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 626-640

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.

SLOVENIA

1. Legal Sources

In Slovenia, the Internet is not governed within a single area of law. The regulation of restrictions to the freedom of the Internet is **enshrined in different legal acts**, such as the one transposing the EU *acquis* on electronic commerce in the first place, as well as the main sectorial law on electronic communications, the obligations code, the law on personal data protection, and the law governing games of chance. This places Slovenia in the group of countries with specific regulation on issues of blocking, filtering and takedown of Internet content, which is however fragmented over a few legal areas.[1]

The Electronic Commerce Market Act (ZEPT, last amended in 2009)[2] defines the scope of **liability** of providers of the information society services. The Code of Obligations (OZ-UPB1, 2007)[3] provides basic **tort principles**, according to which an Internet intermediary may be held liable for illegal Internet content. The main sectorial legal instrument, the Electronic Communications Act (ZEKom-1, its latest amendments are from 2014),[4] prevents unjustified restrictions to the openness of the Internet by the provision aimed at safeguarding **Internet neutrality.** Both the **data protection** law, as set by the Personal Data Protection Act (ZVOP-1-UPB1, 2007),[5] and legislation on **gambling**, enshrined in the Games of Chance Act (ZIS, last amended in 2012),[6] explicitly prevent supervisory authorities to demand blocking or take-down of illegal content from the intermediaries and allow such requests only via courts (by the Article 54/2 of ZVOP-1-UPB1, and by the Article 107a ZIS-UPB3 respectively).

The Directive 2011/92/EU of the European Parliament and of the Council on combating the **sexual abuse** and sexual exploitation of children and child pornography, and replacing the Council Framework Decision 2004/68/JHA, has influenced the Slovenian national legislation, in particularly the Criminal Code, but has not led to adoption of specific law. Decisions on blocking of child abuse content remain within the realm of the judicial branch. The **international standards** contained in the conventions of the Council of Europe related to illegal Internet content, including the ones referring to the sexual exploitation and sexual abuse of children, have also been transposed to the Slovenian national law (via the laws on their ratifications).[7]

---

1 That is the so-called *group A*, according to the classification of the Council of Europe, which identified 3 main categories of countries in relation to the existence or non-existence of specific regulation.

2 The Electronic Commerce Market Act was adopted in 2006 (version published in the Official Gazette of the Republic of Slovenia, No. 61/2006) and amended in 2009. Its official consolidated text was published in the Official Gazette RS, No. 96/2009.

3 Obligations Code, Official Gazette of RS, No. 83/2001 and 32/2004, authentic interpretation of the Article 195, official consolidated text UPB1, No. 97/2007.

4 Electronic Communications Act, Official Gazette RS, No. 109/12, 110/13, 40/14 - ZIN-B, and 54/14 - Decision of the Constitutional Court no. U-I-65/13.

5 Personal Data Protection Act (consolidated version ZVOP-1-UPB1, Official Gazette RS, No. 94/2007).

6 Games of Chance Act (ZIS-UPB3, Official Gazette RS, No. 14/2011, amended by ZIS-E, Official Gazette of the RS, 108/2012).

7 *Zakon o ratifikaciji Konvencije o kibernetski kriminaliteti in Dodatnega protokola h Konvenciji o kibernetski kriminaliteti, ki obravnava inkriminacijo rasističnih in ksenofobičnih dejanj, storjenih v informacijskih sistemih*, Official Gazette RS, No. 62/2004,[7] ratifying the Convention on Cybercrime (Budapest Convention), as well as Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems; *Zakon o ratifikaciji Konvencije Sveta Evrope o preprečevanju terorizma,* Official Gazette RS – International Treaties, No. 16/2009, ratifying the Convention on prevention of terrorism (Warsaw Convention); Zakon o ratifikaciji Konvencije Sveta Evrope o zaščiti otrok pred spolnim izkoriščanjem in

2. Legal Framework

In Slovenia the access to the Internet can be blocked or online content removed on **grounds** such as prevention of public disorder or crime, protection of minors, prevention of hatred based on race, sex, religion or nationality, protection of human dignity, protection of public health, public security, consumer protection, and protection of investors (as stipulated in the Art. 14 of ZEPT 2009). The intermediaries are most commonly asked by courts to intervene for protection of reputation, personal data or right to privacy, but also for protection of business interests of a highly regulated national gambling industry.

The Code of Obligations (OZ-UPB1, 2007)[8] provides basic **tort principles**, according to which an Internet intermediary may be held liable as a primary infringer, but also joint liability can be imposed on relevant participants (Art. 131 and 186). In other words, not only culpability, but also negligence can lead to determination of a person (intermediary) liable. For infringements of personal rights, the Article 134 of OZ represents the legal basis for injunctions requiring blocking or takedown of the Internet content, as it gives the possibility to request from the defendant, via court order, to terminate infringements and refrain from them.

Slovenia's constitution and legal system guarantee a high level of protection of the **right to privacy and personal data**. The Personal Data Protection Act (ZVOP-1-UPB1, 2007)[9] stipulates that the Republic of Slovenia ensures the protection against unlawful and unjustified interventions into the information privacy of an individual. The personal data protection is guaranteed to every individual regardless of his citizenship or place of residence. Without going into detail, personal data can only be processed if the law allows it or with the individual's explicit written consent.

The Information Commissioner acts as the national supervisory authority for personal data, but according to the law the Commissioner cannot order measures against the intermediaries who provide transmission services, data storage and other functions of carrying out or facilitating the transmission of data across networks if they do not have any interests related to the content which contravenes the provisions on data protection (Art. 54/2 of ZVOP-1-UPB1).

Similarly, in case of **defamation** only the Courts can issue injunction. Slovenia is one of the few countries in the region that preserved application of criminal law in defamation cases and was criticized for this by international organizations advocating freedom of media.[10] The case law however shows that Slovenian courts normally take in consideration freedom of expression when taking decisions in defamation cases. Safeguards for freedom of expression are usually contained in the wording of the court orders themselves and are defined on a case-by-case basis. Since neither the freedom of expression nor the right to privacy are absolute rights, they have to be put in balance. According to the Slovenian case law, i.e. the judgement Cp 3057/2013 of the High Court in Ljubljana

---

spolno zlorabo Official Gazette RS – International Treaties, No. 13/2013, ratifying the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention); *Zakon o ratifikaciji konvencije o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov,* Official Gazette RS – International Treaties, No. 3/94 and Official Gazette RS, No. 86/04 – ZVOP-1*, ratifying* the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

8 Obligations Code, Official Gazette of RS, No. 83/2001 and 32/2004, authentic interpretation of the Article 195, official consolidated text UPB1, No. 97/2007.

