Institut suisse de droit comparé
Schweizerisches Institut für Rechtsvergleichung
Istituto svizzero di diritto comparato
Swiss Institute of Comparative Law

COMPARATIVE STUDY

ON

BLOCKING, FILTERING AND TAKE-DOWN OF ILLEGAL INTERNET CONTENT

Excerpt, pages 597-609

This document is part of the Comparative Study on blocking, filtering and take-down of illegal Internet content in the 47 member States of the Council of Europe, which was prepared by the Swiss Institute of Comparative Law upon an invitation by the Secretary General. The opinions expressed in this document do not engage the responsibility of the Council of Europe. They should not be regarded as placing upon the legal instruments mentioned in it any official interpretation capable of binding the governments of Council of Europe member States, the Council of Europe's statutory organs or the European Court of Human Rights.

Avis 14-067

Lausanne, 20 December 2015
National reports current at the date indicated at the end of each report.

Dorigny – CH – 1015 Lausanne - Tel : +41 (0)21 692 49 11 - Fax : +41 (0)21 692 4949 –
www.isdc.ch – info@isdc.ch

I. INTRODUCTION

On 24th November 2014, the Council of Europe formally mandated the Swiss Institute of Comparative Law ("SICL") to provide a comparative study on the laws and practice in respect of filtering, blocking and takedown of illegal content on the internet in the 47 Council of Europe member States.

As agreed between the SICL and the Council of Europe, the study presents the laws and, in so far as information is easily available, the practices concerning the filtering, blocking and takedown of illegal content on the internet in several contexts. It considers the possibility of such action in cases where public order or internal security concerns are at stake as well as in cases of violation of personality rights and intellectual property rights. In each case, the study will examine the legal framework underpinning decisions to filter, block and takedown illegal content on the internet, the competent authority to take such decisions and the conditions of their enforcement. The scope of the study also includes consideration of the potential for existing extra-judicial scrutiny of online content as well as a brief description of relevant and important case law.

The study consists, essentially, of two main parts. The first part represents a compilation of country reports for each of the Council of Europe Member States. It presents a more detailed analysis of the laws and practices in respect of filtering, blocking and takedown of illegal content on the internet in each Member State. For ease of reading and comparison, each country report follows a similar structure (see below, questions). The second part contains comparative considerations on the laws and practices in the member States in respect of filtering, blocking and takedown of illegal online content. The purpose is to identify and to attempt to explain possible convergences and divergences between the Member States' approaches to the issues included in the scope of the study.

II. METHODOLOGY AND QUESTIONS

1. Methodology

The present study was developed in three main stages. In the first, preliminary phase, the SICL formulated a detailed questionnaire, in cooperation with the Council of Europe. After approval by the Council of Europe, this questionnaire (see below, 2.) represented the basis for the country reports.

The second phase consisted of the production of country reports for each Member State of the Council of Europe. Country reports were drafted by staff members of SICL, or external correspondents for those member States that could not be covered internally. The principal sources underpinning the country reports are the relevant legislation as well as, where available, academic writing on the relevant issues. In addition, in some cases, depending on the situation, interviews were conducted with stakeholders in order to get a clearer picture of the situation. However, the reports are not based on empirical and statistical data, as their main aim consists of an analysis of the legal framework in place.

In a subsequent phase, the SICL and the Council of Europe reviewed all country reports and provided feedback to the different authors of the country reports. In conjunction with this, SICL drafted the comparative reflections on the basis of the different country reports as well as on the basis of academic writing and other available material, especially within the Council of Europe. This phase was finalized in December 2015.

The Council of Europe subsequently sent the finalised national reports to the representatives of the respective Member States for comment. Comments on some of the national reports were received back from some Member States and submitted to the respective national reporters. The national reports were amended as a result only where the national reporters deemed it appropriate to make amendments. Furthermore, no attempt was made to generally incorporate new developments occurring after the effective date of the study.

All through the process, SICL coordinated its activities closely with the Council of Europe. However, the contents of the study are the exclusive responsibility of the authors and SICL. SICL can however not assume responsibility for the completeness, correctness and exhaustiveness of the information submitted in all country reports.

2. Questions

In agreement with the Council of Europe, all country reports are as far as possible structured around the following lines:

1. What are the legal sources for measures of blocking, filtering and take-down of illegal internet content?

Indicative list of what this section should address:

- Is the area regulated?
- Have international standards, notably conventions related to illegal internet content (such as child protection, cybercrime and fight against terrorism) been transposed into the domestic regulatory framework?

- Is such regulation fragmented over various areas of law, or, rather, governed by specific legislation on the internet?
- Provide a short overview of the legal sources in which the activities of blocking, filtering and take-down of illegal internet content are regulated (more detailed analysis will be included under question 2).

2. What is the legal framework regulating:

2.1. Blocking and/or filtering of illegal internet content?

Indicative list of what this section should address:

- On which grounds is internet content blocked or filtered? This part should cover all the following grounds, wherever applicable:
  - the protection of national security, territorial integrity or public safety (e.g. terrorism),
  - the prevention of disorder or crime (e.g. child pornography),
  - the protection of health or morals,
  - the protection of the reputation or rights of others (e.g. defamation, invasion of privacy, intellectual property rights),
  - preventing the disclosure of information received in confidence.
- What requirements and safeguards does the legal framework set for such blocking or filtering?
- What is the role of Internet **Access** Providers to implement these blocking and filtering measures?
- Are there soft law instruments (best practices, codes of conduct, guidelines, etc.) in this field?
- A brief description of relevant case-law.

