Jelena Matijašević-Obradović*

UDC343.533::004(4)
Original scientific paper

EUROPEAN STANDARDS IN THE FIELD OF COMBATING CYBER CRIME

Cyber crime is a phenomenon which is often written and spoken about, ever since its inception, in theory, judicial and legislative practice of developed countries and international institutions. It had rapidly developed in the last decade of the 20th century, and in the 21st century its evolution has become even more evident. Countries have responded by introducing new measures in their criminal legislation, in an effort to reconcile traditional criminal law with the demands for perception, investigation and demonstration of new criminal acts. This paper presents and analyzes the most significant European standards adopted in order to create more effective national legislation in the field of combating cyber crime. Standards given in the Convention of the Council of Europe but also the European Union Directives have to a large extent been a guide for national legislations in order to regulate the new situations regarding the misuse of information and communication technologies in the most adequate manner. Among other things, this paper pays special attention to the most important Convention in the field of combating cyber crime, which is the Council of Europe Convention on cyber crime, whose objectives include: harmonization of national legislations with regard to substantive provisions in the field of cyber crime, introduction of adequate instruments in national legislations with regard to process provisions in order to create the necessary basis for investigation and prosecution of offenders in this field and establishment of quick and efficient institutions and procedures for international cooperation.

Key words: cyber crime, European standards, Council of Europe conventions, European Union directives

1. Introduction

There are no technical and technological achievements in the history of mankind that has not encountered various forms of misuse. Their specificities are the phases of development in which the invention has been subject to misuse,

* Jelena Matijašević-Obradović, PhD, Assistant professor, Faculty of Law for Commerce and Judiciary, Universitey of Bussines Academy, Novi Sad, e-mail: jela_sup@yahoo.com

then groups of persons who have committed these acts and various purposes for which such misuse has been performed.

At the beginning of its implementation, computer technology was not suitable for larger misuse, since its implementation was not mass in character, so it addressed only a narrow range of users – IT professionals. What opened the door to the expansion of possibilities to misuse computer technology for various purposes is its rapid development, simplification of its use and its availability to a large number of users.

Nowadays, computers and computer technology may be misused in various manners, and crime itself may take the form of any of the traditional forms of crime, such as theft, evasion and fraud, whereas the data obtained without authorization via misuse of information systems may be used in different manners in order to obtain illegal benefits[1].

Cyber crime in terms of the Law on organization and jurisdiction of state authorities for combating cyber crime[2] is a commission of offences that contain, as the object or tool of criminal offences, computers, computer systems, computer networks, computer data and their products in its material or electronic form (Article 2 of the Law). Products in electronic form especially include computer programs and copyright works that may be used in electronic form.

Cyber crime, within its basic definition, includes the following criminal offences (Article 3 of the Law): offences against the safety of computer data as determined by the Criminal Code; offences against intellectual property, assets, economics and legal transactions, that contain, as the object or tool of criminal offences, computers, computer systems, computer networks, computer data and their products in its material or electronic form, should the number of copies of copyright work exceed 2000 or should the resulting damage exceed the amount of 1.000.000 dinars; offences against the freedoms and rights of man and citizen, sexual freedom, public law and order and constitutional order and security of the Republic of Serbia, which due to the manner of execution or means used may be considered cyber crime offences.

Cyber crime had rapidly developed in the last decade of the 20th century, and in the 21st century its evolution has become even more evident. Countries have responded by introducing new measures in their criminal legislation, in an effort to reconcile traditional criminal law with the demands for perception, investigation and demonstration of new criminal acts. After the initial period of implementation of these measures one may talk about relative success, but also the shortcomings of perceptions that currently prevail in this field need to be pointed out. Unification and harmonization, as well as efficient international cooperation, are the main prerequisites for better coordination of supranational

[1] Kreitzberg, R (1989): Kunstgriffe und Machenschaften, Kriminalistik No.8-9, Heidelberg: Kriminalistik Verlag, p. 453-458.

[2] Official Gazette of RS, no. 61/05 and 104/09

efforts in combating this type of criminal offences. Comparative analysis is not possible without reference to the only relevant international instrument in the field of cyber crime – the Council of Europe Convention on cyber crime and pointing out its significance within global frameworks.[3]

Cyber crime is a phenomenon which is often written and spoken about, ever since its inception, in theory, judicial and legislative practice of developed countries and international institutions. All its aspects are being considered. We are trying to provide more complete answers to numerous and each day more complex questions. The complexity of the issues which we have been facing for over thirty years may partly be anticipated through numerous papers in this field.

The subject of this paper is to present and analyze the most significant European standards adopted in order to create more efficient national legal solutions in the field of combating cyber crime.

2. Council of Europe standards

The Council of Europe is a regional international organization, whose headquarters are located in Strasbourg. The purpose of the Council of Europe is reflected in the achievement of basic personal and democratic rights and freedoms in Europe, and its most important acts are the adoption of the European Convention on Human Rights in 1950 and the establishment of the European Court of Human Rights in 1998 as a permanent legal protection system. The Council of Europe has 47 member states, which are also signatories to the European Convention on Human Rights, 1 candidate state and 5 observer states.