9 Personal Data Protection Act (consolidated version ZVOP-1-UPB1, Official Gazette RS, No. 94/2007).

10 I.e. by the International Press Institute (IPI) and the South East Europe Media Organisation (SEEMO), the details available on http://www.seemo.org/mission-to-slovenia.html, and by OSCE Representative for Freedom of Media Dunja Mijatović, the details available at http://www.osce.org/fom/143006 (07.10.15).

on 12 February 2014,[11] referring to the decision of the European Court of Human Rights (ECHR) in the Von Hannover v Germany case,[12] the journalistic freedom of expression is protected as long as the journalist is acting in the exercise of its mission. If the main aim of the concerned publication is to entertain the public, the level of protection of freedom of expression is lower.

The grounds for blocking the access to non-licensed online **gaming** are stipulated in the Article 107a of the Games of Chance Act (ZIS-UPB3 and ZIS-E, 2012). The Court can issue injunction if the organizer of the illegal online gaming does not eliminate the irregularities identified by the supervisory authority, i.e. the Financial Administration of the Republic of Slovenia (FURS).[13] The decision on the restriction of the access has to be adopted by the Administrative Court of the Republic of Slovenia in 7 days of receipt of the proposal submitted by FURS. The scope of restriction and its execution has to be defined by having regard to the principle of proportionality and technical possibilities. The restriction of access to web pages can be made only to the extent which is strictly necessary for the execution of a decision which prohibits organization of illegal games of chance, and in the least burdensome way for the provider of information society services. As for the legal remedies, the provider can lodge a complaint to the Supreme Court in 3 days and the Court shall decide no later than in 15 days.

In the area of **copyright law**, the Copyright and Related Rights Act (ZASP, last amended in 2015),[14] transposing among others the Directive 2004/48/EC on the enforcement of intellectual property rights,[15] does not refer specifically to the online infringements, but grants the judicial protection to the right holders via the general provisions on what the right holder can claim when its exclusive rights were infringed. Since the very high level of personal data protection in Slovenia does not allow an easy identification of the authors of online posts on the basis of their IP address, this makes it difficult to prevent online copyright infringements, especially if committed by anonymous users.

Public calls to develop blocking measures against the online display of **sexual abuse** of children have not been reflected specifically in the legislation. The area is being regulated by the respective provisions of the Criminal Code (KZ-1-UPB2, 2012).[16]

The **Criminal Code** outlaws the following types of messages, images or activity:

a) the Article 110 criminalizes incitement to and public glorification of terrorist activities;
b) the Articles 158(2), 159(2), 160(2) and 161(2) criminalize public insult, slander, defamation, and calumny;
c) the Article 173a criminalizes grooming via the ICT services;
d) the Article 176 criminalizes sexual abuse of children for production of pictures, audiovisual or other items of pornographic, as well as production, possession, distribution or selling of

---

11 Judgement Cp 3057/2013, 12 February 2014, available at http://www.sodisce.si/vislj/odlocitve/2012032113068455/ (07.10.15).

12 Judgement of ECHR in Case of Von Hannover v Germany (Application no. 59320/00), 24 June 2004, available at http://hudoc.echr.coe.int/eng?i=001-61853#{"itemid":["001-61853"]} (07.05.15)

13 The Financial Administration of the Republic of Slovenia is an administrative body within the Ministry of Finance with the following main tasks: assessment, calculation and collection of taxes and duties, customs clearance of goods, financial supervision, financial investigation, and gaming supervision. More details on http://www.fu.gov.si/en/ (07.10.15).

14 Copyright and related rights law (ZASP, Official Gazette RS, Nos. 21/95, 9/01, 30/01, 43/01, 17/06, 44/06, 139/06, 16/07, and 56/2015).

15 Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (Official Journal L 195, 2 June 2004, p. 16).

16 Criminal Code, KZ-1-UPB2, the Official Gazette of the RS, No. 50/2012.

pornographic or other sexual materials depicting minors or realistic images of minors, or discloses the identity of a minor in such materials;

e) the Article 297 (1) criminalizes hate speech, by stipulating that anyone who publicly promote or incite hatred, violence or intolerance based on national, racial, religious or ethnic affiliation, sex, skin color, origin, property status, education, social status, political or other beliefs, disability, sexual orientation or any other personal circumstances, and the offense is committed in a manner that may endanger or disturb public order and peace, or by threatening, abusive language or insulting, shall be punished with imprisonment up to two years;
f) the Article 297(2) further criminalizes public dissemination of ideas on the supremacy of one race over another, provision of aid for racist activity, denial/diminishment of the significance of genocide, holocaust, crimes against humanity, war crime or aggression, or other criminal offences against humanity;
g) other grounds from the Criminal Code include protection of personal data (Art. 143, para. 1 and 3), preventing unauthorized publication of private writings (Art. 140), preventing the disclosure of information received in confidence (Art. 142) or disclosure of information classified as business secrets (Art. 236) or state secrets (Art. 260), and breaches of confidentiality of court, administrative, misdemeanor or parliamentary investigation procedures (Art. 287).

The main sectorial legal instrument, the Electronic Communications Act (ZEKom-1, its latest amendments are from 2014),[17] addresses the question of blocking or takedown of illegal content only indirectly. The Article 203, aimed at safeguarding the Internet openness and neutrality, sets out the general **net neutrality** principles, according to which the operators have to preserve the open and neutral character of the internet and must not restrict, delay or slow-down the Internet traffic at the level of individual services or applications or implement any measures to degrade them (except in narrowly defined exceptions). The most direct reference to the possibility of blocking, filtering or takedown of illegal content can be found in the provision of the third paragraph of the same article, according to which the principle of openness of the Internet can be breached only upon a court decision.

As for the **self-regulatory** instruments, there are a couple of initiatives worth highlighting. The first one is joining together **the main communication services providers** under the umbrella of the Slovenian Chamber of Commerce and is supported by a mixed group of public institutions, academia and trade associations: the national regulatory authority AKOS, responsible for electronic communications and media, the Academic and Research Network of Slovenia ARNES,[18] the Awareness Centre for Safer Internet SAFE.SI,[19] the Information Commissioner,[20] the Faculty of

17 Electronic Communications Act, Official Gazette RS, No. 109/12, 110/13, 40/14 - ZIN-B, and 54/14 - Decision of the Constitutional Court no. U-I-65/13.

