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 610-625

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.

SLOVAK REPUBLIC

1. Legal Sources

The legal system of the Slovak Republic is strongly shaped by the Constitutional Court (the Court), which has a power to decide on the conformity of acts of authorities and of the laws with the constitutional legal order. Effectively, if the Court has a chance to hear a case, it usually has a "last word" on the human rights standards. The Constitution[1] thus plays a decisive role as a source of law in general.

Apart from the Constitution itself, the ECHR and the Charter of Fundamental Rights (the Charter) of the EU also co-define the system of the constitutional guarantees of freedom of expression. The Convention, as a binding international treaty on human rights, is an integral part of the Slovak legal system and has precedence over the laws, but not the Constitution. The Constitutional Court regularly interprets provisions of the Constitution, including those on freedom of expression, in light of the Convention and the case-law of the ECtHR.

The situations in which *blocking, filtering and take-down* occur are of three kinds: (1) exercise of powers of the public authorities (2) use of entitlements of the private parties and (3) voluntary actions of private parties. Each one of them is governed by slightly different legal rules and might be also subject to different legal doctrines. The area of *blocking and filtering* is generally not explicitly regulated. There are, however, less explicit legal rules at place that could also give rise to such measures. The *take-down of illegal content* is regulated in several different acts as a form of cessation of the illegal conduct, although predominantly the provisions are not specifically targeted at the Internet situations. In all the cases, the legislation is thus fragmented. One notable exception in this regard is the E-Commerce Act,[2] which is the local transposition of the EU's E-Commerce Directive[3] and incorporates horizontal set of defences against potential legal obligations in the entire legal order.

The Slovak Republic is a signatory of the Convention on Cybercrime,[4] but not of its Additional Protocol. The Convention was mainly transposed into the Penal Code[5] and the Penal Procedure Code.[6] The Slovak Republic is also a signatory of the Convention on prevention of terrorism,[7] which was transposed into the Penal Code and the Penal Procedure Code, and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, which was transposed into the Data Protection Act.[8] The Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse was ratified on 1st of March 2016 and comes into force on 1st of July 2016.

1 Act No. 460/1992 Coll. Constitution of the Slovak Republic.

2 Act No. 22/2004 Coll. on electronic commerce.

3 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.

4 Announcement No. 137/2008 of the Ministry of Foreign Affairs of the Slovak Republic about singing of the Convention on Cybercrime.

5 Act No. 300/2005 Coll. Penal Code.

6 Act No. 301/2005 Coll. Penal Procedure Code.

7 Announcement No. 186/2007 of the Ministry of Foreign Affairs of the Slovak Republic about signing of the Convention on prevention of terrorism.

8 Act No. 122/2013 Coll. on protection of personal data.

(1) Various public authorities could theoretically request some form of *blocking, filtering or take-down* measures based on following provisions: Section 3(1) and Section 90 of the Penal Procedure Code, Section 8(1)(d) of the State Control Act,[9] Section 65(1) of the Data Protection Act, Section 15 of the Slovak Intelligence Service Act,[10] Section 15 of the Army Intelligence Service Act[11] and Section 70 of the Confidential Information Act.[12] None of the provisions is, however, specifically worded to achieve this and most of the time very broad reading of the relevant Sections would be required. This reading might be sometimes at odds with the constitutional requirement of the quality of law (see Part 5).

(2) Private individuals could request *blocking, filtering and take-down* orders based on Section 13 of the Civil Code,[13] Section 58(1)(b)(c) of the Copyright Act,[14] Section 16(2)(a)(b) of the Plant Variety Act,[15] Section 8(4) of the Trade Mark Act,[16] Section 32(1) the Patent Act,[17] Section 27(1) of the Design Act,[18] Section 28(2) of the Utility Model Act,[19] Section 9(1) of the Geographical Indications Act[20] and Section 19(1) of the Chip Act.[21] From the provisions listed, only the Copyright Act and the Plant Varieties Act foresee broadly the specific legal action against intermediaries who carry third party rights infringements, irrespective of their innocent role. Other statutes in the field of intellectual property, however, also have to be interpreted in light of the European Union law, specifically Art. 11 third sentence of the Enforcement Directive[22]which requires the availability of this course of action also against innocent intermediaries.[23] Moreover, Section 76(2) of the Civil Procedure Code[24] allows for preliminary injunctions to be imposed on non-defendants such as the Internet access providers.

