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 22-38

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.

ARMENIA

1. Legal Sources

The Constitution of Armenia[1] provides for the right to respect for private and family life, secrecy of correspondence, telephone conversations, mail, telegraph and other communications[2] and the right to freedom of expression including freedom to search for, receive and impart information and ideas.[3] These rights can be restricted by the law and if it is necessary in a democratic society in the interests of national security, public order, crime prevention, protection of public health and morality, constitutional rights and freedoms, as well as honour and reputation of others.[4] The Constitution provides also for the right to freedom of thought, conscience and religion which can be restricted by law and in the interests of the public security, health, morality or the protection of rights and freedoms of others.[5] Despite the above Constitutional norms, there is no specific and comprehensive statutory law regulating blocking, filtering and taking down of illegal internet content in Armenia. Instead, such activities are regulated by sections of different laws laying down the substantive and procedural grounds for blocking and taking down of the content. As to the filtration, there is no legislation or any legal framework as grounds for such activity.

The Criminal Code of Armenia[6] stipulates the substantive grounds for such crimes as spread of pornography and spread and possession of child pornography, cybercrime and cyberterrorism, hate crime and hate speech, denial of genocide, copyright infringement, etc. The crimes related to dissemination of pornographic content, cybercrimes and copyright infringements are the most common actions giving rise to blocking or taking-down of illegal content. Internet service providers, host providers and telecommunication operators are not liable for transmitting illegal content provided that they had no prior knowledge of it. However, they are bound by the Law on Electronic Communications[7] to open access to law enforcement bodies for conducting surveillance. The decision for conducting surveillance over internet content must be taken by court on the basis of the motion by the investigator of the Investigative Committee of Armenia or the NSS to court. As a result of the surveillance, these bodies may decide to start criminal prosecution or cancel the proceedings for the lack of crime. The decision of the investigator can be appealed to the supervising prosecutor and further to the court of the prosecutor refuses the appeal.

The civil laws provide detailed substantive law grounds for declaring as illegal such content as defamation, insult, use of offensive language, copyright violation, dissemination and use of personal information, violation of privacy, etc. There is no effective framework in the Civil Code[8] for ordering content removal or content blocking as measures of civil remedy. An attempt to introduce such legal framework in the Civil Code by a group of parliamentarians last year against wide practice of defamation and offensive language by online media and social networks failed due to the wide protest by the civil society. However, some procedural grounds for blocking or removal of the

1 Constitution of the Republic of Armenia, adopted on 05 July 1995, amended by referendum on 27 November 2005.
2 Article 23.
3 Article 27.
4 Article 43.
5 Article 26.
6 Criminal Code of the Republic of Armenia of 18April 2003.
7 Law of the Republic of Armenia on Electronic Communications, adopted on 8 July 2005.
8 Civil Code of the Republic of Armenia of 5 May 1998.

content still exist in the Civil Code. For example, the judge may impose injunction on the content during the period of court proceedings or order its removal in the judgment as a measure of judicial remedy in order *¨to reinstate the situation existing before the violation¨* as provided by the Civil Code. However, due to the absence of the comprehensive framework in the law this provision is rarely cited by claimants or even by courts. There is also substantial body of case law developed by the Court of Cassation and the Constitutional Court of Armenia concerning defamation and insult which are applicable also to the online content.

There is no legislative basis for monitoring or **filtering** the internet content by ISPs, host providers or operators or any State regulatory or self-regulatory bodies. However, there are allegations that such practice has been exercised by authorities and even by private operators out of the context of criminal proceedings and on case by case basis.

The above national regulation has been largely influenced by various international treaties that Armenia joined since its independence. In October 2006 Armenia ratified the European Convention on Cybercrime.[9] The ratification of this treaty prompted the introduction in the Criminal Code as of 1 January 2006 of a new section about cybercrime, including the establishment in the Police of a special department of prevention of cybercrime which role is to provide technical legal support to investigative bodies investigating online crime. In addition, Armenia ratified in 2005 the Optional Protocol of the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography[10] as a result of which distribution of child pornography on computer networks and even possession of such material in the computer was criminalized in the Criminal Code. On 9 May 2012 Armenia ratified the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.[11] Finally, on 26 April 2002 Armenia ratified the European Convention on Human Rights (ECHR).[12] As a Contracting State to the ECHR, general safeguards on freedom of expression, including in the field of Internet, apply such as the application of the concept of fair balance between the individual and general interests in the matters involving defamation disputes, internet content and freedom of speech in general. These concepts are stipulated in the law, as well as in the above-mentioned case law of the Constitutional Court and the Court of Cassation. In May 2010 the National Assembly decriminalised the defamation which prompted a huge case flow to civil courts. Since then the courts developed substantial body of defamation case law the factual grounds of which largely related to illegal internet content.

On 14 August 2014 the Government of Armenia, by Decree no. 34, issued the “Internet Governance Principles”. The paragraph 16 of the Chapter 2 of the document defined the principle of net neutrality for exclusion of filtering of information flows during public electronic communication on the Web. Under paragraph 2 of the decree, a multi-agency working group called “Conference on Internet governance in the Republic of Armenia” was created which composed of representatives of public, private sector and and civil society.

---

9 Convention on Cybercrime. Budapest. 23/XI/2001. Council of Europe.

10 Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography adopted and opened for signature, ratification and accession by General Assembly resolution A/RES/54/263 of 25 May 2000. Entered into force on 18 January 2002.

11 Convention for the Protection of Individuals with regards to Automatic Processing of Personal Data. Strasbourg. 28.01.1982.

12 European Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocols no. 11 and no. 14. Rome 4.XI.1950.

2. Legal Framework

2.1. Blocking and/or filtering of illegal Internet content

Internet content can be blocked under **Law on Legal Regime of the State of Emergency.**[13] The Section 2 of the article 1 of the law provides the legitimate grounds for interference such as the attempt of violent change or overthrow of the constitutional order of the Republic of Armenia, seizure or usurpation of power, armed disturbances, mass disorder, terrorist acts, seizure or blockage of objects of special significance, arrangement and operation of illegal armed groups, national, racial and religious conflicts accompanied by violent actions, imminent threat to human life and health". The subsection 12 of section 1 of article 7 of the same law provides that measures and temporary limitations of the rights and freedoms may include *"a limitation of the freedom of speech, in particular, a prohibition of certain publications and programs by mass media".* This provision derives from general article 43 of the Constitution permitting restriction of freedom of imparting and dissemination of information in the interests of national security and public order. This law sets also strong guarantees against arbitrariness such as the principle of proportionality and relevancy of measures, the requirement of rational link between the measure and the legitimate aim sought.[14] In addition, as the decision about content blocking in case of state of emergency shall be taken by an administrative body, the **Law on Fundamentals of Administrative Action and Administrative Proceedings**[15] also applies and as such it sets additional guarantees of the necessity and proportionality of measures,[16] legitimacy of aims,[17] limitation of discretionary power,[18] prohibition of arbitrariness[19] of the decision making body and the principle of the presumption of fact.[20] The decision of the administrative body can be challenged to the higher administrative body and, if rejected, to the Administrative Court.