18 The Academic and Research Network of Slovenia (ARNES) is a public institute that provides network services to research, educational and cultural organizations, and enables them to establish connections and cooperation with each other and with related organizations abroad, more info on http://www.arnes.si/en/about-arnes.html (07.10.15).

19 SAFE-SI is a Slovenian national Awareness Centre that promotes and supports awareness on protection and education of children and teenagers using Internet and new online technologies. The Centre is being run by a consortium of partners in a consortium are University of Ljubljana, The Faculty of Social Sciences, ARNES, Slovenian Association of Friends of Youth and the Youth Information and Counselling Centre of Slovenia, as a project under the umbrella of the Safer Internet Programme. It is co-financed by Information Society and Media Directorate-General within European Commission and Slovenian Ministry of Education, Science, and Sport. More info on http://english.safe.si/ (07.09.15).

20 Information Commissioner is an autonomous and independent body, established with the Information Commissioner Act (ZInfP, Official Gazette of the RS, no. 113/2005). The body supervises both the

Security Sciences of the University of Maribor, and the Trade Association for Informatics and Telecommunications. The initiative put in place a Code of Conduct in 2009[21] for the first time and updated it in 2013.[22] The nine-page Code applies to the providers of public electronic communications services, but does not address specifically the issue of blocking, filtering or removal of illegal content. It encourages the providers to facilitate and promote of safe use of their services via a set of rather general recommendations without mentioning the need to safeguard the freedom of expression and proportionality of the measures. As regards the third party unlawful content, it reiterates the intermediaries' commitment to society services cooperate with the responsible authorities of the Republic of Slovenia and non-state institutions in the implementation of their obligations under the Slovenian legislation in the fight against illegal content".[23]

In 2010 six major online media portals signed the **Code for regulation of hate speech on websites**:[24] Delo.si, Dnevnik.si, MMC, Siol.net, Vecer.com, and Zurnal24. A year later the most popular news portal 24ur.com joined in, as well as Slovenskenovice.si and Mediaspeed.net portal. The Code was prepared in cooperation with **the *Spletno oko* hotline**,[25] which operates within the above-mentioned SAFE.SI programme and facilitates anonymous reporting of illegal content online. One of the main goals of the code was provision of uniform guidelines for the regulation of hate speech on Slovenian websites. The Code was originally foreseen to cover strictly hate speech, i.e. only violations of the Article 297 of KZ-1, but later the signatories decided to moderate other forms of intolerance or abusive speech on their portals as well. To this aim, the signatories offer a special button on their portals, aimed at reporting cases of incitement to violence, hatred or intolerance. The reporting button enables direct reporting to the *Spletno oko* hotline together with alarming the administrator of the web portal where they identified a potential example of hate speech. In case the administrator ascertains that the reported content violates the rules of the portal, it can remove it. The *Spletno oko* reviewers simultaneously examine each case and report it to the Police if they identify elements of criminal offense under 297.čl. KZ-1B.

The peak of received **reports on child sexual abuse images and hate speech** was reached in 2012 and was immediately followed by a significant decline. In its report[26] the Safe.si project attributed this drop to the changed legislation, which in 2012 criminalized intentional accessing of child sexual abuse images, and to a clearer definition of illegal hate speech, provided by the Criminal Department of the Supreme Public Prosecutor Office of the Republic of Slovenia via a legal opinion, adopted in February 2013.

---

protection of personal data, as well as access to public information. More info on https://www.ip-rs.si/index.php?id=235 (07.09.15).

21 The Code from 2009 was an adaptation of the European Framework for Safer Mobile Use by Younger Teenagers and Children, signed by 15 representatives of the European operators, members of the GSM Association (GSM Association - GSMA) on 6 February 2007 in Brussels.

22 Gospodarska zbornica Slovenije, Kodeks ravnanja izvajalcev javnih elektronskih komunikacijskih storitev za zaščito uporabnikov, 2013, the Code of Conduct is available in Slovenian only on http://www.ris.org/uploadi/editor/1360137260Kodeks_ravnanja_za_zascito_uporabnikov_2013.pdf (10.09.15).

23 The Code of Conduct, p. 7, available on http://www.ris.org/uploadi/editor/1360137260Kodeks_ravnanja_za_zascito_uporabnikov_2013.pdf (10.09.2015).

24 Available on http://safe.si/sites/safe.si/files/kodeks_oblikovan.pdf (07.10.15).

25 The Slovenian hotline for reporting the illegal Internet content *Spletno oko* is being run by the EU initiated and co-financed project Safe.si aimed at promotion of safer Internet. The hotline, operating since 2007, works in cooperation with the Slovenian police and the Supreme Court, and is a member of the INHOPE network.

26 Ibidem.

In this legal opinion, the Supreme Public Prosecutor Office stressed that criminal proceedings arising from prosecution for an offense under the Article 297 of the Criminal Code (KZ-1) interferes with the constitutionally guaranteed right to **freedom of expression and freedom of the press**. The Office emphasized that in each case of the alleged hate-speech the responsible institutions should assess whether criminal prosecution is really necessary taking into account the **criterion of proportionality** and the premise that sees **penal repression as a last resort** to overcome the negative phenomena in society (principle of *ultima ratio*).[27]

In the two sub-chapters below (2.1 and 2.2) we are explaining the role and practices of the intermediaries in implementing the blocking and takedown measures, together with an insight into the relevant case law.

2.1. Blocking and/or filtering of illegal Internet content

Slovenia's first **attempt of blocking** an Internet site due to its content dates back to 2003, when the Personal Data Protection Inspectorate of the Republic of Slovenia, at that time still a body within the Ministry of Justice,[28] ordered blocking of the website www.udba.net, which published a database with detailed information on persons who supposedly cooperated with the State Security Service in the previous regime or were monitored by this institution. The released data were claimed to be a part of the central registry of the former service of the national security and contained personal data of over one million individuals, and for this considered one of the biggest breach of personal data protection in the history of independent Slovenia. The Police found out that the server of the website was located in Thailand and got the assurances from the Thai authorities that the content would be removed. For the period until the removal, the Chief Inspector for Personal Data Protection issued an oral order to the Slovenian Internet providers to limit the access to the domain, and subsequently delivered written orders, however not all the providers complied with the request. Their professional association, the Section of the Slovenian Internet service providers (SISPA), expressed opposition to the measure, arguing that it was not enforceable in practice, as well as legally questionable and a dangerous precedent. As there were easy ways to circumvent the blockade, the Chief Inspector recognized impossibility of its implementation and canceled the ruling already within one month of its imposition.

