A FEW COMMENTS ON THE COUNCIL OF EUROPE CONVENTION ON CYBERCRIME

Lecturer Adrian Cristian MOISE, PhD.
Spiru Haret University of Bucharest (ROMANIA)
adriancristian.moise.@gmail.com.

Abstract
The Council of Europe Convention on Cybercrime is a treaty in the field of criminal justice that establishes criminal law provisions based on the principles of the rule of law and human rights. The Convention has a relatively broad scope. Convention offences are grouped into four categories. The Council of Europe Convention on Cybercrime criminalizes criminal behaviours in the late 1990s. Thus, in the sixteen years of the Convention, new offences have arisen, and an update of the Convention is absolutely necessary.
Keywords: *cybercrime, computer system, computer data, Convention on Cybercrime.*

Introduction

The Council of Europe Convention on Cybercrime is a legal instrument that has been signed under the auspices of the Council of Europe. Although this Convention does not constitute an own legal instrument of the European Union, it is nevertheless effectively representing the interests of the European Union within its scope. The time of occurrence of the Convention coincides with the growing importance of the e-commerce, intellectual property, rapid access to Internet and the widespread use of mobile telephony [1].

The Council of Europe Convention on Cybercrime, which is a historic milestone in the fight against cybercrime, was signed in Budapest on the 23rd of November 2001 and entered into force on the 1st of July 2004. Today, the total number of signatures from the 47 Council of Europe member states that were not followed by ratifications is 3, while 43 states ratified the Convention, and one state, the Russian Federation, has not yet signed it [2].

The Council of Europe Convention on Cybercrime has a threefold purpose. First, it defines material criminal law in Chapter II, Section 1, which is a legislative harmonization effort aimed at creating a common crime base. Secondly, the investigation measures and criminal proceedings are harmonized in Chapter II, Section

II. Thirdly, ways for international co-operation are opened in Chapter III.

The Council of Europe Convention on Cybercrime creates an obligation for the Member States to introduce the provisions of Chapter II Measures to be taken at the national level in their material criminal law and to allow cooperation in areas of interest. By ratifying the Council of Europe Convention on Cybercrime, the Member States have agreed that their criminal law at the national level should criminalize the facts described in the material criminal law section of the Convention. Those Member States that have not ratified it, we believe that they should assess the opportunity to implement the standards and principles of the Convention in accordance with their legal and practical arrangements and to use the Convention as a guide or as a reference for the development of their internal legislation.

The Council of Europe Convention on Cybercrime criminalizes criminal behaviours in the late 1990s. New types of criminal behaviour in cyberspace must be provided by criminal law, such as botnets, spam, identity theft, virtual world crimes, cyber terrorism and massive and coordinated attacks against information networks. Many countries have adopted or prepared new laws to cover some of these criminal behaviours.

The analysis of crimes under the Council of Europe Convention on Cybercrime

The Convention has a relatively broad scope. Convention offences are grouped into four categories. The first category of offences relates to offences against the confidentiality, integrity and availability of data and information systems. The second category of offences relates to computer-related offences, such as computer-related forgery and computer-related fraud. The third category of offences includes offences related to content, such as offences related to child pornography. The last category of offences includes offences related to infringements of intellectual property and related rights. In 2003, the Additional Protocol to the Council of Europe Convention on Cybercrime was signed in Strasbourg on the criminalization of acts of a racist and xenophobic nature committed through computer systems.

The Council of Europe Convention on Cybercrime contains a provision on illegal access by protecting the integrity of computer systems by incriminating unauthorized access to a computer system in the Article 2.

The analysis of the different approaches regarding illegal access to a computer system in the domestic law of different states shows that the provisions adopted sometimes confuse the illegal access with offences committed after illegal access, or seek to limit the incrimination of illegal access only by committing serious infrigements [3].