Blocking of internet content is not a wide-spread practice in Armenia. The only significant case of content blocking happened in March 2008 when the President of Armenia declared State of Emergency from 1 to 20 March 2008 in Yerevan after clashes between police and demonstrators following the Presidential elections of 19 February which subsequently evolved to wide public protest actions. The decision stating State of Emergency introduced a set of special measures such as banning rallies, demonstrations, strikes and other public protest events. It also imposed an unprecedented limitation on the freedom of media by providing that mass media outlets were allowed during the period of Emergency *"to provide information on state and internal affairs only within the parameters of official information provided by state bodies"*.[21] On the basis of this paragraph, the National Security Service (NSS) demanded the Internet Society of Armenia (ISOC), the company that administered the country code domain names, to block websites of several

---

13 Law of the Republic of Armenia on Legal Regime of the State of Emergency of 21 March 2012.

14 Article 10 of the Law on Legal Regime of the State of Emergency.

15 Law of the Republic of Armenia on Fundamentals of Administrative Action and Administrative Proceedings of February 2004.

16 Article 8.

17 *Ibid*.

18 Article 6.

19 Article 7

20 Article 10.

21 Th. Hammarberg, Council of Europe Commissioner for Human Rights, "Special Mission to Armenia,", Yerevan, 12-15 March 2008. Available at https://wcd.coe.int/ViewDoc.jsp?id=1265025. See section 5 of the report.

independent and opposition media outlets which the latter did.[22] In addition, YouTube web site was blocked from 6 to 13 March as all IP addresses of www.youtube.com were unreachable from within Armenia during this time. It is to be noted that in the case of www.a1plus.am online news outlet, the ISOC blocked the site by way of revoking the ".am" domain as the company managed to circumvent the blockage and impart its news information through proxy servers. The above decision of declaring state of emergency was adopted by reference to the necessity of protecting the "the rights and lawful interests of people". It also referred expressly to section 14 of the article 55 of the Constitution which prescribes "danger to constitutional order" as basis for declaring state of emergency.

The Criminal Code is another legal source providing substantive basis for content blocking. The Code provides several provisions such as the threat to murder or to inflict serious damage to health or destroy property,[23] forcing a person to sexual intercourse,[24] dissemination of information about private and family life,[25] copyright infringement,[26] involvement of a child in prostitution or in preparation of pornographic materials and objects,[27] theft, extortion, dissemination and advertisement of pornographic materials and child pornography.[28] The Code also sets responsibility for publication of state secret wilfully or by negligence.[29] The Criminal Code and the Criminal Procedure Code[30] do not stipulate the guarantees of proportionality and necessity of restrictive measures. In general, the article 10 of the ECHR guarantees are not stipulated in criminal proceedings. However, the Criminal Procedure Code provides that the case law of the European Court of Human Rights can be cited by parties in the proceedings as a binding source of law provided that the facts are similar.[31] In practice, though, this provision has been rarely used.

Despite the wide substantive law basis described above, in practice blocking has been limited to **locally-hosted** illegal content mainly concerning dissemination of pornography and copyright infringement. For example, in 2012 the Armenian police banned a web site hosted in Armenia the owner of which had taken photos and contacts of Armenian girls posted on foreign-hosted sites and published them on his site hosted in Armenia under ".am" domain.[32] **No blocking is imposed on**

---

22 "Armenia imposes internet censorship as unrest breaks out following disputed Presidential elections", 11 March 2008. Available at https://opennet.net/blog/2008/03/armenia-imposes-internet-censorship-unrest-breaks-out-following-disputed-presidential-e.

23 Article 137.

24 Article 140.

25 Article 144.

26 Article 158.

27 Article 166. See the criminal case no. EshD/0132/12 in which the defendant was convicted for getting into contract via www.vk.com social site with a 10-year old girl and while representing himself as a film producer, he attempted to convince the minor to get into sexual intercourse with him. After his arrest, the police found in his cell phone 473 downloaded child pornography movies, pictures and animations. He was convicted under article 166, as well as under article 263(2) for keeping child pornography. The text of the judgment is available at www.datalex.am court decisions database system.

28 Article 263(2). See the footnote 9 above concerning the article 166. It has to be mentioned also that theft committed in petty amounts is liable also under Code of Administrative Violations which is the only substantive ground in this Code for liability of a person for committing administrative offense via net.

29 Article 306.

30 Criminal Procedure Code of the Republic of Armenia of 1 July 1998.

31 Section 4 of the Article 8.

32 See at www.news.am, "Owners of contacts published on armgirls.am were called to the police station," published 27 March 2012, http://news.am/arm/news/98714.html.

pornographic content where the hosting is not local.[33] There have been even reports where internet sites physically located in Russia and blocked by Russian regulatory body Roskomnadzor (under justification of displaying pedophiliac, terroristic content) were automatically blocked in Armenia too. After reports were filed from users in Armenia, the Russian regulatory body unblocked the sites for users in Armenia due to the difference in laws regulating internet content between the two countries.[34] As to the blocking with political motives, as described above in connection with 1 March 2008 events, no such practice was reported in the period following those events.

Another area in the criminal law providing wide basis for blocking of content is **cybercrime**. The Chapter 24 of the Criminal Code titled as "Crimes Against Computer Information Security" defines different types of cybercrimes such as unlawful access to computer or network data, change of information in the computer or in the network, destruction of computer data or software program, appropriation of computer data by way of copying, interception, etc., production and sale of hardware and software for purpose of unauthorized access to computer system or network, as well as use of such software for destruction and change of such data.[35] The most prominent case involving the articles above is the case of Georgi Avanesov who was convicted in Armenia for creating the Bredolab malware by which he broke into protected websites of 59 million users, damaged 194 websites and 30 million computers, and spread 341 special viruses. He was wanted by police of several countries, eventually he was arrested in Armenia upon departure and charged under the articles mentioned above. However, the court dropped charges under articles 254, 255 and 256 due to the general amnesty and sentenced him only under article 253(3) to 4 years of imprisonment in 2012.[36] As already mentioned above, the Criminal Code does not stipulate the article 10 of the ECHR free speech guarantees of proportionality and necessity of interference, the sufficiency and relevancy of measures.