2.2. Take-down/removal of illegal internet content?

Indicative list of what this section should address:

- On which grounds is internet content taken-down/ removed? This part should cover all the following grounds, wherever applicable:
  - the protection of national security, territorial integrity or public safety (e.g. terrorism),
  - the prevention of disorder or crime (e.g. child pornography),
  - the protection of health or morals,
  - the protection of the reputation or rights of others (e.g. defamation, invasion of privacy, intellectual property rights),
  - preventing the disclosure of information received in confidence.
- What is the role of Internet Host Providers and Social Media and other Platforms (social networks, search engines, forums, blogs, etc.) to implement these content take down/removal measures?
- What requirements and safeguards does the legal framework set for such removal?
- Are there soft law instruments (best practices, code of conduct, guidelines, etc.) in this field?
- A brief description of relevant case-law.

3. Procedural Aspects: What bodies are competent to decide to block, filter and take down internet content? How is the implementation of such decisions organized? Are there possibilities for review?

Indicative list of what this section should address:

- What are the competent bodies for deciding on blocking, filtering and take-down of illegal internet content (judiciary or administrative)?
- How is such decision implemented? Describe the procedural steps up to the actual blocking, filtering or take-down of internet content.
- What are the notification requirements of the decision to concerned individuals or parties?
- Which possibilities do the concerned parties have to request and obtain a review of such a decision by an independent body?

4. General monitoring of internet: Does your country have an entity in charge of monitoring internet content? If yes, on what basis is this monitoring activity exercised?

Indicative list of what this section should address:

- The entities referred to are entities in charge of reviewing internet content and assessing the compliance with legal requirements, including human rights – they can be specific entities in charge of such review as well as Internet Service Providers. Do such entities exist?
- What are the criteria of their assessment of internet content?
- What are their competencies to tackle illegal internet content?

5. Assessment as to the case law of the European Court of Human Rights

Indicative list of what this section should address:

- Does the law (or laws) to block, filter and take down content of the internet meet the requirements of quality (foreseeability, accessibility, clarity and precision) as developed by the European Court of Human Rights? Are there any safeguards for the protection of human rights (notably freedom of expression)?
- Does the law provide for the necessary safeguards to prevent abuse of power and arbitrariness in line with the principles established in the case-law of the European Court of Human Rights (for example in respect of ensuring that a blocking or filtering decision is as targeted as possible and is not used as a means of wholesale blocking)?
- Are the legal requirements implemented in practice, notably with regard to the assessment of necessity and proportionality of the interference with Freedom of Expression?
- In the case of the existence of self-regulatory frameworks in the field, are there any safeguards for the protection of freedom of expression in place?
- Is the relevant case-law in line with the pertinent case-law of the European Court of Human Rights?

For some country reports, this section mainly reflects national or international academic writing on these issues in a given State. In other reports, authors carry out a more independent assessment.

SERBIA

1. Legal Sources

The Republic of Serbia is one of the countries that does not have specific regulation on blocking, filtering and take-down of illegal internet content. This area is regulated by various laws, not necessarily meant for the internet activities.

The Republic of Serbia has signed and ratified most of the international documents relevant for the freedom of expression as well as to illegal content on the Internet. The most important Council of Europe **Convention for the Protection of Human Rights and Fundamental Freedoms** was signed by the Republic of Serbia on 4 April 2005 and ratified on 14 April 2009.[1] The Convention has a power of the Law,[2] while freedom of expression from Article 10 with its restriction is regulated mainly by the Law on Public Information and Media,[3] the Law on Electronic Media[4] and the Law on Public Service Broadcasters.[5] It is also relevant the Media Strategy.[6]

Most of the international standards, applicable to filtering and blocking, have been incorporated into the national legislation.

The Republic of Serbia signed the **Convention on Cybercrime** on 7 April 2005, ratified it on 14 April 2009 and it entered into force on 1 August 2009. **The Ministry of Interior of the Republic of Serbia, Directorate of Crime Police, Department for the fight against organized crime** is the central authority in charge of the implementation of the Cybercrime Convention, thus cybercrime. At the same time, Serbia signed/ratified the **Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems** (CETS No. 189).

The **Convention for the Protection of individuals with regard to Automatic Processing of Personal data (CETS No. 108**) was signed by the Republic of Serbia on 6 September 2005, ratified on 6 September 2005 and entered into force on 1 January 2006. Serbia nominated the **Commissioner for Access to Information of Public Importance and Protection of Personal Data** as the competent authority in this matter.[7] The **Additional Protocol to the Convention for the Protection of**

---

1 Entered into force on 1st August 2009.

2 Official Gazette of Serbia and Montenegro, International Contracts, No 9/2003.

3 The Law on Public Information and Media, Official Gazette of the Republic of Serbia, No. 83/2014.

4 The Law on Electronic Media, Official Gazette of the Republic of Serbia, No.83/2014.

5 The Law on Public Service Broadcasters, Official Gazette of the Republic of Serbia, No. 83/2014.

6 The Strategy of Development of Public Information System in the Republic of Serbia until 2016, Official Gazette No. 75/2011.

7 The Republic of Serbia, pursuant to Article 3, paragraph 2, sub-paragraph a of the Convention, shall not apply the Convention with regard to the automatic processing of:

"1. Data that are available to the general public and printed in public newspapers and publications or that are accessible in the archives, museums and other related organizations;

1) Data that are being processed for family and other personal purposes and that are not accessible to a third party;

2) Data relating to members of political parties, associations, trade unions and other associations, that are being processed by these organizations provided that the relevant member states in writing that certain provisions of the law shall not apply to the processing of his personal data for a certain period of time which does not last longer than the duration of his/her membership; and

3) Personal data published by a person capable of looking after his/her own interests.[7]"

Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows (CETS No. 181) was signed on 2 July 2008, ratified on 8 December 2008 and entered into force on 1 April 2009.

The Council of Europe **Convention on Access to Official Documents (CETS No. 205)** was signed on 18th June 2009, but has not been ratified yet (in status as of 22/2/2013).

The Council of Europe **Convention on the Prevention of Terrorism**(CETS No. 196) was signed on 16 May 2005, ratified on 14 April 2009 and entered into force on 1 August 2009.

The Council of Europe **Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse** (CETS No. 201) was signed on 25 October 2007, ratified on 29 July 2010 and entered into force on 1 November 2011. **The Ministry of Interior** is the national authority in charge of the implementation of this Convention.

