CRIMINAL LAW PROTECTION OF PERSONALITY: IMPLEMENTATION OF COUNCIL OF EUROPE'S CONVENTION ON CYBERCRIME NO. 185 OF 2001 INTO SERBIAN LEGISLATIVE

Vida M. Vilić

Clinic of Dentistry Niš,
Niš, Serbia

Abstract:

Along with the development of information technologies, the issue of legal regulations that can prevent and sanction cybercrime has gained worldwide significance. EU's regulatory framework for electronic communications, networks and services is a basis for the national laws of all EU member states. The Council of Europe was one of the first international organisations to put forward an initiative for building up legal presumptions to restrain cybercrime with joint efforts of several countries. The Criminal Code of the Republic of Serbia regulated criminal offences regarding violation of computer data security, thus clearly contributing to a more efficient fight against cybercrime. Still, this regulatory framework did not fully embrace the deviant forms of behaviour manifested as misuse of computer technologies and computer systems (*e.g.* Internet harassment, unauthorised alteration of the contents published on the Internet, *etc.*). Also, the issue of jurisdiction regarding the criminal prosecution of the perpetrators of these crimes still remains unresolved being that most of such offences have an international character. As Serbia signed and ratified the Convention on Cybercrime CETS No. 185 in 2009, the Criminal Code of the Republic of Serbia should recognise as criminal offences numerous deviant forms of behaviour (Internet harassment, unlawful interception, Internet frauds, *etc.*) and determine sanctions for the offenders.

Key words:

cybercrime; Convention on Cybercrime CETS No. 185,
Criminal Code of the Republic of Serbia, regulated offences.

1. INTRODUCTION

With the development of information technologies, the issue of legal regulations aimed to prevent and sanction cybercrime has gained worldwide significance. The EU's regulatory framework for electronic communications, networks and services is a basis for the national laws of all EU member states. The Council of Europe was one of the first international organisations to put forward an initiative for building up legal presumptions to restrain cybercrime with joint efforts of several countries. Relying on the provisions of the Council of Europe's Convention on Cybercrime of 2001 [1], many international organisations have passed numerous recommendations regarding the desirable changes of national criminal justice systems in the field of cybercrime prevention.

The Council of Europe's Convention on Cybercrime no. 185 of 2001 with its additional protocol is undoubtedly the most significant and the

Correspondence:
Vida M. Vilić

e-mail:
vila979@gmail.com

DOI: 10.15308/Sinteza-2016-66-73

most comprehensive international document and its provisions have been incorporated into the national criminal justice systems of the signatory countries and the countries that have ratified this document.

2. CONVENTION ON CYBERCRIME CETS NO. 185

The Council of Europe's Convention on Cybercrime no. 185 of 2001 adopted in Budapest (hereafter called: the Convention), along with its additional protocol still remains the most comprehensive attempt to build a legal framework for the fight against cybercrime at the international level. The Convention entered into force in 2004, setting the grounds to develop national legislatures to combat cybercrime. Up to now, 47 countries, members of the Council of Europe, have signed the Convention, out of which only Andorra, Greece, Liechtenstein, Monaco and Sweden have not ratified it yet. [2]

The Convention was conceived in order to deter action directed against confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data. The ultimate goal was to introduce a system of punishment, sufficient for effectively combating such criminal offences by facilitating their detection, investigation and prosecution at both domestic and international levels and by providing arrangements for fast and reliable international cooperation.

The Convention contains provisions dealing with substantive and procedural criminal law issues. The provisions of the Convention are grouped into four chapters. The language of the Convention is technically neutral so that all the provisions can be applied to both existing and future technology. According to the Convention, all criminal offences must be committed intentionally and in a premeditated way, but the interpretation of the terms "intention" and "premeditation" is left to each party's domestic laws. Also, the access to a computer or computer system must be done without right.