Besides the criminal activities described above which are motivated usually by economic interest, quite often cybercrimes in Armenia occur as a result of political motives in the context of the escalation of border armed conflicts between Armenia and Azerbaijan and, in this connection, the growing war rhetoric between the two countries. Cyberattacks on government and private entities from sources originating in Azerbaijan and Turkey grew significantly in recent years. Since 2013, periodic DdoS attacks have increased and sometimes the sizable attacks amount to 50 Gbps which according to some experts is comparable to the whole Armenian internet traffic.[37] The cyberattacks are often associated with hate speech such as incitement to national, racial or religious hatred,[38] or hate crime such as denial of genocide[39] or destruction or property damage committed on motives of national or racial hatred.[40]The situation grew so worrisome that some experts even proposed to

---

33 Freedom on the Net 2014. Freedom House. Available at https://freedomhouse.org/sites/default/files/resources/Armenia.pdf. See at page 7, par. 4.

34 "Russia Forgot to Remove to Filter": Rostelecom on Sites Erroneously Blocked for Armenia Internet Users". Available at http://www.epress.am/en/2014/05/23/russia-forgot-to-remove-to-filter-rostelecom-on-sites-erroneously-blocked-for-armenia-internet-users.html.

35 Articles 251, 252, 253, 254, 255 and 256 accordingly.

36 The full text of the judgment is available at court database system www.datalex.com case no. EAKD/0144/01/11.

37 S. Martirosyan, DDOS attacks on Armenia cause concerns. Available at http://noravank.am/arm/articles/security/detail.php?ELEMENT_ID=12706.

38 Actions which are liable under article 226 of the Criminal Code.

39 Article 397 of the Criminal Code.

40 Article 185(2)(4) of the Criminal Code in which the term "property" is open to interpretation as meaning also the internet sites that have economic value for the owners. This interpretation derives from the case law of the European Court of Human Rights providing the notion of autonomous

create cyber-defense forces within defense and law enforcement agencies.[41] These politically motivated cybercrimes are also basis for blocking the internet content. However, in practice no wide measures have been taken so far and there is no government policy for taking such measures. Instead, in such cases the affected internet sites are quickly restored and the hate content is removed quickly by measures taken by website owners and host providers.

Besides the grounds within the premise of the criminal law, certain actions under **civil law** area may also form legal basis for the request to block content. In cases of defamation and insult,[42] violation of privacy and copyright,[43] the court may order blocking of content during trial as a **temporary injunction** or may rule on the merits by blocking the content as a **judicial remedy**. Blocking the content as a civil remedy can be ordered by court on the basis of the article 14 of the Civil Code defining the exhaustive list of civil remedies and among them two remedies under subparagraphs 2 and 3 *"to reinstate the situation that existed before the violation"* and *"to prevent the actions that violated the rights or created a threat to its violation"* accordingly. Thus, a party winning the case may ask the court to issue a writ of execution on the basis of which the body responsible for enforcement of court decisions (Department of Enforcement of Judicial Acts under the Ministry of Justice (DEJA)) has to institute enforcement proceedings and request the telecommunication operator, the ISP or the host provider to block the certain content. Such request is mandatory on the basis of the article 71 of the Law on Compulsory Enforcement of Court Orders and therefore the ISPs or the operators have no choice but to comply with the request. Despite the above remedial measures specified in the Civil Code and the Law on Copyrights and Related Rights, no specific safeguards for freedom of expression in relation to blocking of content are stipulated in them.

In addition to the above remedies for defamation and copyright violations, new remedial framework was adopted on 1 July 2015 by adoption of the law on "Protection of personal data". Under articles 15(2), 19(1), 20 and 21 of the law, a person has the right to demand rectification, blocking and removal of web content concerning his/her personal data. The article 1(3) of the law sets balancing test between freedom of expression and personal data protection by stipulating that restrictions of processing personal data shall not apply to processing of data related to journalism, literature and art. The law also set a regulatory body under the Ministry of Justice which has wide competences including, *inter alia*, a power of verifying compliance of personal data with legislation, as well as requesting State and private bodies, physical and legal entities to amend, remove, block or suspend web content. Such request can be made on the ground of a petition by a citizen or at its own initiative. The decision of the regulatory body is an administrative act and as such is subject to judicial review. All of the above-described interfering actions under premises of both criminal law and civil law derive from general article 43 of the Constitution permitting limitation of the freedom of imparting and receiving information for the sake of crime prevention, protection of health and morality, constitutional rights and freedoms, as well as honor and reputation of others.

Besides the above regulatory mechanisms, there are also **self-regulatory mechanism** implemented by ISPs. For example, the Internet Society of Armenia (ISOC) and the Armenia Network Information

---

meaning of the term "property" under article 1 of Protocol 1 of the Convention. *See Van Marle and others v. Netherlands,* no. 8543/79; 8674/79; 8675/79, 8685/79, 26/06/86, p. 41.

41 S. Martirosyan, Proposals regarding cybersecurity of Armenia. Available at http://www.noravank.am/eng/articles/detail.php?ELEMENT_ID=12975.

42 Article 1087.1 of the Civil Code.

43 Copyright infringement is regulated both under the Law on Copyrights and Related Rights of 15 June 2006 and the Criminal Code. The dividing line between these two premises is the amount of the damage. If the damage is substantial, it goes under the Criminal Code.

Center (AM NIC), both as registrars of the top-level domain ".am",[44] have come into an agreement by issuing a joint AM TLD Policy under which they reserve the right to revoke a domain (in fact blocking the content) if the user spreads spam and/or posts illegal or inappropriate content such as "stirring up" an international, ethnic, religious discord, "abetting" in international terrorism, "promoting" violence, hate speech, "boosting" up pornography and "supporting" trafficking. The policy above has not been widely used so far. However, in 2011 the two companies revoked the domains of two online news portals www.xronika.am and www.versiya.am which periodically spread racist hate speech. The revocation of the domains in fact entailed to blocking of the content. The ISOC derives its authority of taking the above restrictive measures on the basis of the agreement with the Ministry of Transport and Communications of the Republic of Armenia under section 1(a) of which the ISOC AM received the right "to manage the Armenian domain zone and perform its role successfully in cooperation with" the Ministry. The decision of restriction or suspension of services can be appealed in general order to court under the Civil Procedure Code.[45] ISOC and AM NIC have the burden of proof that the content was illegal and that the user was in breach of the contract. The Civil Code does not require the license holder to make proportionality assessment before revoking the domain-name.

