aktuelna tema

Mina Zirojević[*]

UDK: 004:343
BIBLID: 0352-3713 (2015); 32, (4-6): 1–15
ORIGINALNI NAUČNI RAD

COMPUTER RELATED CRIME – THE DECISION OF THE COUNCIL OF EUROPE[1]

ABSTRACT: The significance of information and communication technologies has created the need to establish worldwide measures and mechanisms for the protection of both the society and individual against abuses in this area, through adopting appropriate legislative solutions and improving the international cooperation. The result of these efforts, among other things, is the adoption of the Council of Europe Convention on Cybercrime, which has, in the opinion of the international community, established minimum standards that are necessary to meet the national legislation in order to effectively combat the abuse of high technology.[2]

Key words: the Internet, abuse, the Council of Europe, Conventions.

The Decision of the Council of Europe

A. The Convention on Cybercrime

The Council of Europe Convention on Cybercrime was signed in Budapest on 23rd November 2001, and the Additional Protocol referring to the criminalization of acts of a racist and xenophobic nature committed through

[*] LLD Institute of Comparative Law, Belgrade, e–mail: mina.zirojevic@gmail.com

[1] The paper is a part of scientific research and engagement of researchers on the project "Serbian and European law – comparison and harmonization". The Project number 179033 funded by the Ministry of Science and Technological Development and implemented by the Institute for Comparative Law in the period 2011-2014.

[2] The Convention on Cybercrime, the Council of Europe, Budapest, 23rd 2001.; European Treaty Series (ETS) - No. 185 <http://conventions.coe.int/Treaty/en/Treaties/Word/185.doc> (August 5th, 2010).

computer systems was signed in Strasbourg on 28th January 2003. Republic of Serbia signed both documents in Helsinki in 2005, and in 2009 the National Assembly of Republic of Serbia ratified them. By ratifying the Convention and Additional Protocol there should essentially have been innovated all laws that directly or indirectly regulated the area of information and communication technologies, and particularly the laws governing criminal-legal protection of these areas. In this way, the institutional framework was created for a more effective fight against cybercrime.

The Convention defines a total of nine offenses that are classified into four groups.

The Convention consists of four sections: [3]

(I) The use of the term;

(II) Measures to be taken at a national level – substantive criminal law, procedural law and the jurisdiction of the Contracting Parties for the criminal acts prescribed in accordance with the Convention;

(III) International cooperation – general principles, specific provisions;

(IV) Final Provisions.

The first chapter gives a brief overview of the Convention and definitions of key terms used in the text of the Convention.

The second chapter of the Convention, which includes Articles 2 - 22, is divided into several sections and includes substantive and procedural provisions. Within the substantive provisions, there are stipulated nine offenses being grouped into four categories.

The first group of alleged acts constitutes crimes against computers and computer systems in the strict sense. The Convention has named this group as: Criminal offenses against the confidentiality, integrity and availability of computer data and systems.[4]

The second group of criminal acts constitutes crimes classic whose execution is linked to computers as computer related acts.

The third part of the second chapter deals with the criminal acts that are related to the content of the communication on a computer network and it is dedicated to the related crime so- called "Child pornography", or exploitation of children (or minors) in pornography in Article 9 (Offences related to child pornography, Article 9). The States Parties shall, under the national

[3] "The Official gazette of RS", no. 19/09

[4] Offences against the confidentiality, integrity and availability of computer data and systems, Title 1, Section 1, Chapter II, the Council of Europe, the Convention on Cybercrime, ETS No. 185 – Explanatory Report; <http://www.conventions.coe.int/Treaty/en/Reports/Html/185.htm> (December 20th, 2013).

legislation, incriminate the following activities: the production of the child pornography for the purpose of its distributing through a computer system; offering or making the child pornography available through a computer system; the distribution or sending the child pornography through a computer system; procuring the child pornography for oneself or other person through a computer system; the possession of the child pornography in a computer system or on a medium for the transmission of computer data. So, there should be criminalized any behaviour related to the child pornography.