Ever since the 80s of the 20th century, the Council of Europe has been dealing with the issue of combating cyber crime. Two recommendations issued by the Committee of Ministers, which are considered as the first international document on cyber crime, are mainly devoted to the beginnings of the combat against the misuse of computer technology, such as: criminalisation of illicit behavior, separation of legal and illegal actions in national legislations, provisions on the exercise of investigations, obligations of providers to cooperate with investigating authorities etc. These are recommendations[4] that were not binding for member states, but whose primary goal was to draw attention to the emergence of a new type of criminal activities that have a strong international component and that it was made clear to the states that they need to react in a timely manner in order to prevent the spread of such illegal and malicious use

[3] Prlja, D., Reljanović, M. (2009): "Cybercrime - Comparative Experiences", Foreign legal life, 3, p.161.

[4] These are the following recommendations: Recommendation No. R (89)9 i R (95)13. Recommendation No. R (95) 13 of the Committee of Ministers to Member States, Concerning Problems of Criminal Procedure Law Connected with Information Technology

of new technologies.[5] Bearing in mind the hazards brought by the development of information technology, during the second half of the nineties the European Committee on Crime Problems – CDPC)[6] of the Council of Europe has founded an expert group, the Committee of Experts on Crime in Cyberspace – PC-CY, with a mission to prepare the text of the first international convention whose substance would include prevention, capture and punishment of offenders in the field of cyber crime.[7]

The Council of Europe Convention on cyber crime was adopted on November 23rd, 2001 in Budapest[8]. It entered into force on July 1st, 2004 and is open for signature by countries that are not members of the Council of Europe. Serbia signed the Convention on April 7th, 2005 and ratified it on April 14th, 2009 by adopting the Law on Ratification of the Convention on cyber crime.[9]

The Additional Protocol to the Convention on cyber crime concerning the criminalisation of acts of a racist and xenophobic nature, committed through computer systems was adopted in 2003. It entered into force on March 1st, 2006. Serbia has ratified the Additional Protocol by adopting the Law on Ratification of the Additional Protocol to the Convention on cyber crime concerning the criminalisation of acts of racist and xenophobic nature, committed through computer systems.[10]

3. Convention on cyber crime

The Convention has, above all, the following objectives: 1) harmonization of national legislations with regard to substantive provisions in the field of cyber crime; 2) introduction of adequate instruments in national legislations with regard to process provisions in order to create the necessary basis for investigation and prosecution of offenders in this field; 3) establishment of quick and efficient institutions and procedures for international cooperation.[11]

According to the above, "an important part of the Convention on cyber crime is dedicated to the states' obligations to create normative preconditions for the introduction of additional procedures and powers, in order to enable efficient detection and processing of cases of cyber crime. In this sense, the essential

5 Komlen-Nikolić L. *et al. (2010): Combating cyber crime,* Belgrade: Association of Public Prosecutors and Deputy Public Prosecutors of Serbia, p. 41.

6 CDPC/103/211196 decision from November 21st, 1996.

7 Komlen-Nikolić L. *et al.*

8 Council of Europe, 2001, ETS – No. 185.

9 Official Gazette of RS, no. 19/09

10 *Ibid*

11 Matijašević, J. (2013): Criminal legislation of computer crime, Novi Sad: Faculty of Law for Commerce and Judiciary in Novi Sad, University Business Academy in Novi Sad, p. 217.

importance lies in the establishment of special state authorities specialized for the combat against cyber crime. Formally and legally speaking, such obligations have become current only after the ratification of the said Convention and the Additional Protocol".[12]

The Convention consists of four chapters: (I) Use of the term; (II) Measures to be undertaken at the national level – substantive and procedural law; (III) International cooperation; (IV) Final provisions.[13]

The first chapter of the Convention provides a brief overview and definitions of basic terms used in the text of the Convention. Thus, a computer system (Article 1a) is a group of connected devices, of which at least one can perform automatic data processing; computer datum (Article 1b) is any information in a form suitable for processing in a computer system, including programs that can be used to perform certain functions of a computer; the term provider – service provider (Article 1c) is any natural or legal person that provides services that enable communication through a computer network, but also any person that keeps, or processes computer data incurred during such communication; the term datum in traffic (Article 1d) means any computer datum that is related to communication within the system or has emerged as a part of such communication and carries information about the origin and destination of communication, its path, date, time, size and duration, or type of service.

The second chapter of the Convention that includes Articles 2-22 is divided into several parts and includes substantive and procedural legal provisions. The substantive provisions stipulate nine criminal offences, grouped into four categories.

The first group of incriminating acts constitutes of acts against computers and computer systems in the narrow sense. The Convention calls this group "Offences against the confidentiality, integrity and availability of computer data and systems"[14]. This group includes the following offences:

1) Unauthorized access to information contained in a computer or computer system, in order to catch hold of, modify or destroy such information, Art. 2;
2) Unauthorized interception (wiretapping) of personal data transmitted in any way between two computers/networks, Art. 3;

[12] Milošević, M. i Nikač, Ž. (2010): "Changes in the legislation of the Republic of Serbia and the fight against cyber crime", in Petrović, S. (Ed.). Misuse of Information Technology and Privacy (str. 1-9). Belgrade: Association of Court Experts in Information Technology, p.1.