The term access does not specify specific means of communication, but is open to future technical developments [4]. Therefore, this term includes all the means of entry into a computer system, including attacks on the Internet, as well as illegal access to wireless networks [5]. This broad approach demonstrates that illegal access covers not only the subsequent technical developments, but also covers the unauthorized access to computer data by intruders or employees [6]. As with other offences covered by the Council of Europe Convention on Cybercrime, the Article 2 of the Convention also requires the offender to commit the offence of illegal access with intent. However, we note that the Convention does not define the term with intent. The illegal access to a computer system to fall under the provisions of the Article 2 of the Council of Europe Convention on Cybercrime must be done without right. The Convention's legislators also underline that testing or protecting the security of a computer system, authorized by an owner, is done with right.

We believe that the illegal access to a computer systems is in most cases not the end of the illegal act committed by the offender, but rather the first step towards committing additional offences, such as alteration or obtaining stored data.

Under the Article 2 para.2 of the Council of Europe Convention on Cybercrime, it is noted that the possibility exists to restrict the criminalization with additional elements. The Convention includes a provision on the protection of the integrity of non-public transmissions by incriminating their illegal interception under Article 3.

The applicability of Article 3 of the Convention is limited to intercepting transmissions of computer data by technical means. Thus, interception of electronic data

can be defined as any data acquisition action during a transfer process [7]. The provisions of the Article 3 of the Convention applies only to the interception of data transmissions, the access to stored information is not considered as an interception of a transmission [8].

It can be seen from the Explanatory Report to the Convention on Cybercrime para. 55 [9], that the Article 3 of the Convention covers communication processes that take place in a computer system. However, the Convention does not clarify whether the provision in the Article 3 should apply only in cases where victims send data, which are then intercepted by offenders, or, if the provision in the Article 3 applies and when the offender himself/herself operates the computer system. A data transmission is considered non-public if this process is confidential [10].

According to the Convention, the offence of illegal interception of a computer data transmission is committed intentionally. The Convention does not provide a definition of the term of intention and the Explanatory Report to the Convention on Cybercrime para.39 indicates that this definition will occur at national level.

The illegal interception of a computer data transmission to fall under the Article 3 of the Convention must be carried out without right.

Article 4 of the Council of Europe Convention on Cybercrime regulates the protection of the integrity of computer data against illegal interference. The integrity of computer data is affected by the following actions: damaging, deletion, deterioration, alteration and suppression of data in a computer system. In the Explanatory Report to the Convention para.61 these terms are defined: the terms damaging and deteriorating refer to altering the integrity of data and programmes; the term deletion of data means the action of removing computer data from storage devices; the term suppression of computer data is the action that affects the availability of computer data; the term alteration of computer data refers to the action of altering existing computer data, in particular by installing destructive programmes. According to the Article 4 of the Convention, the integrity of computer data is affected intentionally.

Affecting the integrity of computer data to fall under the Article 4 of the Convention must be committed without right.

In order to protect the access of operators and users to Information and Communication Technology, the Convention provided in the Article 5 the criminalization of the hindering of the normal functioning of a computer system.

The offence of affecting the integrity of an information system is accomplished by the following actions: inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data [11]. In addition, the provisions of the Article 5 stipulate that the integrity of the computer system is seriously impaired. According to the Article 5 of the Convention, the integrity of computer systems is affected intentionally and without right.

Convention legislators set out in the Article 6 to incriminate certain deeds in connection with certain devices or access to data used for the purpose of committing offences against the confidentiality, integrity and availability of data or information systems.

Paragraph 1 (a) identifies the device designed for the purpose of committing the offence and the passwords that allow access to the computer system. The term device refers to a hardware and software structure. The Explanatory Report to the Convention on Cybercrime para.72 mentions as an example of software, a virus programme or a computer programme designed or adapted to gain access to computer systems.

Computer passwords, access codes, or similar computer data, as opposed to devices, do not perform operations but access codes.

The Convention criminalizes in paragraph 1 (a) a wide range of actions: the production, sale, procurement for use, import, distribution or otherwise making available of devices and passwords.