Apart from the above legal sources, *take-down* of the content can be required as a consequence of potential liability of an intermediary for its own or for third party content. Such liability is spread around the legal landscape and is not concentrated in one single law. The Civil Code in its Section 415 sets the general duty of care.[25] This provision extends protective duties over certain legally protected interests, such as health and property, beyond typical acts of infringements. What is, however, concentrated, are the liability exclusions set by the Union law (so called “safe-harbours”). The E-Commerce Directive’s transposition in Section 6 of the E-Commerce Act limits the reach of tortious

---

9 Act No. 128/2002 Coll. on state control of the internal market in the matters of the consumer protection.

10 Act No. 46/1993 Coll. on Slovak Intelligence Service.

11 Act No. 198/1994 Coll. on Army Intelligence Service.

12 Act No. 215/2004 Coll. on protection of confidential information.

13 Act No. 40/1964 Coll. Civil Code.

14 Act No. 185/2015 Coll. Copyright Act.

15 Act No. 202/2009 Coll. on Legal Protection of Plant Varieties.

16 Act No. 506/2009 Coll. on Trademarks.

17 Act No. 435/2001 Coll. Patent Act.

18 Act No. 444/2002 Coll. on Designs.

19 Act No. 517/2007 Coll. on Utility Models.

20 Act No. 469/2003 Coll. on Geographical Indication and Indications.

21 Act No. 146/2000 Coll. on Protection of Topographies of Semiconductor Goods.

22 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce').

23 M. Husovec, Zodpovednosť na internete: podľa českého a slovenského práva, CZNIC, 2014; M. Husovec, Injunctions Against Innocent Third Parties: The Case of Website Blocking, 2013 (4) *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* p. 116-129.

24 Act No. 99/1963 Coll.

25 Section 415 of the Civil Code reads: “Everyone must act so as to avoid damages to health, property, nature and environment”.

duty of care, but also obligations under the administrative or potentially criminal law, in case intermediaries carry out certain type of activity (hosting, caching and mere conduit) and as long as they comply with the conditions of the safe harbours.
(3) For the voluntary measures, there is no specific regulation at place. The voluntary enforcement agreements or activities can be, however, potentially subject to consumer laws, competition laws as well as constitutional safe-guards. If the voluntary measures are introduced based on cooperation solely between private parties (horizontal relationships), the Constitution could still impose certain positive obligations on the state to indirectly intervene in these arrangements.

2. Legal Framework

The Slovak Republic belongs predominantly to the "B" Category of the countries. In the field of take-down, no specific legal instruments were created to achieve the take-down of the Internet content. The authorities and private plaintiffs can invoke ordinary competences/entitlement seeking cessation of wrongful conduct. Some specific rules of horizontal nature are included in the E-Commerce Act, which is a direct transposition of the E-Commerce Directive and limits the other parts of the legal order with its liability exclusions.

In the field of website blocking, the same applies,[26] although with two notable exceptions. The first exception concerns enforcement of intellectual property rights. The legal framework, which is based on the European Union law, foresees an entitlement of private plaintiffs to demand that various types of injunctions, including website blocking and filtering, are imposed on the intermediaries by the courts

2.1. Blocking and/or filtering of illegal Internet content

The lack of more explicit legal basis that would include detailed provisions is correlated with the number of official take-down requests made by the Slovak public institutions. According to Google transparency reports, in the period of 2009-2014, only *two* requests were filed by the Slovak authorities.[27] Similarly, when the author of this report enquired in course of the research among the public institutions, such as Slovak Commercial Inspection (that has one of more explicit legal competences for such requests), he was informed that not a single request was made by them until now and thus the legal basis was actually never used in practice.[28]

Until today, according to our information, the two biggest access providers in the country did not encounter a single court/authority request for blocking/filtering of a website.[29] The law enforcement seems to be usually directed rather immediately against persons residing in the Slovak Republic or their assets, such as webservers, than against anonymous websites.[30] For instance, in a criminal case involving hacking to the system of the National Security Agency (Národný bezpečnostný úrad SR), the

---

26 In the past, there were failed attempts by the legislator to enact specific blocking regulation in respect to unauthorized gambling sites that would give specific authority to block website to the tax offices. *See* http://www.eisionline.org/index.php/sk/10-projekty/novinky-z-aktivit/5-hazardny-navrh-zakona.

27 *See* http://www.google.com/transparencyreport/removals/government/SK/?hl=en.