[13] Bjelajac Ž., Matijašević J., Dimitrijević D. (2012): "The importance of establishing international standards in combating cyber crime", International Politics, LXIII, 1146, p. 76-79.

[14] Offences against the confidentiality, integrity and availability of computer data and systems, Title 1, Section 1, Chapter II, Council of Europe, Convention on Cybercrime, ETS No. 185 – Explanatory Report

3) Interference with data (data disruption) on a computer in terms of intentional full or partial damage, deletion, modification of content or any other manner of changes in original data, Art. 4;
4) Interference with the system (system disruption) is an act that is equally defined as the previous criminal act, but is related to a computer system whose operation is disabled or altered via illegal access and modification of data on the network, Art. 5;
5) Misuse of devices as a general provision through which the signatory states commit themselves to punish any intentional illegal manufacture, possession, use or supply, sale and any other form of distribution and making available to anyone who is not entitled to, any device, including computer programs, as well as any form of data which may assist in the execution of criminal offences set forth in the previous Articles of the Convention, Art. 6.

The second group of incriminating acts constitutes of classic criminal acts whose execution is related to the aspect of information technologies.[15] This group includes the following offences:

1) Computer forgery – intentional, unauthorized insertion, deletion, modification or concealment of computer data, that results in altered content of such data, regardless of whether they in this way obtain a different purpose and meaning, or become unusable, Art. 7;
2) Computer fraud – intentional, unauthorized insertion, deletion, modification or concealment of computer data, as well as any other kind of interference with the operation of a computer system, in order to obtain unlawful property gain for oneself or a third person, Art. 8.

The third segment of the second chapter deals with acts that are related to the content of communication on a computer network[16] and is dedicated to criminal acts related to child pornography, in Article 9. Signatory states are obliged to criminalise the following activities as a criminal offence under national legislation: production of child pornography for the purpose of its distribution through a computer system; offering or making available child pornography through a computer system; distribution or sending child pornography through a computer system; procuring child pornography for oneself or others through a computer system; possession of child pornography on a computer system or a medium for transmission of computer data. Thus, any behavior related to child pornography is criminalised.

[15] Computer-related offences, Title 2, Section 1, Chapter II, Council of Europe, Convention on Cybercrime, ETS No. 185 – Explanatory Report

[16] Content-related offences, Title 3, Section 1, Chapter II, Council of Europe, Convention on Cybercrime, ETS No. 185 – Explanatory Report

The fourth segment of the second chapter is dedicated to criminal acts related to infringement of copyright and related rights[17] in Art. 10.

The fifth segment of the second chapter includes criminalisation of attempt to commit, assist in, and incite the said offences (Art. 11), the liability of legal persons (Art. 12) and prescription of sanctions for offences committed under the Convention (Art. 13).

Procedural law is dealt with in the second part of the second chapter of the Convention. These regulations address the procedural authorities of state bodies during the investigation of criminal acts related to new technologies. The Convention[18] has introduced some classic instruments for research of criminal acts in a new virtual environment, thereby respecting the specific nature of cyberspace.[19]

According to the Convention, competent state bodies have the authority to examine and seize any computer or data storage medium which contain or it is suspected that they may contain incriminating materials, as well as to collect data primarily related to the use of the Internet and credit cards from electronic communication providers, through which they can obtain data on potential perpetrators of a criminal act of computer crime (Art. 19 and 20). One of probably the most far-reaching provisions is related to the so-called data interception, i.e. type of wiretapping of electronic communications (Art. 21). The said measure is undertaken only when the proving of existence of an offence requires evidence collected at the time the communication is performed. Such treatment practically violates the privacy right and correspondence right, and the Convention itself does not contain any appropriate restrictions in order to prevent the misuse of such rights. It is stated that this measure shall be undertaken for "serious offences", but the Convention itself does not imply what kind of offences are those. Article 22 deals with the jurisdiction of a signatory state in case of occurrence of any offence under the Convention. The state shall have jurisdiction to prosecute should the offence be committed in its territory, on a ship or airplane carrying its flag, and should the offence be committed by a citizen of that state, provided that it is in another state that acknowledges the same kind of criminalisation, or outside the state territory (e.g. international waters).

The third part of the Convention[20] deals with international cooperation of states in combating computer crime, primarily in the way that should overcome

[17] Offences related to infringements of copyright and related rights, Title 4, Section 1, Chapter II, Council of Europe, Convention on Cybercrime, ETS No. 185 – Explanatory Report

[18] Procedural legal part of the Convention: Articles. 14-22., Council of Europe, Convention on Cybercrime, ETS No. 185 – Explanatory Report

[19] Prlja, D., Reljanović, M., p.62-63.

[20] Third part of the Convention: Articles. 23-35., Council of Europe, Convention on Cybercrime, ETS No. 185 – Explanatory Report

practical obstacles in the implementation of national legislation for offences that typically cross national boundaries, and often involve the participation of individuals from several countries around the world.[21] The main provisions of this act are dedicated to the cooperation of states in an organized or spontaneous exchange of data concerning possible execution of a criminal offence related to the use of electronic communications, as well as the possibility of extraditing the perpetrators of such offences from one signatory state to another (Art. 26). Each signatory state must entrust a particular body the task of cooperation with other states in the field of computer crime, and in case of emergency, the cooperation can be established directly between judicial authorities of the two countries, as well as through Interpol and other relevant channels of cooperation (Art. 27). According to Art. 31 each signatory state may request from another one to carry out certain investigations in its territory should it be necessary for the purposes of investigation in relation to some of the offences provided for in the Convention.