The fourth segment of the second chapter is devoted to criminal offenses related to copyright and related rights in the Article 10 (Offences related to infringements of copyright and related rights, Article 10). The Convention does not devote much space to this problem, primarily because in the field of copyright and related rights there are relevant international instruments, whose scope is now extended to the execution of the alleged acts using computers and computer networks. Therefore, it criminalizes copyright infringement by the definition contained in existing international treaties.

The fifth segment of the second chapter covers the criminalization of attempt to commit, aiding and abetting of the offenses (Article 11), the liability of legal persons (Article 12) and prescribing penalties for offenses committed under the Convention (Article 13).

The second part of the second chapter of the Convention is devoted to the criminal procedure law. These provisions deal with the procedural powers of government bodies in investigations of criminal offenses related to new technologies. The Convention introduces some classic instruments of investigation of criminal offenses in the new virtual environment, thus respecting the specific nature of cyberspace.[5]

In addition to general provisions that require from the states to include the crimes in question in their criminal law, as well as other acts which are not found in the text of the Convention which may be subsumed under this group, a great attention is paid to the method of collecting the data stored on computers or portable devices, and the protection of basic individual rights guaranteed by the European Convention on Human Rights and the Covenant on Human rights of the UN.[6]

Procedural rules should be complied with in respect of the offenses provided by the previously described members of the Convention, as well as the

[5] The procedural part of the Convention: Articles. 14-22., the Council of Europe, the Convention on Cybercrime, ETS No. 185 – Explanatory Report; <http://www.conventions.coe.int/Treaty/en/Reports/Html/185.htm> (December 20th, 2013)

[6] Article 15. of the Convention.

other criminal acts committed by computers, computer systems and networks, as well as in finding, developing, providing and collecting clues in an electronic form related to such offenses.[7]

Under the Convention, the competent national authorities shall have the authority to search and seize any computer or data storage medium on which they are, or where there is a suspicion that they may contain the incriminating materials, as well as from the provider of electronic communications they can collect the data relating primarily to the use of the Internet and credit cards through which one can get information about a potential perpetrator of the offense of cybercrime (Articles 19 and 20). Also, the authorities responsible for prosecuting criminal acts and perpetrators have the powers: to order or similarly obtain or achieve the expeditious preservation of the specified computer data, including the traffic data that have been stored by means of a computer system in those cases where there is reasonable suspicion that the data subject changes or can be lost; [8] to order the surrender of certain computer data to certain persons in whose possession there are included in a particular computer system or a particular medium for storing data; as well as the Internet providers to hand over information about users of services related to such services, which are owned by the Internet Service Provider or its *de facto* authorities; to require a partial disclosure of the traffic data; to review (search) and seizure every computer or a part of computer and data stored on them, as well as a medium for storing of the computer data if there is a reasonable suspicion that they could be considered as incriminating materials; as well as to collect the data relating primarily to the use of the Internet and credit cards from the provider of electronic communications, and on the basis of which there may be the name or IP address of a potential perpetrator of a crime.

The third part of the Convention is dealing with the international cooperation of states in combatting a computer crime, and above all the manner for overwhelming practical obstacles in enforcement of national legislative

[7] http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legislation.pdf p.19. available on 14th March 2010

[8] Article 16 of the Convention. Those data are those which were not deleted until issuing of order. This kind of measure for obtaining data can last up to 90 days by the Convention. Also, there is no obligation of ISP to deliver these data to law enforcement agencies; they should obtain them by themselves. It is important to stress that this power is different than the power of data retention. Nature of communications and contemporary forms of communicating through these channels forces creators of measures to divide forms of activities with data, because of service providers and service users, but as well law enforcement personnel. But the Convention just gives a framework for this and it is on the parties to prescribe their own measures and measures for protecting all communication parties in the communication traffic.

