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 694-710

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.

''THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA''

1. Legal Sources

"The former Yugoslav Republic of Macedonia" is a democratic society which will ensure security and public safety without restricting any democratic principles such as freedom of expression or privacy. Given the achievement in the field of rule of law and valuation of democratic principles and norms, "The former Yugoslav Republic of Macedonia" strives for further improvement and development of information technology in accordance with the standards and practices of the Council of Europe, European Union and EU member-states, as a way to ensure the overall cultural, educational, economic and political progress of the country. Freedom of expression and information in the media is an essential requirement of democracy ***as guaranteed in Article 16 of the Constitution.***

Since 1995, most of the relevant international standards related to illegal Internet content have been transposed into the national regulatory framework: the European Convention for the Protection of Human Rights and Fundamental Freedoms (hereinafter referred to as ECHR) and Amending Protocol,[1] the Convention on Cybercrime and its Additional Protocol,[2] the European Convention on the Prevention of Terrorism,[3] the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and Additional Protocol.[4] One of the most important international standards related to illegal Internet content which have been transposed into the domestic regulatory framework is the European Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, CETS No.: 201.[5]

There is no specific code regulating the issues of blocking, filtering and take-down of the internet content. This area is regulated through several legal acts such as the Criminal Code,[6] the Law on

---

1 The ECHR, CETS No.005, Rome, (4.11.1950) was signed on 9.11.1995, ratified on 10.4.1997 and entered into force 10.4.1997 ; the Protocol to the European Convention for the Protection of Human Rights and Fundamental Freedoms, CETS No.: 009, Paris (20.3.1952) was signed on 14.6.1996, ratified on 10.4.1997 and entered into force 10.4.1997.

2 The Convention on Cybercrime, CEST No.:185 was signed on 23.11.2001, ratified on 15.9.2004; entered into force 1.1.2005. Law on ratification of Convention on Computer Crime, "Official Gazette of the RM" No. 41 (24.06.2004); the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, CEST No.:189 was signed on 14.11.2005, ratified on 14.11.2005 and entered into force 1.3.2006, Law on Ratification of the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems "Official Gazette of the RM" No. 56 (13.07.2005).

3 The European Convention on the Prevention of Terrorism, CETS No.:196, Warsaw (16.5.2005) was signed on 21.11.2006, ratified on 23.3.2010 and entered into force 1.7.2010. Law on Ratification of Convention on the Prevention of Terrorism, "Official Gazette of the RM" No. 20 (16.2.2009).

4 The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CEST No.:108, Strasbourg, (28.1.1981) was signed on 24.03.2006, ratified on 24.03.2006 and entered into force 1.7.2006. Law on Ratification of Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, "Official Gazette of the RM" No.7 (1.02.2005); the Additional Protocol to the Convention, regarding supervisory authorities and transborder data flows, CETS No.:181, Strasbourg, (8.11.2001) was signed on 4.1.2008, ratified on 26.9.2008 and entered into force 1.1.2009. Law on Ratification of Additional Protocol, "Official Gazette of the RM" No.103 (19.8.2008).

5 Signed on 25.10.2007; ratified on 11.6.2012; entered into force 1.10.2012. Law on Ratification of Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, "Official Gazette of the RM" No.135 (8.10.2010).

6 Criminal Code of the Republic of Macedonia, "Official Gazette of the RM" No. 37/1996; 80/1999; 4/2002; 43/2003; 19/2004; 81/2005; 60/2006; 73/2006; 7/2008; 139/2008; 114/2009; 51/2011;

Audio and Audiovisual Media Services,[7] the Law on Electronic Communication,[8] the Law on Media,[9] the Law on Copyright and Related Rights,[10] the Law on Personal Data Protection,[11] the Declaration on Safer Internet,[12] etc.

In "The former Yugoslav Republic of Macedonia", as a democratic society established by the Constitution,[13] the legislation and supervision of illegal internet content is based on the foundations provided by the principle of freedom of expression, guaranteed by Article 10 of the ECHR and by Article 19 of the Universal Declaration of Human Rights.[14] "The former Yugoslav Republic of Macedonia", as a member state of the Council of Europe (hereinafter referred to as CoE) and a country candidate for membership of European Union, has already transposed the most relevant CoE conventions and tends to further harmonize the domestic legislation with EU's *acquis communautaire.*

2. Legal Framework

"The former Yugoslav Republic of Macedonia" belongs to the *"B" Category* of the countries; it has enacted *no specific legal basis* to deal with the filtering, blocking, take-down or removal of the illegal content on Internet.

2.1. Blocking and/or filtering, take-down/removal of illegal Internet content

Protection of certain issues of public interest such as national security, territorial integrity, public safety etc., is regulated by the Constitution and the specific laws, usually within universal access laws or regulations. ***The Constitution*** guarantees the freedom of conviction, conscience, thought and public expression of thought, speech, public address and public information. Free access to information and the freedom of reception and transmission of information are guaranteed. The right of reply via the mass media is guaranteed. The right to a correction in the mass media is guaranteed. The right to protect a source of information in the mass media is guaranteed. ***Censorship is prohibited*** (Article 16). Anything that is not prohibited by the Constitution or by law is permitted in "The former Yugoslav Republic of Macedonia" (Article 8).

Article 3 of ***the Law on media*** guarantees the freedom of expression[15] and freedom of the media may be limited only in accordance with the Constitution. Then again, Article 44 of ***the Law on Audio***

135/2011; 185/2011; 142/2012; 166/2012; 55/2013, 82/2013, 14/2014; 27/2014; 28/2014; 115/14, 132/14; 160/14 and 199 /2014.

7 Law on Audio and Audiovisual Media Services, "Official Gazette of the RM" No. 184/13, 13/14, 44/14, 101/14 and 132/14.

8 Law on Electronic Communication, "Official Gazette of the RM" No. 39/14, 188/14 and 44/15.

9 Law on media, "Official Gazette of the RM" No. 184/13 and 13/14.

10 Law on Copyright and Related Rights, "Official Gazette of the RM" No. 115/10, 51/11 and 147/13 (3.09.2015).

11 Law on Personal Data Protection, "Official Gazette of the RM" No. 7/05, 103/08, 124/10, 135/11 and 43/14.

12 Declaration on Safer Internet, ("Official Gazette of the RM" No. 31, 3.03.2010.

13 Available at http://www.sobranie.mk/the-constitution-of-the-republic-of-macedonia.nspx (14.9.2015).

14 All limitations to the freedom of expression ought to be, in accordance with principles of democratic society, based solely on the specific list provided in Article 10, Paragraph 2 of the ECHR, to be defined in a law, narrowly interpreted, respond to a specific social need, have legitimate goal and be proportional to that goal, and to be deemed necessary in a democratic society.