2. Legal Framework

The Legal Framework relevant for the Internet filtering, blocking or removing of the Internet content is not compiled in one legal document, but rather fragmentized between several laws which will be analysed in details in following sections. The most important are the **Constitution of the Republic of Serbia, the Criminal Code, the Law on Electronic Communications and Media Laws.**

2.1. Blocking and/or filtering of illegal Internet content

The Constitution of the Republic of Serbia prescribes the confidentiality of letters and other means of communications, which may easily refer to the online communication although not directly referred to. The only situations where the derogation may be allowed – for a specific period of time and based on a court decision – is in cases of conducting criminal procedures or protecting the safety of the Republic of Serbia.[8] The Constitution prescribes the restriction of freedom of manifesting religion or beliefs by law only in cases when it is "necessary in a democratic society to protect lives and health of people, morals of democratic society, freedoms and rights guaranteed by the Constitution, public safety and order, or to prevent inciting of religious, national, and racial hatred".[9] Almost the same ground for the restriction goes for the freedom of expression when it is necessary to "protect rights and reputation of others, to uphold the authority and objectivity of the court and to protect public health, morals of a democratic society and national security of the Republic of Serbia".[10] Finally, freedom of assembly may be restricted by the law "only if necessary to protect public health, morals, rights of others or the security of the Republic of Serbia".[11] So, the Constitution prescribes the restrictions on certain grounds and we may imagine a situation where these restrictions could be placed on the Internet. The only issue is related to the host ISP and whether Serbian authorities would have the power to enforce such a restriction.

With the incorporation of the Council of Europe Convention on Prevention of Terrorism in the Serbian **Criminal Code**, there is still no direct reference to blocking and/or filtering of illegal content

---

In accordance with the same Article 3, paragraph 2, sub-paragraph c of the Convention, the Republic of Serbia declares that "the Convention applies to the processing of personal data contained in the database that is not automated".

8 Article 41 of the Constitution of the Republic of Serbia.

9 Article 43 of the Constitution of the Republic of Serbia.

10 Article 46 of the Constitution of the Republic of Serbia.

11 Article 54 of the Constitution of the Republic of Serbia.

on the Internet. Although Serbia claimed in an OSCE survey that it does not have a specific legal provision regulating incitement to terrorism, terrorist propaganda and/or terrorist use of the Internet,[12] **terrorism** as a criminal act is defined as the "destroying of state or public object, traffic system, infrastructure, including the information systems…".[13] In addition, a public provocation to commit terrorist offences is also considered a criminal act,[14] for which the fine is one to ten years. And finally, the recruitment and training for committing terrorist attack[15] is also prescribed by the Criminal law with the fine between one to ten years.

With the incorporation of the Convention on Cybercrime and other Conventions related to children, **child pornography** has become one of the priorities of the Serbian Cybercrime Unite. The child is defined in Serbia as everyone younger than 14 years old, while minors are those between 14 and 18 years old. There is a differentiation on "young minors" – those between 14 and 16 years old and "older minors" – those between 16 and 18 years old. One of the main problems with child pornography is the low reporting of those criminal acts, for which the reasons mainly lays with patriarchal family, fear of parents or those who made pictures or videos and threat to a victim if their identity is revealed.[16]

Therefore, the child pornography is regulated by the Criminal Code which states that "whoever sells, shows or publicly displays or otherwise makes available texts, pictures, audio-visual or other items of pornographic content to a child or shows to a child a pornographic performance, shall be punished with a fine or imprisonment up to six months".[17] Further on, "whoever acquire for him/herself, owns, sells, shows, publicly exhibits or electronically or otherwise makes available pictures, audio-visual or other items of pornographic content … (from previous sentence) shall be punished with imprisonment from three months to three years".[18] The biggest change with the incorporation of the Convention on Cybercrime is that for the first time the criminal offence has become a pure possession and acquiring of pictures, audio-visual and other pornographic materials depicting the abuse of a minor, while before the amendments, it had to be meant for selling and the possession itself was not punishable. So this is a big improvement in Serbian legislation. Finally, the material related to criminal offences will be confiscated.[19] The next criminal act is **inducement of minor to attend the sexual activities,**[20] which is punishable for whoever induce a minor to be present while rape or any other sexual activity with a fine of imprisonment from six months to five year and a fine, while if this criminal act is done with a use of force or threat or to a child, the punishment will be from one to eight years of imprisonment.[21] And final criminal act is **the use of computer network or communications by other technical means for execution of criminal acts against sexual freedom towards the minor.**[22] This is probably one of the most important articles that protect children and minors from physical contact with predators. The criminal act is for whoever, using computer network or communications or other technical means, with the aim to rape, have sexual intercourse with a helpless person, have a sexual intercourse with a child, have a sexual intercourse through

---

12 Freedom of Expression on the Internet, A study of legal provisions and practices related to freedom of expression, the free flow of information and media pluralism on the Internet in OSCE participating States; http://www.osce.org/fom/80723?download=true.

13 Article 391 of the Criminal Code.

14 Article 391a of the Criminal Code.

Article 391 b of the Criminal Code.

16 http://www.mup.gov.rs/cms_lat/saveti.nsf/saveti-zastitimo-decu-od-pedofilije-na-Internetu.h (accessed on 23 October 2015).

17 Article 185 of the Criminal Code.

18 Article 185, Para 4 of the Criminal Code.

19 Article 185, Para 5 of the Criminal Code.

20 Article 185 a of the Criminal Code.

21 Ibidem.

22 Article 185 b of the Criminal Act.

abuse of position, prohibited sexual acts, pimping and procuring, wants to mediate in prostitution, shows or publicly displays or otherwise makes available texts, pictures, audio-visual or other items of pornographic content to a child or shows to a child a pornographic performance of minor to attend the sexual activities using computer network or communication by other technical means, agrees with minor the meeting and show up at the agreed place for a meeting will be punished by imprisonment from six months to five years and a fine, while whoever does it to a child will be put in prison between one and eight years.[23] The items used for these criminal acts will be confiscated.

