# Elena Mujoska Trpevska, PhD<sup>1</sup>

# CONTROLLING ILLEGAL CONTENT ON INTERNET PLATFORMS

1.02 Review Article UDK 343.272:341.24 343.272:341.645.5(44)(094.8)

#### **Abstract**

The Article 16 of the Constitution of RNM guarantees freedom of conviction, conscience, thought and public expression. Also, the freedom of speech, public address, public information and free establishment of institutions for public information is guaranteed. Similarly, free access to information, the freedom to receive and impart information, the right of reply via the mass media, the right of correction in the mass media and the right to protect the source of information in the mass media is guaranteed. Censorship is prohibited as well. Having that said, this article deals with the (or lack of) mechanisms counteracting the distribution of illegal and harmful and often offensive content of the Internet platforms in our country.

Are the methods that we are using sufficient for the increasing amount of illegal content on the Internet? According to the results of the research in this article<sup>2</sup>, an imminent new and modern, specific code regulating the issues of detecting and removing of the illegal Internet content is much needed in the Republic of North Macedonia.

**Keywords:** illegal, content, harmful, free speech, ECHR.

# 1. Background of the research<sup>3</sup>

The Republic of North Macedonia (hereinafter referred to as RNM) 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, especially after signing the "Prespa Agreement", RNM 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

<sup>1</sup> Research Fellow in the Center for Strategic Research "Ksente Bogoev", Academy of Sciences and Arts in RNM. *Contact:* <u>emujoska@manu.edu.mk.</u>

<u>General: http://www.coe.int/en/web/freedom-expression/study-filtering-blocking-and-take-down-of-illegal-content-on-the-internet.</u> Country reports and State comments: <a href="http://www.coe.int/en/web/freedom-expression/country-reports">http://www.coe.int/en/web/freedom-expression/country-reports</a>, last visit: 8.6.2019.

<sup>&</sup>lt;sup>2</sup> I would like to thank Dr. Snezana Trpevska for helping me to conceptualize the research problem and her useful comments.

<sup>&</sup>lt;sup>3</sup> In 2016 a 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, was published. This article is part of that research. As mentioned in the document, the opinions which are expressed 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. The document is available at:

Convention for the Protection of Human Rights and Fundamental Freedoms (hereinafter referred to as ECHR) and Amending Protocol<sup>4</sup>, the Convention on Cybercrime and its Additional Protocol<sup>5</sup>, the European Convention on the Prevention of Terrorism<sup>6</sup>, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and Additional Protocol<sup>7</sup>. 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<sup>8</sup>.

# 1. Legal Sources

In RNM, there is no specific code regulating the issues of removal illegal content on the Internet. This area is regulated through several legal acts such as the Criminal Code<sup>9</sup>, the Law on Audio and Audiovisual Media Services<sup>10</sup>, the Law on Electronic Communication<sup>11</sup>,

<sup>4</sup> 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.

<sup>&</sup>lt;sup>5</sup> 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 RNM" No. 56 (13.07.2005).

<sup>&</sup>lt;sup>6</sup> 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 RNM" No. 20 (16.2.2009).

<sup>&</sup>lt;sup>7</sup> 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 trans border 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 RNM" No.103 (19.8.2008).

<sup>&</sup>lt;sup>8</sup> 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 RNM" No.135 (8.10.2010).

<sup>&</sup>lt;sup>9</sup> Criminal Code ("Official Gazette of the RNM" nos. 37/1996, 80/1999, 4/2002, 43/2003, 19/2004, 81/2005, 60/2006, 73/2006, 7/2008, 139/2008, 114/2009, 51/2011, 135/2011, 185/2011, 142/2012, 166/2012, 55/2013, 82/2013, 14/2014, 27/2014, 28/2014, 41/2014, 115/2014, 132/2014, 160/2014, 199/2014, 196/2015, 226/2015, 97/2017 and 248/2018). Decisions of the Constitutional Court of the RNM: U. no. 220/2000 dated 30 May 2001, published in the "Official Gazette of the RNM" no. 48/2001; U. no. 210/2001 dated 06 February 2002, published in the "Official Gazette of the RNM" no. 16/2002; U. no. 206/2003 dated 09 June 2004, published in the "Official Gazette of the RNM" no. 40/2004; U. no. 228/2005 dated 05 April 2004, published in the "Official Gazette of the RNM" no. 50/2006; and U. no. 169/2016 dated 16 November 2017, published in the "Official Gazette of the RNM" no. 170/2017.