solutions embodied in criminal acts which normally cross borders of national boundaries, and also include involvement of individuals from different countries all over the world. The Convention prescribes general principles of the international cooperation in Article 23, general principles of extradition in Article 24, general principles on mutual legal assistance in Article 25, even in cases of missing of applicable international treaties (Article 27). Articles 29 and 30 deal with the expedited preservation of the recorded computer data at the international level and the expedited preservation of the recorded communication traffic at the international level again. Especially Article 31 is dealing with accessing to the recorded computer data within a framework of mutual legal assistance and Articles 33 and 34 cover gathering the information about traffic in real time and the interception of the content data at the international level. Article 35 brings, in the course of expedited acting especially in cases of preserving of communication data in other states, a network of 24/7 points of contact.[9] It is conceived to support the police and other authorities, as well as the contact for all information and the starting point for all requirements concerning the prosecution and investigation of cybercrimes. States are left to correct in practice the existing differences through additional bilateral agreements, and to further specify the kind of cooperation for which there is a special interest. According to Article 31, each State Party may request the other one to carry out a specific investigation on its territory if it is necessary for the purposes of an investigation in a connection with any of the offenses provided for in the Convention.

When the Extradition is about, there are situations where a state shall not be obliged to extradite a person. This is primarily the case when it comes to the lack of dual criminality, but the Convention provides an additional condition – the criminal act must be labelled as seriously in the law itself, or, for its enforcement, it shall be punishable by a minimum sentence of one year imprisonment, except as otherwise provided in some other international agreement between states in terms that can be applied to a given situation (Article 24). Also, among the countries having reciprocal bilateral or multilateral extradition treaties, the Convention shall serve as the basis for extradition.

The provision concerning the establishment of 24/7 network with points in each country will serve as support for the police and other authorities, as well as the contact for all information and the starting point for all

[9] This cooperation incorporates: providing of technical advice, securing and expedited preserving of the traffic data and data of communication content, finding and gathering of the data and traces of the committed criminal act.

requirements concerning the prosecution and investigation of computer crime offenses (Article 35).

The Convention is specific by its, again, negative aspect, which could be sought earlier in the text – the specificity of the slow ratification by the developed countries. Talking about the modern technology, the highly developed countries which have ratified the Convention are the United States (2006), France, Denmark and Norway. The same hasn't been signed by Monaco, Russia (which clearly refused to join the signatories in August 2009) and San Marino. On the other hand, it is interesting that within the EU, for example, Monaco, San Marino, Poland, Ireland, Liechtenstein and Sweden, although it was signed by them, they didn't ratify it. Why is this happening? Some authors cite as the main reason already mentioned procedural powers of state agencies, which the Convention provides almost with no limits. [10] Many critics point out the negative traits of the Convention, for diverse reasons.[11]

The fourth chapter contains the final provisions of the Convention. It is of special interest to countries that are not members of the Council of Europe, because it allows an agreement on the implementation of the Convention approaches and states that are not in the Council of Europe.

B. The Additional Protocol to the Convention on cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems

In 2003 there was signed the Additional Protocol to the Convention on cybercrime under the title CETS no. 189. It refers to the criminalization of acts of a racist and xenophobic nature committed through computer systems and it was entered into force on 1st March 2006. Of the countries in the region which have ratified it we could state the following: Albania, Bosnia and Herzegovina, Croatia, Macedonia, Romania and Montenegro, while Hungary and Bulgaria have neither signed nor ratified it, and, for example, Spain, Sweden and Switzerland have only signed, but not ratified it.[12]

---

[10] Komlen-Nikolić, L. et all. Op. cit. p. 51.

[11] EFF (*Electronic Frontier Foundation* http://www.eff.org, 1st October 2014) calls it the worst internet law in the whole world. More of other reasons at: Nate Anderson, *World's Worst Internet Law*, http://arstechnica.com/news.ars/post/20060804-7421.html, 1st October 2014.

[12] The State Union of Serbia and Montenegro signed it on 7th April 2005. The list of ratifications can be found at: http://conventions.coe.int/treaty/Commun/ChercheSig.asp?NT=189&CM=&DF=&CL=ENG,11thFebruary 2014.

The main purpose of the adoption of the Additional Protocol relating to the criminalization of acts of a racist and xenophobic nature committed through computer systems is the incrimination of behaviour not covered by the Convention as well as the spread of hatred, intolerance and bigotry toward racial, national, religious and other groups and communities, using computers as a means of communication and dissemination of propaganda. The activities in question carry a great social danger because of inability to control the availability and distribution of highly flammable contents. We are not talking about the right to publicly express their opinions, but this is a very complex phenomenon, which carries abuse on this or other rights at the Internet or another network by using a computer, where the ability of reacting an adequate authority is significantly reduced. The Protocol is primarily focused on the criminalization and punishment of such incidents, regardless of whether they are spreading hatred, intolerance or historical facts being represented in a false way, or by any other means discriminate against or denigrate certain ethnic, racial, religious group or organization that they represent.