15 Article 3, par.2 of the Law on media: The freedom of the media shall particularly include: freedom to express opinions, independence of the media, freedom to collect, research, publish, select and transmit information for the purpose of informing the public, pluralism and media diversity, freedom

and Audiovisual Media Services guarantees the freedom of reception and re-transmission of audio or audiovisual media service on the territory of "The former Yugoslav Republic of Macedonia", the EU member states and other European countries signatories of the European Convention of Transfrontier Television of the CoE.

In the **Criminal Code** of the Republic of Macedonia (hereinafter referred to as CCRM), the chapter of *criminal offences against the rights and freedoms of human beings and citizens* (Ch. XV) in Article 144 titled *Endangering the security* stipulates that: a person who endangers the security of another by a serious threat to attack his/her life or body, or the life and body of some person close to him/her, shall be punished by the law (par.1).

If the threat is performed via information system (Article 144 par.4) it is considered ***as more severe form***. Unlike the main offence, in which the threat may be given in any manner or any mean of communication that reaches the victim, the more severe form of offence is conducted ***"via information system",*** that is, via message transmitted to the victim, directly or indirectly (via social network), with any kind of computer characters (text, graphic design, etc.).

As far as the issue of ***public safety*** is concerned, activities such as public provocation to commit terrorist offences, recruitment for terrorism or training for terrorism or any content related to terrorism, have been criminalized as well. The legislator is aware of the grave concern caused by the increase of terrorist offences and the growing terrorist threat and is also aware that ***CCRM is not sufficient to prevent terrorism*** and to counter, in particular, public provocation to commit terrorist offences. Therefore, the authorities signed and ratified the European Convention on the Prevention of Terrorism, which improves the domestic legal framework with harmonized legal basis, recruitment and training for terrorism ***through the Internet.*** The practice of terrorists and violent extremists using the Internet for propaganda, communication, recruitment and/or financing purposes is increasing as the use of the Internet becomes more widespread and efficient.

There is no general national policy aimed at the analysis, detection, prosecution and prevention of cybercrime and the misuse of cyberspace for terrorist purposes. However, there are specific criminal acts in the area of computer crime which are defined in CCRM. Thus, "The former Yugoslav Republic of Macedonia" joined the other countries in their attempt to oppose the different forms and types of abuse of computer and IT systems.

The national legal system distinguishes several types of criminal acts in the field of computer crime which in some cases can be used for terrorist purposes, as follows:

- Endangering security – Article 144, par.4 CCRM
- Violation of confidentiality of letters or other parcels – Article 147 CCRM
- Misuse of personal data – Article 149 CCRM
- Prevention of an access to a public information system – Article 149-a CCRM
- Violation of an author's right and related rights – Article 157 CCRM
- Violation of the rights of distributors of technically and specially protected satellite signals -Article 157-a CCRM
- Piracy of audiovisual products - Article 157-b CCRM

---

of flow of information and openness of the media towards various opinions, beliefs and content, access to public information, respect of human individuality, privacy and dignity, freedom to establish legal persons for providing public information, publishing and distributing printed media and other domestic and foreign media, production and broadcasting of audio/audiovisual programmes, as well as other electronic media, independence of the editor, the journalist, the authors or creators of contents or programme associates and other persons in accordance with rules of the profession.

- Piracy of phonograms - Article 157-c CCRM
- Showing pornographic materials to a juvenile - Article 193 CCRM
- Production and distribution of child pornography - Article 193-a CCRM
- Enticement of a child under the age of 14 into statutory rape or other sexual activities - Article 193-b CCRM
- Damaging and unauthorised entry into computer system – Article 251 CCRM
- Making and uploading computer viruses – Article 251a CCRM
- Computer fraud – Article 251b CCRM
- Violation of rights arising from reported or protected innovation and topography of integrated circuits - Article 286 CCRM
- Computer forgery – Article 379a CCRM
- Dissemination of racist and xenophobic material through computer system - Article 394-g CCRM

Terrorism as a criminal act against the state is provided for under Article 313, titled Terrorist endangerment of the constitutional order and security of the Criminal Code. ***The Internet can also be used to publish threats*** to cause an explosion, fire, flood or to carry out any other generally dangerous action or an act of violence, for instance *on the webpage of a specific terrorist organisation*, or by *hacking into a webpage of a state authority*, or in another manner, thus creating a feeling of insecurity or fear among the citizens. This means that the committing of the criminal act of "terrorism", i.e. via the misuse of computer and IT systems or unauthorised access to a web page of a state body or another institution which in fact means the misuse of cyber (virtual) space for terrorist purposes, **it is implemented in the Criminal Code**, as follows:

Article 394- b, Terrorism:
(2) Any person who seriously threatens to commit the crime referred to in paragraph (1) of this article directly or indirectly*, by using electronic means or other ways*, with the intention to endanger human life and body and to create feeling of insecurity or fear among citizens, shall be sentenced to imprisonment;
(3) Any person who *publicly calls for, by spreading a message or making it publicly available in any other manner,* with an intention to instigate some of the activities referred to in paragraph (1) of this article, when the appeal itself creates a danger of committing such a crime, shall be sentenced to imprisonment.

Article 394-d, Dissemination of racist and xenophobic material through computer systems:

- Any person who, through a computer system, is distributing racist and xenophobic written material, image or other representation of an idea or theory that advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, color, national or ethnic origin, as well as religious belief, shall be sentenced to imprisonment;
- The sentence referred to in paragraph (1) of this article shall be also imposed upon any person who commits the crime ***through other means of public information***, and
- Any person who commits the crime referred to in paragraphs (1) and (2) of this article by abusing the official position or authority, or if such a crime has resulted in disturbances and violence against other people or in property damage of large proportions, shall be sentenced to imprisonment.