Paragraph 1 (b) discusses the regulations of paragraph 1 (a) in addition by criminalizing the possession of devices or passwords if they are related to the intention to commit a cybercrime.

The offence provided for in the Article 6 of the Convention must be committed intentionally and without right. At the same time, the Convention requires in the Article 6 that devices be used with the intention of committing one of the offences referred to in the Articles 2-5.

Following the debate on the need to criminalize the possession of devices, the Convention offers the option of a complex reservation in the Article 6, paragraph 3. If a Party uses this reservation, it may exclude the criminalization of the possession of instruments and of a number of illegal actions under paragraph 1 (a).

Articles 7 and 8 of the Convention refer to the computer-related offences.

The article 7 of the European Council Convention on cybercrime comprises the provisions regarding the computer-related forgery offence.

The target of a computer-related forgery offence is represented by computer data. The Convention defines in Article 1 par. b) the notion of computer data, these being „any representation of facts, information or concepts in a form for processing in a computer system, including a program suitable to cause a computer system to perform a function". Thus, the offence stipulated at article 7 of the Convention is committed by the actions of input, alteration, deletion or suppression, intentionally and without right of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. The offence stipulated at article 7 is committed intentionally and without right.

The article 7 of the Convention offers the opportunity to make a reserve in order to limit the criminality by imposing additional elements, such as the intention to fraud before the criminal liability could intervene [12].

The article 8 of the Convention, which refers to the computer-related fraud offence, stipulates the adoption of some legislative and other measures as may be necessary to establish as criminal offence according to the domestic law of a state, when committed intentionally and without right, the causing of a loss of property to another person by:

a) any input, alteration, deletion or suppression of computer data;

b) any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

In most of national systems of criminal law, the criminal act which occurred must lead to economic losses. The Convention pursues a similar concept and limits the criminalization to those acts which cause a direct economic loss. As in the case of other offences stipulated in the Convention, the computer-related fraud offence too is intentionally committed. Additionally, the Convention imposes the condition that the offender must have acted with the fraudulent intention to gain economic benefits for oneself or for other person. The offence stipulated at Article 8 of the Convention, in order to be incriminated, must be committed without right.

The Article 9 in the Convention of the European Council on cybercrime refers to the offence of child pornography. The offence consists in the following conduct, which is committed intentionally and without right by producing child pornography, offering or making available child pornography, distributing or transmitting child pornography, procuring pornographic materials having children as subjects, through a computer system.

The Article 9 of the Convention requires the following elements [13]:

-Age of the person concerned

Article 1 of the United Nations Convention on the Rights of the Child defines the term minor, this being any child below the age of eighteen years old. The Council of Europe Convention on Cybercrime defines the term minor in accordance with the United Nations Convention on the Rights of the Child. However, in recognition of the differences that exist in the national legal systems, the Council of Europe Convention on Cybercrime allows parties to be able to claim a lower age limit, which must be at least 16 years old.

-Incriminating the possession of child pornography

Possession of such pornographic material could encourage child sexual abuse, so that Convention legislators suggest that an effective way to reduce the production of child pornography materials is to criminalize the illegal possession of such materials [14].

However, the Convention allows parties in paragraph 4 of the Article 9 to eliminate the incrimination of possession of pornographic material with minors.

-Creating or integrating fictitious images

Paragraph 2 (a) of the Convention focuses directly on children abuse.

Paragraph 2 (b) and 2 (c) of the Convention covers images that where produced without violating children's rights, e.g. images that have been created through the use of 3D modelling software. The reason for the criminalization of the fictive child pornography is the fact that these images can, without necessarily creating harm to a real child, be used to seduce children into participating in such acts [15].

The Article 9 of the Convention requires that the offender is carrying out the offences intentionally. In the Explanatory Report of the Council of Europe Convention on cybercrime, the drafters of the Convention pointed out that interaction with child pornography without any intention is not covered by the Convention. Lack of intention can be relevant especially if the offender accidentally opened a webpage with child pornography and despite the fact that he/she immediately closed the website some images were stored in temp-files [16].

