

Global Alliance against Child Sexual Abuse Online

Report of Republic of Serbia

Criminal legal framework

In 2009 the Republic of Serbia ratified the Convention on Cybercrime adopted in Budapest 2001 as well as the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. By adopting the Law Amending the Criminal Code on 31 August 2009 which was published in the Official Gazette of the Republic of Serbia 72-09 (the amendments refer to the Criminal Code of the Republic of Serbia which entered into force on 1 January 2006 and was published in the Official Gazettes no 85/2005, 88/2005, 107/2005), the national criminal legislation has been harmonised with the recommendations of the Convention on Cybercrime.

The Law on Organisation and Competences of Government Authorities Responsible for Combating High Technology Crime which was published in the Official Gazette of the Republic of Serbia no 61/05 of 15 July 2005 has, for the first time, established the legal framework for setting up institutions for combating high technology crime. Such institutions are entrusted with the prevention of the criminal offences against computer data security as well as criminal offences against intellectual property, assets, and legal transactions where the object or instrument of crime is a computer, computer network, computer data, or their products in material or electronic form.

The Law Amending the Law on Organisation and Competences of the Government Authorities Responsible for Combating High Technology Crime has created additional facilities for a more efficient fight against high technology crime by extending their competencies to other criminal offences.¹

Article 2 of the said Law on Amendments states that Article 3 shall be amended and that the Law shall be applied for detection, criminal prosecution, and trial of:

1. criminal offences against computer data security which are stipulated by the Criminal Code;
2. criminal offences against intellectual property, assets, economy, and legal transactions where the object or instrument of crime is a computer, computer network, computer data, or their products in material or electronic form, if the number of copies of copyrighted work is more than 2,000 or the caused damage exceeds 1,000,000 dinars;
3. criminal offences against freedoms and rights of man and citizen, **sexual freedom**, public peace and order and constitutional order and security of the Republic of

¹ Published in the Official Gazette of the Republic of Serbia no. 104-09 on 11 December 2009.

Serbia which, due to their method of committing or instruments used, may be considered high technology crime, in line with Article 2, Para 1, of the Law.

Item 3 is particularly important, saying that criminal offences against sexual freedom may be considered high technology crime due to their method of committing or instruments used.

This form of committing criminal offences has been defined in the Serbian Criminal Code under Chapter XVIII entitled "Criminal Offences against Sexual Freedom" with the following criminal offences:

Showing, Obtaining and Possession of Pornographic Material and Abuse of a Minor for Pornography

Article 185

(1) Whoever sells, shows, publicly displays or otherwise makes available texts, pictures, audio-visual or other items of pornographic content to a minor or shows a pornographic performance to a minor, shall be punished with a fine or up to six months imprisonment.

(2) Whoever uses a minor to produce photographs, audio-visual or other items of pornographic content or for a pornographic show shall be punished with six months to five years imprisonment.

(3) If the offence specified in Paragraphs 1 and 2 of this Article is committed against a child, the offender shall be punished with six months to three years imprisonment for the offence under Paragraph 1 and one to eight years imprisonment for the offence under Paragraph 2.

(4) Whoever obtains for oneself or another person, or possesses, sells, shows, publicly displays, or electronically or otherwise makes available pictures, audio-visual or other items of pornographic content resulting from the abuse of a minor, shall be punished with three months to three years imprisonment.

(5) Items specified in Paragraphs 1 through 4 of this Article shall be confiscated.

Abuse of Computer Networks or Other Technical Means of Communication for Committing Criminal Offences against Sexual Freedom of the Minor

Article 185b

(1) Whoever with intent to commit criminal offence specified in Articles 178, paragraph 4, 179, paragraph 3, 180, paragraphs 1 and 2, 181, paragraphs 2 and 3, 182, paragraph 1, 183 paragraph 2, 184 paragraph 3, 185, paragraph 2 and 185a of this Code, makes appointment with a minor using a computer network or other technical means of

communication and appears at the arranged place of the appointment, shall be punished with six months to five years imprisonment and a fine.

(2) Whoever commits criminal offence specified in Paragraph 1 of this Article against the child shall be punished with one to eight years imprisonment.

Subject to the said legal framework a Department for High Technology Crime was established in 2007 in the Ministry of the Interior as a part of the service for Combating Organised Crime of the Criminal Police Directorate. The Department consists of the Section for E-crime Suppression and the Section for Intellectual Property Crime Suppression. It has jurisdiction over the entire territory of the Republic of Serbia. Furthermore, a Special Department for High Technology Crime has been established as a part of the Higher Public Prosecutor's Office of Belgrade, which also has jurisdiction over the entire territory of Serbia.