The national legal system differentiates ***the protection of health and morals*** through several types of criminal acts in *CCRM*, in the field of illegal content on the Internet. One of the main criminal acts is **Article 193, *Showing pornographic materials to a juvenile***:

- A person who sells, shows or ***by public presentation in some other way makes available*** pictures, audio-visual or other objects with a pornographic content to a juvenile, under the age of 14, or shows him a pornographic performance, shall be punished with imprisonment [...].
- If the crime has been committed ***through the public information media***, the perpetrator shall be sentenced to imprisonment.
- The punishment from item 2 shall be applied to a person who abuses a juvenile in the ***production of audio-visual*** pictures or other objects with a pornographic content or for pornographic presentations as well as the person who participates in such presentation. [...] (6) If the crime referred to in this Article is committed by a legal entity, the legal entity shall be subject to a fine. (7) The items referred to in paragraphs 1, 2, 3 and 4 ***shall be confiscated.***

The acts of ***owning*** child pornography are incriminated in **Article 193-a**, ***Production and distribution of child pornography:***

(1) The person who produces child pornography with the purpose of its distribution or transfers it and offers it and makes child pornography available in any other manner shall be punished by imprisonment.
(2) The person who shall ***purchase child pornography*** for him/herself or for other person or owns child pornography shall be punished by imprisonment.
(3) If the crime from paragraphs (1) and (2) of this article has been committed through a computer system or other means of mass communication, the perpetrator shall be punished by imprisonment.

The person producing child pornography in order ***to distribute or transfer or offer it, or on other manner makes it available,*** or if the person is purchasing child pornography for himself or for another person, or owns a child pornography, shall be punished by the law. If the act from previous paragraphs is committed ***through a computer system or other means of mass communication***, the offender shall be punished with at least eight years of imprisonment. Safeguards which protect freedom of expression are not included.

The implementation of the new Law on Criminal Procedure (hereinafter referred as LCP) started in December 2013. With the adoption of the New LCP[16] from 2010, ***special investigative measures[17] may be ordered*** **when there are grounds for suspicion for the criminal acts regarding terrorism, protection of health and morals, etc.** Thus, they may be applied to the criminal offences of showing pornographic materials to a juvenile from Article 193, production and distribution of child pornography from Article 193–a as well as criminal acts regarding terrorism as from Article 394-b and financing terrorism as from Article 394-c, or for criminal offenses against the state (Chapter XXVIII, CCRM), crimes against humanity and the international law (Chapter XXXIV, CCRM).

The National Action Plan for Prevention and Handling Sexual Abuse of Children and Paedophilia, with activities for 2014/2015 is in preparation. Also, in preparation is a protocol for acting and in-depth assessment of the legislative provisions and their implementation. In addition, multidisciplinary teams are established, whose activities are conducted engaging foreign and domestic experts from UNICEF and WTO.[18]

---

16 Law on Criminal Procedure, ("Official Gazette of the Republic of Macedonia" No. 150, 18.11.2010), available at http://www.pravo.org.mk/documentDetail.php?id=5060 (13.9.2015).

17 Chapter XIX, Special Investigative measures, Law on Criminal Procedure.

18 Strategic plan of the Ministry of Labor and Social Policy, 2015-2017, Skopje 2014, available at http://www.mtsp.gov.mk/dokumenti.nspx (14.9.2015).

In 2012, Macedonia abolished defamation as a criminal offence and adopted *The Law on Civil Liability for Defamation and Insult*.[19] Decriminalisation of defamation was required by the national journalist association as a ***significant step in the context of freedom of expression and the media***, which is a cornerstone of any democracy. *The Law on civil Liability explicitly states that the case law of the European Court of Human Rights (ECtHR) on freedom of expression is considered to be part of the law in force in Macedonia (Article 2)*. According to this Law, a person is liable for **insult** if he/she intentionally disparages another person or through statement, behaviour, publication or other medium expresses derogatory thoughts toward another person. Entities protected by the law are natural persons, groups of individuals, deceased persons and also legal entities (Article 6). A person is liable for **defamation** if he/she presents or disseminates before a third party untrue facts harming the honour and reputation of another person with the intention of harming that person's honour and reputation, while knowing or having been obliged to know and may know that the facts are false.

The two main laws governing the area of ***intellectual property rights*** are the Law on Copyright and Related Rights[20] and the Law on Industrial Property.[21] Article 159 of the *Law on Copyright and Related Rights* provides that copyright and related rights are protected by different codes. Thus, the CCRM and the LCP apply to the *criminal protection* of copyright and related rights. Also, the protection of copyright and related rights includes the protection of technological measures against rights infringement which includes any technology, computer program, device or their components, which in their normal course of operation are designed to prevent or restrict acts of infringement of the rights provided by this Law which are not authorized by the right holder (Article 63). There are several provisions in the CCRM which determine that violation of copyright and related rights is a criminal act (Articles 157, 157-a, 157-b and 157-c). The act of violation of copyright and related rights is any act committed without authorization, in their own name or on behalf of others, of publishing, showing, reproducing, distributing, performing, broadcasting or in any other way of reaching without authorization another's copyright or related right, i.e. copyright work, performance or item of related right. This criminal act can be sentenced to imprisonment of six months to three years (Article 157). Article 166 and 173 of the *Law on Copyright and Related Rights* provide legal basis for protection of copyright or related rights, including the possibility of the right holders to apply to the Judicial authorities: ***for a termination of the infringement act and for removal of the items (or content) which is disseminated without the permission of the right holder***. Article 173 stipulates the specific circumstances to be taken into consideration by the Court when deciding on imposing a removal of the disseminated items or content, especially the proportionality between the severity of the infringement and the requests and interests of the right holders for protection of their rights.

The ***protection of privacy*** can be also used as a ground for blocking, filtering or removing content on Internet. The ***Law on personal data protection***[22] defines the types of personal data that are treated as "protected" (Article 2 and Article 5) and entitles the *Directorate for Personal Data Protection* to conduct supervision over all "controllers" or "processors" of personal data collections, that is all physical and legal entities which collect and process personal data (Article 2, par.5). The providers of Internet are also subject to regulation with this Law, in the sense that they are obliged "[…] to apply proper technical and organizational measures for protection […] especially when the processing includes transmission of data over a network and protection of any kind of illegal forms of processing" (Article 23, par.1). In addition to that, the providers are also obliged to adopt and apply a Privacy Protection Policy describing the technical and organizational measures for providing secrecy

---

19 Law on Civil Liability for Defamation and Insult, "Official Gazette of the RM" No. 143, 14.11.2012.

20 Law on Copyright and Related Rights, "Official Gazette of RM", No. 115/10, 140/10, 51/11, 147/13 and 154/15.

21 Law on Industrial Property, "Official Gazette of RM", No. 21/09, 24/11, 12/14 and 41/14.

22 Law on Personal Data Protection, "Official Gazette of RM", No.07/05, 103/08, 124/10, 135/11, 43/2014, 153/15.

and protection of the personal data processing (Article 23, par.4). The Directorate is in charge for supervision over the work of all controllers and processors (including Internet providers) registered in the country and can impose measures, including a prohibition for further processing of the personal data or file a misdemeanour procedure to the Court (Article 41). The provisions of this Law are applied also to the controllers that are not established in the country or do not have authorized representative with head office in the country, but the equipment used for personal data procession is located in "The former Yugoslav Republic of Macedonia", unless the equipment is used only for transit through the territory of the State (Article 7-b).