A few other examples of restricting access to websites, induced by breaches of legislation governing games of chance, followed this case, however in these twelve years the Slovenian legislature repeatedly rejected the possibility of action without judicial intervention, while the findings of the responsible institutions also showed that the blocking measures were never truly effective.

This applies also to the area of **copyright protection**. In 2008, the attorney of an organisation for protection of collective rights related to audiovisual works urged without success the Slovenian ISPs to block all the IP addresses between 77.247.176.1 and 77.247.176.255, commonly used by the Pirate Bay.[29] On the other hand, in 2011 the copyright protection was according to the sources familiar with the case used as an argument to finally convince YouTube to remove the leaked

---

27 Vrhovno državno tožilstvo Republike Slovenije, Pregon kaznivega dejanja Javnega spodbujanja sovraštva, nasilja ali nestrpnosti po 297. členu KZ-1 – pravno stališče, available at http://safe.si/spletno-oko/pravno-stalisce-tozilstva-o-pregonu-kaznivega-dejanja-javnega-spodbujanja-sovrastva-nasi (11.9.15).

28 In 2005 merged with Commissioner for Access to Public Information into Information Commissioner with status of independent public body.

29 More details in the Monitor Magazine article, Blokada Pirate Baya tudi v Sloveniji? 11 November 2008, available on http://www.monitor.si/novica/blokada-pirate-baya-tudi-v-sloveniji/136968/?xURL=301 (03.09.15).

audiovisual recordings of closed government sessions from its platform.[30] The Government had to repeat its claim a few times, as the removed recordings kept reappearing.[31]

The amended Act on Electronic Commerce Market (ZEPT-A), adopted in 2009,[32] granted the power of ordering blocking access to websites or Internet traffic to **civil or criminal courts**, if the measure was justified by *lex specialis*, and limited the possibility to implement it via administrative measures.[33] The proposer of the law, the Ministry of Economy, underlined in its explanation that takedown or blocking of illegal content on the internet was a heavy and exceptional measure, associated with risks of restricting the freedom of internet and hence also the freedom of expression as one of the constitutionally guaranteed rights.[34] The intermediaries are obliged by the Articles 9, 10 and 11 of the ZEPT 2009 to react to the court order and terminate or prevent an infringement, despite the exclusion of their liability for the third-party services or content. The court may order them to remove illegal content or blocking access to it for the detection and prevention of crime, protection of privacy, protection of classified information and business secrets. Their liability slightly varies in relation to the type of services they provide; the caching service providers are expected not only to react to a court order or a notice on unlawfulness of content, but also to remove or disable access to the stored content, as soon it is informed that the source of content has been removed from the network.

The ZEPT 2009 defines the **liability** of providers of the information society services (i.e. sole transmission providers, caching service providers, and hosting service providers) in line with the general principles set down by the e-commerce Directive 2000/31, but without a detailed elaboration. The grounds for requesting blocking or takedown of an online content are limited to detection and prevention of crime, protection of privacy, protection of classified information, and business secrets (Articles 9, 10 and 11). If the service providers originate in other member state of the European union (MS), the restriction measures can be taken only when necessary to achieve the objectives of ensuring public order, especially the prosecution of criminal offenses, the protection of minors, the prevention of hatred based on race, sex, religion or nationality, protection of human dignity or for the protection of public health, public security or consumer protection, including protection of investors, as long as these measures are proportionate to the objectives (Article 14). Generally, the Internet service providers are not considered liable for the third party content. They are not obliged to monitor or store the data other providers send or store via their services, nor expected to actively investigate the circumstances indicating the illegality of the information provided by the recipient of the service (Article 8). Unlike the e-commerce Directive 2000/31, according to which blocking or removal of illegal content may be ordered by a court or an administrative authority, in accordance with the Member States' legal systems (Articles 12, 13, 14, 19), the Slovenian transposition law envisaged this role solely for courts.

Until 2011 the Games of Chance Act (ZIS) however allowed the gambling supervision authority to take **administrative Internet blocking** measures, preventing the foreign gambling sites to be accessed from Slovenia. In 2006 the regulator responsible for games of chance, at that time still a

---

30 Zakaj so sploh hranili posnetke sej vlad?, 24ur.com, 09.12.11, available on http://www.24ur.com/novice/slovenija/objavili-tajne-seje-vlade.html?ts=1396782597&stream_cat=2 (07.05.15).

31 Vlada še ni ugotovila kdo je odtujil posnetke sej, Večer, 26.01.2012, available on http://www.vecer.com/clanek2012012605740029 (07-10.15).

32 in 2015 the law was further amended and it current version is ZEPT-B, however the amendments are not relevant for this report, since they did not change the regulation of blocking the Internet.

33 See the articles 9, 10 and 11 of the Act.

34 Ministrstvo za gospodarstvo Republike Slovenije. 2009. Zakon o spremembah in dopolnitvah zakona o Elektronskem poslovanju na trgu - redni postopek, 12. 03. 2009 (EVA: 2009-2111-0020) available at http://www.mgrt.gov.si/fileadmin/mgrt.gov.si/pageuploads/DEK/Novi_dokumenti_2009/Predlog_ZEPT-A_za_medresorsko_usklajevanje.pdf (07.09.15).

part of the Ministry of Finance,[35] issued 6 administrative orders to block access to foreign Internet gambling sites via the Slovenian Internet service providers and more than 230 administrative orders to block access to websites. Another series of blocking orders followed in 2010, just before the controversial Article 107 of the ZIS (Official Gazette of the RS, No 27/1995) was amended by the Article 107a of ZIS-D (Official Gazette of the RS, No 106/2010), which abolished the administrative measure and introduced the possibility of blocking the access to non-licensed online gaming sites only on the basis of court decisions upon the proposal of the supervisory authority.