In addition, the most recent amendments to the Criminal Code of the Republic of Serbia which entered into force on 15 January 2013 introduced a larger number of criminal offences where special evidentiary actions may be applied. Thus, it is possible to specify a special evidentiary action for the criminal offence of Showing, Obtaining and Possession of Pornographic Material and Abuse of a Minor for Pornography under Article 185 CC. It is possible to apply surveillance of communications, covert surveillance and recording, simulated services, computer data search, controlled delivery and undercover agent.

Results of the Department for High Technology Crime in the fight against abuse of minors for pornography on the Internet

In 2010 the Department for High Technology Crime started the operation code named ARMAGEDDON the purpose of which being the suppression of abuse of minors for pornography on the Internet. So far, 69 criminal charges have been filed against 69 persons on the grounds that they have committed the criminal offence of Showing, Obtaining and Possession of Pornographic Material and Abuse of a Minor for Pornography under Article 185 CC. In 2010, 10 criminal charges were filed against 10 persons, 40 criminal charges were filed against 40 persons in 2011, 15 criminal charges were filed against 15 persons in 2012, while in 2013 4 criminal charges have been filed against 4 persons since they are believed to have committed the criminal offence of Showing, Obtaining and Possession of Pornographic Material and Abuse of a Minor for Pornography under Article 185 CC.

In the course of the said operation, more than 15 terabytes of material have been seized that resulted from the sexual abuse of minors for pornography, while the most common activity of paedophiles in our country is obtaining the said material over the Internet via peer-to-peer networks, and possession of such electronic material in computer systems.

On the basis of the information provided by the Department for High Technology Crime of the MoI of the Republic of Serbia, several dozens of persons have been arrested in Great

Britain, USA and other states for the said criminal offences. The Department for High Technology Crime has actively exchanged information about the said criminal offences and their perpetrators through international police cooperation with many countries worldwide.

Preventive Activities of the Department and cooperation with the private sector and non-governmental organisations

In addition to the said activities, police officers of this Department have been actively engaged in raising awareness among citizens (minors and their parents) at a number of round tables, public debates, seminars, etc. The public is informed through mass media about the current situation and uncovered cases. Also, good cooperation has been established with both public and private sectors. Examples of such cooperation are **Telenor LLC** and **Microsoft Software LLC**.

The cooperation with Microsoft Software LLC relates to further modernisation of the present infrastructure and related applications, better definition of long-term strategic goals and wider promotion of the results achieved by the Department. The cooperation should move towards upgrading the system for the prevention of abuse of children through pornographic material on the Internet, direct contact regarding cyber risks and threats, and assistance in the development of a cyber security strategy.

The cooperation with Telenor LLC develops in line with the memorandum on cooperation regarding filtering and blocking material showing sexual abuse of minors for pornography on the Internet. According to the said memorandum, the company is provided with the content (electronic addresses containing the said material) based on which the company blocks user access in its system with a notice on prohibited content.

On 14 March 2012 the Ministry of the Interior adopted a Special Protocol on the Police Officers' Conduct while Protecting Minors against Abuse and Neglect. On the web site of the Ministry of the Interior one may find instructions for parents how to protect their children against the above phenomenon, as well as the e-mail address for reporting cases of the above criminal offences.

The Department for High Technology Crime actively cooperates with non-governmental organisation as well. An example of such cooperation is the Memorandum on Cooperation on the establishment of the efficient system for children protection against abuse and exploitation using information technologies in the Republic of Serbia (signed between MoI of the Republic of Serbia and *Save the Children* organisation on 22 November 2011). Seminars and training courses were designed in 2012 for the Department staff and other employees of the related services in the Criminal Police Directorate. Their delivery started in 2013, where the Department staff attended the training course entitled *Understanding Child sex Offenders – A behaviour analysis framework*. The Department also delivered training for other police staff regarding cyber crime and handling digital evidence.

Funded by EC, implemented by B92 Fund, and supported by Serbian MoI, the Safe Internet Centre will be established in 2013 aiming to address this issue systematically and in line with EU principles. The Centre shall be important for gathering organisations which are involved in these activities for the purpose of a comprehensive joint action which will be comprised of three components – awareness raising, hotline, and helpline – in line with EC recommendations.