When it comes to extradition, there are situations where the state is not obliged to extradite a person. This is especially the case when there is a lack of double criminalisation, but the Convention also provides an additional condition – the act must be labeled as serious within the law itself, i.e. its execution should be punishable by a minimum sentence of one year in prison, unless provided otherwise by some other international agreement among states in question, that may be applied in a given situation (Art. 24). Also, among states that do not have mutual bilateral or multilateral extradition treaties, the Convention shall serve as the basis for extradition.[22]

There is also an interesting provision regarding the establishment of a 24/7 network in each country, that would serve as support to police and other authorities, as contact for all information and a starting point for all requests concerning the processing and investigation of criminal acts of computer crime (Art. 35).

4. Additional Protocol to the Convention on cyber crime concerning the criminalisation of acts of a racist and xenophobic nature, committed through computer systems

Additional Protocol to the Convention on cyber crime concerning the criminalisation of acts of a racist and xenophobic nature, committed through computer systems[23] was adopted on January 28th, 2003 and came into force on March 1st, 2006.

[21] Prlja, D., Reljanović, M., p.62-63.

[22] Matijašević J., p. 220.

[23] Council of Europe, 2003, CETS No.: 189

In addition to the Preamble, the Additional Protocol consists of four chapters: I – Common provisions, II – Measures to be taken at national level, III – Relations between the Convention and this Protocol, IV – Final provisions.

The main purpose of the adoption of this Protocol is the criminalisation of behavior that is not covered by the Convention, and which is related to the spread of hatred, intolerance and animosity towards racial, national, religious and other groups and communities, use of computers as a means of communication and dissemination of propaganda.[24]

For the purpose of this Protocol, "racist and xenophobic material" is any written material, any image or any other representation of ideas or theories that advocate, promote or incite hatred, discrimination or violence, against any individual or group of individuals, based on race, skin color, inherited, national or ethnic origin, as well as religion, if used as a pretext for any of these factors (Article 2 of the Protocol).

In the second chapter, entitled "Measures to be taken at national level", the Protocol introduces an obligation for signatory states to criminalise the following conducts in the national legislation:

1.) Dissemination of racist and xenophobic material through computer systems (Article 3 of the Protocol) – means any action by which this kind of material is made available to the public, using a computer or a computer system.

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: distributing, or otherwise making available, racist and xenophobic material to the public through a computer system. (paragraph 1, Article 3 of the Protocol).

A Party may reserve the right not to attach criminal liability to conduct as defined by paragraph 1 of this article, where the material, as defined in Article 2, paragraph 1, advocates, promotes or incites discrimination that is not associated with hatred or violence, provided that other effective remedies are available. (paragraph 2, Article 3 of the Protocol).

Notwithstanding paragraph 2, a Party may reserve the right not to apply paragraph 1 to those cases of discrimination for which, due to established principles in its national legal system concerning freedom of expression, it cannot provide for effective remedies as referred to in the said paragraph 2 (paragraph 3, Article 3 of the Protocol).

2.) Racist and xenophobic motivated threat (Article 4 of the Protocol) – is presenting to an individual or a group that a serious criminal offense shall be committed against them, as defined in the domestic legislation of countries, through a computer or computer systems. An individual or group should be dis-

[24] Komlen-Nikolić L. et al. p. 52.

tinguished according to their race, skin color, origin, national, ethnic or religious affiliation, in order for this offence to obtain a specific form provided by the Protocol.

Specifically, "Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: threatening, through a computer system, with the commission of a serious criminal offence as defined under its domestic law, (i) persons for the reason that they belong to a group, distinguished by race, color, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors, or (ii) a group of persons which is distinguished by any of these characteristics" (Article 4).

3.) Racist and xenophobic motivated insult (Article 5) – has the same elements as the previous case, but does not concern threats but insulting an individual or a group, based on race, skin color, origin, national, ethnic or religious affiliation.

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: insulting publicly, through a computer system, (i) persons for the reason that they belong to a group distinguished by race, color, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors; or (ii) a group of persons which is distinguished by any of these characteristics (paragraph 1, Article 5 of the Protocol).

A Party may: a) require that the offence referred to in paragraph 1 of this Article has the effect that the person or group of persons referred to in paragraph 1 is exposed to hatred, contempt or ridicule; or b) reserve the right not to apply, in whole or in part, paragraph 1 of this Article. (paragraph 2, Article 5 of the Protocol).

4.) Denial, gross minimization, approval or justification of genocide or crimes against humanity (Article 6) – introduces an interesting concept of punishment for alleged actions committed through computers or computer systems in cases that were subject to decisions by international courts. This kind of content must be somehow made available to a larger number of people who use computers and the Internet or any other computer network.