In the part of the Convention addressing the issues of substantive criminal law, the member states are advised to establish as criminal offences under their domestic law: (a) the offences against confidentiality, integrity and availability of computer data and systems (Art. 2-6): illegal access, interception, data interference – alteration of computer data, deletion or damaging, hindering without the right of functioning of a computer or computer system, misuse of devices - production, sale, distribution or use of any device designed to be used for the purpose of committing any of the above-mentioned offences; (b) Computer-related offences (Art. 7-8): computer-related forgery, computer-related fraud; (c) Content-related offences (Art. 9) and (d) Offences related to infringements of copyright and related rights (Art. 10).

3. LEGAL REGULATIONS OF THE REPUBLIC OF SERBIA RELATED TO CYBERCRIME AND THEIR HARMONISATION WITH THE PROVISIONS OF THE CONVENTION

The Republic of Serbia signed both the Convention and the Protocol in Helsinki on 7 April 2005, at the time of the State Union of Serbia and Montenegro, and the National Parliament of the Republic of Serbia ratified both documents in 2009 [3]. The compulsory application of the Convention commenced in August 2009. The mentioned documents served as a legal basis for domestic laws and standards, as well as for establishing specialised state bodies to combat cybercrime in general. The most important regulations adopted and adjusted to the provisions of the Convention include: the Criminal Code [4], the Law on the Liability of Legal Entities for Criminal Offences [5], Criminal Procedure Code [6], the Law on Special Measures for the Prevention of Crimes against Sexual Freedom Involving Minors [7], the Law on Seizure and Confiscation of the Proceeds from Crime [8], and the Law on Special Authorizations for Efficient Protection of Intellectual Property [9]. However, some issues remain legally unregulated and unsanctioned.

I) The first regulatory document within the positive legislation of the Republic of Serbia to be considered in the light of the issue of cybercrime is the Criminal Code of the Republic of Serbia [10]. The Criminal Code addresses criminal offences connected with the use of computers, implementing the provisions of the Convention in the domestic legislation.

   In Article 112, item 9, "a juvenile" is defined as "a person over 14 years of age but who has not attained 18 years of age", while item 10 of the same Article defines "a minor" as "a person who has not attained eighteen years of age". Thus, the domestic legislation embraces the provisions of Article 9 of the Convention, according to which the term "minor" includes all persons less than 18 years of age, partially renouncing a discretionary power given to each and every country ratifying the Convention to establish a lower age limit, provided that it cannot go lower

than 16 years of age. This is particularly important when it comes to defining a criminal offence referred to in Articles 185-185b of the Criminal Code of the Republic of Serbia, *i.e.* in Article 9 of the Convention regarding child pornography.

In Article 112, items 16-20 and 33-34, the Code defines the terms such as "computer data", "computer network", "computer programme", "computer virus", "computer" and "computer system". By recognising a computer data as movable, the Code set a basis to adjust and "modernise" many other established criminal offences by recognising the offences done by a computer or by abusing computer programmes or systems as forms of the existing criminal offences.

The national legislation has made a significant progress regarding the issue of criminal law protection against cybercrime by establishing and sanctioning the following criminal offences within Chapter XXVII concerning criminal offences against computer data security. Subsidiary nature of criminal legal protection of individuals' right to privacy means that in most cases criminal law provisions could be applied when privacy protection can not be achieved by other means. On the other hand, criminal protection is fragmented, which means that it is only used in severe cases of violation of the right to privacy [11]. The Criminal Code specifies the protection of privacy rights by providing only a few criminal offences.

a) The offence of "Damaging Computer Data and Programs" (Art. 298 of the Criminal Code of the Republic of Serbia) states that illegal deletion, alteration, damaging, concealing or any other deterioration resulting in the uselessness of computer data or programmes shall be punishable. The mentioned offence is in complete conformity with the offence of "Data Interference" established in Article 4 of the Convention which refers to alteration, deletion or damaging of computer data. In line with the discretionary power given to the countries to introduce tougher punishments for more serious forms of this offence resulting in a significant material damage, the Code has additionally introduced some more severe punishments for this offence if the damages caused exceed four hundred and fifty thousand dinars (RSD), *i.e.* one million five hundred thousand dinars.