28 Email from Petra Blehová from the Slovak Commercial Inspection (9th September 2015).

29 In 2009, the operators said this for the article J. ANDACKÝ, Ako cenzúrou neuškodiť internetu (eTrend), available at http://www.etrend.sk/ekonomika/zavory-na-webe-2.html (17.9.2015); when the author of this report enquired in September 2015, he received the same answer from one of the operators.

30 J. ANDACKÝ, Ako cenzúrou neuškodiť internetu (eTrend), available at http://www.etrend.sk/ekonomika/zavory-na-webe-2.html (17.9.2015).

rented servers of a webhosting company were seized.[31] Informal talks with the police corps has revealed that most of the blocking cases are usually only channeled further via local branch of EUROPOL or INTERPOL[32].

Apart from the absent legal basis, one of the reasons why public institutions do not engage in significant policing of the Internet could be also attributed to existence of *voluntary initiatives* of some of the Internet access providers. In 2009, it was reported that at least two of the biggest national access providers, T-Mobile and Orange, started to subscribe to the databases of the Internet Watch Foundation.[33] Both operators said that they use only the IWF black-lists related to child pornography.[34] Some of these efforts were triggered by the European Framework for the Safer Use of Mobile Phones by Younger Teenagers and Children.[35] The Slovak INHOPE contact point, "Stopline.sk", moreover lists[36] also other providers such as O2 and Slovanet as partners of the filtering/blocking efforts. In addition to this effort, beginning in January 2017, the Slovak domain name authority will implement an alternative dispute resolution system for trademark online disputes concerning the domain names[37].

The following provisions of laws can be interpreted in a way which gives rise to *website blocking* and *filtering* in the Slovak Republic:

1. *Section 3(1) of the Penal Procedure Code*

   ("(..) [O]ther legal persons and natural persons are obliged to cooperate with law enforcement authorities and the court in fulfilment of their duties, which are related to the criminal proceedings.")

   This provision is included in the general section of the Penal Procedural Code. This means that there is no limitation as to the type of offences to which it would apply to. Therefore, offences covered by the provisions include a crime of distribution of child pornography (Section 369 of the Penal Code), defamation (Section 373), unjustified interference with personal data (Section 374), endangerment of confidential information (Sections 319, 320), treason (Section 311), distribution of extremist materials (Section 422b), denial of holocaust (Section 422d) or instigation of racial hatred (Section 424).

2. *Section 90 of the Penal Procedure Code*

("(1) If the clarification of facts relevant for criminal proceedings requires to safeguard stored

---

31 The servers were then returned after two years – *see* EDITORIAL, Disky zadržané políciou po 2 rokoch vrátené (Websupport), available at <http://www.websupport.sk/blog/2009/06/disky-zadrzane-policiou-po-2-rokoch-vratene/> (17.9.2015).

32 *See* <http://www.interpol.int/Crime-areas/Crimes-against-children/Access-blocking>

33 The Internet Watch Foundation (IWF) is a registered charity based in Cambridgeshire, England. The IWF was established in 1996 by the internet industry to provide the UK internet Hotline for the public and IT professionals to report criminal online content in a secure and confidential way. In the meantime, some parts of its black-list database are used also in other countries, including Slovak Republic.

34 P. HORNÍK, Ako funguje blokovanie stránok u T-Mobile, je jednoducho obíditeľné (Dsl), available at http://www.dsl.sk/article.php?article=8368 (17.9.2015); P. HORNÍK, Ako funguje blokovanie stránok u Orange, je jednoducho obíditeľné (Dsl), available at http://www.dsl.sk/article.php?article=8187 (17.9.2015).

35 *See* <http://www.gsma.com/publicpolicy/wp-content/uploads/2012/03/Safer_Mobile_Flyer.pdf>

36 *See* <http://www.stopline.sk/sk/partneri>

37 *See* < https://www.sk-nic.sk/documents/pdf/Pravidla_2017_priloha1_Alternativne_riesenie_sporov.pdf >

computer data, including operational data saved through the computer system, the presiding judge of a panel or a prosecutor prior to the commencement of criminal prosecution or in pre-trial proceedings, respectively, may issue an order based on circumstantial reasons to the person who has possession of or control over such data, or to the provider of such services, requesting them to

a) safeguard and maintain integrity of such data,

b) enable making and keeping copies of such data,

c) prevent access to such data,

d) remove such data from the computer system,

e) surrender such data for the purposes of criminal proceedings.")