Each Party shall adopt such legislative measures as may be necessary to establish the following conduct as criminal offences under its domestic law, when committed intentionally and without right: distributing or otherwise making available, through a computer system to the public, material which denies, grossly minimizes, approves or justifies acts constituting genocide or crimes against humanity, as defined by international law and recognized as such

by final and binding decisions of the International Military Tribunal, established by the London Agreement of 8 August 1945, or of any other international court established by relevant international instruments and whose jurisdiction is recognized by that Party (paragraph 1, Article 6 of the Protocol).

A Party may: a) require that the denial or the gross minimization referred to in paragraph 1 of this Article is committed with the intent to incite hatred, discrimination or violence against any individual or group of individuals, based on race, color, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors, or otherwise b) reserve the right not to apply, in whole or in part, paragraph 1 of this Article. (paragraph 2, Article 6 of the Protocol).

5.) Aiding and abetting (Article 7) - Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, aiding or abetting the commission of any of the offences established in accordance with this Protocol, with intent that such offence be committed.

The third chapter, entitled "Relations between the Convention and this Protocol" specifies which provisions of the Convention shall be applied to this Protocol mutatis mutandis, as well as the provisions of the Convention whose scope may be extended to the application of the Protocol by each Party.

5. Convention for the Protection of individuals with regard to automatic processing of personal data

Convention for the Protection of individuals with regard to automatic processing of personal data[25] was opened for signature to member states on January 28th, 1981, and came into legal force on October 1st, 1985.

Namely, it is necessary that the persons who have access to information and data stored in computers and computer systems are prevented and disabled to commit fraud or any illegal use of such data. This approach is particularly significant in situations of so called "cross-border information flow", since it has turned out that the quality of personal data protection gets weaker as the observed space expands geographically. On the other hand, when this issue is observed within national frameworks, it may be noted that not all national legislations provide a sufficient level of protection to the citizens in this field.

The Convention is related to personal data collected in both public and private sectors. The essential part of the Convention contains substantive provisions in the form of basic principles that apply to all major segments in this field (quality and categories of data collected, security, safety measures,

[25] Council of Europe, 1981, ETS – No. 108.

exceptions and limitations, sanctions etc.). The Convention also resolves the issue of cross-border traffic of automatically collected personal data, and provides mechanisms of cooperation of the contracting states.

The intention of the Convention is that the signatory states harmonize their national legislations with the basic principles and recommendations contained in this document. Respecting the rule of law, human rights and basic freedoms, the Convention intends to bring its members together, to extend the protection of basic rights and freedoms of individuals, especially the right of privacy, when it comes to automatic processing of personal data. The states have the initiative to, in the process of regulation of this matter, decide on the content, scope and coverage of personal data protection, with the possibility of expressing certain specificities. In doing so, each state must adhere to the principles established.[26]

One of the basic principles of personal data protection is the principle of legality and impartiality. This means that personal data are collected, processed and used in accordance with the law. (…) This also implies that personal data are collected, processed and used impartially and in a manner that does not injure the personal dignity of man. (…) Regulations governing the protection of personal data should also include provisions based on the principle of data accuracy. (…) The rights of persons whose data are collected and processed to be informed of which collections contain data related to them, which data, who processes them, for what purpose and on what basis, as well as who are users of such data, are all contained in the principle of purpose determination. (…) The principle of data availability, which includes the right of the person whose data are recorded to be informed of the existence of a collection or other records containing personal data, the right to have access to his personal data, to request the correction of inaccurate data related to him, delete the data should their processing be against the law or contract, prohibit the use of inaccurate, outdated and incomplete data related to him, i.e. to prohibit the use of such data should they not be used in accordance with the law or contract. The rights stipulated by the principle of purpose determination and principle of data availability to the person whose data are collected and processed, may be restricted and be used to the extent necessary for the protection of national security, public safety, monetary interests of the state or the suppression of criminal offences, as well as rights and freedoms of others.[27]

[26] Prlja, D., Reljanović, M., Ivanović, Z. (2012): "Internet Law", Belgrade: Institute of Comparative Law, p. 91.

[27] *Ibid*

6. Convention on the Protection of children against exual exploitation and sexual abuse

Convention on the Protection of children against sexual exploitation and sexual abuse[28] was opened for signature to member states on October 25th, 2007, and came into legal force on July 1st, 2010.

The purpose of the Convention is to establish the possibilities for more effective criminal proceedings in which children appear as victims of sexual exploitation and abuse.

From the aspect of combat against cyber crime, the Convention is a backbone for harmonization of national legislations with regard to substantive criminal law in all cases in which the elements of computer technology are used for the purpose of distribution, exchange and storage of illegal content. The Convention, among other things, has been implemented due to a perceived increase in the degree of sexual exploitation of children, especially in the form of child pornography and prostitution, as well as all other forms of child abuse that are destructive to children's health and their psychosocial development. Particularly noteworthy is the significance of considering the need for preparing a comprehensive international instrument for the prevention, protection and criminal and legal aspect of the combat against all forms of sexual exploitation and sexual abuse of children, with particular importance being put on the creation of a special mechanism for monitoring the implementation of the Convention.

The Convention contains the following chapters: I - Purposes, non-discrimination principle and definitions; II – Preventive measures; III - Specialised authorities and co-ordinating bodies; IV - Protective measures and assistance to victims; V - Intervention programmes or measures; VI – Substantive criminal law; VII - Investigation, prosecution and procedural law; VIII - Recording and storing of data; IX – International co-operation; X – Monitoring mechanism; XI - Relationship with other international instruments; XII - Amendments to the Convention; XIII – Final clauses.

