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 490-498

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.

MONTENEGRO

1. Legal Sources

Montenegro does not have a law that specifically regulates blocking, filtering and take-down of illegal content. The Internet is rather regulated within several different legal documents, on various levels – from Constitution, via various laws, such as Law on Media, Law on Electronic Media, The Criminal Law, the Law on Electronic Commerce, towards the self-regulatory mechanisms of the Agency for Electronic Media and Media Council for Self-Regulation.

Montenegro has signed and ratified the Council of Europe **Convention for the Protection of Human Rights and Fundamental Freedoms** that regulates freedom of expression in its Article 10, on 4 April 2005 and ratified on 14 April 2009.[1] The Convention has a power of the Law, while freedom of expression from Article 10 with its restriction is regulated mainly by the **Law on Electronic Media.**[2]

Regarding other international instruments, Montenegro signed **the Convention on Cybercrime** on 7 April 2005, ratified it on 3 March 2010[3] and it entered into force on 1 July 2010. Montenegro, at the same time, signed and 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 body in charge of "sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution in the absence of an agreement" will be the **Ministry of Justice of Montenegro,**[4] the same authority in charge with "making and receiving requests for extradition in the absence of an agreement", while "the authority responsible for making and receiving requests for provisional arrest in the absence of an agreement"[5] will be the **NCB Interpol** in Podgorica.

When Ratifying the Additional Protocol, Montenegro expressed the Reservation where it requires "that the denial or the gross minimization, approval or justification of acts constituting genocide or crimes against humanity, be committed with the intent to incite hatred, discrimination or violence against an individual or group of individuals based on race, color, descent or national or ethnic origin, as well as religion if used as pretext for any of these factors, or otherwise".[6]

---

1 Entered into force on 1st August 2009.

2 Official Gazette No. 46/2010.

3 Montenegro made several Reservations while ratifying the Cybercrime Convention, which are the following:

- Montenegro declares that "obtaining child pornography through computer systems for oneself and other persons and possession of child pornography in computer systems or on mediums for storage of computer data shall not be considered offences in case the person displayed in these materials turned fourteen years of age and gave his/her consent".
- Montenegro also declares that "materials which visually display face by which it can be concluded that the person is a minor engaged in an explicit act (as stated in Article 9, paragraph 2, item b)… shall not be considered child pornography".
- Montenegro declares that "measures from Article 20 of the Convention shall be applied solely on the basis of the decision of a competent Montenegrin court, if it is necessary for conducting a criminal procedure or for reasons of safety in Montenegro".

4 List of declarations made with respect to treaty No. 185 Convention on Cybercrime, Status as of 15/9/2015.

5 List of declarations made with respect to treaty No. 185 Convention on Cybercrime, Status as of 15/09/2015.

6 In accordance with Article 6, Paragraph 2, item b and Article 12, paragraph 3 of the Additional Protocol, The List of declarations made with respect to Treaty No. 189, Status as of 14/09/2015.

Further on, Montenegro signed the **Convention for the Protection of individuals with regard to Automatic Processing of Personal data** (CETS No. 108), ratified it on 6 September 2005 and it entered into force on 06 June 2006. The authority in charge of implementing this Convention shall be the **Secretariat for development of the Republic of Montenegro**. Montenegro, regarding this Convention, declares that it will apply, "in accordance with Article 3, paragraph 2 of the Convention, the Convention to automated databases containing personal data being kept in accordance with criminal records and State security regulations".[7] The **Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data**, regarding supervisory authorities and transborder data flows (CETS No. 181) was signed on 24 February 2009, ratified on 3 March 2010 and has entered into force on 1 July 2010.

The Council of Europe **Convention on Access to Official Documents** (CETS No. 205) was signed on 18 June 2009 and ratified on 23 January 2012.

The Council of Europe **Convention on the Prevention of Terrorism** (CETS No. 196) was signed on 16 May 2005, ratified on 12 September 2008 and entered into force on 1 January 2009.

The Council of Europe **Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse** (CETS No. 201) was signed on 18 June 2009, ratified on 25 November 2010 and entered into force on 1 March 2011. The competent national authority will be the **Police Directorate of Montenegro, Forensic Center**. Also, Montenegro declares that it "considers Article 18, paragraph 1, item a, as applying to a person younger than 16 years, and item b to a person younger than 18".[8] In addition, Montenegro declares that "it will take over prosecution for the case stipulated in Article 25 paragraph 1, item e, in accordance with its own criminal legislation".[9] Finally, Montenegro declares that the Convention shall apply to the territory of Montenegro.[10]

2. Legal Framework

The Montenegrin legal framework related to blocking and/or filtering of illegal online content as well as take down/removal of illegal content on the Internet are covered by several documents of various legal strength.