The offence stipulated by the Article 9 of the Convention, in order to be criminalized, must be committed without right. However, we noticed that the drafters of the Convention did not specify in which cases the Internet user is acting with authorisation.

The Convention seeks to provide fundamental principles on copyright infringement in order to harmonize the existing national legislation.

Infringements of patents or trademarks are not included in the provisions of the Article 10 of the Council of Europe Convention on Cybercrime [17].

The Convention does not outline the facts that are to be incriminated, but instead refers to a number of international treaties on intellectual property, which is one of the questionable aspects of the Article 10.

Member States that have not signed the international agreements on intellectual property are not required to sign these agreements, nor can they be forced to criminalize acts related to the international agreements that they have not signed [18].

The Council of Europe Convention on Cybercrime criminalizes only those deeds which have been committed through a computer system, intentionally and on a commercial scale. The limitation of the Convention to acts committed on a commercial

scale takes into account Trade-Related Aspects of Intellectual Property Rights Agreement (TRIPS), which provides for criminal sanctions for piracy on a commercial scale. The Article 61 of the TRIPS states that these deeds are committed intentionally [19]. The deeds provided for in Article 10 of the Convention to be incriminated must be committed without right.

Paragraph 3 of the Article 10 of the Convention allows signatories to reserve the right not to impose criminal liability under paragraphs 1 and 2 of this Article, provided that other effective remedies are available and provided that such a reservation does not infringe the international obligations incumbent upon signatories in the application of the instruments referred to in paragraphs 1 and 2 of this Article.

Conclusions

The Council of Europe Convention on Cybercrime is a guide for many countries around the world that they have used it as a legislative model when these countries have established their internal legal framework for cybercrime. Unlike other conventions or treaties, we believe that this international legal instrument is an international convention, officially debated and adopted, and this is also the legal framework governing cooperation between Member States. The Convention may be reinforced or supplemented by other additional instruments, such as the good practice guides.

The Council of Europe Convention on Cybercrime has encouraged the harmonization of cybercrime legislation worldwide. The United Nations has recommended that Member States use this Convention by developing an internal legal framework on cybercrime investigation.

Cybercrime is a phenomenon of constant change. With the change in technologies and criminal behaviour, criminal law needs to adapt to these changes, too. Thus, in the sixteen years of the Convention, new offences have emerged, such as spam, identity theft through the Internet, cyberterrorism, data spying, erotic and pornographic materials and illegal gambling on the Internet, and an update of the Convention we appreciate it is absolutely necessary.

The Convention does not explicitly criminalize spam (the unsolicited message). Convention legislators have suggested that criminalization of these acts should be limited to serious and intentional obstructions in communications [20].

Regarding the erotic and pornographic materials, Convention legislators have only focused on the harmonization of legislation on child pornography, and have excluded the incrimination of erotic and pornographic materials in a wider sense.

Not all countries have implemented provisions in the national criminal law systems that would criminalize all acts of identity theft. The only consistent elements of identity theft crimes refer to the following deeds: [21] the act of obtaining identity information; the act of holding or transferring identity information; the act of using identity information for criminal purposes. Although identity theft through the Internet is not expressly provided for in the Convention, this international legal instrument offers some solutions for criminalizing this deed. Thus, with regard to the act of obtaining information on identity, the Convention contains a number of provisions that criminalize the acts of identity theft through the Internet: illegal access (Article 2); illegal interception (Article 3); data interference (Article 4). Regarding the act of using identity information for criminal purposes, it is covered by the Convention through the Article 8, which deals with computer-related fraud. We can provide an example of computer-related fraud that uses identity theft, which is the fraud through bank cards. The act of holding or transferring identity information is not covered by the Council of Europe Convention on Cybercrime.

Even if the act of spying on computer data is not provided for in the Convention, we still believe that this act may be incriminated by the provisions of the Article 3, which refers to the illegal interception of a computer data transmission.