The Criminal Code recognizes criminal offences against honor and reputation. **Defamation** was considered a criminal act until 2012,[24] when it was simply deleted. However, the **Insult** and Dissemination of Information on Personal and Family life are still offences regulated by Criminal Code. According to the Criminal Code, whoever insults another person, will be fined[25] and if the insult is committed via press, radio, television or other media or at a public gathering, whoever commits the act will be punished with a fine from one hundred and fifty to four hundred and fifty thousand dinars.[26] If the insulted person returns the insult, the court may either punish or remit punishment of both parties and one party. In any of the above mentioned cases, there will be no punishment if the insult statement is given "within the framework of serious critique in a scientific, literary or art work, in discharge of official duty, journalist tasks, political activity, in defense of a right or defense of justifiable interests, if it is evident from the manner of expression or other circumstances that it was not done with intent to disparage".[27] In the case of **Dissemination of Information on Personal and Family Life**, "whoever disseminates information of anyone's personal or family life that may harm his honor or reputation, shall be punished with a fine or imprisonment up to six months",[28] while if such a offence is committed through the press, radio, television or other media or at a public gathering, the punishment will be for up to one year in imprisonment. If there was a serious consequence for the injured party, the offender may be punished with imprisonment for up to three year. However, the offender will not be punished for this criminal act if the dissemination of information was part of official duty, journalist profession, defending a right or justifiable public interest as well as if the true of the allegations or reasonable grounds for believing that the allegations were true.[29] Although the defamation was deleted from the Criminal Code, the Insult and the Dissemination of Information on Personal and Family life continue to be regulated by the Criminal Code. For defamation, there could be a civil law suit.

The **hate speech** is prohibited by criminal, civil and administrative laws. The **Constitution** of the Republic of Serbia prohibits "any inciting of racial, ethnic, religious or other inequality or hatred".[30] Further on, the **Criminal Code** prohibits the instigation of national, racial and religious hatred and intolerance and prescribes six months to five years of imprisonment for whoever does it among the peoples and ethnic communities living in Serbia.[31] For the offence "committed by maltreatment, compromising security, exposure to derision of national, ethnic or religious symbols, damage to other persons, goods, desecration of monuments, memorials or graves"[32] the punishment will be imprisonment between one and eight years. And finally, when any of the criminal acts related to inciting racial, ethnic and religious hatred is committed by abuse of position or authority or the

---

23 Article 185 b of the Criminal Act.

24 The Law on amendments to the Criminal Code, Official Gazette of the Republic of Serbia No. 121/2012.

25 Between forty thousand and two hundred thousand dinars.

26 Approximately between 1250€ and 3750€ (October 2015).

27 Article 170 of the Criminal Law.

28 Article 172, paragraph 1 of the Criminal Law.

29 Article 172, paragraph 4.

30 Article 49 of the Constitution of the Republic of Serbia.

31 Article 317, Paragraph 1 of the Criminal Code.

32 Article 317, Paragraph 2 of the Criminal Code.

offence results in riots, violence or other consequences to co-existence of people, national minorities or ethnic groups living in Serbia, will be punished for imprisonment of either one to eight or two to ten years.[33] The **Law on Public Information and Media** prohibits hate speech by prescribing that "ideas, opinion and information published in media cannot encourage discrimination, hate or violence towards the person or group of people for their belonging or not belonging to a race, religious, gender, for their sexual orientation or any other personal condition, no matter whether by publishing was done the criminal offence".[34] However, there will be no responsibility if such an information is part of the journalistic article and is published without any intent to encourage the discrimination, hate or violence against person or group of people for their personal prerequisite or when the journalistic article is published in order to critically present the discrimination, hate speech or violence against people for their personal conditions.[35] In accordance with the **Law on Electronic Media**, the Regulatory authority (**The Agency for Electronic Media**) is in charge of making sure that the content provided by providers of audiovisual media services does not contain any information that could call for discrimination, hate or violence for someone's race, skin color, citizenship, nationality, language, religious or political beliefs, gender, sexual orientation, health, marital status, disability and other personal conditions.[36]

So, even without a direct mentioning of implementation of those acts on the Internet, it may be possible to imagine that any of the above mentioned categories – from terrorism via child pornography to hate speech may take place online.

The **Law on Electronic Communications** (LEC) regulates **the role of Access Providers** by obliging them to "offer all electronic media broadcasters, under fair, reasonable and non-discriminating terms, technical services which give their subscribers the access to media content by means of conditional access devices".[37] Further on, the conditional access services operator "may not hinder the reception of media content which are distributed and broadcast without conditional access".[38]

---

33 One to ten years for criminal offence from Paragraph 1 and two to ten years for criminal offence from Paragraph 2 of the Article 317.

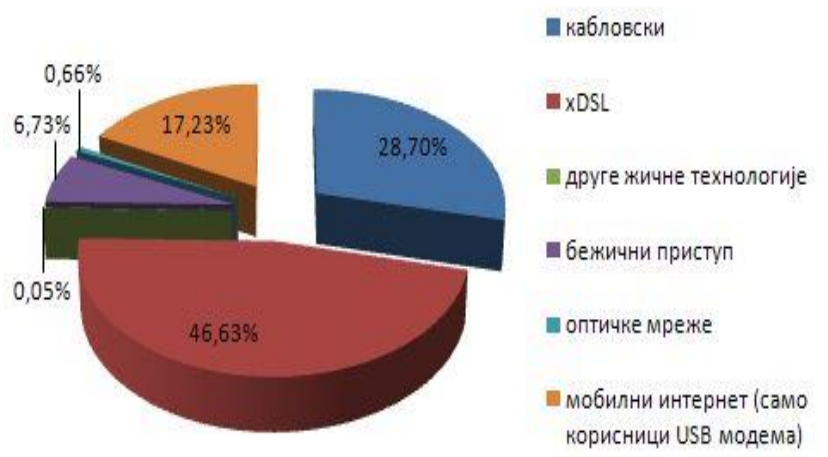
34 Article 75 of the Law on Public Information and Media.