The **Constitution of Montenegro** confirms that "ratified and published international contracts and generally accepted rules of international law are part of the internal legal framework and have the primacy over the national legislation and are implemented directly when regulating differently from national laws".[11] This means that all the above mentioned international documents that are signed and ratified by Montenegro have the stronger power than existing national legislation. Further on, the Constitution deals with the Freedom of expression, the discrimination, hate speech, right to respect for religious freedoms and prescribes the umbrella rules that should be regulated in details by various laws. The **Criminal Code** has incorporated many international standards, but, in accordance to **Ombudsman** opinion,[12] there are still few missing related to information society.[13] The

---

7 The List of declarations made with respect to treaty No. 108, status as of 14/09/2015.

8 In accordance with Article 18, paragraph 2 of the Convention; List of declarations made with respect to treaty No. 201, Status as of 14/09/2015.

9 In accordance with Article 25, paragraph 3 of the Convention; List of declarations made with respect to treaty No. 201, Status as of 14/09/2015.

10 In accordance with Article 47, paragraph 1 of the Convention.

11 Article 9 of the Constitution of Montenegro.

12 "The Abuse of Children on the Internet", the Report of Ombudsman of Montenegro, Podgorica, March 2013

Law on Electronic Communications regulates the role of citizens/users and those of Internet service providers as well as their liability. The **Agency for Electronic Communication**[14] is in charge of protecting the interests of users, solving the disputes on the electronic communications market, monitors the work of operators, in accordance with the law, technical regulations and standards in Montenegro.[15] The **Agency for Electronic Media** monitors the work of the electronic media in line with the **Law on Electronic Media.**[16] In accordance with this law, the electronic publications are "edited Internet portals that publish either electronic versions of print media and/or information from media that enable the general public access to it, despite the real coverage".[17] Therefore, the Agency for Electronic Media can issue the general authorisation "for broadcasting the digital or analogue terrestrial, cable, Internet or satellite broadcasting",[18] except Internet webcasting for which there is no authorization required.[19] As a result, the authorization for providing audiovisual media services may be withdrawn, if the AVM provider continues to breach the provisions on programme standards, prescribed by this law, after previously being issued warning and fine.[20] The **Law on Electronic Commerce** is important for uninterrupted commerce on the Internet. Finally, Montenegro has strong self-regulation mechanisms in accordance with the **Ethical Codex of Journalism**. The authority in charge of monitoring and implementing it is the **Media Council for Self-regulation**.

2.1. Blocking and/or filtering of illegal Internet content

The **Constitution of Montenegro**[21] says that "everyone has the right to freedom of expression, by speech, in writing, by picture or any other way. The right to freedom of expression can be restricted only by someone else's right to dignity, honor or by threatening public moral or security of Montenegro".[22] Further on, the Constitution prohibits the encouraging or inducing hatred or intolerance on any grounds[23] and any direct or indirect discrimination on any grounds.[24] And finally, the freedom of thought, conscience or religion is guaranteed as well as a right to change it. The right to respect the religious freedoms can be restricted only "if it is necessary to protect lives and health, public order and peace, as well as other rights protected by the Constitution".[25]

The Criminal Code prescribes a set of criminal offences that are either directly or indirectly related to illegal content on the Internet.

The first group of criminal acts is **against sexual freedoms**. The first criminal act is against "anyone who sells of displays to a child or by public displaying or in some other way makes available text, pictures, audio-visual or other objects of pornographic content or displays to it a pornographic show, shall be punished by a fine or an imprisonment sentence not exceeding six months".[26] The imprisonment sentence of six months to five year will be placed upon "anyone who uses a child to produce pictures, audio-visual or other objects of pornographic nature or for a pornographic

---

13 For example, the Ombudsman refers that there is no definition of "sexting", "grooming" or "cyber bullying" while these are the acts that the children complain the most of.