As to **filtering**, there is no law or any legal framework providing legal ground for such activity. Moreover, there is no evidence to prove that such mechanisms are used. The ISOC has announced publicly about absence of censorship on internet in Armenia. The Freedom House assessed the internet freedom status in 2013 and 2014 as free.[46] However, given the situation described above concerning the substantial grow of politically motivated cybercrime activities, there are allegations that such mechanisms exist. According to the survey carried out by the OpenNet Initiative in 2010, despite absence of evidence, there were strong indications of existence of second-or third-generation filtering mechanisms in Armenia. The survey further provides that there was substantial political filtering and selective filtering of information covering social issues, as well as issues concerning conflict and national security.[47] This information is not confirmed under present day condition. It is highly possible that this survey was based largely on the events that occurred in March 2008 when the state of emergency was declared and the freedom of speech and free flow of information on the net were substantially limited.

2.2. Take-down/removal of illegal Internet content

The removal of the internet content is regulated by similar substantive grounds as above. In the sphere of the **criminal law** and for preventing criminal activity, the content can be removed if its publication on the internet constitutes a crime under the Criminal Code. Mostly such actions refer to dissemination of information about private and family life, threat to murder or inflict physical injuries, publication of state secrets,[48] substantial copyright infringement, dissemination and advertisement of pornographic materials, child pornography, [49] as well as committal of lecherous act against minor by way of electronic network.[50] Certain crimes under Chapter 24 of the Code described

---

44 The ".am" is the mostly used domain by the population of Armenia according to the survey carried out by the ISOC. The full text of the survey in Armenian is available at https://www.isoc.am/publ/penetration_am.pdf. According to the survey, 22.71% of respondents use domain ".am" in comparison to 22% of the respondents who said they used domain ".com", and 83.1% of the users in Armenia is the .am as compared to 82% of users giving preference to .com.

45 Civil Procedure Code of the Republic of Armenia of 17 June 1998.

46 Reference 12.

47 The full report is available at https://opennet.net/sites/opennet.net/files/ONI_Armenia_2010.pdf

48 Articles 306-307.

49 References 8-10 above.

50 Article 142(2)(6) of the Criminal Code.

as cybercrime may also be reason for content removal such as the change, obstruction, mutilation of the content in the computer or in the network.[51] Actions amounting to hate crime such as incitement to national, racial or religious hatred,[52] genocide denial, destruction of property[53] can also be taken as basis for content removal.

However, in practice in recent years the most frequent type of criminal activity for which contents were removed concerned the publication of pornographic content by the motive of revenge or extortion of money. Some cases with elements of child pornography have also been reported. For example, the person who disseminated via social network pornographic scenes of supposedly of his girlfriend was sentenced to pay a fine for publication of private information and to 3 years of imprisonment for spreading pornography.[54] Or the adult male person who on the social network www.odnoklassniki.ru created his individual page with obscene wording and who sent obscene texts via the network to boys of 7-12 years old, offered them to watch online child pornography and showed them by Skype his private parts was sentenced to 4 years of imprisonment for committal of lecherous acts and for child pornography. All the relevant contents were naturally removed by the social network based on the notice from the law enforcement bodies.[55]

Quite often the private site owners or the government entities have to remove the hate speech content displayed as a result of activities coming under article 253 of the Criminal Code with political motives.[56] In recent years such cyberattacks have become mutual between Armenian and Turkish or Armenian and Azerbaijani hackers. In all such cases, the affected parties in each country have to remove the unwanted content from their pages and restore their original content.[57] The content is removed by the host provider upon request made by the private owner of the site or the government entity such as the NSS or the Investigative Committee. For this kind of cyberattacks the formal criminal proceedings are not used since the cyberattack is committed from the territories of countries with which Armenia does not have mutual legal assistance framework. The removal of the content is therefore the only remedy that the victims may hope.

Despite the above widely stipulated substantive grounds, the Criminal Code, as well as the Criminal Procedure Code, do not provide the freedom of expression safeguards such as the principles of proportonality and necessity of measures. Moreover, it is not in a legal culture to apply freedom of expression safeguards in criminal proceedings. Despite there is provision in the Criminal Procedure Code providing that the case law of the European Court of Human Rights, especially the findings and interpretations of this court in specific cases, are applicable and can be referred to by parties as a binding authority, in cases involving internet content the ECHR case law is not cited in criminal proceedings by parties.

In the sphere of the **civil law**, the content can be ordered to be removed by court as a measure of judicial remedy on the basis of the article 14 of the Civil Code to reinstate the situation that existed before the violation or to prevent the actions that violated the rights or created a threat to its violation (as in the cases of content blocking described above). In such cases, the decision is made by

---

51 Reference 14. Article 253 of the Code.

52 References 17.

53 References 18- 19.

54 The criminal case no. EKD/0287/01/11. The court decision is not available on www.datalex.am system due to the closed hearings that took place in this case.

55 See more at http://www.lragir.am/index/arm/0/country/view/97810#sthash.azYBmxx5.dpuf

56 Reference 16.

57 See, for example, the following press article about one of the recent major cyberattacks displaying how the original content is distorted and replaced with hate speech content. The full article is available at: https://www.hackread.com/armenia-turkish-hackers-cyberwar/.

court which then issues a writ of execution on the basis of which DEJA in its turn opens enforcement proceedings in the framework of which it orders the content holder or the owner to remove it. The content can be removed for defamation, insult and violation of business reputation,[58] infringement of intellectual property rights, dissemination of private information about a person without his/her consent, publication of banking[59] and trade secrets,[60] medical records, professional secrets such information possessed in notarial records or possessed by advocates.[61] All these grounds derive from the article 43 of the Constitution providing bases for limitation of freedom of receiving information for protection of constitutional rights and freedoms, honor and reputation of others, protection of public health and morality, national security and public order. However, the above laws, with small exception of defamation norms in the Civil Code mentioned below, do not specify freedom of expression safeguards in their texts such as the necessity to democratic society, sufficiency and relevancy of measures, legitimacy of aims pursued, etc.