We note that the Council of Europe Convention on Cybercrime does not contain any provision on the criminalization of illegal Internet gambling and cyberterrorism.

In view of the six types of offences that we have just mentioned, we believe that the legislators of the Council of Europe Convention on Cybercrime should at least express a point of view on a possible criminalization of these acts in the Convention.

References

[1]Féral-Schuhl, Christiane (2010). Cyberdroit. Le droit à l' épreuve de l' Internet, Sixième Édition. Paris: Dalloz, pp. 910-912.
[2]According to the site of the Council of Europe, Retrieved 10th of November 2017 from:http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG
[3]Schjolberg, Stein (2003). The Legal Framework-Unauthorized Access To Computer Systems-Penal Legislation In 44 Countries, Retrieved 10th of November 2017 from:http://www.mosstingrett.no/info/legal.html.
[4]Gercke, Marco (2009). Council of Europe. Economic Crime Division. Directorate General of Human Rights and Legal Affairs. Strasbourg, Octopus Interface 2009, Cybercrime training for judges:Training manual(draft), March 2009, p. 27.
[5]Gercke, Marco (2012). International Telecommunication Union. Understanding Cybercrime: Phenomena, Challenges and Legal Response, p. 179.
[6]Computer Security Institute (2007). CSI Computer Crime and Security Survey 2007, p. 12.
[7]Gercke, Marco (2012). International Telecommunication Union. Understanding Cybercrime: Phenomena, Challenges and Legal Response, p. 121.
[8]Gercke, Marco (2009). Council of Europe. Economic Crime Division. Directorate General of Human Rights and Legal Affairs. Strasbourg, Octopus Interface 2009, Cybercrime training for judges:Training manual(draft), March 2009, p. 30.
[9]The Explanatory Report to the Convention on Cybercrime para. 55. Retrieved 10th of November 2017 from: http://conventions.coe.int/treaty/en/reports/html/185.htm.
[10]The Explanatory Report to the Convention on Cybercrime para. 54. Retrieved 10th of November 2017 from: http://conventions.coe.int/treaty/en/reports/html/185.htm.
[11]The Explanatory Report to the Convention on Cybercrime para. 61 and para. 66. Retrieved 10th of November 2017 from: http://conventions.coe.int/treaty/en/reports/html/185.htm.
[12]The Explanatory Report to the Convention on Cybercrime para. 85. Retrieved 10th of November 2017 from: http://conventions.coe.int/treaty/en/reports/html/185.htm.
[13]Gercke, Marco (2009). International Telecommunication Union. Understanding Cybercrime: Phenomena, Challenges and Legal Response, p. 135.
[14]The Explanatory Report to the Convention on Cybercrime para. 98. Retrieved 10th of November 2017 from: http://conventions.coe.int/treaty/en/reports/html/185.htm.
[15]The Explanatory Report to the Convention on Cybercrime para. 102. Retrieved 10th of November 2017 from: http://conventions.coe.int/treaty/en/reports/html/185.htm.
[16]Gercke, Marco (2009). International Telecommunication Union. Understanding Cybercrime: Phenomena, Challenges and Legal Response, p. 196.
[17]The Explanatory Report to the Convention on Cybercrime para. 109. Retrieved 10th of November 2017 from: http://conventions.coe.int/treaty/en/reports/html/185.htm.
[18]The Explanatory Report to the Convention on Cybercrime para. 111. Retrieved 10th of November 2017 from: http://conventions.coe.int/treaty/en/reports/html/185.htm.
[19]The Explanatory Report to the Convention on Cybercrime para. 113. Retrieved 10th of November 2017 from: http://conventions.coe.int/treaty/en/reports/html/185.htm.
[20]The Explanatory Report to the Convention on Cybercrime para. 69. Retrieved 10th of November 2017 from: http://conventions.coe.int/treaty/en/reports/html/185.htm.
[21]Gercke, Marco (2007). Council of Europe. Economic Crime Division. Directorate General of Human Rights and Legal Affairs, Internet-Related Identity Theft, pp. 19-22.