b) The offence of computer sabotage, as regulated by Art. 299 of the Criminal Code, involves entering, destruction, deletion, alteration, concealing or any other deterioration resulting in uselessness of computer data or programmes or destruction or damaging of a computer or any other device for electronic processing and data transfer intended to prevent or significantly disrupt electronic processing and transfer of the data important for the state authorities, public services, institutions, companies or other entities. The Convention does not recognise an offence that would fully correspond to this offence, as established and punishable in the Serbian national legislature in the above-specified way. Instead, the Convention only recognizes acts intended to disrupt normal functioning of a computer or a computer system, as well as misuse of devices with intent to be used to commit any of the previously mentioned offences (Art. 5 and 6), but it does not specify that such acts must target the data of importance for state authorities, public services, institutions, companies or other entities.

c) The offence of creating and introducing computer viruses (Art. 300 of the Code) involves the creation of a computer virus with intent to introduce it into another computer or computer network as well as the act of introducing such virus into another computer or computer network resulting in damage. Art. 5 of the Convention refers to the hindering of the functioning of a computer or a computer system as an offence that involves inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data, resulting in serious hindering of the functioning of a computer or computer system. The Convention makes no mention of a computer virus being created or introduced into a computer or computer system, but the consequence of this offence largely corresponds to the consequence of the offence established by the Serbian Criminal Code.

d) Computer fraud (Art. 301 of the Code) is an offence committed by a person who enters incorrect data, fails to enter correct data or otherwise conceals or falsely represents data and thereby affects the results of electronic processing and transfer of data, with the intention to acquire unlawful material gain for himself or for another person, thus causing material damage to another person. This offence is fully compliant with the computer-related offences referred to as "Computer-related fraud" in Art. 8 of the Convention involving any premeditated input, alteration,

deletion or suppression of computer data or any interference with the functioning of a computer system causing a loss of property to other persons with the aim of procuring a significant economic benefit for oneself or for another person.

e) The offence of unauthorised access to a computer, computer network or electronic data processing (Art. 302 of the Code) involves infringing security measures by unauthorised breaking into a computer or computer network, or illegal accessing electronic data processing, as well as use of data obtained in such a way. The Convention does not explicitly recognise this particular offence, but the act is in it essence identical to the one established by Articles 2 and 3 of the Convention, referring to illegal access and illegal interception.

f) The offence of preventing or restricting access to a public computer network (Art. 303 of the Code) occurs if a person prevents or hinders access to a public computer network while a more serious form of this offence involves a person in an official capacity committing this act in the discharge of duty. In this case, too, the Convention does not explicitly recognise this offence, but the act is in it essence identical to the one established by Articles 2 and 3 of the Convention, referring to illegal access and illegal interception.

g) The offence of unauthorised use of a computer or computer network (Art. 304 of the Code) is committed by anyone who illegally uses computer services or a computer network with the intent to acquire unlawful material gain for oneself or for another person. Differently from the previous ones, this offence can only form the basis of a civil action. The provisions referring to the mentioned offence in the Criminal Code is in conformity with Articles 2 (illegal access) and 6 of the Convention (misuse of the devices designed for the purpose of committing criminal offences).

h) The offence of designing, acquiring and giving to somebody else the means for the purpose of committing criminal offences against security of computer data (Art. 304a of the Code) occurs when a person owns, acquires, makes or gives to somebody else computers, computer systems, computer data and programmes for the purpose of committing any of the offences from Chapter XXVII of the Criminal Code. This offence is also recognized by the Convention on Article 6 which defines misuse of the devices designed to commit offences and suggests to the countries, signatories of the Convention, to sanction the following forms of behaviour as offences: production, sale, procurement for use, import, distribution or any other way of making available the devices, computer programmes, computer passwords, access codes and similar data which may be used to commit any of the previously mentioned offences or to access a computer system as a whole or part of it with the intent to use it for the purpose of committing any of the mentioned offences, as well as owing of computer programmes, computer passwords, access codes and similar data in order to use them to commit any of the mentioned offences.