35 Article 76 of the Law on Public Information and Media.

36 Article 51 of the Law on Electronic Media.

37 Article 103, Law on Electronic Communications (Official Gazette of the Republic of Serbia No. 44/2010, 60/2013 and decision of the Constitutional Court 62/2014).

38 Article 103 of the LEC.



Cable

xDSL

Other wire technologies

Wireless access

Optical networks

Mobile Internet (only for users of USB modem)

Picture 1: The Overview of the Representation of the Access to Internet Services in Serbia. Source: RATEL.[39]

In practice, **the first blocking of Internet content** in Serbia was dated back in 1998, when most of the Council of Europe countries did not even consider blocking of the Internet as an option to restrict the freedom of expression. At that time, Serbia was under the Milosevic's regime and the independent media were often shut down. B92 was one of the few radio stations that was banned by the regime. In order to try to still provide citizens with accurate information, B92 started to offer its programme on the Internet via live stream. However, "the Internet was not spared from the seizure – in December 1998 the Serbian University network set filters to prevent users from accessing the Open Net website, the Internet branch of Radio B92. However, after numerous Internet sites set up mirror sites to host Open Net, filtering of most of the Open Net websites stopped".[40] Human Rights Watch condemned the Internet censorship by the Serbian State-ran University.[41]

The next important case happened after the democratic changes, but with very strong state **monopolies** left in many sectors. Telecommunications were one of them. The incumbent, Telekom Serbia, had exclusive rights over fixed phone lines in Serbia until 9 June 2005, defined by the Law on Telecommunications from 2003[42]. Although the Voice-over-Internet-Protocol (VoIP) did not exist when the contract on exclusive right was signed in 1998, Telekom Serbia was claiming that VoiP services also fall under its monopoly. However, many Internet Service Providers (ISPs) in Serbia were of the opposite opinion and they were offering VoIP services to its users. As a result, "Telekom Serbia firstly reduced their leased capacities and then switched them off the public switched telephone network (PSTN) services. This was done without prior notice, warning, or consent. The affected ISPs brought their cases to the Commercial Court in Belgrade and the Inspector of the Ministry of

39 On the date: 31 December 2014; Available at: http://ratel.rs/upload/documents/RegionalniPregled Interneta_2014/index.htm (accessed on 7 October 2015).

40 Jelena Surculija, "The Situation in Serbia and Montenegro" in "Spreading the Word on the Internet", The OSCE Representative on Freedom of the Media (RFOM), Vienna, 2003.

41 https://www.hrw.org/news/1998/12/20/serbian-state-run-university-censors-internet (accessed on 29 September 2015).

42 Jelena Surculija, "The Situation in Serbia and Montenegro" in "Spreading the Word on the Internet", The OSCE Representative on Freedom of the Media (RFOM), Vienna, 2003.

Transport and Telecommunications of the Republic of Serbia, which both ruled in favor of the ISPs. These decisions also ordered Telecom Serbia to fully restore the disconnected services to ISPs and to stop any practices of this sort. To date Telecom Serbia has refused to comply with these decisions."[43] As a result, even Vecernje novosti, national daily newspapers, were disconnected from its Internet service provider (Memodata) on 11th February 2003, due to the limitation of the speed from the incumbent towards the ISP. After that, Telekom Srbija offered VecernjeNovosti the high speed Internet and it had to accept it. Memodata was later fully disconnected and lost all of its leased lines.[44]

Share foundation[45] raised the issue of **filtering and blocking of the content by Academic Network of Serbia (AMRES).**[46] AMRES claims to have 150.000 active users on its network.[47] The aim of the AMRES filtering, in accordance to its official web site, is done on two levels: a) filtering of applications and services using the Access Control List (ACL) on the network equipment and b) filtering of the Internet content using the device for filtering of the Internet content. ACL defines the rules on which protocols and ports are allowed for the network traffic. On the other hand, content filtering is done by the categorization done by the manufacturer of equipment (CISCO) while IronPort devices take over the classification every five minutes. AMRES claims not to have anything to do either with creation of categories nor in the process of categorization. AMRES filters six main categories of content: Child Abuse Content, Gambling, Hate Speech, Illegal Drugs, Pornography, Filter Avoidance. In addition, the manufacturer of equipment uses web pages reputation as criteria for filtering, thus the web sites with bad reputation are automatically blocked, average reputation is scanned by antivirus and web sites with good reputation is allowed.[48] The result of the Share foundation research of the AMRES filtering was that there were no clear rules when and why a content can be blocked for reasonable purposes (torrents, pornography, etc.), but that often the users can not access the scientific data that they could from a commercial provider. Also, users were complaining that they can not use viber, but can use skype. One of the scientists could not access the foreign journals from AMRES network, but could do it from the commercial provider. The Share proposal is to create clearer rules for filtering and blocking on the academic network.[49]However, there is a question whether that is possible to achieve under the current circumstances or users of AMRES network should simply use the possibility to inform AMRES web masters about the problem they face with the web site they would like to access and thus solve the problem. It is not always a good solution (especially during the weekend), but at least they are open for changes.

Finally, there is also a strong cooperation with the private sector. In June 2011, Telenor Serbia signed a long term agreement with the Ministry of Interior regarding filtering and blocking material showing sexual abuse of minors for pornography on the Internet.[50]

---

43 Ibidem.

44 Ibidem.

45 http://www.shareconference.net/en (accessed on 25th October 2015).

46 AMRES is a public information-communications company established by the Government of the Republic of Serbia in order to "built, develop and manage the educational and scientific/research computer network in the Republic of Serbia". It enables the access and use of the Internet to educational and scientific/research organizations as well as to other members and their access to national and international computer networks.