The purposes of this Convention are to (paragraph 1, Article 1 of the Convention): a) prevent and combat sexual exploitation and sexual abuse of children; b) protect the rights of child victims of sexual exploitation and sexual abuse; c) promote national and international co-operation against sexual exploitation and sexual abuse of children.

It is interesting to mention the types of preventive measures foregrounded by the Convention in order to prevent all forms of sexual exploitation and sexual abuse of children and the protection of children. These measures are the following: recruitment, training and awareness raising of persons working in contact with children (Article 5), education for children (Article 6), preventive intervention programmes or measures (Article 7), measures for the general

[28] Council of Europe, 2007, CETS No. 201.

public (Article 8), participation of children, the private sector, the media and civil society (Article 9).

The chapter that is related to substantive criminal includes the following offences: sexual abuse (Article 18), offences concerning child prostitution (Article 19), offences concerning child pornography (Article 20), offences concerning the participation of a child in pornographic performances (Article 21), corruption of children in order to perform sexual abuse, where the act is considered finished at the moment of recruitment/corruption of the child (Article 22), acts that include misuse of information and communication technology in order to promote pornographic material for the purpose of committing any of the above acts and the performance of such act (Article 23).

In relation to the misuse of computers and information technology in general, stress is put on criminal offences related to child pornography (Article 20 of the Convention) which, at the national level, recommends the criminalization of producing child pornography, offering or making available such materials, as well as their distributing or transmitting, procuring child pornography for oneself or for another person, possessing such material, as well as knowingly obtaining access, through information and communication technologies, to child pornography.

In the chapter relating to investigating, prosecuting and court proceedings, the Convention requires that each signatory state takes the necessary legislative or other measures to ensure that investigations and criminal proceedings are carried out in the best interests and respecting the rights of the child. Also, each state should adopt a protective approach towards victims, ensuring that the investigations and criminal proceedings do not aggravate the trauma experienced by the child, and that, in doing so, the proceedings are treated as priority and carried out without any unjustified delay (Article 30).

7. Convention on the prevention of terrorism

With regard to the combat against terrorism, in 1977 the Council of Europe adopted the Convention on the suppression of terrorism, amended in 2005 by the Convention on the prevention of terrorism[29], which entered into force on December 1st, 2009.

The part which in details presents the manifestations of computer crime, also shows the manners of connecting and impact of terrorism and information technology. It is pointed out that information technologies may be targets of terrorist organization attacks[30], but the capacities of computer technology can be

[29] Council of Europe, 2005, CETS No. 196

[30] More recently, the term "cyberterrorism" has been used as a special kind of terrorist attacks that are directed towards computer systems and networks with the intention of achieving certain political goals.

used for distribution of various content, as well as raising funds that enable further terrorist activity (spreading propaganda, sending threats, fundraising etc.). Finally, the Internet as a global network serves also as a means of communication among group members, as well as an instrument of planning and support.

Important articles of the Convention are Articles 5-7, which are related to certain preparation acts that are of such quality and importance that they have the potential to cause or assist terrorist acts (public invitations, recruiting for the commission of terrorist acts, training future terrorists).

Article 5 of the Convention is related to "Public provocation to commit a terrorist offence".

For the purposes of the Convention, "public provocation to commit a terrorist offence" means the distribution, or otherwise making available, of a message to the public, with the intent to incite the commission of a terrorist offence, where such conduct, whether or not directly advocating terrorist offences, causes a danger that one or more such offences may be committed (paragraph 1, Article 5).

Each Party shall adopt such measures as may be necessary to establish public provocation to commit a terrorist offence, as defined in paragraph 1, when committed unlawfully and intentionally, as a criminal offence under its domestic law (paragraph 2, Article 5).

Article 6 of the Convention is related to "Recruitment for terrorism".

For the purposes of this Convention, "recruitment for terrorism" means to solicit another person to commit or participate in the commission of a terrorist offence, or to join an association or group, for the purpose of contributing to the commission of one or more terrorist offences by the association or the group (paragraph 1, Article 6).

Each Party shall adopt such measures as may be necessary to establish recruitment for terrorism, as defined in paragraph 1, when committed unlawfully and intentionally, as a criminal offence under its domestic law (paragraph 2, Article 6).

Article 7 of the Convention refers to "Training for terrorism". For the purposes of this Convention, "training for terrorism" means to provide instruction in the making or use of explosives, firearms or other weapons or noxious or hazardous substances, or in other specific methods or techniques, for the purpose of carrying out or contributing to the commission of a terrorist offence, knowing that the skills provided are intended to be used for this purpose.

8. European Union standards

Apart from the fact that it recommends to the member states to sign and adopt the conventions and conclusions of the Council of Europe, the European Union has adopted specific acts aimed at effective combat against cyber crime.