The authors of the Protocol in the preamble invoke the European Convention on Human Rights and Fundamental Freedoms, the Protocol 12 to the European Convention, which prohibits any form of discrimination against individuals or groups on the basis of a protected personal characteristics, and the Convention on the Elimination of All Forms of Racial Discrimination, which was adopted within the United Nations in 1965.

The Protocol consists of four chapters:

- General provisions (Articles 1-2)
- Measures to be taken at the national level (Articles 3-7)
- Relations between the Convention on Cybercrime and its Additional Protocol (Article 8)
- Final provisions (Articles 9-16).

In a relatively short text, the Protocol establishes the obligation of States Parties to the national legislation criminalizing the following conduct: [13]

1) Dissemination of the racist and xenophobic material through computer systems means any act by which the material is made available to the public, using a computer or computer system. The material can be made available in a variety of ways, such as sending it to a large number of e-mail addresses or presenting it at the Internet; States are allowed to say whether this process will

[13] Art. 3-6. Of Protocol, Council of Europe, Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems CETS No.: 189, Convention Explanatory Report, Strasbourg, 28.I.2003 http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm> (December 20, 2013)

be introduced in the criminal law (to be criminalized), and given the possibility of making a reservation on those behaviours, which can, under domestic law, be considered to represent a form of expression freedom of speech.

2) The threat motivated by racism or xenophobia represents making it inevitable to an individual or group towards which there would be committed a serious crime, as defined in the domestic law of the states, by using a computer or computer system. An individual or group should be individualized according to their race, colour, descent, national, ethnic or religious affiliation, to have this criminal act regarded as a specific form provided by the Protocol;

3.) The insult motivated by racism or xenophobia has the same elements as the previous act, only it is not a threat, but rather insulting an individual or group based on race, colour, descent, national, ethnic or religious affiliation; the State can make a reservation to this article fully, or may limit criminalization to those offenses spreading hatred, or through which an individual or group is humiliated or shamed to ridicule. Probably the specificity and diversity of the Internet communications with a combination of the right of exercising a free expression of opinion in public have allowed the creators of the Protocol to define this offense in this way.

4) Denial, reduction, approval or justification of genocide or crimes against humanity introduces an interesting concept of punishment for the alleged acts committed via a computer or computer system if the subject cases were decisions by international tribunals. Also, this content must and alike has to somehow be made available to a larger number of people who use computers and the Internet or other computer networks.

Each Party shall adopt such legislative provisions that would previously elaborated actions qualify as a criminal offense if they are made of premeditation, aiding or incitement to commit any of these offenses.

In this section, subject to execution are the cases that were subject to decisions by international criminal courts, starting with the International Military Tribunal in Nuremberg in 1945, through the processes of Tokyo in 1946 onwards, which implies the offenses as subject to decisions of the Tribunal for war crimes in the former Yugoslavia as well as Rwanda, the International Criminal Court in Rome.

The decision on the implementation, the practices and international cooperation enshrined in the Convention shall also apply to the acts that are established by the Protocol.

C. The Convention on the Protection of Individuals with regard to the Automatic Processing of Personal Data (ETS 108)

The Convention was concluded on 28th January 1981 and entered into force on 1st October 1985.[14] The main objective of the Convention was to strengthen the legal framework in the field of personal data protection because of the increased usage of a computer technology for administrative purposes (especially the introduction of a governance), and the possibilities of abuse that it brings. The issue is based on the assumption that, in modern societies, passing many decisions concerning the exercise of the rights of individuals is based on the information and data stored in computers and computer systems (the data necessary for the calculation and payment of salaries, the data related to the creditworthiness of persons, social and medical care, the data on the health status of individuals, etc.). It is necessary to prescribe the conditions for the usage of such information and to make them available to persons who meet appropriate conditions and pass required procedures and thus reduce the possibility of abuse. It is particularly interesting to look at the proposals for the modernization of the Convention since the majority of EU member states have harmonized legislation according to EU directives and that in one or another legal system has certain shortcomings. The Explaining report[15] states that the national legislation of the Member States do not provide the necessary level of protection of citizens in this area, particularly with regard to the mechanisms of effective control over citizens' personal information being collected and used by state agencies and other entities. This is explained by the existence of certain social responsibilities of these agencies or persons processing the data to be given the power to carry such information with them and process them separately.