47 https://www.amres.ac.rs/index.php?lang=en (accessed on 29th September 2015).

48 https://www.amres.ac.rs/index.php?option=com_content&task=view&id=297&Itemid=308 (accessed on 29th September 2015).

49 See in more details at: http://www.shareconference.net/sh/defense/access-denied-blokiranje-sadrzaja-na-akademskoj-mrezi-srbije-amres (accessed on 29th September 2015).

50 http://www.telenor.rs/en/About-Telenor/Telenor-in-Serbia/Expo-and-Intro-Center/Events/Press-Conference-Filters-for-Blocking-Access-to-Illegal-Websites-with-Elements-of-Sexual-Abuse-of-Children (accessed on 23 October 2015).

2.2. Take-down/removal of illegal Internet content

The new Internet era has launched the host providers and even more social media and search engine as parallel structures that can decide on removal of the content, very often without any judicial review of that decision. Bearing that in mind, it seems that one of the easiest ways to ask for the removal of the content to these providers is simply claiming the copyright infringement.

The **copyright** in Serbia is regulated by Law on Copyright and Neighbouring Rights and Criminal Code. The criminal offences against intellectual property include the violation of moral right of author and performer, unauthorized use of copyrighted work or other work protected by similar right, unauthorized removal or altering of electronic information on copyright and similar rights, violation of patent rights and unauthorized use of another's design. The prosecution is in charge of initiating the investigations when someone, under his/her name or the name of another, "publishes or puts into circulation copies of another's copyrighted work or performance or otherwise publicly presents another's copyrighted work or performance, entirely or in part"[51] as well as when someone, without the author's permission, "alters of adapts another's copyrighted work or alters another's recorded performance".[52] The punishment for the first offence can be a fine or imprisonment up to three years, while for the second can be a fine or imprisonment up to one year. However, in the case when someone puts into circulation copies of another's copyrighted work or performance "in a manner insulting the honor and reputation of the author or performer",[53] the author and performer may start a private action. In all three cases of violation of copyright the material will be seized.

Regarding unauthorized use of copyrighted work or other work protected by similar rights, the publication, record, copy or other form of copyrighted work, performance, phonogram, videogram, show, computer programme or database, whoever does any of the acts will be punished with a fine or imprisonment up to three years.[54] The same punishment will be imposed on a person who "puts into circulation or with intent to put into circulation keeps illegally multiplied or illegally put into circulation copies of copyrighted work, performance, phonogram, videogram, show, computer program or database".[55] For acquiring financial gain of any of the offences mentioned above, the punishment may be the imprisonment from three months to five years.[56] And final offence is related for whoever "produces, imports, puts into circulation, sells, rents, advertises for sale or renting, or keeps for commercial purposes, equipment and devices whose basic or prevailing purpose is to remove, bypass or forestall technological measures intended for prevention of violation of copyright and other similar rights, or who uses such equipment or devices with an aim to violate copyright or other similar right"[57] and the punishment is either a fine or the imprisonment of up to three years. The entire material used for unauthorized use of copyrighted work shall be not only seized but also destroyed.

The **Criminal Code** prescribes the offence of unauthorized removal or altering of electronic information on copyright and similar rights, which prescribes also putting these works into circulation, export and import, broadcast or otherwise presentation in public, from which electronic

51 Article 198, Paragraph 1 of the Criminal Code.
52 Article 198, Paragraph 2 of the Criminal Code.
53 Article 198, Paragraph 3 of the Criminal Code.
54 Article 199, Paragraph 1 of the Criminal Code.
55 Article 199, Paragraph 2 of the Criminal Code.
56 Article 199, Paragraph 3 of the Criminal Code.
57 Article 199, Paragraph 4 of the Criminal Code.

information on rights was removed or altered without authorization. The prescribed sanction is a fine and imprisonment of up to three years, while the material will be seized and destroyed.[58]

The seizure and destruction of material is prescribed for the violation of patent rights,[59] together with a fine and imprisonment of up to three years, and for unauthorised use of another's design[60] for which the punishment is a fine and imprisonment of up to one year.

The other important aspect is take-down/removal of Internet content for political reasons, claiming it is illegal. In spring 2014, there were several situations where the content on the Internet was removed for various reasons and it was all happening during the pre-election campaign.

First, there was a very cold and snowy winter and some parts of Serbia were cut off. The Prime Minister was with Lifeguards in one of the strongly affected areas and he was personally carrying a boy to the rescuing helicopter, which was filmed by the Serbian Public Service Television (RTS - Radio Television Serbia).[61] Almost the same night, the Internet was filled with the parodies to the reporting, mostly by adding various text lines to the video. In the next few days, all of the satirical videos were **removed** from youtube channel, due to the infringement of copyright.

Second situation was again related to the natural disaster. There was a heavy flooding in Obrenovac, one of the Belgrade far suburbs. The Government claimed the state of emergency, that lead to regular Prime Minister's Press conferences, broadcast live and transmitted by most of the television channels. Despite official source of information, media did not offer any other facts, from their independent sources or journalistic research. Almost everyone in Serbia had someone affected by the flood and people were keen to know whether people were saved, as the water was literarily flooding the houses without upper floors. So, the Internet was seen, again in Serbian history, as alternative source of information. The people were sharing various information on what was happening in the field, sometimes accurate sometimes not. In one moment, the blog "Telepromter" was removed for criticizing the behaving of the Prime Minister at the Government meetings during the state of emergency and use of media for that. The second incident happened on the "Blic" blog section of the web site, from where the text by journalist Dragan Todorovic titled "I, AV, resign".[62] After his reaction on twitter, the entire "Blic" blog section was removed, then it was returned but without disputable text. Blic is a daily newspaper which is owned by Ringier-Axel Springer. At the same period of time, make-up artist Jelena Macic was arrested for "Spreading the panic" on the Internet. Up to today it is not clear what was the legal basis for that nor why was she **arrested** for writing on her personal Facebook account, in the moment where tabloids had cover pages that were actually spreading the panic.[63]

Finally, another popular form of taking-down the Internet content was **hacking of the web sites**. During the described pre-election period of time, several web sites were seriously attacked and thus taken down. One of them was site "Pescanik", which existed as a radio programme on Radio B92 and then simply moved online and continued to offer independent content. Pescanik was the first one to publish the letter of Serbian scientists working at the United Kingdom Universities, claiming that the

58 Article 200 of the Criminal Code.
59 Article 201 of the Criminal Code.
60 Article 202 of the Criminal Code.
61 Official RTS video: https://www.youtube.com/watch?v=_y7BrrlVtRk (accessed on 5th October 2015).
62 http://blog.b92.net/text/24227/Autocenzura-medija%3A-AV-ostavka.
63 http://www.vreme.com/cms/view.php?id=1200959&print=yes.