In September 1990, the Commission of the European Community published a decision in the field of information security, which consisted of six sections related to personal data protection and information security. This decision upheld, for a period of two years, an activity plan that did not explicitly involve criminal law assistance, but included the following activities: development of strategic order of information security, analysis of needs for information security, solutions for emergency and temporary needs, specification, standardization and verification of information security, integration of technological and operational achievements within information security through general strategy and integration of reliable security functions into the information system.[31]

In 2000, within the framework of the European Union, the Directive on electronic commerce[32] was adopted, and paid special attention to the problem of malevolence, but also numerous other acts, from the Decision of the Council of Europe on the prevention of child pornography on the Internet, to the recommendations and strategies for the new millennium on the protection and control of computer crime. Each of these acts is an act of constructing a safer information society through improvement of security of information infrastructure and the combat against computer crime.

There are two Directives that are significant in the combat against cyber crime, which are presented below.

9. Directive of the Council of the European Community on the legal protection of computer programmes

This Directive,[33] was published in the "Official Journal of the European Community" on May 17th, 1991, with the duty of implementation in the member states, starting from January 1st, 1993, prior to which date they had been obliged to harmonize their national legislation with the content of the Directive. The need for uniform solutions in the field of legal protection of computer programs was imposed by the differences in national legislations of member states, that had an adverse impact on the functioning of the common market.

In accordance with the provisions of the Directive, the member states protect computer programs by copyright as literary works, in terms of the provisions of

[31] Sieber, U. (1992): The International Emergence of Criminal Information Law, Köln: Carl Heymanns Verlag KG, p. 80.

[32] EC. (2000): Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), Official Journal of the European Communities, L 178, 17. 07. 2000

[33] EEC. (1991): Council Directive 91/250/EEC of 14 May 1991 on the Legal Protection of Computer Programs, Official Journal L 122/42, Done at Brussels, 17/05/1991 P. 0042 – 0046

the Berne Convention for the protection of literary and artistic works, and the term "computer program" includes the preparatory design material. The concept of computer program author has also been determined, and legal protection is offered to any natural or legal person falling under the provisions of national legislations in the field of copyright law applicable to literary works.

The Directive provides for an obligation to sanction precisely specified conduct, duration of protection provided for computer programs, and also prescribes the obligation of seizure of any illegal copy of a computer program in accordance with the procedure laid down by procedural rules of national legislations.

10. Directive 2006/24/EU of the European Parliament and of the Council on storing data generated or processed in the provision of publicly available electronic communications services or of public communications networks

From the standpoint of efficient detection and prosecution of any criminal offences whose execution leaves "electronic trails" that in properly conducted proceedings may gain the force of incontrovertible evidence before the court, this Directive,[34] as well as the procedures set out in its provisions, represents an essential step towards the suppression of activities that endanger the security of computer data.

The main objective of the Directive is to harmonize the provisions of the member states concerning the obligations of providers of publicly available electronic communications services and public communications networks to store certain data received or processed in order to ensure that these data are available for the purpose of investigation, detection and prosecution of serious criminal offences. It should be noted that the Directive is applied only to the data on traffic and location of legal and natural persons and to the related data necessary for the identification of the subscriber or registered user.

For the purposes of the Directive, at the beginning, there are definitions of the most significant terms, and in Art. 4 there is a rule who and under what conditions may gain a right of access to information of a member state. The central part of the Directive is the categorization of data stored, which are enumerated and sorted into categories and subcategories. In accordance with the provisions, the member states undertake to store all of the said data categories for a period of not less than six months nor more than two years from the date of communication (Art. 6), and the provisions of the Directive also regulate the issue of legal protection of persons whose data are collected and stored for a certain period of time.

[34] EC, 2006, L 105.

11. Conclusion

Although today life and functioning of a society as a whole is impossible without the use of computers and modern information technology, we are experiencing growth in the awareness that these useful and necessary assets may be used for illicit, illegal purposes, primarily for obtaining illegal material gain for a certain person or for causing harm to others. Since our society has, in recent years, recorded numerous cases of computer misuse for criminal purposes, it is high time to recognize the need for striving towards adequate legislation in the field of cyber crime, which will to some extent be able to respond to the irresponsible conduct of individuals and groups in this segment.

Hundreds of millions of people who daily use cyberspace for business or personal use often do not have enough attention, time or will to properly protect themselves and get to know potential mishaps that may befall them if they are gullible or not serious enough when entering into various types of transactions or communications. The fact is that many classic criminal acts may be committed on the Internet, as well as that through obtaining information about users one may prepare or enable the execution of almost any criminal offence against life and physical integrity, property, copyright and many others. In addition there are crimes whose emergence and development are related exclusively to the development of electronic communications and the Internet. It is a wide range of conducts that may be harmless, but also may lead to the most serious crimes. All these illegal conducts are included in the definition of new criminal offences that follows a series of procedural and forensic specificities.[35]

This paper presents and analyzes the most significant European standards adopted in order to create more effective national legislation in the field of combating cyber crime. Standards given in the Convention of the Council of Europe, with special regard to the Convention on cyber crime, but also the Directives of the European Union, have to a large extent been a guide for national legislations in order to regulate the new situations regarding the misuse of information and communication technologies in the most adequate manner.

Literature

- Bjelajac Ž., Matijašević J., Dimitrijević D. (2012): "The importance of establishing international standards in combating cyber crime", *International Politics*, LXIII, 1146, p. 66-84
- Council of Europe (2001, November 23): *Convention on Cybercrime*, European Treaty Series – No. 185, Budapest

[35] Prlja, D., Reljanović, M., Ivanović, Z., p. 152.