The central and essential part of the Convention is the second chapter in which the substantive provisions contained in the form of basic principles (such as a minimum protection that must be given to the processing of

[14] "The Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data", (ETS No.108, 28th January 1981, Entry into force: 1st October1985). Serbia signed and ratified the Convention on 6th September 2005 and it came into force on 1st January 2006. With this Convention there came along the additional protocols: the Additional Protocol to the Convention for the Protection of Individuals with regard to ETS no. 181, the Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows, Strasbourg, 8th November 2001. Serbia signed that Protocol on 2nd July 2008. and ratified it on 8th December 2008. It came into force on 1st April 2009.

[15] http://conventions.coe.int/Treaty/en/Reports/Html/108.htm last accessed on 26th February 2010.

personal data) concerning: 1) the quality of the data collected (the pattern in the data collection, the data for purposes permitted by law, the accuracy and timeliness of the data as well as keeping them in a shape and form which permits identification, Article 5 of the Convention), 2) the special categories of the data (the data on racial and political affiliation, religious beliefs, as well as the data concerning a health status, sexual orientation and prior convictions cannot automatically be collected and made publicly available unless the law provides special measures of protection in respect of the above data, Article 6 of the Convention), 3) the security of the data collected (the obligation to apply appropriate security measures to thwart an accidental or unauthorized destruction of the data collected as well as a loss, unauthorized access, modification or distribution of the automatically collected data, Article 7 of the Convention), 4) additional safety measures referring to persons on whom information are collected automatically (concerning the right of the access to any analysis of the automatically collected information, the right to request a deletion of illegally collected data and the right to a remedy if these requirements cannot be met, Article 8 of the Convention), 5) exceptions and limitations (the rights prescribed in Articles 5, 6 and 8 of this Convention may be limited only by a certain law of the Member State in cases when it is necessary in order to protect the national security, public order, the monetary system of the country, the suppression of criminal offenses as well as to protect the persons about whom the data are collected or other persons` rights and freedoms, Article 9 of the Convention). States are obliged to provide for appropriate sanctions to effectively avert any injury or abuse of the rights provided by the Convention.

The third chapter contains the provisions relating to the cross-border traffic of automatically collected personal data. The essence of these provisions is to ensure the free flow of information between Member States and to ensure the absence of any special control mechanisms or the existence of the regime of permits or approvals. This solution is logical, bearing in mind that the Convention lays down the basic principles for the automatic collection of information that make up the so-called "common core" among member states so as there does not exist the need for additional regulation or individual restrictions in the trade of personal data (except, of course, those restrictions that are established by the Convention in Article 12, paragraph 3). This "common core" also solved the problem of the possible application of the laws of certain states in the territories of other countries – the conflict of law jurisdiction.

The fourth and fifth chapters of the Convention prescribe the mechanisms of cooperation of States Parties, in certain cases (Chapter IV – relating

to a cooperation between the competent bodies and assistance to persons who are residents of a Contracting State other than their own), but also in terms of issues relating the application of the Convention as such (chapter V - the consultative Council for the implementation of the provisions of the Convention.)

D. Other documents

The Convention on the Protection of Children against a Sexual Exploitation and Sexual Abuse (ETS201) is a significant international document which should lead to the increased efficiency of criminal proceedings in which children are victims of a sexual exploitation and abuse. Its aim is also to bring about the harmonization of national legislations with regard to substantive criminal legislation in the works in which a computer technology and networks are used for the purpose of distribution, exchange and storage of illegal content.