In defamation cases substantial part of court cases are related to internet content. The central regulatory legislative norm is the article 1087.1 of the Civil Code. The Constitutional Court of Armenia and the Cassation Court of Armenia both have developed a substantial body of case law interpreting the various provisions of this article which are equally applicable on cases involving online content. According to the Constitutional Court, in dealing with defamation cases the national courts have to take into account the relevant case law of ECHR concerning article 10 of the Convention, including such underlying principles as the necessity to democratic society, the proportionality and relevancy of measures, the balancing test between the public interest and the interest of the individual, legitimacy of the purpose of interference, the grounds under which the public interest prevails such as the wide scope of permissible criticism of politicians and public figures, the special role of media and its wide protection under article 10, protection of the speech contributing to general public debates, unacceptability of rendering protection to certain speech such as hate speech, intolerance, racist remarks, etc. conflicting with democratic values.[62]

According to the case law of the Court of Cassation, the section 6 of the article 1087.1 of the Civil Code provides the concept of good faith publisher according to which the latter shall not be held liable for defamatory remarks if he/she properly cited the source at the time of the publication. The term “source” is interpreted as meaning “an author” or “a news agency” which must be a physical or a legal person.[63] Thus, if the source appears to be unknown or fake, the publisher is found liable for defamation. This approach is based on the concept of good faith publication under sections 6 and 9 of the article 1087.1. *Post factum* disclosure of the source, e.g. during court proceedings, does not release the publisher of responsibility.[64] For purposes of this report, this approach will be referred to as liability for non-publication of sources.

Some courts interpreted specific terms related to online content such as the concept of “publication” in online environment as meaning a measure by which information is made accessible “to all at a

---

58 These three terms have different definitions under article 1087.1 of the Civil Code.

59 The Law on Banking Secrets.

60 The Law on Trade and Services.

61 See also the Freedom of Information Act, article 8 providing the grounds of limitation of provision of information.

62 Constitutional Court decision no. SDV-997 of 11 November 2011, at section 10.

63 Case no. EKD/2293/02/10 of the Court of Cassation, page 14, at last paragraph: The Court of Cassation has the status of supreme court with authority to issue final and binding decisions (case law) for the purpose of ensuring unified application of laws under article 92 of the Constitution.

64 *Ibid*., at page 15, paragraph 5.

time and simultaneously".[65] One of the trial courts ruled that the publisher was not liable for defamatory comments posted by third parties because the claimant had not notified the publisher to take down the content before he had brought his claim to court.[66] For purposes of this report this approach is referred to as knowledge-based-liability. However, that decision by its nature was not a binding precedence as only the decisions of the Court of Cassation as a supreme court are binding for lower courts in similar cases. Moreover, this approach of the lower court did not go popular especially after adoption by the European Court of Human Rights of the judgment on *Delfi AS v. Estonia* case.

Despite the article 1087.1 of the Civil Code sets detailed substantive and procedural grounds such as definitions of defamation and insult, the grounds of liability, exceptions to liability deriving from prevailing public interest, the grounds for claiming monetary compensation against pecuniary and non-pecuniary damage, as well as for court costs, the periods of limitation, several defense concepts such as good faith reproduction, etc. It does not include a specific reference to removal of content as a remedy. As a result to it, while the aggrieved party may win the case in the court against online media entity and receive court declaration on violation and as a result receive a monetary compensation, the abusing content may still remain and circulate in the web.

The only means in the Civil Code that can be interpreted as giving the aggrieved party a right to demand removal of the content, as mentioned already, is the general article 14 of the Civil Code stipulating the exhausting list of civil remedies and among them the "reinstatement of the situation preceding the violation", i.e. the status-quo ante under section 2 or "*"to prevent the actions that violated the rights or created a threat to its violation"* under section 3. However, out of more than 100 cases filed in the courts since May 2010 when defamation was decriminalized and the article 1087.1 was introduced in the Civil Code, the remedy under section 2 was used by claimant only in one case[67] while the other remedy under section 3 has never been used.

This gap in the law was the reason, including the Chamber judgment of the European Court of Human Rights in Delfi case in October 2013, that two members of the Parliament introduced a bill of amendments to the article 1087.1 of the Civil Code (a supplementing article 1087.2) by which they proposed to add specific reference to content removal in the text of the article as a remedial measure. The bill introduced also liability of online media entities for third-party defamatory comments published on the portal of the entity by anonymous or fake account holders which is very wide practice in Armenia. The bill was admitted by civil society with strong criticism. The media community contended that the bill would jeopardise the free speech on internet. On 14 March 2014, nine journalistic associations disseminated a joint statement urging the parliamentarians to withdraw the initiative.[68] On 30 March, Reporters Without Borders (RSF) urged the parliamentarians to withdraw the draft law and support the solution of the problem through self-regulatory mechanisms.[69] Under pressure of the civil society, the parliamentarians withdrew the bill for an indefinite period of time.

---

65 Glendale Hills CJSC v. "Skizb Media Kentron" Ltd. (the case of Zhamanak daily, civil case no. EKD/1963/02/10, at page 20.

66 Decision of the First Instance Court of Kentron and Nork-Marash Communities of Yerevan in the civil case of EKD/2491/02/11 in which the court ruled that the requirement to remove the comments of a third person from the news portal of online news agency was a measure not necessary in a democratic society.

67 Case of singer *Lilith Hovhannisyan v. Aram Antinyan* (editor of news aggregator www.blognews.am), civil case no. EAKD/2638/02/14, 04.06.2015.

68 The full text is available here: http://ypc.am/oldypc/bulletin/t/45853/ln/en.

69 The full text of the statement is available here: https://en.rsf.org/armenia-bill-poses-danger-to-online-30-03-2014,46060.html.

Thus, at present there are no clear-cut statutory grounds for removal of content, and there is no developed practice in this area too. Instead, the content removal is mostly self-regulated and the media outlests actively monitor and moderate their news portals for removal of illegal content containing defamation, insult and hate speech. While doing so, the content moderators of media entities rely on their own ethics rules, if they have such, or on their absolute discretion. They also may take as guidance the ethics rules[70] developed by the Media Ethics Observatory (MEO), a self-regulatory body on media ethics, as well as is recently published **guideline** for online media entities and journalists based on the findings of the European Court in *Delfi* case.[71] The media ethics rules provide general human rights safeguards such as the prevailing public interest test, the respect to private and family life, personal correspondence, wider scope of criticism of public figures, the balancing test between conflicting legitimate rights, prohibition of discrimination, prohibition of hate speech and hate content.