However, as if craving for turning back time, the draft bill from 2013, suggesting another substantial revision of the ZIS act, envisaged a solution according to which the information society service providers should deny access to web sites from the list of illegal online gambling providers composed by the supervisory body.[36] The bill evoked a lot of debate and was criticized by the Information Commissioner of the Republic of Slovenia among others. In the opinion addressed to the Ministry of Finance, Commissioner Nataša Pirc Musar highlighted the importance of the open Internet and network neutrality and stressed that restricting access to websites for whatever reason is controversial in itself. The policy maker did not insist on the proposed solution. The recently published draft Law Amending the Games of Chance Act (ZIS-F, June 2015)[37] does not suggest any change regarding the legal definition of liability of Internet services providers and does not expand the space for administrative ordering of blocking or filtering of the Internet.

2.2. Take-down/removal of illegal Internet content

As explained to a greater detail in the previous chapter, the Internet mere conduit, host and caching service providers are obliged by the Articles 9, 10 and 11 of the ZEPT 2009 to react to the court order and terminate or prevent an infringement, despite the exclusion of their liability for the third-party services or content. The court may order them to remove illegal content or blocking access to it for the detection and prevention of crime, protection of privacy, protection of classified information and business secrets.

In Slovenia, most cases of withdrawal of illegal content from the Internet refer to **defamation** cases or breaches of **privacy** or **personal data protection**. The latter two are among the constitutionally[38] protected human rights and fundamental freedoms, alongside the freedom of expression, which they are often in conflict with. Both the personal data infringements and defamation can be dealt with

---

35 Currently the Financial Administration of the Republic of Slovenia (FURS) is responsible for this area.

35 The proposed changes are summarised in the press release of the bill proposer: Ministrstvo za finance predstavilo nov Zakon o igrah na srečo, of 24 September 2013, available at http://www.mf.gov.si/nc/si/medijsko_sredisce/novica/article//1767/ (03.09.15).

35 Zakon o spremembah in dopolnitvah zakona o igrah na srečo (ZIS-F), available at http://www.mf.gov.si/ fileadmin/mf.gov.si/pageuploads/Igre_na_sreco/Zakonodaja/ZIS-F_160615_objava. pdf (01.09.15).

35 Constitution of the Republic of Slovenia, Official Gazette RS, No. 33/91-I, 42/97, 66/2000, 24/03, 69/04, 68/06 and [35] Currently the Financial Administration of the Republic of Slovenia (FURS) is responsible for this area.

36 The proposed changes are summarised in the press release of the bill proposer: Ministrstvo za finance predstavilo nov Zakon o igrah na srečo, of 24 September 2013, available at http://www.mf.gov.si/nc/si/medijsko_sredisce/novica/article//1767/ (03.09.15).

37 Zakon o spremembah in dopolnitvah zakona o igrah na srečo (ZIS-F), available at http://www.mf.gov.si/fileadmin/mf.gov.si/pageuploads/Igre_na_sreco/Zakonodaja/ZIS-F_160615_ob-java.pdf (01.09.15).

38 Constitution of the Republic of Slovenia, Official Gazette RS, No. 33/91-I, 42/97, 66/2000, 24/03, 69/04, 68/06 and 47/13, available on http://www.us-rs.si/o-sodiscu/pravna-podlaga/ustava/ (14.09.15).

under the criminal law. The Slovenian Criminal Code retains four separate defamation-related offences.
The ZEPT 2009 addresses its provisions on takedown of illegal content specifically to the providers of the access to the Internet, mere conduit, hosting and caching services. However, the judgment II Cp 4539/2010 of 15 December 2010,[39] adopted by the High Court in Ljubljana, in which the Court ordered removal of the user generated defamatory content from one of the chat rooms, could be understood in a way that injunctions, including the temporary ones, are possible also for websites and their owners.[40]

In another judgment I Cp 3037/2011, adopted by the High Court in Ljubljana on 9 May 2012[41] concerning the blog severely damaging the reputation of a journalist, which was hosted by one of the services of the state owned telecommunication incumbent for at least a year and a half, the court confirmed the conclusions of the court of the first instance, according to which the service provider was not liable for the data stored at the request of the recipient of services who was not acting within its powers or under its control, but only if the provider was not aware of the unlawful activity or information, as well of facts or circumstances from which the criminal liability derived. Since the plaintiff informed the intermediary of breaches of her rights via the blog hosted by the intermediary, the Court concluded the intermediary was aware of them and thus became liable.

Since similar stances were taken in cases I Cp 252/2014, 19 March 2014, High Court in Ljubljana,[42] I Cp 11/2015, 18 February 2015, High Court in Maribor,[43] and Cp I 570/2015 of 17 June 2015, High Court in Ljubljana,[44] we can sum up that according to the case law the provider is obliged without delay, as soon as it becomes **aware of the unlawfulness**, to remove the information or disable the access to it.[45]

3. Procedural Aspects

As described and discussed in the previous sections **only judiciary bodies** can decide on blocking, filtering and take-down of illegal internet content.

---

39 Judgment II Cp 4539/2010, 15 December 2010, available on https://www.sodnapraksa.si/?q=4539/2010%20&database[SOVS]=SOVS&database[IESP]=IESP&database[UPRS]=UPRS&_submit=išči&rowsPerPage=20&page=0&id=2010040815252998 (14.09.15).

40 See R. Čeferin and Š. Mežnar, Online Hate-speech and Anonymous Internet Comments: How to Fight the Legal Battle in Slovenia?, 2014 24(3) *Annales* p. 477 et seq., 488.

41 Judgment I Cp 3037/2011, 9 May 2012, available on https://www.sodnapraksa.si/?q=%20I%20Cp%203037/2011&database[SOVS]=SOVS&database[IESP]=IESP&database[UPRS]=UPRS&_submit=išči&rowsPerPage=20&page=0&id=2012032113044794 (14.09.15).

42 Judgment I Cp 252/2014, 19 March 2014, available on https://www.sodnapraksa.si/?q=Cp%20252/2014&database[SOVS]=SOVS&database[IESP]=IESP&database[UPRS]=UPRS&_submit=išči&rowsPerPage=20&page=0&id=2012032113070688 (14.09.15).

43 Judgment I Cp 11/2015, 18 February 2015, available on https://www.sodnapraksa.si/?q=cp%2011/2015&database[SOVS]=SOVS&database[IESP]=IESP&database[UPRS]=UPRS&_submit=išči&rowsPerPage=20&page=0&id=2012032113077029 (14.09.15).