Certain safeguards to protect freedom of expression are incorporated in the articles 4-a and 5 of the Law. For example, Article 4-a provides that the provisions of the Law shall not be applied to processing of personal data carried out for the purpose of professional journalism, but only in the case when the public interest prevails over the private interest of the subject of personal data. Also, Article 5 states that personal data shall be: "processed justly and pursuant to law; - collected for specific, clear and legally determined purposes and processed in a manner pursuant to those purposes, [...] appropriate, relevant and not too extensive in relation to the purposes for collecting and processing...". There is an appealing mechanism incorporated in the Law which is implemented in accordance with the provisions of the Law on General Administrative Procedure (Articles 4-a and 50-a).

Law on classified information[23] regulates the classification of information, conditions, criteria, measures and activities undertaken for their protection, rights, obligations and responsibilities of the creators and users of classified information, international exchange, as well as other issues related to the use of classified information (Article 1). The objective of this Law is provision of legal use of classified information and disabling any type of illegal access to information (Article 2). This Law applies to the protection of the classified information received from foreign countries and international organizations or created in mutual cooperation if not otherwise regulated by the ratified international agreements (Article 3). The Directorate for Security of Classified Information has been established for implementing the policy for protection of classified information (Article 4). Referring to Article 7 information is classified according to its content, therefore authorized person according to this law assigns the level of classification of information. Information is designated with one of the following levels of classification: state secret, highly confidential, confidential and internal. Article 8 stipulates that information classified with level "state secret"[24] is information whose unauthorized disclosure would endanger and cause irreparable damage to the vital interests of "The former Yugoslav Republic of Macedonia". In order to protect the classified information, measures are undertaken for administrative, physical, personnel, information and industrial security (Article 24). The administrative measures include also prevention of unauthorized takeout or publication of the classified information (including publication on the Internet), prevention of the disclosure of the secrecy of the classified information and removal or destruction of the classified information (Article 25). The information security measures among other things include also assessment for possible security infringement of the classified information by intrusion in the information system and use and destruction of the classified information processed and stored in communication and information systems (Article 28). The possibility of blocking, filtering or take-down of content that is classified is not explicitly mentioned in the Law, neither are the safeguards to protect freedom of expression. While assessing the proportionality of restrictive measures for disclosure of classified

---

[23] Law on classified information, (Official Gazette of RM, No. 9/04, 113/07, 145/10 and 80/12), available at http://www.pravo.org.mk/documentDetail.php?id=106 (13.09.20154).

[24] Article 316, par.6. CCRM: A *state secret* is considered to be the information or documents which by law or by some other regulation, or by the decision of a competent authority which is passed based on the law, are declared to be a state secret, and whose disclosure has or could have damaging consequences for the political, economic or military interests of the Republic of Macedonia.

information the Courts should directly apply the EHCR case law, however there were no such cases identified in practice. *The Criminal Code* states that punishment shall be applied to a person who tells, hands over or makes available an entrusted state secret to the public or to an unauthorized person; or a person who tells, hands over or makes available to the public or to an unauthorized person, information or documents for which he/she knows are a state secret, and which he/she acquired in an unlawful manner (Article 317, par.1 and2).

In terms of ***self-regulation or co-regulation,*** there have been several initiatives so far, undertaken either by governmental or civil society organisations, to promote privacy protection on Internet or safety from harmful content, hate speech and discrimination. In 2008 the Association Internet Hotline Provider Macedonia in communication with EC Safer Internet Programme, INHOPE-International internet hotline provider association and Insafe- supported by EC programme, initiated a project to establish Safer Internet Center in "The former Yugoslav Republic of Macedonia". The Government accepted the initiative and in 2012 announced a project[25] for protection of children and youth from illegal and harmful content on Internet. It was envisaged to establish a national Safer Internet Center, to develop a national Programme and Action plan for prevention and protection of children and youth from internet abuse, to enhance the control and sanctioning of internet abuse of children etc. As part of this initiative, an Advisory Body for protection of children and youth on Internet was established, composed of representatives of the Ministry of Interior Affairs (Unit for Cyber Crime), the Agency of Electronic Communication, the Directorate for Personal Data Protection, Macedonian Association of Information Technologies (MASIT), the Faculty of Information Sciences and the Association Internet Hotline Provider Macedonia. Also, the Association Internet Hotline Provider Macedonia wrote the Action plan for protection and prevention of children and youth from illegal content and conduct on internet on voluntary base. Blocking is foreseen in the Action plan, but only of content defined as illegal in the CCRM. However, the Action plan has not been published, because the confidentiality level of its content was considered as very high.[26] It was approved by the Government in January 2013, as a form of self-regulatory initiative, but concrete implementation has not started yet.

The nongovernmental sector has implemented a range of projects and activities in this field. For example, there are several projects and websites focused on children protection and safety on Internet. The most positive example is the Website "bezbednonainternet.org.mk" (Safe on internet)[27] initiated and maintained by the NGO Metamorphosis. The Web site contains a lot of educative content for better protection and safety on internet adapted for children and teenagers, for parents and for teachers. In addition, in cooperation with the Directorate for Personal Data Protection, the NGO Metamorphosis published a Guideline for Parents for protection of children's privacy and personal data on Internet.[28]

Several projects have been initiated by the NGO sector focused on preventing hate speech on Internet. One example is the Website "bezomrazno.mk" (hate less), developed by the NGO Macedonian Institute for Media[29] where the users may find many international guidelines and other educative documents on the human rights protection and fight against the hate speech on Internet. Another example is the web site "nemrazi.mk" (Do not hate), created by the NGO Metamorphosis, which contains a lot of examples of hate speech and instruction how to report a case of hate speech

---

25 Source available at http://www.mio.gov.mk/?q=node/3172 (14.9.2015).

26 Information given by the representative of the Association Internet Hotline Provider Macedonia (Violeta Georgievska), October 6th 2015.