Aside from the criminal offences established in Chapter XVII of the Criminal Code of the Republic of Serbia regarding the security of computer data, the mentioned Code in Chapter XVIII deals with sexual offences and establishes the following offences that directly rely on Art. 9 of the Convention: showing, procuring and possessing pornographic material and exploiting of minors for pornography (Art. 185) as well as using a computer network or other technical devices for the purpose of committing sexual offences against minors (Art. 185b). In Art 9, the Convention establishes a group of offences related to the content of the published data specifying all punishable offences regarding the content of the published data. The Article establishes as a sexual offence every premeditated act of child pornography that includes producing child pornography for the purpose of its distribution through a computer system, offering or making available child pornography through a computer system, distributing or transmitting child pornography through a computer system, procuring child pornography through a computer system for oneself or for another person, as well as possessing child pornography in a computer system or on a computer-data storage medium. In the spirit of the Convention, the term "child pornography" includes pornographic material that visually depicts a minor engaged in sexually explicit conduct, a person appearing to be a minor engaged in sexually explicit conduct, as well as realistic images representing a minor engaged in sexually explicit conduct. The criminal law solutions in our Code are in full compliance with the above-given provisions of the Convention.

Article 10 of the Convention on Cybercrime specifies the offences related to infringements of copyright and related rights including reproduction and distribution of unauthorised copies of any work through computer systems. The Criminal Code of the Republic of Serbia also establishes the offences which are directly in compliance with Article 10 of the Convention.

The Convention on Cybercrime in Art. 7, par. 1 suggests to the national legislatures to establish as a criminal offence the act against computer-related forgery. The Criminal Code of the Republic of Serbia does not recognize offences of computer-related forgery in the same strict sense as the Convention, but incriminates the following acts which do contain certain elements from the Convention: in Chapter XXII as criminal offences against the economy - counterfeiting money (Art. 223), forging securities (Art. 224), forgery and misuse of credit cards (Art. 225), forging value tokens (Art. 226), forging symbols for marking of goods, measures and weights (Art. 245), and in Chapter XXXII, as criminal offences against legal instruments - forging a document (Art. 355) and special cases of document forging (Art. 356), as well as forging of official documents.

On top of the offence of computer fraud established in Article 301, the Criminal Code of the Republic of Serbia also recognizes the following offences containing certain elements from the Convention: in Chapter XXI, as criminal offences against property – fraud (Art. 208), frauds in insurance (Art. 208a), petty theft, embezzlement and fraud (Art. 210), and in Chapter XXXIII, as criminal offences against official duty - fraud in service (Art. 363) and embezzlement (Art. 364).

In the Criminal Code of the Republic of Serbia, there are numerous criminal offences that need to be adjusted to the provisions of the Convention. This primarily refers to criminal offences against the freedoms and rights of man and the citizen, honour and reputation, humanity and other values protected by the international law (racial and other discriminations, human trafficking), criminal offences against life and body (suicide incitement and help) which can be committed in the virtual space, in which a computer may serve as a means of committing a crime while using certain social networks may be the very act of crime.

In Chapter XIV – Criminal Offences against Freedoms and Rights of Man and Citizen, the Criminal Code of the Republic of Serbia recognises the criminal offence of violation of privacy of letter and other mail (Art. 142), which also sanctions e-mail violation. In pretty much the same way, the positive legislation regulates the issues of eavesdropping and recording of chat rooms which is very frequent on social networks. The same chapter establishes the offence of unauthorised wiretapping and recording (Art. 143), but without any concrete reference to cyberspace communication. With regard to frequent surveillance of the communications carried out through social networks and in chat rooms, it is necessary to widen the scope of this offence to embrace electronic communications, without limitation to conversations, statements or declarations. The offences of unauthorised photographing (Art. 144) and unauthorised publication and presentation of other person's texts, portraits and recordings (Art. 145) do not include unauthorised photographing or publication of the data published on the Internet or on social networks.