44 Judgment I Cp 570/2015, 17 June 2015, available on https://www.sodnapraksa.si/?q=Cp%20570/2015&database[SOVS]=SOVS&database[IESP]=IESP&database[UPRS]=UPRS&_submit=išči&rowsPerPage=20&page=0&id=2015081111383802 (14.09.15).

45 Further reflections on interpretation of the safe harbour concept and its limits by the Slovenian courts can be found in the section on Slovenia in the World Intermediary Liability Map (WILMap) (contribution by Damjan Bonač), available on https://cyberlaw.stanford.edu/our-work/projects/world-intermediary-liability-map-wilmap (15.09.15).

The law does not prescribe the procedural steps for **notifying** intermediaries on the allegedly illegal content on their services, but is rather specified in defining the legal basis for **injunctions**. The articles 9, 10, 11, 14, and 18 of the ZEPT 2009 limit the possibility to issue an injunction explicitly to courts. The decision on the way of its implementation is however left to the ISP concerned.

The Article 18 of the ZEPT 2009 together with the Article 134 of the OZ 2007 offers the possibility to ask for a **temporary injunction** to anybody believing that the service provider violates his or her rights. The provision makes possible rather quick interventions regarding the potentially illegal content on the Internet. It is backed by the Article 134 of the OZ 2007, according to which everyone has the right to request the court or other competent authority to order the cessation of acts which infringe the inviolability of the human personality, personal and family life or other personal rights to prevent such conduct or to remedy its consequences.

There are **no references to freedom of expression** in the ZEPT 2009 and neither is **proportionality** of the blocking measure addressed in detail. There is only a general provision requiring that the restriction is proportionate to the objective pursued (Article 14/1 of ZEPT 2009). Furthermore the Games of Chance Act stipulates that a restriction of access to web pages can be made only to the extent strictly necessary for the execution of a decision, which prohibits organization of games of chance, and in the least burdensome way for the provider of information society services (Art. 107a/Paragraph 4 of ZIS-UPB3 and ZIS-E, 2012). There is also a reference to a **legal remedy**, saying that the information society service provider can complain against such a decision within 3 days, and that the Supreme Court of the Republic of Slovenia shall decide no later than in 15 days after the receipt of the complaint (Art. 107a/Paragraph 5 of ZIS-UPB3 and ZIS-E, 2012).

The **proceedings for temporary injunctions** follow the principles set by the Act governing the enforcement and insurance (ZIZ, last amended in 2015).[46] The court may, by an interim injunction prohibit the imminent infringements or infringements already commenced, as well as restrict the provision of information society services so as to impose a service provider to remove or disable access to the data it holds. The court may issue a temporary injunction even without the hearing of the opposing party, if the applicant proves that any delay would prevent the achievement of the purpose of injunction or make it difficult to remedy damage to the applicant. The Court is expected to immediately inform the other party of the interim measures issued, no later than at the execution of the injunction. At the same time the court has to determine the deadline by which the applicant can file a lawsuit (not longer than 30 days). The defendant, on the other hand, can use all the usual **remedies** available in the court proceedings.

The EU initiated and co-financed project Safe.si,[47] which operates the Slovenian hotline for reporting the illegal Internet content *Spletno oko,* promotes the **notice and takedown** approach. The hotline works in cooperation with the Slovenian Police and the Supreme Court, and is a member of the INHOPE network of 51 hotlines in 45 countries (as of 15 September 2015) for reporting illegal online content.[48]

---

46 Enforcement and Insurance Act (ZIZ, Official Gazette RS, No. 3/07 – official consolidated text, 93/07, 37/08 – ZST-1, 45/08 – ZArbit, 28/09, 51/10, 26/11, 17/13 – odl. US, 45/14 – odl. US, 53/14 in 58/14 – odl. US, No. 54/2015).

47 The project Safer Internet Centre Slovenia (safe.si) promotes a better Internet for kids. In Slovenia it is co-funded by the Ministry of Education, Science and Sport and run by a consortium of partners coordinated by the Faculty of Social Sciences at the University of Ljubljana. The other 3 partners are: the Academic and Research Network of Slovenia, the Slovenian Association of friends of youth and the Youth Information and Counselling Center of Slovenia. The Safer Internet Centre Slovenia carries out activities within three different, but connected components: the Awareness Centre Safe.si; the Helpline Tom telefon; and the Hotline Spletno oko.

48 More information on the INHOPE network can be found on www.inhope.org (15.09.15).

The *Spletno oko's* **reviewers, trained by the Police and the Prosecutor's Office** and in specialized training courses abroad, are carrying out the evaluation of reports. The *Spletno oko* declares to the Police each content for which it estimates that it could contain elements of a criminal offense under the Article 297 of the KZ-1 2012, i.e. public incitement to hatred, violence or intolerance, or the Article 176 of the KZ-1 2012, i.e. presentation, manufacture, possession and distribution of pornographic material. When a potential example of sexual abuse of children is identified on a Slovenian server, usually the Police inform the hosting provider and ask him to remove the content.

The *Spletno oko* does not act on its own. It approaches the relevant provider only if the Police confirm the identified unlawfulness of the reported content. The hosting company then autonomously decides on how to react. Each report to the provider of the service is solely informative and the notification is issued only once. There is no special guidance on how this should be done and neither are there any explicit recommendations on how the freedom of expression should be safeguarded. The intermediaries are free to decide whether to follow the invitation or not, as only the Court has the power to impose the duty to block or remove the illegal content.

In 2014 *Spletno oko* identified 2 cases of alleged sex abuse of children on the **Slovenian servers**. One of them was removed, while the other one was found not to be illegal.[49] If the suspected illegal content is **hosted outside Slovenia,** the *Spletno oko* notifies both the Slovenian police and the INHOPE network, to make sure the relevant partner body in the country, where the server is located, handles the report. According to the *Spletno oko's* statistics, the majority of the potentially illegal content of child sexual abuse identified in Slovenia originated from servers in the United States (42) and the Netherlands (27), followed by those located in Japan (8), Sweden (6), Russia (4) and Latvia (3).[50]

In the context of this assessment the *Spletno oko* hotline's activity is of particular importance, since it reduces the possibility of the Internet and information society services providers to rely to the so-called **safe harbour** provisions, guaranteeing the provider some protection against the liability for the third party content, when providing the mere conduit, caching and hosting services. Namely, as we discuss it elsewhere, when a provider acquires information on illegal content on its services or facilities and does not remove it or block it, it becomes inevitably liable for it, even if it does not own it.