The purpose of the **Convention on the Prevention of Terrorism (ETS 196)** is to increase efforts to prevent terrorism and its negative effects on the freedoms and rights of citizens, to influence a creation of the measures to be taken at both the national and international levels, as well as through an international cooperation. On the one hand, through the achievement of these objectives the Convention attempts to criminalize the behaviour (including certain preparatory actions) that can lead to acts of terrorism (a public provocation or public incitement to commit terrorist acts, the recruitment and training of the members of terrorist organizations). On the other hand, it provides empowerment and collaboration, internally, at the level of creating a national policy for the prevention and, internationally, through a number of measures - through, when it is necessary, the modification of existing agreements on extradition and legal assistance. The Convention makes this through the exercise of the exchange of information, imposition of obligation to the authorities to prosecute and investigate such crimes, but also through the introduction of liability for legal persons (in addition to individuals) for crimes in this area together with the imposition of obligation to proceed with the prosecution of the perpetrators of the territory of a country that has refused the extradition. It is necessary to point out that this Convention naturally leans to the criminalization of the Additional Protocol to the Convention on Cybercrime, CETS No. 189, specifically Article 3 of the same.

In order to support this view there goes the opinion of the Committee of experts on terrorism (CODEXTER) from 10th November 2005 which was issued at the request of the Committee of Ministers concerning cyber-terrorism

and the use of the Internet for the purpose of carrying out terrorist acts. The author highlights the issues regarding cyber-terrorism which should be set in relation to the assessment of the effects of implementation of the Convention on Cybercrime. Since it has been noticed that most of the issues related to attacks on computer systems and networks are adequately covered by the provisions of the Convention on Cybercrime, it is necessary to carry out a continuous evaluation of the effects of the Convention and, if necessary, to complete the provisions with indispensable solutions which may occur. As a conclusion it is stated that the focus needs to be accomplished to achieve an effective and consistent application of the provisions of the Convention on the Prevention of Terrorism and Cybercrime and to encourage states to fully implement the Convention.

The Convention on the Rights of the Child. By ratifying the Convention on the Rights of the Child,[16] Contracting States are, inter alia, pledged to provide every child a protection from exploitation and performing any work that is likely to be hazardous to life or health of the child, or constituting the violation and/or breach of its physical, emotional and sexual integrity. By the ratification of the Convention on the Rights of the Child (hereinafter CRC), our country has assumed an obligation to take measures to prevent violence against children and to ensure the protection of all its forms (in the family, institutions and the broader social environment, etc.). Also, contracting parties are committed to provide measures to promote a physical and psychological recovery of a child victim - all forms of exploitation, and to ensure a social reintegration, or provide a child's integration into a new social environment (Article 39 CRC).

Conclusion

In this segment, a significant concern was created on the issue of the organization of the judicial system of the state towards creating conditions for a successful combat against new forms of a criminal activity. Specifically, whether to opt for a comprehensive systemic change, or change a number of regulations in order to create an adequate legal framework, or be oriented towards a partial amendment of certain legal provisions in order to create conditions for a timely and adequate response to new forms of a criminal behaviour, that is the question each state has solved or is dealing with in accordance with their capacities. The first method is without a doubt very effective,

[16] *Law on ratifying of The Convention on the Rights of the Child,* The Official Gazette of SFRY – International contracts, no. 15/90.

but also very demanding, since it requires a high degree of political and social consciousness of the necessity of changes that should be followed, while the second method is more economical and less demanding one. It does not impinge on the basis of the system, but on a series of unresolved issues such as the question of jurisdiction for certain crimes, the collision of a new and existing legislation, and so on.

Dr Mina Zirojević
Institut za uporedno pravo, Beograd

ZLOČIN POVEZAN SA UPOTREBOM KOMPJUTERA – ODLUKA EVROPSKOG VEĆA

REZIME: Zbog značaja informacionih i komunikacijskih tehnologija javila se potreba da se širom sveta utvrde mere i mehanizmi da bi se i društvo i pojedinac zaštitili od zloupotreba u ovoj oblasti putem usvajanja odgovarajućih pravnih rešenja i unapređenja međunarodne saradnje. Rezultat ovih napora, pored još nekih drugih stvari, jeste usvajanje Konvencije Evropskog Veća o kibernetičkom zločinu, koja je, po mišljenju međunarodne zajednice, utvrdila minimalne standarde neophodne za usklađivanje sa nacionalnim zakonodavstvom radi efikasne borbe protiv zloupotreba u domenu visoke tehnologije.