The ISPs, host providers and other operators, as already mentioned above, do not bear an obligation under law to remove illegal content. Similarly, they are not liable for the illegal content (such as child pornography, cybercrime, crime committed online such as theft) unless it is proved that they had prior knowledge of the content. It has been many cases of prosecution of users for spreading illegal content via Internet in Armenia but in none of them the ISPs, host providers or operators were subjected to criminal or civil liability for failure to take down the content.

3. Procedural Aspects

Within the framework of declaration of state of emergency, the decision about blocking of content, as described above, is taken by the NSS. The Presidential decree announcing state of emergency may provide only the general scope such as that mass media outlets shall be allowed *"to provide information on state and internal affairs only within the parameters of official information provided by state bodies"*.[72] Based on such a broader scope defined in the Presidential decree, the Police of Armenia, based on article 7(1)(12) of the Law on Legal Regime of the State of Emergency, chooses the internet sites that must be blocked and adopts the relevant decision. With the next step, the Police notify the domain registrar, or the ISP or the host provider of the decision and demand to fulfil the decision. The decision of the NSS is by its nature an **administrative act** and as such it can be challenged to higher administrative instance or to the Administrative Court of Armenia. The judgment of the Administrative court can be appealed to the Administrative Appeal Court and further to the Court of Cassation of Armenia.

For the purpose of crime prevention or criminal prosecution, there is no specific decision-making process about removal or blocking of content by investigative bodies. However, in the course of the instituted pre-trial investigation and if the webpage is hosted in Armenia, the investigator may seize the telecommunication devices located at intermediary's premises. The seizure is done for the purpose of conducting forensic examination of the hardware or the software as far as it concerns the alleged illegal content. As a result of the seizure, the content is automatically "blocked" and remains as such until the final court decision on the merits is made. Thus, the decision on seizure accidentally plays the role of temporary injunction. In general, the Criminal Procedure Code does not prescribe

---

70 Code of Ethics of Armenian Media and Journalists. Adopted on 10 March 2007. The code was revised on 16 May 2015. Available at http://ypc.am/wp-content/uploads/2014/06/Code-of-Ethics_eng.pdf

71 MEO Guidelines: Guidelines for Armenian Media, Developed Based on the *Delfi AS v. Estonia* European Court of Human Rights Judgment – adopted at the session of the Media Ethics Observatory, 23 July 2015. Available at: http://ypc.am/self-regulation/activities-of-the-media-ethics-observatory/meo-guidelines/.

72 Reference 6.

any freedom of expression standards and procedural guarantees. Moreover, it is not yet in a legal culture in criminal proceedings to consider freedom of expression guarantees in cases dealing with internet content.

If the host is located outside Armenia, the investigative body (the Investigative Committee of Armenia or the Department of Investigation of the NSS) may ask the foreign host provider or the content holder directly to remove the content as regular users do. Such requests are done on common grounds; as regular citizens do. However, this is not a wide practice. According to Google Transparency Report, throughout the whole reporting period since 2009 only one request was made from Armenia which was a request by *"a politician to remove three YouTube videos that used profane language in reference to him"*.[73] However, this request was turned down by the Google on the basis that the content did not violate the policy of the company. The investigative bodies may also refer to their foreign colleagues with the request to carry out certain investigative actions, including taking down of the content, through the mutual legal assistance treaties such as the Minsk Convention among the CIS states[74] or bilateral treaties that Armenia has signed with a number of countries. Such requests can also be sent also through the Interpol 7/24 data exchange program.

The ISPs or host providers in Armenia may challenge the investigator's decision of seizure of the hardware to the prosecutor supervising the activities of the investigator within the framework of the instituted criminal investigation (i.e. pre-trial investigation). If the appeal is rejected by the prosecutor, the claimant may further appeal the investigator's decision to the court of general jurisdiction. The court may overturn the investigator's decision and order to eliminate the violation. [75] The Police has in its structure the Cybercrime Prevention Department (also known as No 1 Division of no 3. Department of the Central Anti-Organized Crime Department of the Police of Armenia) which provides technical legal support to the above investigative bodies.

If the above law enforcement bodies need to conduct surveillance before starting criminal prosecution against specific physical person, they need to obtain court permission for surveillance. This procedure is regulated by the Criminal Procedure Code and by the Law on Operative and Search Measures the articles 14(1)(11) and 14(1)(12) of which permit the police and the NSS to conduct surveillance of telephone, correspondence and other communications on the basis of court order. For that purpose, the article 50(3) of the Law on Electronic Communications imposes an obligation on operators and ISPs to provide access to Police and NSS officers to "communication devices, infrastructures, switch on/off, directing and other similar devices necessary to carry out surveillance".

Failure to provide such access may result in breach of license which in turn may result in suspension or revocation of license by the regulatory body Public Service Regulatory Commission (PSRC).[76] The decisions of this body are **administrative acts** and as such they can be challenged to the Administrative Court. Despite the law does not provide explicit ground for the intermediaries to

---

73 Report period January-June 2013. See at: http://www.google.com/transparencyreport/removals/government/notes/?hl=en#authority=AM&period=all.

74 Convention on Legal Aid and Legal Relations in Civil, Family and Criminal Cases, adopted in Minsk on 22 January 1993. The convention was revised on 7 October 2002 in Chisinau, Moldova. The member states are Azerbaijan, Armenia, Belarus, Georgia, Kazakstan, Kirgizstan, Moldova, Russia, Tajikistan and Ukraine.

75 Reference 52.

76 Article 12(2)(4) of the Law on Electronic Communications provides "intentional failure to fulfill the conditions of the license or the permission" as one of the basis for suspension or revocation of the license by the regulatory body.

refuse the access, technically the intermediaries may challenge the court surveillance order to higher court in the order prescribed under Criminal Procedure Code.[77]

Moreover, they can also challenge the decision of blocking the content to the supervising prosecutor in the same order as above, and, if the appeal is not granted, further complaint can be brought to court in the order prescribed under Criminal Procedure Code.

As already described above under chapter 2.2., the intermediaries such as domain registrars may also block the content on their own initiative if they find that the content violates their ethics rules or conditions under which domains were issued. As to the removal, the ISPs or operators are unable to take down the specific content and they have no such obligation under law.