14 Official Gazette of Montenegro, No. 40/2013

15 Article 11 of the Law on Electronic Communications

16 Official Gazette of Montenegro, No. 46/10, 40/11, 53/11

17 Article 8, Paragraph 1, Point 18 of the Law on Electronic Media.

18 Article 98, Paragraph 1 of the Law on Electronic Media.

19 Article 98, Paragraph 2 of the Law on Electronic Media.

20 Article 142, Paragraph 1, Point 3 of the Law on Electronic Media.

21 Official Gazette of Montenegro, No 1/2007.

22 Article 47 of the Constitution of Montenegro

23 Article 7 of the Constitution of Montenegro.

24 Excluding positive discrimination, Article 8 of the Constitution of Montenegro

25 Article 46 of the Constitution of Montenegro

26 Article 211, Paragraph 1 of the Criminal Code.

show",[27] shall be punished by an imprisonment sentence of six months to five years. And finally, "anyone who sells, shows, publicly exhibits or in electronic or some other way makes available pictures, audio-visual or other objects of pornographic character resulting from acts referred to in Paragraph 2 of this Article shall be punished by a maximum sentence not exceeding two years".[28] The important segment is that the objects use for the commitment of this criminal act will be confiscated and destroyed.[29]

The Internet Watch Foundation (IWF) had revealed, in its Annual Report from 2010, that online child sexual abuse content is highly dynamic and transient, as a result of which the IWF blocking list is updated twice a day. According to the IWF 2010 report, over 70 ISPs, search and content providers, mobile operators and filtering companies take steps to prevent their customers from being exposed to child sexual abuse content. Furthermore, the IWF webpage blocking list is deployed across six continents and in countries including Montenegro.[30] The **Ombudsman** monitors the implementation of human rights on the Internet has raised several issues related to the abuse of children on the Internet.

The next group of criminal acts relevant for this research are criminal acts **against the Constitutional order and security of Montenegro**. The criminal act on causing national, race and religious hatred[31] says that "anyone who publicly encourages to violence or hatred towards the group or group member related to race, skin color, religious, the origin, state or national affiliation, will be punished by imprisonment for a term of six months to five years".[32] The same punishment will be call on anyone who "publicly approves, denies existence or significantly decreases the heaviness of genocide, crime against humanity and war crimes against group or group member set based on the race, skin colour, religion, the origin or state or national affiliation" if it can cause violence or hatred towards to group or group member, if such criminal acts are legally decided by judgment in effect of either Montenegrin or international criminal court. The major amendment within the Criminal Code since its adoption in 2003, related to this criminal act is the verb **publicly** as it can now be interpreted as happening on the Internet, as well. The same refers to the criminal act **associating for unconstitutional activities,**[33] where the law can be interpreted as associating on the Internet. And finally, the criminal act **preparing acts against the constitutional order and security**[34] can also be executed in the online world (the "preparation" part).

The next important criminal act is on **racial and other discrimination**. Article 443 says that "anyone who, on grounds of a difference in race, skin colour, nationality, ethnical origin, or some other personal characteristic violates fundamental human rights and freedoms guaranteed by generally recognized principles of the international law and international treaties ratified by Montenegro, shall be punished by imprisonment for a term of six months to five years".[35] The same punishment will be imposed to a person who persecutes organizations or individuals for their efforts to ensure equality of people. Finally, the punishment by imprisonment for a term of three months to three years will be

---

27 Article 211, Paragraph 2 of the Criminal Code.

28 Article 211, Paragraph 3 of the Criminal Code.

29 Article 211, Paragraph 4 of the Criminal Code.

30 The OSCE Report: 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, The Office of the Representative on Freedom of the Media.

31 Article 370 of the Criminal Code

32 Ibidem.

33 Article 372 of the Criminal Code.

34 Article 373 of the Criminal Code.

35 Article 443, Paragraph 1 of the Criminal Code.

placed upon "anyone who spreads ideas about the superiority of one race over another, or promotes racial hatred, or instigate racial discrimination".[36]

The Criminal Code prescribes the legal offence for **unlawful circumvention of the protection measures intended to prevent violation of copyright and related rights** and information on rights for "anyone who produces, imports, puts into circulation, sells, leases, advertises with the aim to sell or to lease or who keeps for commercial purposes the devices or instruments intended mainly or predominantly to remove, circumvent or evade technological measures intended to prevent violation of copyright and related right or who uses such devices or instruments with the aim to violate copyright and related right".[37] The punishment for such an offence will be a fine or an imprisonment sentence for a term of up to three years, while "the instruments of commission of criminal offence and the instruments which were used or intended for commission of the criminal offence... shall be seized, while the instruments of commission of criminal offence shall be destroyed".[38]