Ključne reči: *internet, zloupotreba, Evropsko veće, konvencije.*

B i b l i o g r a p h y

1. Brkić, S. (2010). Krivično procesno pravo II, Pravni fakultet u Novom Sadu, Novi Sad
2. Grupa autora: (2008). Priručnik za istragu krivičnih dela u oblasti visokotehnološkog kriminala, Savet Evrope
3. Komlen-Nikolić, L., Gvozdenović, R.; Radulović, S.; Milosavljević, A.; Jeković, R.; Živković, V.; Živanović, S.; Reljanović, M.; Aleksić, I. (2010). Suzbijanje visokotehnološkog kriminala, Beograd, Udruženje javnih tužilaca i zamenika javnih tužilaca Srbije
4. Lazarević, Lj. (2006). Komentar Krivičnog zakonika Republike Srbije, Beograd, Savremena administracija

5. Prlja, D. i Reljanović, M. (2010). Pravna informatika, Beograd, Pravni fakultet Univerziteta Union, Javno preduzeće Službeni glasnik
6. Korać, S. (2008). Suzbijanje dečije pornografije na Internetu: EU standardi, *Revija za bezbednost.* 2 (11), str. 46-51.
7. Prlja, D., Reljanović, M. (2009), Visokotehnološki kriminal – uporedna iskustva, *Strani pravni život* (3), str. 161-184.
8. Radulović, S. (2008). Specifičnost pribavljanja elektronskih dokaza o izvršenju krivičnih dela visokotehnološkog kriminala, *Revija za bezbednost*, 2 (12) 17-22
9. Urošević, V. (2009). Nigerijska prevara u Republici Srbiji, *Bezbednost,* 51 (3), str. 145-156.
10. Criminal Code, "The Official Gazette of RS", no. 85/2005, 88/2005 - corr., 107/2005 - corr., 72/2009, 111/2009 and 121/2012
11. The Code of Criminal Procedure, "The Official Gazette of RS", no. 72/2011, 101/2011, 121/2012, 32/2013 and 45/2013
12. Law on Ratification of the Convention on Cybercrime, "The Official Gazette", no. 19/2009
13. Law on Amendments to the Criminal Law of the Republic of Serbia, "The Official Gazette of RS ", no. 39/2003
14. "The Official Gazette of RS", no. 85/2005, 88/2005 - corr., 107/2005 - corr., 72/2009, 111/2009 and 121/2012
15. Law on Organization and Jurisdiction of Government Authorities in the fight against cyber- crime, "The Official Gazette of RS", no. 61/05 and 104/09
16. The Act on Mutual Legal Assistance in Criminal Matters, "The Official Gazette of RS", no. 20/2009
17. Aćimović, B.: „Žestok DoS napad na pet gigantskih sajtova", Linux.rs, <http://www.linux.rs/content/view/112/20/> (May 7th , 2009);
18. The Convention on Cybercrime, The Council of Europe, Budapest, 23rd November 2001.; European Treaty Series (ETS) - No. 185 <http://conventions.coe.int/Treaty/en/Treaties/Word/185.doc> (August 5th , 2010)
19. The Council of Europe, The Convention on Cybercrime, ETS No. 185 – Explanatory Report <http://www.conventions.coe.int/Treaty/en/Reports/Html/185.htm> (December 20th, 2013)
20. „Podignuta optužnica protiv autora Sassera", Mikro-PC World; <http://www.mikro.co.yu/main/index.php?q=vestiarhiva&godina=&mesec=&ID=6192> (May 7th , 2009)
21. „Softverska piraterija oštetila budžet za 72 miliona dolara", Danas, 09.05.2008.; <http://www.danas.rs/vesti/ekonomija/softverska_pirateri-

ja_ostetila_budzet_za_72_miliona_dolara.4.html?news_id=92482> (May 10th, 2009)

22. <http://arstechnica.com/tech-policy/news/2007/04/child-porn-case-shows-that-an-open-wifi-network-is-no-defense.ars> (May 1st , 2009)