<sup>&</sup>lt;sup>10</sup> Law on Audio and Audiovisual Media Services, "Official Gazette of the RNM" No. 184/13, 13/14, 44/14, 101/14, 132/14, 168/2018, 248/2018 and 27/2019.

<sup>&</sup>lt;sup>11</sup> Law on Electronic Communication, "Official Gazette of the RNM" No. 39/14, 188/14, 44/15, 193/2015, 11/2018, 21/2018 and 98/2019.

the Law on Media<sup>12</sup>, the Law on Copyright and Related Rights<sup>13</sup>, the Law on Personal Data Protection<sup>14</sup>, the Declaration on Safer Internet<sup>15</sup>, etc.

As a democratic society established by the Constitution<sup>16</sup>, the legislation and supervision of illegal Internet content in the country 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.<sup>17</sup> RNM 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 Republic of North Macedonia has no specific legal basis to deal with the filtering, blocking, or removal of the illegal content on Internet.

#### 2.1 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 as mentioned above, and the specific laws, usually within universal access laws or regulations.

Article 3 of *the Law on media* guarantees the freedom of expression<sup>18</sup> and freedom of the media may be limited only in accordance with the Constitution. Then again, Article 44 of *the Law on Audio and Audiovisual Media Services* guarantees the freedom of reception and re-transmission of audio or audiovisual media service on the territory of RNM, 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 RNM (hereinafter referred to as CC), 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

<sup>13</sup> Law on Copyright and Related Rights, "Official Gazette of the RNM" No. 115/10, 51/11, 147/11, 154/15 and 27/16.

<sup>&</sup>lt;sup>12</sup> Law on media, "Official Gazette of the RNM" No. 184/13 and 13/14.

<sup>&</sup>lt;sup>14</sup> Law on Personal Data Protection, "Official Gazette of the RNM" No. 7/05, 103/08, 124/10, 135/11, 43/14, 153/2015, 99/2016 and 64/2018.

<sup>&</sup>lt;sup>15</sup> Declaration on Safer Internet, "Official Gazette of the RNM" No. 31, 3.03.2010.

<sup>&</sup>lt;sup>16</sup> Available at <a href="http://www.sobranie.mk/the-constitution-of-the-republic-of-macedonia.nspx">http://www.sobranie.mk/the-constitution-of-the-republic-of-macedonia.nspx</a> (14.9.2018).

<sup>&</sup>lt;sup>17</sup> 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.

<sup>&</sup>lt;sup>18</sup> 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 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.

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 *CC* 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 CC. 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 CC
- Violation of confidentiality of letters or other parcels Article 147 CC
- Misuse of personal data Article 149 CC
- Prevention of an access to a public information system Article 149-a CC
- Violation of an author's right and related rights Article 157 CC
- Violation of the rights of distributors of technically and specially protected satellite signals -Article 157-a CC
- Piracy of audiovisual products Article 157-b CC
- Piracy of phonograms Article 157-c CC
- Showing pornographic materials to a juvenile Article 193 CC
- Production and distribution of child pornography Article 193-a CC
- Enticement of a child under the age of 14 into statutory rape or other sexual activities Article 193-b CC
- Damaging and unauthorised entry into computer system Article 251 CC
- Making and uploading computer viruses Article 251a CC
- Computer fraud Article 251b CC
- Violation of rights arising from reported or protected innovation and topography of integrated circuits - Article 286 CC
- Computer forgery Article 379a CC
- Dissemination of racist and xenophobic material through computer system Article 394-  $\operatorname{g} \operatorname{CC}$

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:

- (1) 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;
- (2) 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
- (3) 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 *CC*, in the field of illegal content on the Internet. One of the main criminal acts is **Article 193**, *showing pornographic materials to a juvenile*:

- (1) 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 [...].
- (2) If the crime has been committed *through the public information media*, the perpetrator shall be sentenced to imprisonment.
- (3) 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

[...]

- (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<sup>19</sup> from 2010, special investigative measures<sup>20</sup> 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, CC), crimes against humanity and the international law (Chapter XXXIV, CC).