As the OSCE Report on Freedom of Expression on the Internet says, Montenegro had no general legal provisions regulating the blocking on the Internet, but was one of the countries that legally protected the right to access the Internet.[39] However, that was part of the previous Law on Electronic Communications[40] that provided for the right to access the Internet[41] and said that "everyone has a right to use the public electronic communications services, under known conditions and prices, and if there is technical availability".[42] However, with the adoption of the new **Law on Electronic Communications** from 2013, that replaced the previous one from 2008, the citizens still have a right to access the Internet, but not in a form of a human right, but rather as a commercial contract. In the new law, "the user of public communications services has a right to access the public electronic communications network, eight days after it requested it, if there is technical possibility".[43] The user is here defined as "physical or legal person that uses or requests the public communications services". Although both laws provide for the access to electronic communications networks, it seems that 2013 law lost the "human rights touch" that the Law from 2008 had regarding access to the Internet. In this law, **the operator** has competencies to warn or temporarily block the user account in case it has evidence that the user sent spam or that the use abused the user account of electronic mail.[44] If the user continues to abuse the electronic mail, the operator can permanently delete the users electronic email account and revoke the contract. However, that will not happen if the electronic mail was not abused by the user, but by the third person unless the user avoided operators warnings to use the protection.[45] The **Agency for electronic Communications and Post** is in charge of prescribing conditions to prevent and repress the misuse and frauds related to electronic mail services.[46]

---

36 Article 443, Paragraph 3 of the Criminal Code.

37 Article 235, Paragraph 1 of the Criminal Code.

38 Article 235, Paragraph 2 of the Criminal Code.

39 The OSCE Report: 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, The Office of the Representative on Freedom of the Media.

40 Official Gazette ...

41 The OSCE Report: 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, The Office of the Representative on Freedom of the Media and Article 102 of the previous Law on Electronic Communications.

42 Article 102 of the old Law on Electronic Communications 2008.

43 Article 147 of the Law on Electronic Communications, Official Gazette 40/2013.

44 Article 179 of the Law on Electronic Communications, Official Gazette 40/2013.

45 Ibidem.

46 Ibidem.

In **Montenegro**, the EU E-Commerce Directive 2000/31/EC was incorporated in **the Law on Electronic Commerce.**[47] **Providers of the information services** are not held liable for **cashing** of the content when they remove or block the access to data as soon as they find out that data has to be removed from the network or that the court/authorised state authority had ordered its removing/blocking.[48] On the other hand, providers of the information services are not held liable for **hosting** of the user's data if, immediately after receiving information that the data held is illegal, removing it from the network or blocking access to it.[49] The same applies for the providers of information services that offer access to third data (**linking**).[50]

2.2. Take-down/removal of illegal Internet content

The institution in charge of reporting to take-down and remove the illegal content in Montenegro is called the **National Montenegrin Computer Incident Response Team** (**CIRT**). It is responsible to the Assistant Minister of Information Society and Telecommunications[51] and has the responsibility to coordinate and assist the whole country of Montenegro, especially the state institutions and critical infrastructure, to implement pro-active services in order to decrease the risk of computer incidents as well as to make a response to such incident in case they occur.[52] CIRT is also working on awareness raising and education on how to recognize the cyber threats and cybercrime.

Although CIRT is not a member of INHOPE initiative,[53] the procedure for removing the illegal Internet content is very similar to it. The reporting is done via web site and CIRT has to respond to it within 24 hours. If the content is identified as not appropriate and damaging for children, but not illegal, CIRT will inform the administrator of the web site about it and request that the material is measured to be appropriate for children. In case the content is disturbing, and it can hurt the physical or mental integrity of children, the material needs to be located. If the material is located on an Internet Host Provider from Montenegro or on an user account hosted by the ISP in Montenegro, the identity of the ISP where the user's account is based is determined. Finally, CIRT informs the Ministry of Interior, the department in charge, via special e-mail address. **Internet Service Provider** is in charge to remove the content from its server. However, in case of emergency, the CIRT will phone the Ministry of Interior and inform them directly about the case in question. After receiving the information, The Ministry of Interior will investigate the case and press criminal charges further on, in accordance with the law.[54] Unfortunately, the statistics of incidents and annual reports were not available, so it would be good to monitor the CIRT web site for the future reference. The Ministry of Information Society and Telecommunications has a project in cooperation with the Ministry of Education and Telenor on Safer Internet (Connecting Generations).[55]