For the purpose of civil liability, any person may bring a case to court against publisher of illegal content and claim declaration of court for violation, as well as compensation against pecuniary and non-pecuniary damage, including for court costs. The claimant may also claim to block or take down the content although the substantive grounds for such claims are not clearly established in the law.
The self-regulatory bodies such as domain registrars and ISPs may also decide to block the specific webpage if domain registration rules are violated as a result of the publication of the illegal content by the domain holder (see section 2.2. above). Such decisions can be challenged to civil courts by the affected parties. In addition, as already mentioned above, most media entities operating online and many interactive service providers moderate their content and within the framework of such activity remove the content which violates their ethics rules. The removal can also be challenged to civil courts by the affected parties. There have been few cases where the claims were brought also to the MEO although the decision of this body is not binding. **As a measure of civil legal remedy**, the civil court may issue a judgment to remove the specific content to reinstate the situation before the violation. In addition, before or during the trial the civil court may order to block the specific content as a measure of temporary injunction before the final decision by court is made. In all cases above in connection with court decisions, the court decision is submitted to DEJA which institutes enforcement proceedings in the framework of which it notifies the content owner to remove the content.[78]

As to the filtration of the internet content, there is no legislative framework for such activity and therefore there is no body to take a decision on that matter.

4. General Monitoring of Internet

The telecommunication regulatory authority, the Public Services Regulation Commission (PSRC), which regulates the licensing of telecommunication operators and ISPs, does not monitor the content and it has no such authority under law.[79] Contrary to this, the operators such as domain registrar bodies monitor the content to make sure that the domain user does not breach the domain contract by publishing, for example, hate speech or pornography. The domain registrar has power

---

77 Under article 290 of the Criminal Procedure Code.

78 Enforcement proceedings are regulated by the Law of Republic of Armenia on Compulsory Enforcement of Judicial Acts, adopted on 5 May 1998.

79 The PSRC's authority, mechanisms of its members' appointments, and budgeting principles are defined under the Law on State Commission for the Regulation of Public Services. It develops regulations and criteria for license holders, their reporting standards, standards for cost accounting, quality of service, and cost calculation standards for the operators and service providers. All these regulatory papers do not concern the internet content.

under its license and based on the civil contract with the domain user to suspend or terminate the domain in such cases.

The online news agencies and media outlets do active moderation of their news portals to avoid liability for the comments of their readers – especially when they act anonymously or under false identity. For example, the Media Ethics Observatory (MEO), a self-regulatory body on media ethics established in 2007 issued a **guideline** in June 2015 for online media entities and journalists about how to avoid the situation under *Delfi* case.[80] It recommended in the guideline to actively moderate the reader comments in order to avoid appearance of illegal content in the news portal. It further recommended that in case if such comments were received, it would be advisable to remove such content immediately and as soon as possibly instead of formally waiting for a written notice by an affected party to arrive.

In addition to issuing ethics regulations, MEO is also a dispute resolution self-regulatory body. In 2007 it invited media entities to sign the Code of Conduct of Armenian Media and Journalists.[81] As of today, 39 media entities have signed the document, thus, jointly bounding themselves by the ethics norms stipulated in it. Any person or an entity may bring an application against an entity which signed the above paper and the MEO board, which has 14 members, would decide on whether the given entity violated the above self-regulatory norms. However, the Code of Conduct is not precise whether the entity, along with finding a violation, has also the authority to decide to remove the content as well. The question of removing the content is is left totally to the discretion of the party against which the violation is found.[82]

Nearly all online media outlets do content moderation. Some of them post ethics and publication rules on the website informing the reader normally about three basic rules; 1) the content is under copyright protection of the publisher, 2) proper citation has to be done in reprinting or reproducing the content, including obtaining permission for comprehensive reproduction, 3) illegal content such as defamation, hate speech, foul language, information violating privacy will be removed prior or after publication.[83] Not only the media outlets, but interactive service providers also do moderation such as online advertisement businesses,[84] an entity which provides paid services to drivers such as provision of information about traffic tickets, car sales, car safety and security services,[85] property management companies running condominium services,[86] and even web design businesses which offer moderation as a distinct service along with other services such as web maintenance and data

---

80 MEO Guidelines: Guidelines for Armenian Media, Developed Based on the *Delfi AS v. Estonia* European Court of Human Rights Judgment – adopted at the session of the Media Ethics Observatory, 23 July 2015. Available at: http://ypc.am/self-regulation/activities-of-the-media-ethics-observatory/meo-guidelines.

81 Code of Ethics of Armenian Media and Journalists. Adopted on 10 March 2007. The code was revised on 16 May 2015. Available at http://ypc.am/wp-content/uploads/2014/06/Code-of-Ethics_eng.pdf.

82 For example, in the case of *Arpri Voskanyan v. 1in.am* the dispute concerned the unauthorized use of satirical poetry by the media entity. The author applied to the MEO for a solution. The MEO decided that the media entity had violated the author's copyright by publishing without authorization the distorted text of the poem. At the same time, the MEO did not express any opinion about removal of the illegal content.

83 See, for example, the Rules of Publication by "Hetq" Investigative Journalists at http://hetq.am/arm/terms/ the "Rules of Writing on the Website of Aravot Daily Newspaper" at www.aravot.am, the section "Comments and Moderation" under chapter About Us at http://media.am/about-us.

84 See the "Rules and Conditions of Placement of Online Advertisement" at http://my.mamul.am/.

85 "General Terms and Conditions" at http://4car.am/Home/Rules#.

86 "General Terms and Conditions at www.login.am under http://login.am/hy/terms.

entry.[87] There are also public initiative groups among the civil society which by their own initiative monitor the web content for identifying copyright violations[88] by media entities and journalists, as well as other statutory law and ethics violations by journalists.[89]

In the criminal law sphere, there are allegations that the Cybercrime Prevention Department of the Police monitors the web for identifying criminally liable content such as child pornography and hate speech despite that it formally states that its function is to provide technical legal support to the Investigative Committee and the investigation department of the NSS on case by case basis.

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

The Constitution specifies the general article 10 safeguards of the ECHR such as the test of necessary in a democratic society and the principles of legality and legitimacy of aims. However, the statutory laws regulating the internet content in general lack those principles.