In 2012, RNM abolished defamation as a criminal offence and adopted <u>The Law on Civil Liability for Defamation and Insult</u><sup>21</sup>. 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 RNM (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 and the Law on Industrial Property<sup>22</sup>. Article 159 of the *Law on Copyright and Related Rights* provides that copyright and related rights are protected by different codes. Thus, the CC 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

<sup>&</sup>lt;sup>19</sup> Law on Criminal Procedure, ("Official Gazette of the RNM" No. 150, 18.11.2010), available at <a href="http://www.pravo.org.mk/documentDetail.php?id=5060">http://www.pravo.org.mk/documentDetail.php?id=5060</a> (13.9.2015).

<sup>&</sup>lt;sup>20</sup> Chapter XIX, Special Investigative measures, Law on Criminal Procedure.

<sup>&</sup>lt;sup>21</sup> Law on Civil Liability for Defamation and Insult, "Official Gazette of the RM" No. 143, 14.11.2012.

<sup>&</sup>lt;sup>22</sup> Law on Industrial Property, "Official Gazette of RNM", No. 21/09, 24/11, 12/14 and 41/14.

are not authorized by the right holder (Article 63). There are several provisions in the CC 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 removing content on Internet. The Law on personal data protection<sup>23</sup> 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 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<sup>24</sup> regulates the classification of information, conditions, criteria, measures and activities undertaken for their protection, rights, obligations

<sup>&</sup>lt;sup>23</sup> Law on Personal Data Protection, "Official Gazette of RNM", No.07/05, 103/08, 124/10, 135/11, 43/2014, 153/15.

<sup>&</sup>lt;sup>24</sup> Law on classified information, (Official Gazette of RNM, No. 9/04, 113/07, 145/10 and 80/12), available at <a href="http://www.pravo.org.mk/documentDetail.php?id=106">http://www.pravo.org.mk/documentDetail.php?id=106</a> (13.09.20154).

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"<sup>25</sup> is information whose unauthorized disclosure would endanger and cause irreparable damage to the vital interests of RNM. 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 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 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).

#### 3. Self-regulation or co-regulation

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 RNM.

The Government accepted the initiative and in 2012 announced a project<sup>26</sup> 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

<sup>&</sup>lt;sup>25</sup> Article 316, par.6. CC: 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 RNM.

<sup>&</sup>lt;sup>26</sup> Source available at <a href="http://www.mio.gov.mk/?q=node/3172">http://www.mio.gov.mk/?q=node/3172</a> (7.6.2019).

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 CC. However, the Action plan has not been published, because the confidentiality level of its content was considered as very high<sup>27</sup>. 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)<sup>28</sup> 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<sup>29</sup>.

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<sup>30</sup> 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 to the respective institutions or to the Helsinki Committee in the country which could provide an advice<sup>31</sup>.

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 RNM, 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<sup>32</sup> (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.

<sup>-</sup>

<sup>&</sup>lt;sup>27</sup> Information given by the representative of the Association Internet Hotline Provider Macedonia (Violeta Georgievska), October 6<sup>th</sup> 2015.

<sup>&</sup>lt;sup>28</sup> Source available at: <a href="http://bezbednonainternet.org.mk/content/view/13/40/lang,mk/">http://bezbednonainternet.org.mk/content/view/13/40/lang,mk/</a> (8.6.2019).

<sup>&</sup>lt;sup>29</sup>Source available at: <a href="http://metamorphosis.org.mk/izdanija">http://metamorphosis.org.mk/izdanija</a> arhiva/vodich-za-roditeli-za-zashtita-na-privatnosta-i-lichnite-podatoci-na-decata-na-internet/ (13.9.2015).

<sup>&</sup>lt;sup>30</sup> Source available at: <a href="http://bezomrazno.mk/">http://bezomrazno.mk/</a> (14.9.2015).

<sup>&</sup>lt;sup>31</sup> Source available at: http://nemrazi.mk/za-proektot/ (14.9.2015).

<sup>&</sup>lt;sup>32</sup> 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: <a href="http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32010L0013">http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32010L0013</a>

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 if an effective court decision has banned activities of the Provider of On-demand Audiovisual Media Service

# 4. Relevant cases of removal illegal content from Internet

Case (1)<sup>33</sup> 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.