27 Source available at: http://bezbednonainternet.org.mk/content/view/13/40/lang,mk/ (7.10.2015).

28 Source available at: http://metamorphosis.org.mk/izdanija_arhiva/vodich-za-roditeli-za-zashtita-na-privatnosta-i-lichnite-podatoci-na-decata-na-internet/ (13.9.2015).

29 Source available at: http://bezomrazno.mk/ (14.9.2015).

to the respective institutions or to the Helsinki Committee in the country which could provide an advice.[30]
With the amendments of the Criminal Code of 2009, a new provision in Article 106 is implemented and is referring to: *Special registry for person sentences for criminal acts for sexual harassment of minors and paedophilia*. On the basis of these provisions is adopted the *Law for Special Register for Persons Sentenced for Criminal Acts for Sexual Abuse of Minors and Paedophilia*[31] as well as *Rulebook for the manner of inserting data for persons sentenced for crimes for sexual abuse of minors and paedophilia, as well as for the manner of mutual reporting and collaboration.*[32]

The ***Special registry*** for persons sentenced for criminal acts for sexual abuse of minors and paedophilia is available online, through the web-site www.registarnapedifili.mk.[33] The aim of this innovation is to raise the public awareness for the problem which is the sexual abuse of children and paedophilia, as well as motivating the children who have already been exposed to sexual abuse and paedophilia, to report such activities. This web-page has the information on who can be a victim of sexual abuse, which is the profile of the offenders, information for the ways to recognize if a child has been exposed to sexual harassment and what is more important - information on where to go for help. Also, on the web-page there is a blog through which any visitor can ask a question on which the expert team from PI Institute for social activities will respond.

The Law on Audio and Audiovisual Media Services provides special prohibitions. Therefore the audio and audiovisual media service must not contain programmes that threaten the national safety, call for violent destruction of the constitutional order of the "The former Yugoslav Republic of Macedonia", call for military aggression or armed conflict, incite or spread discrimination, intolerance or hatred based on race, sex, religion or nationality (Article 48, par.1). *These special prohibitions shall meet the terms of the ECHR practice* (Article 48, par.2). This article concerns both traditional broadcasting (radio and television) and on-demand audiovisual media services as defined in the European Audiovisual Media Services Directive[34] (Article 24), including the so-called nonlinear TV services distributed via internet. Article 23 provides that, in case of violation of any provision of the Law or subsequent by-laws, the regulatory body can impose the following measures to the provider of on-demand AVM services (which can be also registered as provider of Internet services): to issue a warning, to file a misdemeanor procedure in case the provider of on-demand AVM services continues with the same violation, and to remove the Provider of On-demand AVM services from the Registry. However, Articles 147, 148 and 149 of the Law do not provide a sanction (fine) for the violation of Article 48 and therefore, the Courts do not accept the misdemeanor procedures filed by the regulatory body. The Agency **shall remove** the Provider of On-demand Audiovisual Media Service from the Registry (if it is registered in the country), in the following cases, inter allia i**f an effective court decision has banned activities of the Provider of On-demand Audiovisual Media Service**.

---

30 Source available at: http://nemrazi.mk/za-proektot/ (14.9.2015).

31 Law for Special Register for Persons Sentenced for Criminal Acts for Sexual Abuse of Minors and Paedophilia, "Official Gazette of the RM" No. 11/12 and 112/14.

32 Rulebook for the manner of inserting data for persons sentenced for crimes for sexual abuse of minors and paedophilia, as well as for the manner of mutual reporting and collaboration, ("Official Gazette of the Republic of Macedonia" No. 11/12 and 112/14), available at http://www.slvesnik.com.mk/Issues/B4A60914A225C7428A7DAF7A2AE927C0.pdf (13.09.2015).

33 The data in the Registry is inserted, changed and updated manually and electronically by an official from the PI Institute for Social Activities – Skopje, in accordance with the adopted Rulebook.

34 Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) (Text with EEA relevance), available at: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32010L0013.

Relevant cases of removal illegal content from Internet. Case (1)[35] *The Skopje Fortress incident* began during the weekend when a group of Albanian citizens dissatisfied with the agreement of the authorities to construct an Orthodox Church-Museum on the Kale Fortress demolished a part of the new construction. Two days later, a group of "supporters" *(Macedonian football fan group Komiti)* of the construction of the church and a group of "supporters" *(Albanian football fan group Shverceri)* of the demolition of the church, gathered, at the same time at the Skopje Fortress to express their opinion through "peaceful" protest which eventually developed into massive fight and stoning and resulted in eight persons injured, one person stabbed with knife, panic throughout the media, criticism towards the politicians, ethnic intolerance. The protests, which turned into an incident, were actually organized by informal groups on Facebook. Part of the groups had been taken down. The Ministry of Interior acted ex officio and requested from Facebook administrators to take them down on the ground of disseminating hate speech or incitement to religious and ethnic hatred (Article 39, par.5 of the Criminal Code). Facebook responded positively and removed the profiles of the groups that called for violence.

Case (2)[36] in the first half of 2015, after the public releases of the massive phone-tapped recordings by the opposition parties, the Helsinki Committee registered an increase of the hate speech towards the citizens, civil movements, citizens associations and members of political parties who were constantly exposed to aggressive campaign (lead by certain pro-governmental proponents) by which they are labelled as: traitors, "commies", "Sorosoids", snitches, etc. in order to impose perception that they work against the interests of the state. The public speeches of certain civil movements and public persons using the media as a tool to incite hatred towards individuals or groups due to their opposite opinions for the work of the ruling parties were of great concern. Additionally, the Committee expressed a concern for the calls for violence by public persons declaring themselves as journalists, as well as the use of social networks and media for having a showdown with the political opponents. The Committee invited the competent institutions to finally undertake measures in their competence and to publicly dissociate themselves from these views. Otherwise they would be considered as direct participants in the creation of an atmosphere of fear and approval of these acts. The competent institutions did not undertake any action to filter or block this content from internet (either on social networks, blogs, news portals etc.).