4. General Monitoring of Internet

In Slovenia no official institution is in charge of overall monitoring of the Internet content and neither are the providers of the Internet services expected to check the data of other providers that are being distributed via their services. The Article 8 (3) of the ZEPT 2009 explicitly **excludes the general monitoring** obligation. As stipulated in the Article 8 (2) of the same act, the intermediaries are liable exclusively for the data provided by themselves alone, according to the general rules of obligations and criminal law, and are not obliged to monitor or store the data or to actively investigate the circumstances indicating the illegality of the information provided by other sources.

The most consistent monitoring of the Internet content with regard to hate speech or sexual abuse

---

49 Spletno oko, Annual report/Letno poročilo 2014, dosegljivo na http://safe.si/sites/safe.si/files/files/Spletno%20oko%20-%20Letno%20poročilo%202014.pdf (13.09.15).

50 Final Report of the Programme Safer Internet in Slovenia / Program Varnejši internet v Sloveniji, Javno končno poročilo: Marec 2012 — December 2014, available on http://www.fdv.uni-lj.si/docs/default-source/cdi-doc/koncno-porocilo-2012-2014.pdf?sfvrsn=0 (03.09.2015).

of children is being carried out by the ***Spletno oko* hotline**. Since its launch in 2007, the number of cases reported to *Spletno oko* has nearly quintupled. From 2012 to 2014 it received almost 11 thousand reports of illegal content on the Internet. The majority of them were submitted via the online reporting platform http://safe.si/spletno-oko or via reporting forms on news web portals. More than 80 percent reports informed about cases with elements of hate speech and the remaining nearly 20 percent reported of alleged child sexual abuse images. When checked by the trained reviewers, the vast majority of reports on hate speech did not meet the legal criteria for illegal hate speech, which are rather narrow in Slovenia, while about one fifth of reported cases of child abuse images appeared to be justified. In total, 417 cases contained signs of illegal acts and were forwarded to the Police for further investigation in the reporting period from 2012 and 2014. [51]
In **the Slovenian Police** a special branch, called the Centre for Computer Investigating, is in charge of investigating crimes committed through the Internet. They actively look for indices of crime and react upon requests or reports. The Centre covers three main areas of work:

a) Investigation of computer crime (e.g. abuse of personal data, violation of copyright rights, attacks on information system, production and acquisition of devices intended for offenses);
b) Investigation of seized e-devices or e-data (i.e. computer forensics);
c) Technical assistance to other areas of crime investigation (e.g. child abuse online, online fraud, racial hatred on the Internet, tax evasion, corruption, abuse of e-banking).

An interesting case regarding the monitoring of the Internet by the Police came to public in 2012. The National Supervisor for Protection of Personal Data at the office of the Information Commissioner revealed that for years no Police request, addressed at the players running the websites or providing the Internet related services, was backed by the relevant provision of the Electronic Commerce Act. Instead, the Police quoted **inadequate provisions** of the Criminal Procedure Act, the Police Act, the Law on Protection of Personal Data, and in some cases did not refer to any legal basis at all.[52]

The National Supervisor for Protection of Personal Data concluded that the Police was either not familiar with the governing law or deliberately ignored the provisions of the ZEPT. The Supervisor also estimated that the Police was not aware of the differences between operators of electronic communications, i.e. providers of publicly available electronic communications networks and services), which are primarily regulated by Electronic Communications Act (ZEKom-1), and information society service providers, which are regulated by ZEPT. Similarly, the latter were not familiar with the legislation either, as they in most cases provided the requested information to the Police without the court order.[53]

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

After a series of attempts of blocking the Internet in the 2000s, described above, mostly motivated by financial interests pursued by the state in gaming industry, and in one case required for protection of personal data of a larger group of people, in which different regulatory authorities tested the then available administrative measures without desired effects, the room for Internet blocking, especially for a non-targeted one, was narrowed down. The last allowed form of **administrative orders** of blocking or removal of the online content was **abandoned in 2011**, and the Slovenian legislature so

---

51 Final Report of the Programme Safer Internet in Slovenia / Program Varnejši internet v Sloveniji, Javno končno poročilo: Marec 2012 — December 2014, available on http://www.fdv.uni-lj.si/docs/default-source/cdi-doc/koncno-porocilo-2012-2014.pdf?sfvrsn=0 (03.09.2015).

52 A. Tomšič, Poročilo o uporabi pooblastil za posredovanje osebnih podatkov uporabnikov spletnih strani z vsebino, ki jo posredujejo prejemniki storitve, 2.12.13, available on https://slo-tech.com/clanki/14001/ (03.09.15).

53 Ibidem.

far resisted to occasional attempts by the policy makers to re-open the space to other measures than those based on a court decision. Correspondingly, the awareness of the public seem to be substantial, since any suggested change evokes media attention and anything that is recognised as a measure interfering with the principles of the internet openness and freedom of expression is criticised.

The **case law of the European Court of Human Rights** is often referred to in advocating the proposals related to legal changes. In the already mentioned case from 2013, when the government presented the bill on amendments to the law regulating games of chance, according to which blocking of the access to illegal gambling sites would be imposed via a list composed by a supervisory authority, the critics drew the attention to the judgment of the European Court of Justice in Case C-70/10 Scarlet Extended SA v Société Belge des Auteurs, compositeurs et éditeurs SCRL (SABAM),[54] underlining that the Union law precludes injunctions against ISPs requiring from them to install systems for filtering electronic communications passing via their services as a preventive measure.