PhD of the Minister of Interior was a plagiarism,[64] the web site was under constant hacking attack for six days and night and was during that time not accessible to readers.[65]

As a result, Dunja Mijatovic, the **OSCE Representative on Freedom of the Media** (RFOM) raised concern about the online censorship that happened in Serbia during April and May 2014 and "urged the authorities to nurture uncensored debate on issues of public interest, especially in times of crisis, such as the current situation with flooding in the region".[66] Ms. Mijatovic pointed out that the arrest of people for their writing is not acceptable and added that it can lead to self-censorship.[67] After that warning, many concluded that self-censorship is already in place as the Government can not be in charge of removing the content, but rather people who are afraid of the possible consequences of publishing something not positive for the Government. In the interview to Al Jazeera Balkan, **the Commissioner for Access to Information of Public Importance and Protection of Personal Data**, Rodoljub Sabic also thought that there was a strong self-censorship in Serbia and offered two possible causes for that, one - "that of the fear of political revenge and pressure, as direct threat, which is less possible and second - the economic pressure that is more often present".[68] However, after the OSCE RFOM raised concern about the online censorship in Serbia, the Prime Minister responded quickly by asking OSCE FROM to either offer any proof for its allegation or offer an apology.[69] That lead to a "constructive conversation" between the Prime Minister and Dunja Mijatovic where he promised to "personally take care to solve the problem of filtering and blocking"[70] in Serbia. Ms. Dunja Mijatovic repeated her concerns related to censorship on the Internet, adding that it was not a new problem in Serbia, and asked the Government to investigate who stands behind blocking and hacking of web sites, as the role of the Government is "to protect freedom of expression, whether it is on the Internet or not".[71]

3. Procedural Aspects

As explained above, it seems that the judicial bodies have lost their battle to be the only censors in the online environment over the Internet companies. Youtube has a policy to take down the content if claiming the copyright infringement and more and more people use it as a shortcut or simply to avoid the judicial procedure.

Within the frame of the national legislation, there are few scenarios.

When there is a **criminal offence**, like it was in a case of the attack to the web site "Pescanik", the Ministry of Interior initiated the investigation, based on the request by the Higher Public Prosecutor in Belgrade, to explore preventing and restricting the access to the Internet Domain

---

64 http://pescanik.net/getting-a-phd-in-serbia-the-case-of-minister-stefanovic (accessed on 11th October 2015).

65 http://pescanik.net/free-people (accessed on 11 October 2015).

66 http://www.osce.org/fom/119173 (accessed on 8 October 2015). Also: http://www.rferl.org/content/osce-warns-serbia-against-internet-censorship/25401767.html (accessed on 8th October 2015).

67 Ibidem.

68 http://balkans.aljazeera.net/vijesti/sabic-srbija-ima-problem-snazne-autocenzure (accessed on 8 October 2015).

69 http://www.b92.net/info/vesti/index.php?yyyy=2014&mm=06&dd=02&nav_category=11&nav_id=855900 (accessed on 10 October 2015).

70 http://www.b92.net/info/vesti/index.php?yyyy=2014&mm=06&dd=02&nav_id=856110 (accessed on 10 October 2015).

71 Ibidem.

www.pescanik.net.[72] The investigation aimed to identify the executor of the criminal act "preventing and restricting of the access to public computer network".[73] As explained above, there are many criminal acts where the prosecutor would react *ex officio*, while there are also criminal offences as well as breaches of other laws, where an injured person has a right to claim the private complaint. And finally, there are situations, like in implementing the Law on Electronic Media, where independent regulatory authority can also react towards unwanted material, such as hate speech.

4. General Monitoring of Internet

The general monitoring of the Internet is done in several directions.

First, there is a Department for Cybercrime (**Cybercrime Unite**) at the Ministry of Interior and they are in charge of monitoring and reacting upon suspecting any cybercrime. They are in charge of implementing the Criminal Code. So far, this department has achieved a great success participating in "Armagedon", an international action that lead to the arrest of many pedophiles who have produced and/or distributed child pornography online.[74]

The Cybercrime Unite is in charge of the following criminal acts:

- Damage of computer data and programme
- Computer sabotage
- Creation and import of computer viruses
- Computer fraud
- Unauthorized access to protected computer, computer network and electronic data
- Prevention and limitation of access to public computer network
- Unauthorized use of computer or computer network.

In addition, the Ministry of Interior, Cybercrime Unite stated the criminal acts related to intellectual property, computer networks, computer data, but also criminal acts where the computer and computer networks are medium for criminal acts, such as in electronic commerce, banking, child pornography, hate speech and other.[75]

The ISPs have the obligation, under the **Law on Electronic Communications** (LEC), "to introduce the measures for the prevention and the suppression of abuse and fraud associated with the use of electronic communications networks and services".[76] In addition, they are in charge of protecting personal data and privacy within the electronic communications sector[77] and to "protect users' rights in the electronic communications sector".[78] **The Agency for Electronic Communications** is in charge of monitoring the implementation of the Law on Electronic Communications, thus the fulfillment of the ISPs obligation.[79]

---

72 Ministry of Interior Press Release No. 256/14 of 2 June 2014, http://www.mup.gov.rs/cms_cir/saopstenja.nsf/arhiva-saopstenja-MUP-2014 (accessed on 7th October 2015); Also: http://mondo.rs/a697725/Info/Drustvo/MUP-pokrenuo-istragu-zbog-hakovanja-Pescanika. html.