Being that violation of privacy in cyberspace can be done in manifold ways, the criminal offence of unauthorised collection of personal data (Art. 146) should include sanctioning of such behaviour if done with the data published by social networks' users for the purpose of informal communication with other users. The Convention does not regulate the issue of the right to privacy and personal data protection in cyberspace or in computer-based communications in an explicit way. Indirectly, the Convention does so by sanctioning illegal access to computer data, their forging and fraud practices, as well as through the offences regarding child pornography which can be interpreted as violations of the right to privacy. Still, the entire regulation deals with technical issues, leaving aside the essential issues related to protection against such criminal forms of behaviour. For instance, it does not provide for a specific protection of the persons whose photographs have been made in public because the standpoint taken regarding this issue does not recognize the very act of taking someone's picture as privacy jeopardising. Also, the positive legislation does not contain any provisions to protect the users of social networks from disturbance, sexual harassment, cyber mobbing, bullying, false representation, internet frauds and the like. With regard to the existing practices, it is also necessary to recognise using social networks for the purpose of human trafficking as a separate offence.

Aside from substantive provisions of the Convention, our national legislation also incorporated the provisions regarding the scope of criminal legislation and competences for the prosecution of offenders: the criminal legislation of the Republic of Serbia applies

to everyone committing a criminal offence on its territory or on a domestic vessel, regardless of where the vessel is at the time of committing the act, in a domestic aircraft while in flight or in a domestic military aircraft. Thus, Articles 6-10 of the Criminal Code of the Republic of Serbia are fully harmonised with Article 22 of the Convention, on reciprocity condition. In accordance with Article 6, par. 5 and Articles 10 and 24 of the Convention, the Code also establishes extradition and criminal prosecution of foreigners on condition of reciprocity and provided that such criminal offence is punishable pursuant to laws of the country of the commission, or based on a special approval given by the republican public prosecutor.

II) As for the liability of legal entities for criminal offences in the field of cybercrime, the legal solutions contained in the Law on the Liability of Legal Entities for Criminal Offences [12] rely to a certain degree on Art. 12 of the Convention which establishes liability of legal entities for the offences recognised by the Convention if such offences are committed by a natural person who has a leading position within such legal entity acting either individually or as part of an organ of the legal person. The Law on the Liability of Legal Entities for Criminal Offences defines in Art. 7 that the liability of a legal entity rests on the culpability of the responsible persons, *i.e.* natural persons who have been entrusted, either legally or actually, a certain scope of duties in the legal entity, authorised persons and persons authorized to act on behalf of the legal entity.

Depending on the seriousness and form of the criminal offence, as well as on the type and seriousness of the resulting consequences, the Convention establishes that the liability of a legal entity may be criminal, civil, or administrative without prejudice to the criminal liability of the natural persons who have committed the offence. The national legislation establishes the following penal sanctions that may be imposed against a legal entity for the commission of criminal offences: sentence (fine and termination of the status of a legal entity which may be imposed solely as principal sentences), suspended sentence (with or without protective supervision) and security measures (prohibition to practice certain registered activities or operations, confiscation of instruments, and the publicizing of the judgment). The criminal proceedings are instituted and conducted jointly by a legal entity and the responsible person, and a single sentence is passed (Art. 35).