In the more recent case of the draft law amending the Media Act 2006[55] the Ministry of Culture suggested extending the liability of the websites by referring to the Delfi AS vs. Estonia case(app. No. 64569/09), even before the European Court of Human Rights issued its judgment on 16 June 2015.[56] The draft law, presented in May 2015, proposed a provision, aimed at prevention of hate speech in commentaries in online news portals. The suggested provision stipulated that the editor-in-chief should be held **liable for user-generated content**, including comments and audiovisual material, and shall delete all the items not in line with the rules in the shortest time possible. The envisaged fine for editor-in-chief failing to meet the obligation spanned from 500 to 5000 euros. The media reacted unanimously and the Information Commissioner joined them in saying that such a regime could seriously impede constitutionally protected freedom of expression, as well as lead to the general monitoring obligation, which is not supported by the EU law (Article 15 of e-Commerce Directive 2000/31, transposed by the Article 8 of ZEPT 2009). The proposer accepted the arguments and provided a reformulated, watered down solution in the second, modified version of the draft law, without mentioning explicitly the liability of editors-in-chief.[57]

The legal provisions governing the Internet blocking, filtering and removal of illegal content are spread across different legal acts and the main law referring to liability of the intermediaries is not more specific or precise than the corresponding EU directive. Case law is also relatively scarce. Its scope is limited to blocking of foreign/unlicensed gambling websites and to takedown of online content infringing personal rights (protection of privacy and personal data, as well as defamation). The examined acts, the case law and the practice of intermediaries and the responsible institutions nevertheless allow for the conclusion that the laws referring to blocking and takedown of the Internet content provide a **solid, although not very precise basis** to maintain the openness of Internet and prevent the threats to the freedom of expression.

---

54 The European Court of Justice Judgement in Case C-70/10 is available at http://curia.europa.eu/juris/document/document.jsf?docid=115202&doclang=en (08.09.2015).

55 Zakon o medijih, uradno prečiščeno besedilo (ZMed-UPB1, Official Gazette RS, No. 110/2006), available at https://www.uradni-list.si/1/content?id=76040 (15.09.2015).

56 The European Court of Justice Judgment in Case Delfi AS vs. Estonia case (app. No. 64569/09) is available at http://hudoc.echr.coe.int/eng#{%22appno%22:[%2264569/09%22],%22itemid%22:[%22001-155105%22]} (15.09.2015).

57 Predlog Zakona o spremembah in dopolnitvah Zakona o medijih (EVA 2013-3340-0029), available on http://www.mk.gov.si/fileadmin/mk.gov.si/pageuploads/Ministrstvo/Zakonodaja/Predpisi_v_pripravi/2015/ZMed-koncna.pdf (15.09.15).

The main safeguard to prevent the abuse of power and guarantee targeted decisions, instead of wholesale preventive blocking, is the regime in which **only courts can impose the injunctions**, guaranteeing the affected parties legal remedies. The **liability** of intermediaries is determined via tortious liability, defined by the Code of Obligations, as there are no precise enough provisions in the Electronic Commerce on the Market Act to form a special liability basis for intermediaries.

The **strengths** of this scheme are (a) its targetedness, as it is being carried out on a case by case basis; (b) its proportionality, since it makes possible to face and balance competing interests and fundamental rights and to determine the necessity of measures with lesser discretion and with respect to collateral effects; and (c) broad possibility for judicial review to correct the possible mistakes of lower courts. The main **weakness** with reference to the ECRH case law, on the other hand, is (d) its limited foreseeability, as it can take a lot of time and uncertainty until the final decision, and if the intermediary did not do anything to prevent the alleged illegal activity, it could be – according to the Slovenian case law – automatically attributed liability and its inaction interpreted as a dereliction of a duty of care.

The **self-regulatory framework** has been established among the main communication services providers and the main news portals, as described in detail in Chapter 2. However, the respective codes of conduct[58] do not go further than the existing legislation. They do not envisage any enforcement mechanisms and neither they contain explicit references to the need of proportionality and safeguarding freedom of expression. The same is true for another non-institutional mechanism, the *Spletno oko* hotline, which is a tool for reporting of alleged illegal content with its own system of reviewing of validity of complaints in cooperation with the Police.

Both the providers of public electronic communication services and the news portals providers only scantily referred to the illegal content in their Codes.[59] The electronic communication services providers defined it as the content contrary to the national and EU law and declared their readiness to cooperate with the national authorities and non-governmental institutions in the implementation of their obligations under the existing Slovenian legislation in the fight against it. As for the third-party content, the operators stressed that they assumed only the indirect responsibility for the content and committed themselves to inform the content providers with whom they had contractual relationships about the Code, and to invite them to adhere to it.

We could conclude that the self-regulating framework in its present form hardly interferes with the freedom of expression. Rather than an independent bottom-up system of private actors, it is more a commitment of operators to proceed according to the law and to cooperate with each other and with responsible institutions in the matters related to the illegal content on the Internet.

The risks arise mostly from the **expertise and professionalism** of the reviewers. The cases of misapplication of laws by the Police and information society service providers, but also other intermediaries, such as news portals and content aggregators, indicate their limited knowledge and competences. The indication that practices of tackling the potentially illegal content, that were commonly used over a relatively long time, were not always transparent and legally founded, signifies a risk to the fundamental rights and freedoms and could lead to over-blocking.

---

58 The Code of Conduct of the ISPs is available in Slovenian only on http://www.ris.org/uploadi/editor/1360137260Kodeks_ravnanja_za_zascito_uporabnikov_2013.pdf, and the Code of Conduct of the News Portals – in Slovenian – can be found at http://safe.si/sites/safe.si/files/kodeks_oblikovan.pdf (07.10.15).

59 Ibidem.

In the context of discussing the potential restrictions to the openness of the Internet and risks for the freedom of expression it is worth mentioning that Slovenia is one of a few countries **mandating net neutrality by law**. In the EU only the Netherlands and Slovenia have implemented so strict rules and tested them in practice. The Slovenian regulator for electronic communications, AKOS, imposed measures to protect net neutrality to a few operators with different models of vertical integration in 2014 and 2015. The actions were directed against price discrimination (zero rating) in relation to music services and cloud storage services, but represented a resounding effort of the regulator, given that in the time of adoption of the first decisions there was no case law from this area available in the EU.

In a nutshell, the evolution of the Slovenian regulation of the field has been quite dynamic and characterised by occasional slips towards restrictiveness, but the current legal framework and case law indicates certain sensitivity for safeguarding the openness of the Internet, which is one of the prerequisites of the freedom of expression. On the other hand, the practices of determining the liability of intermediaries require further attention, as there seem to be some room for risks to freedom of expression to arise. In the lack of clarity, the intermediaries could be more prone to preventive restrictive measures and over-blocking. The same is true for the legislation criminalizing defamation via offences punishable by not less then six months in prison, and therefore representing a potentially fertile ground for (self) censorship.

Tanja Kerševan Smokvina
7 October 2015