The article 10 safeguards are well established in the case law of the Constitutional Court and the Court of Cassation concerning defamation and insult cases. As far as the legal issue concerns the internet content, the courts have to consider the balancing test under article 10 by striking fair balance between the individual interest and the general interest of the community, including the legitimacy of the aim pursued. In comparison to the case law, the statutory norms partially stipulate the article 10 guarantees such as the prevailing public interest test as a defence in defamation cases in defining whether the given content amounts to defamation. At the same time, the civil laws (the Civil Code and the Civil Procedure Code) and the relevant case law provide vague mechanisms about removal or blocking of content. The court practice in this respect is weakly developed. Usually, the courts decide whether the content is defamatory and then decide on remedies such as payment of monetary compensation, publication of judgment, publication of refutal or public apology. As content removal or content blocking are not specified in the Civil Code as remedial measures against defamation, the courts usually do not rule on those issues when declaring a violation. There have been few cases in which the courts, while finding a violation, have also ruled to remove the content but they did so without referring to article 10 safeguards but rather as a consequence of violation.

The laws governing the operation of ISPs, host providers and domain registrars do not specify the principles of legitimacy and proportionality in the context of freedom of expression. As to the principle of the legality, as a typical civil law country that principle can be found in every statutory law in Armenia but without express reference to legal certainty as an integral part of that. Given this background, the ISPs, host providers and domain registrars are not bound by freedom of speech safeguards when they block the content or revoke the domain of their subscribers. This is confirmed by the wording in the AM TLD Policy document between the ISOC and the AM NIC. The same concerns the civil contracts that these operators sign with service users, which lack wording about freedom of expression safeguards, as well as the license on the basis of which these companies gain their authority from the state regulator Public Service Regulation Commission to operate electronic service networks. The laws governing the procedures and substantive grounds of licensing in general

---

87 By ESA Studio at http://esa.am/services/support.

88 This group is named "For the Sake of Good Faith Journalism" at https://www.facebook.com/groups/337831742965973/ which monitors mostly ethical and copyright violations by journalists and media entities.

89 This group is called "Medialiteracy" which monitors the content for contributing in public discussions involving larger aspects such as scope of permissible criticism, media role, irresponsible journalism, cybercrime, etc.

and for companies operating in the sphere of electronic communications[90] do not stipulate freedom of expression safeguards.

Where the matter concerns the administrative bodies such as, for example, the NSS taking a decision of blocking certain web sites under the state of emergency or the Public Service Regulation Commission suspending or revoking license of the operator, the Law on Fundamentals of Administration and Administrative Procedure applies. This is the only law in Armenia which specifies the general principles of proportionality and necessity of the interference, the sufficiency and relevancy of the measures, the legitimacy of aims pursued, and the fundamental principle of legal certainty. The general human rights safeguards expressed in the law regulating administrative proceedings above are open for wide use by the Public Service Regulation Commission in granting or revoking the license of electronic communication operators. However, in practice the Commission does not refer to them in its decisions.

The freedom of expression safeguards are not stipulated in the laws governing the criminal proceedings and criminal punishment such as the Criminal Code, the Criminal Procedure Code and the Law on Operative and Search Measures (the surveillance law).[91] The only avenue through which the safeguards can be applied in criminal proceedings is the article 8(4) which provides that the decisions of the European Court of Human Rights and particularly its findings and interpretations can be referred to by parties during criminal proceedings. However, there are no records that the ECHR case law has been used in criminal proceedings involving internet content.

There are legal norms that lack legal certainty from the perspectives of the principle of lawfulness. The article 7(1)(12) of the Law on Legal Regime of the State of Emergency provides in a generalized manner *"a limitation of the freedom of speech, in particular, a prohibition of certain publications and programs by mass media"* as one of the measures that state bodies are allowed to take during state of emergency. Such vague wording grants the NSS outright discretion in choosing the content that has to be blocked. The law as such lacks legal certainty and foreseeability as it has to set the nature and categories of the content to be removed, the time limit on the duration of blocking of the content, the procedure to be followed in notifying the intermediaries, the content that the decision must contain, etc. Due to absence of such requirements in the law, the NSS as a decision making body is vested with unfettered power and discretion which, including the fact that the operation of the NSS as a national security body is not open to public scrutiny, is contrary to the fundamental principle of the rule of law. Another example is the article 50(3) of the Law on Electronic Communications which provides that operators and ISPs must provide access the Police and the NSS to *"communication devices, infrastructures, the switch on/off, the directing and other similar devices; including the devices necessary to carry out telephone tapping".* This obligation is stipulated in the law in an absolute form without specifying whether the intermediaries can reject the request for access and challenge the decision authorizing to carry out surveillance. As a result to this, the operators usually do not challenge the requests for access which is due largely to uncertainty of lack of mechanisms. The Law on State and Official Secrets[92] defines in general terms the sensitive spheres with relation to which information may be classified as involving state secret. The law further stipulates that every government agency, which is allowed to handle state secret, must elaborate more detailed "agency lists" with more detailed description of the spheres. The law also stipulated that the "agency lists" were also secret and as such were not subject to publication. Thus, it was a secret what meant a secret. Such regulation resulted in that the indefinite scope of the concept of

---

90 The law of the Republic of Armenia on Licensing, adopted on 30 May 2001. The law on Electronic Communications, cited above. The Law of the Republic of Armenia on the Public Service Regulatory Commission, adopted on 25 December 2002.

91 The Law on Operative and Search Measures of the Republic of Armenia, adopted on 22 October 2007.

92 Law of the Republic of Armenia on State and Official Secret, adopted on 3 December 1996.

state secret made it absolutely impossible for users (i.e. journalists) to define whether the specific content published on internet would bring to liability for publication of state secret. On 6 March 2012, the Constitutional Court of Armenia decided that the section 7 of article 12 conflicted with the article 27 of the Constitution (freedom of expression). The court found that the classification of agency lists did not pursue legitimate aim of protection of national security under article 27 of the Constitution as long as it did not concern the classification of a concrete information objectively classified as secret. This finding of the Constitutional Court contributed to the general principle of legal certainty under European Court's case law under which the law must be sufficiently clear in its terms and it would be contrary to the rule of law for the legal discretion granted to the executive or to a judge to be expressed in terms of an unfettered power (*Liberty and Others v. United Kingdom,* no. *58243/00*, July 1, 2008, § 52).

Ara Ghazaryan
09.10.2015

Revised on 15.04.2016 taking into consideration comments from Armenia on this report