It is relevant to mention the newest proposal of two parliamentarians from the ruling parties VMRO-DPMNE and DUI (Macedonian and Albanian coalition partners in the Government) to adopt a Law on banning the publication and possession of wiretapped content. This case was commented in the public as an attempt of the Government to ban the publication of the content from the wiretapped recordings which revealed a large-scale criminal and corruption of the public officials. The draft-Law was submitted on 6th October 2015 and became immediately subject to severe criticism by experts,[37] journalists associations[38] and international community. The draft-Law consists of only six articles. It is explicitly stated that the purpose of this Law is to regulate the prohibition of possession, processing and publication through media, social networks, Web portals and any other means of publication of materials that are gathered through unlawful interception of communications (Article 1, par.1).

---

35 Source available at http://it.com.mk/drushtvenata-omraza-i-incidentot-na-kale/ (14.9.2015).

36 Source available at http://b2.mk/news/helsinshki-zagrizhuva-ushte-pozasilenotokoristenje-na-mediumite-za-shirenje-na-omraza?newsid=U6cg (14.9.2015).

37 The professor in Constitutional Law, д-р Светомир Шкариќ emphasized that the draft-Law violates fundamental freedoms, especially the freedom of speech which is guaranteed in the Article 16 of the Constitution, see more: "Шкариќ – Цензурата на бомбите е морбидна" (Skaric – the Censorship of the 'bombs' is morbid), Radio Slobodna Evropa.
Source available at: http://www.makdenes.org/content/article/27293474.html (7.10.2015).

38 Association of Journalists, SEEMO and NGO Infocenter react to the Law that bans the wiretapped materials, Published by daily Vest on 7th October 2015, Available at : http://vest.mk/?ItemID=BA747E08F441584D939D9EF5210DC0E2 (7.10.2015).

Article 2 provides that anyone who speak, writes or comments about the recordings shall be punished with four years imprisonment. In the two introductory paragraphs that present the justification for adopting such Law, it is stated that the ban for possession, processing, publication and usage of materials that are collected by means of unlawful interception of communications is not regulated at all. It is also emphasized that the unlawful interception of communications is a direct violation of the constitutionally guaranteed protection of all types of communication. However, neither the justification of the draft-Law nor any article contains a reference on the balance between this freedom and the freedom of expression. The draft-Law was withdrawn two days after its submission.

Government requests for removal[39]

Every year, government officials make requests for data to social networks, as part of official investigations. For government requests to restrict access to content, this report provides the number of pieces of content restricted due to violations of local law.

The requests from "the formal Yugoslav Republic of Macedonia" are as follows:

- In the period from July, 2014 – December, 2014: there were 5 requests for data, 8 user/account requested, ***0 content blocked***.
- In the period from January, 2014 – June, 2014: there were 10 requests for data, 12 user/account requested, ***0 content blocked.***
- In the period from July, 2013 – December, 2013: there were 6 requests for data, 14 user/account requested, ***0 content blocked.***
- In the period from January, 2013 – June, 2013: there were 9 requests for data, 11 user/account requested.

There is no available information of removal request on other social networks (twitter,[40] yahoo,[41] etc.).

There is no available information of received requests from national courts and government agencies to remove information from Google products, such as blog posts, YouTube videos, or search results.

3. Procedural Aspects

With the adoption of the New LCP from 2010 ***the public prosecutor*** (hereinafter referred to as PP) has a new, so-called, proactive role. The rights and obligations of the public prosecutor are defined in Article 39:

(1) The public prosecutor's general right and duty shall be to prosecute perpetrators of criminal offenses, which are to be prosecuted ex-officio.

(2) In cases of crimes which are prosecuted ex-officio, the public prosecutor shall have specific rights and duties.[42]

(3) The public prosecutor shall initiate special procedures and shall participate in them when that is prescribed with a separate law.

---

39 As part of ongoing effort to share more information about the requests that Facebook have received from governments around the world, it regularly produces a *Government Requests Report,* source available at https://govtrequests.facebook.com/country/Macedonia/2014-H2/ (14.9.2015).

40 Source available at https://transparency.twitter.com/removal-requests/2015/jan-jun (14.9.2015).

41 Source available at https://transparency.yahoo.com/government-removal-requests/index.htm (14.9.2015).

42 Article 39, par.2 Law on Criminal Procedure.

Having in mind his/her new position during the investigation, PP must also possess adequate knowledge in the area of computer crime. The prosecutor must know how the computer and Internet networks operate and how to understand the expert reports, and he/she must know also in which direction and in which manner to lead the investigation and what kind of duties he/she will address to the judiciary police. During the entire procedure, the prosecutor should have knowledge and skills of the manner of performing supervision of the collected evidence, how to protect and provide them, especially if the evidence are provided outside national jurisdiction.

The Judiciary Police is another body dealing with this issue. The members of the judiciary police, ex officio or by order of the public prosecutor, undertake measures and activities in order to detect and perform criminal investigation of criminal acts, prevent further consequences of the criminal acts, capture and report the perpetrators, provide evidence and other measures and activities which can be used for uninterrupted implementation of the criminal procedure (Article 46, par. 1 of LCP). The judiciary police conducts investigation and actions imposed or assigned by the court and the public prosecution (Article 46. par. 2 of LCP).

The ***special investigative measures specified in the LCP*** are as follows:

Article 252, LCP, Purpose and types of special investigative measures:

(1) If likely to obtain data and evidence necessary for successful criminal procedure, which cannot be obtained by other means, the following special investigative measures may be ordered:

1) Monitoring and recording of the telephone *and other electronic communications* under a procedure as stipulated with a separate law;
2) Surveillance and recording in homes, closed up or fenced space that belongs to the home or office space designated as private or in a vehicle and the entrance of such facilities in order to create the required conditions for monitoring of communications;
3) Secret monitoring and recording of conversations with technical devices outside the residence or the office space designated as private;
4) Secret access and search of computer systems;
5) Automatic or in other way searching and comparing personal data of citizens;
6) Inspection of telephone or other electronic communications;
7) Simulated purchase of items;
8) Simulated offering and receiving bribes;
9) Controlled delivery and transport of persons and objects;
10) Use of undercover agents for surveillance and gathering information or data;
11) Opening a simulated bank account; and
12) Simulated incorporation of legal persons or using existing legal persons for the purpose of collecting data.

(2) In case when no information is available on the identity of the perpetrator of the criminal offence, the special investigative measures as referred to in paragraph 1 of this Article may be ordered also in respect of the object of the criminal offense.

Article 256, LCP, Authorized body for ordering special investigative measures

The measures referred to in Article 252, paragraph 1, items 1, 2, 3, 4 and 5 of this Law, upon an elaborated motion ***by the public prosecutor*** shall be ***ordered by the preliminary procedure judge*** with a written order. The measures referred to in Article 252, paragraph 1, items 6, 7, 8, 9, 10, 11 and 12 of this Law shall be ordered ***by the public prosecutor*** with a written order.