III) As for the procedural provisions which are directly connected with detection of cybercrime offences, the Criminal Procedure Code [13] establishes specific evidentiary actions for cybercrime offence detection. Namely, Article 162, par. 3 states that a special evidentiary action may be ordered for unauthorised exploitation of copyrighted work or other works protected by similar rights (Article 199 of the Criminal Code), damaging computer data and programmes (Article 298 paragraph 3 of the Criminal Code), computer sabotage (Article 299 of the Criminal Code), computer fraud (Article 301 paragraph 3 of the Criminal Code) and unauthorised access to protected computers, computer networks and electronic data processing (Article 302 of the Criminal Code) in which case the court may, upon a substantiated proposal of the public prosecutor, order surveillance and recording of the communication carried out via phone or other technical devices or surveillance of the e-mail or other address of the suspected party as well as confiscation of the letters and other mailings. Such a special evidentiary action can be ordered against a person for whom there are grounds for suspicion that he has committed a criminal offence, and evidence for criminal prosecution cannot be acquired in any other manner, or their gathering would be significantly hampered (Art. 161, par. 1), *i.e.* against a person for whom there are grounds for suspicion that he is preparing one of the criminal offences and the circumstances of the case indicate that the criminal offence could not be detected, prevented or proved in another way, or that it would cause disproportionate difficulties or substantial danger (Art. 161, par. 2).

In spite of the attempts to get harmonised with the Convention, the Code does not establish a definition of electronic evidence in cases of cybercrime offences.

IV) Aside from the criminal law provisions of substantive character contained in the Criminal Code of the Republic of Serbia, the field of legal protection of intellectual property rights within the fight against cybercrime is also regulated by the Law on Special Authorizations for Efficient Protection of Intellectual Property [14]. The mentioned Law is fully harmonized with Art. 10 of the Convention, because it bans production, possession and placing into circulation of goods and supply of services that infringe upon the intellectual property rights established by the applicable law or an international agreement (Art. 4), as well as broadcasting and re-broadcasting of a

radio or television program that contains authors' works or any subject-matter of related rights, if the obligation to pay a remuneration for the use of such rights is not regulated in conformity with the law that regulates collective protection of copyright and related rights (Art. 5, par.1).

V) The Law on Special Measures for the Prevention of Crimes against Sexual Freedom Involving Minors [15], reconfirms sanctioning of criminal offences referred to in Art. 9 of the Convention on Cybercrime as well as in Articles 185 and 185b of the Criminal Code of the Republic of Serbia regarding the criminal offences of child pornography and exploitation of minors for pornography. As stated in Article 3, the Law applies to the offenders of age who have committed, among other things, the acts of showing, procuring, and possessing pornographic material and exploiting a minor for pornography, as well as the act of exploiting a computer network or any other means of communication for committing criminal offences against sexual freedom involving minors. This Law is an important step forward because it states that the criminal offences targeted by this Law are not subject to a statute of limitations.

VI) In accordance with the provisions of the Convention and the Criminal Code of the Republic of Serbia which prescribe security measures of confiscation or confiscation and destruction of instruments, the Law on Seizure and Confiscation of the Proceeds from Crime [16] specifies in Article 2, par. 1, item 3 that the provisions of that Law must be applied to the criminal offences of showing, procuring and possessing pornographic material and child pornography (Articles 185-185b of the Criminal Code of the Republic of Serbia).

4. CONCLUSION

Cybercrime belongs to recent forms of crime and its emergence is a result of a huge advancement of technology in the field of telecommunications. A growing use of the Internet and social networks, as well as an increasingly wider use of computer technology in everyday life, embodies a tremendous progress from the standpoint of social development. On the other hand, the use of computer technology, particularly of the Internet and social networks exposes a huge number of users to daily victimisation if the data transmitted by the Internet and social networks happen to be misused.

The protection of personal information in a virtual environment as a basic level of human rights' protection mostly refers to the protection of information systems, information itself and information networks, as a private property of individuals or public and private organisations [17]. Significant misuse of computers at the time of their construction and gradual upgrading was practically impossible because their usage required special education undertaken only by a relatively limited number of IT experts since computers were not used on a large scale. Everyday use of computers by a wide stratum of people, accompanied by a liberal approach to communication and information networks, led to a point when cybercrime that once belonged to the futuristic spheres became a dangerous and hard-and-fast form of present-day crimes.