- Council of Europe (1981, January 28): *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, European Treaty Series - No. 108.
- Council of Europe (2007, October 25): *Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse*, CETS No. 201, Lanzarote
- Council of Europe (2005, May 26): *Convention on the Prevention of Terrorism*, CETS No. 196, Warsaw
- EEC. (1991): Council Directive 91/250/EEC of 14 May 1991 on the Legal Protection of Computer Programs, *Official Journal* L 122/42, Done at Brussels, 17/05/1991 P. 0042 – 0046
- EC. (2000): Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), *Official Journal of the European Communities*, L 178, 17. 07. 2000
- EC. (2006): Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, *Official Journal* L 105 , 13/04/2006 P. 0054 – 0063
- Komlen-Nikolić L., Gvozdenović R., Radulović S., Milosavljević A., Jeković R., Živković V., Živanović S., Reljanović M., Aleksić I. (2010): *Combating cyber crime*, Belgrade: Association of Public Prosecutors and Deputy Public Prosecutors of Serbia
- Kreitzberg, R (1989): *Kunstgriffe und Machenschaften, Kriminalistik No.8-9*, Heidelberg: Kriminalistik Verlag
- Matijašević, J. (2013): *Criminal legislation of computer crime*, Novi Sad: Faculty of Law for Commerce and Judiciary in Novi Sad, University Business Academy in Novi Sad
- Milošević, M. i Nikač, Ž. (2010): "Changes in the legislation of the Republic of Serbia and the fight against cyber crime", in Petrović, S. (Ed.). *Misuse of Information Technology and Privacy* (str. 1-9). Belgrade: Association of Court Experts in Information Technology
- Prlja, D., Reljanović, M. (2009): "Cybercrime - Comparative Experiences", *Foreign legal life*, 3, 161-184.
- Prlja, D., Reljanović, M. (2010): *Legal Informatics*, Belgrade: Faculty of Law of Union University, Public Enterprise „Official Gazette"
- Prlja, D., Reljanović, M., Ivanović, Z. (2012): "*Internet Law*", Belgrade: Institute of Comparative Law

- Sieber, U. (1992): *The International Emergence of Criminal Information Law*, Köln: Carl Heymanns Verlag KG
- Law on Organization and Jurisdiction of Government Authorities in fight against cyber crime, Official Gazette RS, no. 61 (2005) and 104 (2009)
- Law on Ratification of the Convention on Cybercrime, Official Gazette RS, no. 19 (2009)
- Law on Ratification of Additional Protocol to the Convention on cyber crime concerning the criminalisation of acts of a racist and xenophobic nature, committed through computer systems, Official Gazette RS, no. 19 (2009)

Paper received: October 13th, 2014
Approved for publication: November 5th, 2014

Rad primljen: 13. oktobar 2014.
Odobren za štampu: 5. novembar 2014.

Doc. dr Jelena Matijašević-Obradović,
Pravni fakultet za privredu i pravosuđe u Novom Sadu,
Univerzitet Privredna akademija u Novom Sadu

EVROPSKI STANDARDI U OBLASTI SUZBIJANJA VISOKOTEHNOLOŠKOG KRIMINALA

S a ž e t a k

Visokotehnološki kriminal je pojava o kojoj se, od samog njenog nastanka, u teoriji, sudskoj i zakonodavnoj praksi razvijenih država i međunarodnih institucija, dosta piše i govori. Naglo se razvila u poslednjoj deceniji XX veka, a u XXI veku njegova evolucija je još evidentnija. Države su odgovorile uvođenjem novih mera u svoja krivična zakonodavstva, pokušavajući da pomire tradicionalno krivično pravo sa zahtevima za percipiranjem, istraživanjem i dokazivanjem novih krivičnih dela. U radu su predstavljeni i analizirani najznačajniji evropski standardi usvojeni u cilju stvaranja što efikasnijih nacionalnih zakonskih rešenja u oblasti suzbijanja visokotehnološkog kriminala. Standardi dati u Konvencijama Saveta Evrope, ali i Direktivama Evropske unije, u velikoj meri su vodilja nacionalnim zakonodavstvima kako bi se nove situacije u vezi sa zloupotrebama informaciono-komunikacionih tehnologija, što adekvatnije pravno regulisale. Između ostalih, u radu je posebna pažnja posvećena najznačajnijoj Konvenciji u oblasti suzbijanja visokotehnološkog kriminala, a to je Konvencija Saveta Evrope o visokotehnološkom kriminalu, čiji su ciljevi: usklađivanje nacionalnih zakonodavstava kada je reč o materijalnim odredredbama u oblasti visokotehnološkog kriminala, uvođenje adekvatnih instrumenata u nacionalna zakonodavstva kada je reč o procesnim odredbama u cilju stvaranja neophodnih osnova za istragu i krivično gonjenje učinilaca krivičnih dela iz ove oblasti i ustanovljavanje brzih i efikasnih institucija i procedura međunarodne saradnje

Ključne reči: visokotehnološki kriminal, evropski standardi, konvencije Saveta Evrope, direktive Evropske unije