73 Article 303 of the Criminal Code of the Republic of Serbia.

74 http://www.mup.gov.rs/cms_lat/saveti.nsf/saveti-sajber-kriminal.h (accessed on 10 October 2015).

75 Ibidem.

76 Article 37, Para 2, point 15 of the LEC.

77 Article 37, Para 2, point 14 of the LEC.

78 Article 37, Para 2, point 12 of the LEC.

79 Article 1 of the LEC.

There is a **self-regulation** civic society initiative "**Center for Safer Internet**" that runs the "Net patrol" hotline (**Netpatrola**),[80] part of the INHOPE center initiative. Net Patrola is a civic initiative with several aims: to prevent dissemination of the online content that is harmful, "to assist in reporting of video materials and images containing representation of child sexual abuse, sexual exploitation and physical and psychological assaults against children, to provide for the necessary preconditions for the relevant state bodies to enable their further investigations and assessments of the contentious contents."[81] Upon the acceptance of the complaint, Netpatrola analyses it and then decides further steps based on the result. The reported content can be judged as:[82]

1. "probably illegal",
2. "legal, but harmful to children",
3. "legal and not harmful to children".

When "probably illegal", the procedure depends on whether the content is located in Serbia or whether the content is located abroad, again depending whether the country is part of the INHOPE. When the content is located in Serbia, Net patrol sends the information to the ISP, and then the ISP is in charge of removal of the content from their server. At the same time, Net patrol sends the report about the illegal content to the Police, or if the case is urgent and the child in danger they will make a phone call to the Cybercrime department. Finally, upon the request from Net patrol, the Police will investigate the report and file criminal charges to the Republican Public Prosecutor's Office in accordance with the Law. In case that the reported content is located within the country where the INHOPE operator works, Net Patrol will forward the information to INHOPE for their further action. And finally, if the material is hosted in a country without the INHOPE representative, the Net patrol will ask the Serbian Ministry of Interior to look for an international legal assistance in that matter.

When the content is "legal, but harmful to children", Net patrol sends the information to the ISP and if the content is located in Serbia, it should be removed.

Finally, Net patrol will not take any action if the reported content is "legal and not harmful to children".

5. Assessment as to the case law of the European Court of Human Rights

After the recent case law[83] of the European Court of Human Rights, it is expected that many other Council of Europe countries will follow its path.

Apart from the cases described above, related to blocking of ISPs offering Voice-over-IP services or arresting people for their speech on the Internet, there was not much legal practice in Serbia in this domain. Therefore, it is hard to assess any case as to the case law of the European Court of Human Rights. However, there is a new regulatory framework which may lead to some judgments in the near future.

---

80 www.netpatrola.rs.

81 "Reports Submission and Processing Procedure", Net Patrola, http://www.netpatrola.rs/en/operational-procedure.1.70.html (accessed on 1st October 2015).

82 Ibidem.http://www.netpatrola.rs/en/operational-procedure.1.70.html and http://www.netpatrola.rs/en/schematic-representation-of-the-procedure.1.72.html#!prettyPhoto (accessed on 1st October 2015).

83 For example: Neij and SundeKolmisoppi v. Sweden, AhmetYildirim v. Turkey, Akdeniz v. Turkey, Ashbi Donald and Others v. France, Delfi AS v. Estonia and other.

The **Constitution** and newly adopted **Media Laws** guarantee the freedom of expression and point out the situation where it can be restricted. The **Criminal Code** prescribes situations that may lead to limitation of freedom of expression and the removal of Internet content (e.g. in cases of child pornography), when it is prescribed by the law. However, there are no specific safeguards as set by the European Court of Human Rights regarding any limitation of freedom of expression in general and more specifically blocking, filtering and taking down of illegal content in other laws so far.
The **Law on Public Information and Media** for the first time defines the "freedom of spreading information and ideas over the Internet and other platforms"[84] as one of the ways to implement the freedom of expression in general sense in Serbia. At the same time, Internet portals and Internet pages with editorial control are for the first time defined as "media",[85] while search engines, Internet platforms, such as forums and social networks remain outside the scope of the definition of the media,[86] thus the UGC remains outside the regulation of this law.

In the above described cases in the first part of 2014, there was the discrepancy between the necessity and proportionality of the interference with the freedom of expression on the Internet. The **European Commission Progress Report for 2014** expressed concern about the "deteriorating conditions for the full exercise of freedom of expression in Serbia. More generally, there is a growing trend of self-censorship which, combined with undue influence on editorial policies, and a series of cases of intervention against websites, are detrimental to freedom of the media… In this respect the efforts are expected to identify and prosecute suspects of violations of Internet freedoms".[87]

To conclude, **the freedom of expression on the Internet is still very fragile** in Serbia, and blocking, filtering, taking-down of illegal Internet content is not always done in accordance with the law nor following the procedures. The occasional hacking attacks that lead to web sites being unavailable for several days, look like a new form of censorship that should be taken into closer consideration by the Council of Europe in its future policy work.

Jelena Surculija Milojevic
Faculty of Political Sciences, University of Belgrade
02.11.2015

---

84 Article 3, Para 1 of the Law on Public Information and Media, Official Gazette of the Republic of Serbia, No.83/2014.

85 Article 29, The Law on the Law on Public Information and Media, Official Gazette of the Republic of Serbia, No.83/2014.

86 Article 30, Para 1 of the Law on Public Information and Media, Official Gazette of the Republic of Serbia, No.83/2014.

87 Serbia Progress Report, October 2014; http://ec.europa.eu/enlargement/pdf/key_documents/2014/20140108-serbia-progress-report_en.pdf (accessed on 12th October 2015).