In order to reduce misuse of computer systems and threats to the right to privacy of their users, it is necessary to come up with appropriate legal mechanisms and legal regulations for tracing and sanctioning such socially unacceptable forms of criminal behaviour. Also, it is very important to report cybercrime offences to the competent authorities in order to decrease „the gloomy number of crimes" and accomplish better preventive actions, recognition and monitoring of such offences, as well as to overcome the problems connected with a failure to report such offences. However, as cybercrime has become a transnational problem with consequences far beyond the borders of any single country, it is clear that the mechanisms for fighting against such offences must not remain focused only on the change of national criminal law legislatures, but should foster undertaking of appropriate technical, structural and educational measures, passing of appropriate international technical and legal instruments and creating awareness of the importance of the information bearing potential risk for the occurrence of cybercrime.

Successful prevention of misuses of computers, computer systems, the Internet and social networks is extremely important because this form of criminal behaviour creates tough and often incurable consequences. A detailed legal regulation, tracing and sanctioning of all forms of misuse of computers and computer systems followed by heightened attention, constant monitoring and control by both administrators and users are only some of the most important forms of preventive activities. Daily development of the Internet requires a lot of attention and skills for tracking cybercrime. For this reason, users' substantial computer education is necessary so that they would be able to detect Internet misuses in a timely manner, recognise and report any form of on line attacks

against privacy and thus contribute to reducing „the gloomy number“ of cybercrime cases.

REFERENCES

[1] Convention on Cybercrime CETS No. 185), 2001., http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm, and http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=&CL=ENG retrieved on 02.08.2015.

[2] Council of Europe – Treaty Office, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG, retrieved on 31.07.2015

[3] Act of Formal Confirmation of the Convention on Cybercrime „ Official Gazette of the Republic of Serbia“ no. 19/2009.

[4] Criminal Code („Official Gazette of the Republic of Serbia” no.85/2005, 88/2005, 107/2005, 72/2009, 111/2009, 121/2012 and 104/2013)

[5] Law on the Liability of Legal Entities for Criminal Offences („Official Gazette of the Republic of Serbia” no.97/2008)

[6] Criminal Procedure Code („Official Gazette of the Republic of Serbia” no. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013 and 55/2014)

[7] Law on Special Measures for the Prevention of Crimes against Sexual Freedom Involving Minors („Official Gazette of the Republic of Serbia” no. 32/2013)

[8] Law on Seizure and Confiscation of the Proceeds from Crime („Official Gazette of the Republic of Serbia” no.32/2013)

[9] Law on Special Authorizations for Efficient Protection of Intellectual Property („Official Gazette of the Republic of Serbia” no. 46/2006 and 104/2009)

Criminal Code

[10] Sinđelić, Žarko: „Pravo na privatnost – krivično-pravni, krivičnoprocesni i kriminalistički aspekti“, Београд, 2012., www.doiserbia.nb.rs/phd/university. aspx?-BG20107404sinđelić, retrieved in 22/10/2015

[11] Law on the Liability of Legal Entities for Criminal Offences („Official Gazette of the Republic of Serbia ” no.97/2008)

[12] Criminal Procedure Code („Official Gazette of the Republic of Serbia” no. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013 and 55/2014)

[13] Law on Special Authorizations for Efficient Protection of Intellectual Property („Official Gazette of the Republic of Serbia” no. 46/2006 and 104/2009)

[14] Law on Special Measures for the Prevention of Crimes against Sexual Freedom Involving Minors („Official Gazette of the Republic of Serbia” no.32/2013)

[15] Law on Seizure and Confiscation of the Proceeds from Crime („Official Gazette of the Republic of Serbia” no.32/2013)

[16] Putnik, Nenad, Gavrić, Nevena: “Mere i strategije zaštite informacionih sistema od visokotehnološkog kriminala”, Зборник радова, међународна научностручна конференција, Сузбијање криминала и европске интеграције с освртом на вискотехнолошки криминал, Лакташи 28-30.03.2012., p. 218 , http://education.muprs.org/wp-content/uploads/2014/12/Zbornik-Visokotehnoloski-kriminal.pdf, retrieved 21/07/2015