Image source: https://www.it.mk/drushtvenata-omraza-i-incidentot-na-kale/

Case (2)<sup>34</sup>. 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

<sup>&</sup>lt;sup>33</sup> Source available at http://it.com.mk/<u>drushtvenata-omraza-i-incidentot-na-kale/</u>, last visit: 6.7.2019.

<sup>&</sup>lt;sup>34</sup> Source available at <a href="http://b2.mk/news/helsinshki-zagrizhuva-ushte-pozasilenotokoristenje-na-mediumite-za-shirenje-na-omraza?newsid=U6cg">http://b2.mk/news/helsinshki-zagrizhuva-ushte-pozasilenotokoristenje-na-mediumite-za-shirenje-na-omraza?newsid=U6cg</a> (14.9.2018).

political parties who were constantly exposed to aggressive campaign (lead by certain progovernmental 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.)



Image source: <a href="https://www.it.mk/drushtvenata-omraza-i-incidentot-na-kale/">https://www.it.mk/drushtvenata-omraza-i-incidentot-na-kale/</a>

It is relevant to mention the proposal of two parliamentarians from then ruling parties (then 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 6<sup>th</sup> October 2015 and became immediately subject to severe criticism by experts<sup>35</sup>, journalists associations<sup>36</sup> 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

<sup>&</sup>lt;sup>35</sup> 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 (7.10.2018).

<sup>&</sup>lt;sup>36</sup>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 (7.10.2018).

networks, Web portals and any other means of publication of materials that are gathered through unlawful interception of communications (Article 1, par.1). 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.

# 5. Government requests for removal<sup>37</sup>

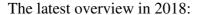
Every year, government officials make requests for data to social networks, as part of official investigations.

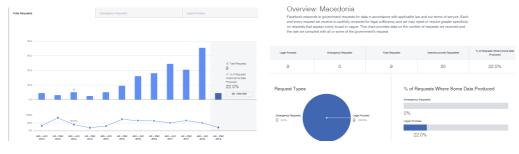
# Macedonia information requests Report Account information requests Percentage where some information produced specified July 7 0% 7 December 2018 1 0% 1 July December 2017 2017 2017 July 2017 7 Rer 2017 8

The latest information requests in 2018:

Source: https://transparency.twitter.com/

For government requests to restrict access to content, this report provides the number of pieces of content restricted due to violations of local law.





<sup>&</sup>lt;sup>37</sup> 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 <a href="https://govtrequests.facebook.com/country/Macedonia/2014-H2/">https://govtrequests.facebook.com/country/Macedonia/2014-H2/</a> (6.7.2019).

1

0%

# Source: <a href="https://govtrequests.facebook.com/">https://govtrequests.facebook.com/</a>

The information of removal request on every social networks are available online.<sup>38</sup>

#### 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<sup>39</sup>.
- (3) The public prosecutor shall initiate special procedures and shall participate in them when that is prescribed with a separate law.

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;

4) Secret access and search of computer systems;

(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.

\_

<sup>&</sup>lt;sup>38</sup> Source available at: <a href="https://transparencyreport.google.com/?hl=en">https://transparencyreport.google.com/?hl=en</a> (6.7.2019).

<sup>&</sup>lt;sup>39</sup> Article 39, par.2 Law on Criminal Procedure.

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, CC: 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, CC: 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, CC: 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, CC: The prosecution for violation of a moral right is undertaken *upon a proposal*.

The prosecution of the crimes in CC, 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<sup>40</sup>. The court, the Public Prosecutions Office and the police shall be obliged to advise the victim of thier rights (Article 54 par.2 LCP).

The prosecution of the crimes of CC 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.

14

<sup>&</sup>lt;sup>40</sup> 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 CC 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**.

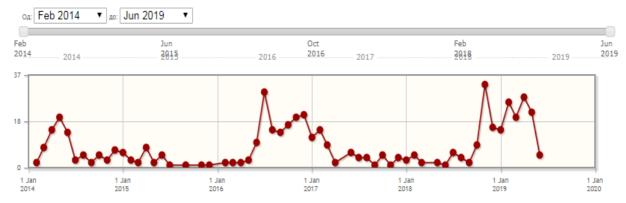
The Law on Audio and Audiovisual Media Services guarantees the freedom of reception and retransmission of the audio and audiovisual media services from the countries signatories to the CoE Convention on Transfrontier Television (Article 44). The Law also provides conditions for restriction of reception 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*<sup>41</sup>. 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.

