1) letter i) of the Romanian special law.

The limits of the punishment stipulated in Article 374 paragraph (2) in the future Romanian Criminal Code for this crime (imprisonment for 2 to 7 years) are under those stipulated in the Romanian special law (Article 51) for the same crime (imprisonment for 3 to 12 years).

6 Comparative Analysis of the Manner to Incriminate the Offences Related to Infringements of Copyright and Related Rights

The 10th Article of the CoE's Cybercrime Convention, after presenting the recommendation to incriminate (in paragraphs 1 and 2) the damages to the „intellectual property" and the „related rights", stipulates the terms: „ where such acts are committed willfully, on a commercial scale and by means of a computer system". There are three cumulative terms:

- the acts have to be committed willfully
- the acts have to be committed at a commercial scale
- the acts have to be committed by means of a computer system.

The Romanian lawgiver partially observed such incrimination recommendations. Thus, it stipulated, as requirement of the subjective element, the commercial purpose (in Article 139^6, 140, 143), setting its meaning as (Article 139^6 paragraph 9) „the aim to obtain, directly or indirectly, an economic or material advantage" and by specifying (Article 139^6 paragraph 10) that 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". It also stipulated the committing of facts „in the digital environment" as requirements of the material element (in Article 143) and even incriminated (in Article 139^9) „the unauthorized reproduction of computer software on calculation systems".

Although such requirements are not stipulated cumulatively, as recommended by the Convention, it may use the provisions of Article 10 paragraph (3) in the CoE's Cybercrime Convention, the existing incrimination provisions being effective and ensuring the protection of intellectual property rights and the related rights.

7 Comparative Analysis of the Manner to Implement Some of the Procedural Provisions

7.1 Application Field of Procedural Measures

Comparing the provisions of Article 14 in the CoE's Cybercrime Convention, we can observe that the Romanian lawgiver took over the provisions partially, *omitting to apply the special provisions in the collection of digital evidence referring to any other „classic" criminal offence* which can be found in a computer system. *In practice*, the result is a situation which is not entirely logical. Thus, such provisions do not apply to „classic" crimes (other than as incriminated through Title III or Romanian Law no. 161/2003 and those committed by means of computer systems) and the result is that *certain procedural acts* (such as the investigation of computer

systems or the computer data storage media) can be decided upon by the prosecutor as well.

The application fields of procedural provisions should be extended to *the situation stipulated in Article 14 paragraph 2 letter c)*, „the collection of evidence in electronic form of a criminal offence", in order to avoid the situation generated at present when the same computer systems and digital evidence are subject to distinct procedural rules.

8 Conclusions

The main conclusion of the presented analysis is that the most provisions in the national legislation comply with the CoE's Cybercrime Convention provisions, and even go beyond them.

At least at statement level, we can boast with a modern legislation in the field of cybercrime prevention.

However, there are certain incompatibilities, which in practice generate/may generate problems (Ioniţă, 2009). Thus, partially taking over the provisions of Article 14 in the CoE's Cybercrime Convention by omitting to apply the special provisions in the collection of digital evidence referring to any „classic" criminal offence which can be found in a computer system, generates at present a somewhat illogical situation: that the same computer systems and digital evidence are subject to distinct procedural rules.

In the same line of thought, another problem occurs in the activity of forensic investigation of computer systems and cybercrime prosecution. Thus, the *Division for Cybercrime Prevention* subordinate to the Direction of Organized Crime Prevention, carries out both investigating activities and forensic investigations to fight cybercrimes. *The Office for Investigation and Analysis of Computer Systems* within the same direction, *carries out (in fact) the activity of forensic investigation of computer systems*, an activity which should be realized by the forensic experts in the forensic sectors/National Forensics Institute. This situation is unacceptable, i.e. that persons who carry out the activity of criminal investigation of cybercrimes also realize the activity of forensic investigation of computer systems. It is not possible that in the case of any other crimes (other than cybercrimes), the activity of forensic investigation of computer systems is performed by forensic specialists within the forensic sectors/National Forensics Institute, and in the case of cybercrimes, such activities are carried out by the criminal investigation bodies within the Office for the Investigation and Analysis of Computer Systems.

Furthermore, still with respect to cybercrime prevention and fight, **it is necessary** to introduce ***special causes of non punishment or punishment reduction*** for the

persons who denounce or facilitate the identification and criminal accountability of other participants, since, in time, they have proven their efficiency in reducing the dark figure of crime (in the case of other manifestation forms as well), but also in rapidly solving the crimes under investigation. A new article should be included in Romanian Law no. 161/2003 which should read as follows:

(a) *„The persons who committed one of the offences stipulated in Article … is not punished if, during the criminal investigation, s/he denounces and facilitates the identification and criminal accountability of other persons who committed …*"

(or/and)

(b) *„The person who, during the criminal investigation, denounces and facilitates the identification and criminal accountability of other persons who committed…., benefits from a reduction by half of the punishments stipulated in Article …*".

References

Council of Europe. *Convention on Cybercrime* (CETS no: 185). Taken from http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

Ioniță, G.I. (2009). *Cybercrime*, Ph.D. thesis (unpublished). Bucharest: Police Academy „Alexandru Ioan Cuza".

Law no. 161/2003 published in the Official Gazette no. 279/21.04.2003.

Law no. 8/1996 published in the Official Gazette no. 60/26.03.1996.

Law no. 286/2009 published in the Official Gazette no. 510/24.07.2009.

New Romanian Criminal Code (Law no. 286/2009) published in the Official Gazette no. 510/24.07.2009.

Romanian Criminal Code (Law no. 15/1968) republished in the Official Gazette no. 65/16.04.1997.