Article 258, LCP, Authorized entity for the implementation of special investigative measures:

(1)The measures referred to in Article 252 of the LCP shall be implemented by ***the public prosecutor or by the judicial police***, ***under the control of the public prosecutor***. During the execution of the measure, the judicial police shall produce a report that is going to be submitted to the public prosecutor, upon his or her request. The prosecution of the criminal acts that contain illegal Internet content or somehow are intruding the individual rights and freedoms are undertaken differently.

All state entities, public enterprises and institutions shall be obliged ***to report crimes that are being prosecuted ex-officio***, about which they have been informed or found out about them otherwise (Article 273, par.1 LCP). When filing charges, the applicants as referred to in paragraph 1 of this Article shall also specify any evidence known to them and take necessary measures to preserve any traces of the criminal offence, items that have been used while it was committed or resulted from the commission of the criminal offense and other evidence (par.2). Anyone may report a crime that is being prosecuted ex-officio (par.3).

Article 274 Filing criminal charges (1) Any criminal charges shall be filed ***with the competent public prosecutor***, in writing or verbally, by telephone, electronically or through the use of other technical devices and means (Article 274 par.1).

The criminal acts that are not prosecuted ex officio are explicitly prescribed in a separate paragraph. For example, the criminal acts in the field of computer crime which in some cases can be used for terrorist purposes are prosecuted as follows:

Article 144 (par. 5), Endangering security, CCRM: The prosecution of the crime from paragraph (1) is undertaken ***upon private complaint.***

Article 147 (par. 4), Violation of confidentiality of letters or other parcels**,** CCRM: The prosecution of the crime from items 1 and 2 is undertaken ***upon private complaint.***

Article 149-a (par. 4), Prevention of access to a public information system, CCRM: The prosecution shall be performed on the basis of ***a private complaint.***

Article 157 (par. 8), Violation of an author's right and related rights, CCRM: The prosecution for violation of a moral right is undertaken ***upon a proposal.***

The prosecution of the crimes in CCRM, from Article 193, Showing pornographic materials to a juvenile; Article 193-a, Production and distribution of child pornography and Article 193-b, Enticement of a child under the age of 14 into statutory rape or other sexual activities, ***are undertaken ex officio.*** The manner of implementation of the special measures of process protection of child victims is regulated with a separate law (Article 55 par.6, LCP). The victims of above mentioned crimes also have additional rights.[43] The court, the Public Prosecutions Office and the police shall be obliged to advise the victim of their rights (Article 54 par.2 LCP).

[43] LCP, Article 55, *Special rights of victims of crimes against gender freedom and gender morality, humanity and international law:* (1) Apart from the rights established in Article 53, the victim of crimes against gender freedom and gender morality, humanity and international law, shall also have the following rights: 1) before the interrogation, to speak to a counsellor or a proxy free of charge, if he or she participates in the procedure as an injured party; 2) to be interrogated by a person of the same gender in the police and the public prosecution office; 3) to refuse to answer questions that refer to the victim's personal life, if those are not related to the crime; 4) to ask for an examination with the use of visual and audio means in a manner established in this Law; and 5) to ask for an exclusion of the public at the main hearing.

The prosecution of the crimes of CCRM from Article 251, Damage and unauthorized entering in a computer system; Article 251-a, Production and spreading of computer viruses and Article 251-b, Computer fraud ***are undertaken ex officio.*** There is one exception in Article 251 – b, par.10: For the crime stipulated in the paragraph 4 (The one that will perform the crime with sole intention to damage somebody else), the procedure is performed ***upon private lawsuit.***

The prosecution of the crimes of CCRM from Article 286, Violation of rights arising from reported or protected innovation and topography of integrated circuits, Article 379a, Computer forgery and Article 394-g Dissemination of racist and xenophobic material through computer system, are also ***undertaken ex officio.***

The Law on Audio and Audiovisual Media Services guarantees the freedom of reception and retransmission of the audio and audiovisual media services from the countries signatories to the CoE Convention on Transfrontier Television (Article 44). The Law also provides conditions for restriction of reception and retransmission of audiovisual media service *from other countries* (including on-demand AVM services distributed via internet), in Article 45: The Agency can undertake *adequate measures to provisionally limit the freedom of transmission and reception* of audio or audiovisual media service from other countries in the territory of "The former Yugoslav Republic of Macedonia", if the program services of the broadcasters from other countries, seriously or gravely violate the provisions of Article 48 and Article 50 of this Law and incite racial, gender, religious or ethnic hatred and intolerance (Article 45, par.1, 2). The Measure of paragraph (1) of this Article shall be enforced in relation to the on-demand audio and audiovisual media service, provided the following requirements have been met: the measure is necessary in particular for protection, research, disclosure and prosecution of criminal acts, including the protection of minors and the fight against incitement of racial, gender, religious or ethnic hatred; also against violation of human individual dignity, safeguarding public health, public safety, including the safeguarding of national security and defence; also protection of consumers including the investors (Article 45, par.3) In some emergencies, the Agency can digress from the requirements stipulated in paragraph (3), items 4 and 5 of this Article, and in such occurrences it shall in the shortest time possible notify the European Commission and the member state under the jurisdiction of which the Provider of Media Service is, or the state signatories of the European Convention of Trans-frontier Television of the CoE about the enforced measures, *stating the reasons behind which the case has been considered an emergency* (Article 45, par.4).

In order to define more specifically how the prohibition on hate speech in the audiovisual media services (Article 48 of the Law on Audio and Audiovisual Media Services) should be interpreted in practice, the regulatory body (Agency on Audio and Audiovisual Media Services) adopted ***Guidelines for monitoring hate speech***.[44] The Guidelines provides detailed explanation on the European and national regulatory framework on hate speech, examples from the ECtHR case law on hate speech in the media, as well as specific recommendations for the different aspects to be taken into consideration by the regulator while assessing hate speech. However, the regulator uses the Guidelines only to assess whether a specific audiovisual service (either traditional TV or TV-like service distributed on Internet) can be defined as hate speech and took a position to not file misdemeanour procedure to the Court, because the Law does not prescribe a sanction. More severe cases of hate speech are forwarded to the public prosecutor to be assessed on the basis of the Criminal Code.

[44] Available at: http://www.avmu.mk/images/Guide_to_monitor_hate_speech.pdf (9.10.2015).