3. Procedural Aspects

The Ombudsman, in his report "Abuse of Children on the Internet – The Research of Ombudsman of Montenegro", concluded that the reporting of abuse of children using information-communications technologies is rare, and that they come to institutions in charge only in few numbers. He added that in Montenegro "there are neither still efficient mechanisms to report, discover, protect, punish nor

47 Official Gazette of the Republic of Montenegro No. 80/2004; http://www.cirt.me/dokumenta/Zakon-o-elektronskoj-trgovini.pdf (accessed 12th October 2015).
48 Article 19 of the Law on Electronic Commerce.
49 Article 20 of the Law on Electronic Commerce
50 Article 21 of the Law on Electronic Commerce
51 http://www.cirt.me/organizacija (accessed on 8th October 2015).
52 http://www.cirt.me/misija (accessed on 8th October 2015).
53 http://www.inhope.org/gns/home.aspx (accessed on 8th October 2015).
54 http://www.cirt.me/kutak (accessed on 8th October 2015).
55 http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/global-alliance-against-child-abuse/docs/reports-2014/ga_report_2014_-_montenegro_en.pdf

institution in charge of implementation, support and help"[56] for such cases. The Ombudsman had in mind the report of cases of abuse of children via information technologies, as he concluded that there are occasional reports, usually just orally, about the abuse via the Internet, but not as much as it should be in accordance with cases reported in his research. After the research for this report, the same conclusion can be drawn for general cases related to information society and use of new technologies in Montenegro.

Regarding the procedural aspects for criminal acts – there are two options. First is the criminal offence for which the prosecutor reacts ex officio, where the public prosecutor has the obligation to undertake measures to direct the police in the investigation, can postpone the criminal prosecution in accordance with the law, can reject criminal reports for the reasons of fairness, can execute the investigation, collect evidences, close agreements on admittance of guilt and many more. Therefore, the police is obliged to inform the public prosecutor before any activity they may undertake, except in case of emergency.[57]

And second option is for criminal acts that are not prosecuted ex officio, but are prosecuted upon private complaint. It has to happen within three months since private prosecutor has found out about the criminal act and perpetrator.[58] For example, investigations of some of the criminal acts against intellectual property are undertaken upon a private complaint.[59] Also, when there is a private complaint for a criminal act of insult, the defendant can file a contra-private complaint against the person that insulted him/her back. In this case, the court will file one verdict.[60]

4. General Monitoring of Internet

There is no single body in charge of monitoring the Internet content in Montenegro. However, there are several bodies that, from various aspects, review the online content and assess its compliance with various laws.

First, the **Police Directorate of Montenegro, Forensic Center** monitors the implementation of the Criminal Code.

The **Agency for Electronic Media** is in charge of implementing the Law on Electronic Media which defines electronic publications as "Internet pages and/or portals that have editorial control and consists of electronic versions of print media and/or information from media to wider public, not matter of its scope".[61] The Agency is in charge of issuing broadcasting licenses via digital or analogue, terrestrial, cable, Internet or satellite transmission. However, the broadcasting of the programme via global information network (Internet webcasting) does not fall under the obligation to obtain the license.[62] As an example, The Agency for Electronic Media had noticed that in October 2011 there was the expansion of information that contains direct description of violence and its consequences or videos of victims that can be disturbing for audience on both Internet portals and in Montenegrin electronic media. The Agency also observed that there were an increased number of warnings to disturbing content before broadcasting it than before, but there was also much more illegal content,

---

56 "The Abuse of Children on the Internet", Report of Ombudsman of Montenegro, Podgorica, March 2013.

57 Article 44 of the Law on Criminal Procedure.

58 Article 51, Paragraph 1 of the Law on Criminal Procedure.

59 Article 233, Paragraph 3, of the Criminal Code.

60 Article 51, Paragraph 2 of the Law on Criminal Procedure.

61 Article 8, Paragraph 1, Point 19 of the Law on Electronic Media.

62 Article 98 of the Law on Electronic Media.

explicit violence and its consequences in both broadcast video as well as in comments by audiences. The Agency warned that such a practice seriously threats the implementation of legal and ethical framework as well as possibility that the public is informed true, objectively and timely. As a result, the Agency published the Press Release where invited electronic media and Internet portals to respect and protect the public interest, especially of minors, the respect of privacy and ethical values of citizens of Montenegro. The Agency had stressed that if the practice like that continued, it would have to undertake not only preventive, but also other legal measures in order to protect the public interest and citizens of Montenegro.[63]