Statistical overview of hate crime and hate speech records, Feb. 2014 – June 2019:

\_

<sup>&</sup>lt;sup>41</sup> Available at: <a href="http://www.avmu.mk/images/Guide">http://www.avmu.mk/images/Guide</a> to monitor hate speech.pdf (9.10.2018).



Source: http://www.govornaomraza.mk/main

# 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). <sup>42</sup> 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<sup>43</sup>. 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

\_

<sup>&</sup>lt;sup>42</sup> Available at: <a href="http://www.mvr.gov.mk/">http://www.mvr.gov.mk/</a> (5.09.2018).

<sup>&</sup>lt;sup>43</sup> Law on electronic management, "Official Gazette of the RNM" No.105/09, 47/11, 193/15, 52/2016 and 99/18.

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.<sup>44</sup>

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

There has been no case regarding removal 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. <sup>45</sup> 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<sup>46</sup>. Also, in comparison to other countries, the faculties in the country do not have specific courses which are focused on the theoretical and practical aspects of the application of the ECHR case-law.

#### 6. Conclusion

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 removal of illegal and harmful 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 legal provisions outlined in the article do not explicitly mention the possibilities for elimination of any illegal 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 CC described in Section 2 meet this criterion.

As a result, the procedures to be undertaken by the respective public authorities to request blocking or take-down measures are not clearly stipulated and quite confusing. On the other side, the private parties who want to request 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.

<sup>44</sup>Broadcasting Council of RNM, Strategy for development of broadcasting activity in the RNM (proposal) for the period 2013-2017, available at <a href="http://avmu.mk/images/Strategija\_so\_Akciski\_plan-Angliski.pdf">http://avmu.mk/images/Strategija\_so\_Akciski\_plan-Angliski.pdf</a> (3.09.2018). <sup>45</sup>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: <a href="http://www.echr.coe.int/Documents/CP">http://www.echr.coe.int/Documents/CP</a> The former Yugoslav Republic of Macedonia ENG.pdf (15.09.2018).

<sup>&</sup>lt;sup>46</sup> 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.

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.

# **Д-р Елена Мујоска Трпевска**<sup>47</sup>

# КОНТРОЛИРАЊЕ НА НЕЛЕГАЛНАТА СОДРЖИНА НА ИНТЕРНЕТ

1.02 Прегледна научна статија УДК 343.272:341.24 343.272:341.645.5(44)(094.8)

#### Апстракт

Членот 16 од Уставот на Република Северна Македонија гарантира слобода на уверувањето, совеста, мислата и јавното изразување на мислата. Се гарантира слободата на говорот, јавниот настап, јавното информирање и слободното основање на институции за јавно информирање. Исто така, се гарантира слободниот пристап кон информациите, слободата на примање и пренесување на информации. Еднакво, се гарантира правото на одговор во средствата за јавно информирање, правото на исправка во средствата за јавно информирање, правото на заштита на изворот на информацијата во средствата за јавно информирање а цензурата е забранета. Имајќи го сето ова предвид, во трудот се прави осврт на (односно недостатокот на) механизми кои го спречуваат производството и дистрибуцијата на нелегални, штетни и често навредливи содржини на Интернет мрежата во нашата земја.

Дали методите што ги користиме се доволни за зголемениот обем на нелегални содржини на Интернет? Според резултатите од истражувањето во овој член, во Република Северна Македонија повеќе од неопходен е нов, модерен, специфичен модел на заштитни механизми кој ги од една страна ќе ги спречат а од друга страна ќе пружат заштита при откривање и отстранување на нелегалните интернет содржини.

Клучни зборови: омраза, интернет, штета, слободен говор, ЕСЧП.

<sup>&</sup>lt;sup>47</sup> Научен соработник, Центар за стратегиски истражувања "Ксенте Богоев", Академија на науките и уметностите на Република Северна Македонија – МАНУ. *Контакт: emujoska@manu.edu.mk.*