4. General Monitoring of Internet

For effective and efficient performance of specific and complex police tasks requiring a high degree of specialization, including general monitoring of the Internet, ***Central Police Services*** were established within the Public Security Bureau (Ministry of Interior).[45] Central Police Services also perform activities of fighting organized crime, forensic work and expertise, work on supporting the execution of specific and complex affairs in the area of the departments of the Interior and the regional centers for border affairs, etc. The ***Department for Computer Crime and Digital Forensics - Department of Investigation of Cybercrime*** is responsible for reviewing the Internet content and assessing the compliance with legal requirements.

The Agency for Audio and Audiovisual Media Services, established via the Law on Audio and Audiovisual Media Services, is the legal successor of *the Agency of "The former Yugoslav Republic of Macedonia", as independent, non-profit, regulatory body with public competencies in the broadcasting sector.* It has the authorisation to supervise the implementation of the program principles, program requirements and restrictions (programming standards), as well as the fulfilment of the other conditions in the license for performing broadcasting activity. This is performed through regular and ad hoc monitoring of the program services of all types of broadcasters and all broadcasting levels. The supervision of meeting the working conditions is conducted by the ***Agency for Electronic Communications*** and the ***Ministry of Information Society and Administration***.

The issue of providing information security is implemented in the Law on Electronic Management.[46] According to Article 33, the authorities are obliged to apply the measures for information security of the information system used to communicate electronically (par. 1). Specific standards and rules for information security system referred to in paragraph 1 of this Article shall be approved by the Minister of Information Society (par. 2).

The Agency monitors only in terms of technical equipment of broadcasters' study, in terms of compliance with the bylaws of the Agency. The Agency has no inspection powers in supervising whether the copyright and related rights are respected by the broadcasters and operators of public communications networks. As a regulator, it monitors the situation in this regard by means of independent monitoring within the activities of the Coordinating Body for Intellectual Property, established by the Government in which, besides the other subjects, the ***Agency for Electronic Communications, Ministry of Internal Affairs and the Ministry of Culture*** participates as well. The monitoring is performed by going on the field and through the system for monitoring program packages of the operators of public communications networks. It remains necessary to retain the right of the regulator's supervision in relation to: Respecting the regulatory obligations of copyright and related rights for the created, broadcasted, retransmitted and otherwise distributed audio and audiovisual media content, which will cover all subjects of supervision - providers of linear and non-linear audio and audiovisual media services; compliance with the obligations provided in primary and secondary legislation, program requirements and restrictions, and conditions in the license for performing activities and obligation of subjects for supervision at the expense of the Agency (by the license fee and supervision fee) technically to connect to Agency's monitoring system due to transmission of the signal to the system's location. The marking of the contents should be a legal obligation for broadcasters.[47]

---

45 Available at: http://www.mvr.gov.mk/ (5.09.2015).

46 Law on electronic menagment, ("Official Gazette of the RM" No. 109/09 and 47/11.

47 Broadcasting Council of Republic of Macedonia, Strategy for development of broadcasting activity in the Republic of Macedonia (proposal) for the period 2013-2017, available at http://avmu.mk/images/Strategija_so_Akciski_plan-Angliski.pdf (3.09.2015).

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

There has been no case regarding blocking, filtering or take-down of illegal content on Internet or cases dealing with Article 10. One case is partly related to violation of Article 10: *Vraniskoski v. "The former Yugoslav Republic of Macedonia (no. 2)* which was declared inadmissible on 26 May 2009. There has been no final decision. [48]

The legal provisions outlined in the previous sections do not explicitly mention the possibilities for blocking, filtering or take-down of any content on Internet, but in general they provide sufficient legal ground for the respective *public authorities* to undertake such measures. However, the analysis of these provisions shows that in most of the cases they are not sufficiently clear, detailed and foreseeable and thus, do not satisfy the quality criterion. We may say that only some of the provisions of the CCRM described in Section 2 meet this criterion. As a result, the procedures to be undertaken by the respective public authorities to request blocking, filtering or take-down measures are not clearly stipulated and quite confusing.

On the other side, the private parties who want to request filtering, blocking or take-down measures as a response to infringement of their rights are generally protected with the Constitution which introduces a positive obligation on the state to protect the rights of third parties with an effective remedy. The respective provisions of the Law on Personal Data Protection Act and the Law on Audio and Audiovisual media services, if read in the light of case-law of the CJEU, are quite foreseeable. Hence, the legal basis in the field of intellectual property rights enforcement, but also privacy protection rights enforcement, will most likely satisfy the conditions of the quality of the law.

Since there was no filtering or blocking case-law in the national courts, the aspect of application compliance of the national legislation with the ECHR case-law cannot be evaluated at this stage. For example, even if website blocking, filtering or take-down is possible as a remedy, it cannot be determined whether the decisions on the implementation of such measures were proportionate, taking into consideration certain safe-guards. What is especially missing in the present legal system are clear provisions related to the safeguards to freedom of expression. And, since there were almost no measures of filtering, blocking and take-down of Internet content neither a national case-law related to such measures, it is impossible to evaluate how the legal requirements are implemented in practice, particularly with regard to the assessment of necessity and proportionality of the interference with freedom of expression.

The same conclusion can be made in respect to the alignment of the national case-law with the pertinent case-law of the European Court of Human Rights. There is a general consideration that the relevant case law of the European Court of Human Rights has not been properly implemented in the national legal practice, mostly due to the insufficient knowledge of the judges about the ECHR case law as a legal source.[49] Also, in comparison to other countries, faculties of law in Macedonia do not have specific courses which are focused on the theoretical and practical aspects of the application of the ECHR case-law.

Elena Mujoska, 1.11.2015

---

48 Concerned complaints by a former bishop of the Macedonian Orthodox Church: - about his conviction for inciting ethnic, racial and religious hatred and intolerance and sentencing to 18 months' imprisonment (second case). In particular, Articles 6 (right to fair trial), 9 (freedom of religion) and *10 (freedom of expression*). Source available at: http://www.echr.coe.int/Documents/CP_The_former_Yugoslav_Republic_of_Macedonia_ENG.pdf (15.09.2015).

49 This is a statement given by Dr Mirjana Lazarova-Trajkovska, Macedonian judge in the European Court for Human Rights in the article: "The Journalists demand for a full implementation of the Strasbourg' case-law", Deutche Welle Macedonian Dpt, 27 October 2014.