Second, the **Media Council for Self-Regulation** is an independent self-regulatory body that monitors the broadcasting, print and online media in Montenegro. The aim of the Council is to develop and improve the media self-regulation in Montenegro in order to protect citizens from non-ethical reporting in media and raises the awareness on the importance of truthful and timely reporting.[64] The Media Council monitors the implementation of Codex of Montenegrin Journalists[65] in media and acts as a mediator between unhappy readers and media. In addition, the Media Council decides on citizens' complaints on media and protects the public from unprofessional and manipulative journalistic reporting. Finally, it publishes quarterly reports which are available on its web site.[66]

Finally, **the Agency for Electronic Communications and Post** monitors the implementation of the Law on Electronic Communications. In case of fraud or misuse, the operator has the obligation that, upon the request of the Agency or on its own initiative but with the Agency's approval, blocks the access to certain numbers and services.[67]

The Ombudsman monitors the protection of children on the Internet and has made several recommendations in his above mentioned report. The Ombudsman recommends **the establishing of the unique database** on all cases of abuse of children on the Internet – in all segments, from oral reporting to cases that were processed. The Ombudsman is of opinion that it would enable monitoring of cases related to abuse of children on the Internet, as well as better data flow between various institutions.[68]

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

The main issue in Montenegro seems to be the publishing of UGC (user generated content) comments on the web portals, especially mass media web sites where many times the European Court of Human Rights standards are not met. The Media Council for Self-Regulation (MCSR) publishes quarterly reports on the work of Montenegrin media in that period. The last part of every report is related to Internet portals of media outlets that are subject to monitoring. The main remark of most of the reports is a problem of hate speech or insulting comments, published on media portals. The Media Council for Self-Regulation invites media to strengthen the rules on non-publishing of such a speech, rather than to react once the illegal comments are already published and sometimes voluntarily remove it or not.[69] The Media Council explains that "despite the fact that

63 The Press Release No. 02-1221 of the Agency of Electronic Media, Podgorica, 25.10.2011.

64 http://medijskisavjet.me (accessed 7th October 2015).

65 www.medijskisavjet.me/wp-content/uploads/2013/03/CODEX-OF-MONTENEGRIN-JOURNALISTS.doc (accessed on 7th October 2015).

66 http://medijskisavjet.me/en/dokumenti (accessed on 7th October 2015).

67 Article 145, The Law on Electronic Communications.

68 "The Abuse of Children on the Internet", the Report of Ombudsman of Montenegro, Podgorica, March 2013.

69 For example, Report No 15. Covering the period 01.12.2014 – 15.02.2015.

the Codex of Journalists of Montenegro does not explicitly mention online journalism, bearing in mind that it deals with ethical standards of journalists profession (mass media, social networks, whatever), the Media Council has taken the stand that the ethical rules apply to portals and comments of readers as that relationship opens a great interaction between media and readers, and is often a place where freedom of expression is abused. The Media Council stand point is that the media editorial is responsible for content published on Internet portal. It often breaches internal "Users' manual" that it will not publish the information that call for racial, religious and national hater or use them in any context of bad language and call for violence".[70] The Media Council stresses that media portals that want to open the public debate "has to take into consideration not only their own dignity but also of consequences of public words that can threat someone's life, destroy the family and the public debate itself".[71] The Media Council has recommended that some categories of news should not be commented at all, such as chronics when someone dies or gets killed, or when someone is called guilty without trial, etc.

This approach is in line with the European Court of Human Rights stand point, especially with the latest "Delfi vs Estonia" case[72] where Delfi, news portal, was held liable for the offensive comments that its readers were leaving online.

To conclude, even though in some cases, such as self-regulatory mechanisms at the Media Council, the regulatory framework has precise and specific rules on the scope of the restrictive measure of blocking/filtering, this still does not necessarily mean that these rules will be implemented in practice. The best example are the rules that almost every media with Internet portal has, about non-publishing hate speech, insults, etc., and then when real comments arise, there is no editorial control over them.

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

70 Ibidem.
71 Ibidem.
72 European Court of Human Rights Case of Delfi AS v. Estonia, Application no. 64569/09, 16.06.2015.