3. *Section 8(1)(d) of the State Control Act*

   ("With its decision, the authority[38] may (…) *prohibit provision of an information society service* if it demonstrably endangers life or health of people, property or environment")

4. *Section 65(1) of the Data Protection Act*

   ("If the Office[39] determines violation of rights of the claimant, the natural person in the proceedings without proposal or neglect of the duties stipulated by the Law in the course of personal data processing, *it shall impose by decision on the controller or the processor to take measures in order to remove determined deficiencies and their causes in a determined period*; otherwise shall terminate personal data proceedings.")

   By virtue of this provision, the Slovak Data Protection Office is allowed to require third parties cessation of their conduct that is contrary to the legal framework on data protection under a treat of imposing a penalty. Therefore, for instance when third parties publish personal data on their websites without consent of the data subject, they can be requested to take-down the particular information.

5. *Section 15 of the Slovak Intelligence Service Act*

   ("The Slovak Intelligence Service may, within its authority, *request help*, documents and information, which can contribute to clarification of facts relevant for fulfilment of its duties under the Act, from the state bodies, legal persons and natural persons. (..) Nobody may be forced to provide the help, documents and information.")

6. *Section 15 of the Army Intelligence Service Act*

   ("The Army Intelligence Service may, within its authority, *request help*, documents and information, which can contribute to clarification of facts relevant for fulfilment of its duties under the Act, from the state bodies, legal persons and natural persons. (..) Nobody may be forced to provide the help, documents and information.")

7. *Section 70 of the Confidential Information Act*

   ("The Office, in fulfilment of its duties under paragraph 1(e) may *request help*, documents and information, which can contribute to prevention and removal of security threats, from the state bodies, legal persons and natural persons. (..) Nobody may be forced to provide the help, documents and information.")

   The set of the last three identical provisions is also capable of giving effect to take-down or

---

38 The Slovak Commercial Inspection.

39 The Slovak Data Protection Authority.

blocking requests. This requires, however, that a possibility to "request help" is read as a separate competence along two other possibilities, namely to request "documents" and "information, which can contribute to prevention and removal" of certain results. Take-down of the content, filtering and blocking measures could then qualify as a form of "help" from private parties.

8. *Section 13 of the Civil Code*
   ("The individual shall be entitled in particular to demand that unlawful violation of his or her personhood be abandoned, that consequences of this violation be removed and that an adequate satisfaction be given to him or her.")

9. *Section 56(1)(b)(c) of the Copyright Act*
   ("The author the rights of who were infringed upon unlawfully or the rights of who are in jeopardy to be infringed unlawfully, may especially request (..) b) prohibiting jeopardising of his rights including the prohibiting to repeat such jeopardising, namely *including against a person who indirectly participated in jeopardising these rights*; c) prohibiting unlawful infringement of his rights, namely *including against a person who indirectly participated in jeopardising of these rights* including prohibition pursuant to S. 59 and 60;")

10. *Section 16(2)(a)(b) of the Plant Variety Act*
    (*Ibid* as the Copyright Act)

11. *Section 8(4) of the Trade Mark Act*
    ("If an rights conferred by the trade mark were infringed, the proprietor of the trade mark shall have the right to apply for prohibition of an infringement or jeopardising of his rights and to remedy the consequences of such action")

12. *Section 32(1) the Patent Act*
    (*Ibid* as the Trade Mark Act)

13. *Section 27(1) of the Design Act*
    (*Ibid* as the Trade Mark Act)

14. *Section 28(2) of the Utility Model Act*
    (*Ibid* as the Trade Mark Act)

15. *Section 9(1) of the Geographical Indications Act*
    (*Ibid* as the Trade Mark Act)

16. *Section 19(1) of the Semiconductor Protection Act*
    (*Ibid* as the Trade Mark Act)

    The abovementioned provisions of the intellectual property acts are an implementation of Article 11 third sentence of the Enforcement Directive and Article 8(3) of the InfoSoc Directive[40]. Both provisions were interpreted by the Court of Justice of the European Union as permitting certain types of website-blocking and filtering injunctions[41].

17. *Section 76(2) of the Civil Procedure Code*

---

[40] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society

[41] *See* Case C-314/12 (2014) *UPC Telekabel Wien* ECLI:EU:C:2014:192; [41] Case C-324/09 *L'Oréal and Others* [2011] ECLI:EU:C:2011:474; Case C-70/10 *Scarlet Extended* [2011] ECLI:EU:C:2011:771

("The preliminary measures can impose obligations on persons other than parties to the proceedings only if this can be required of them under principles of justice.")

As can be seen, the legal basis can be divided into two types: (a) explicit and (b) non-explicit. Only Section 90 of the Penal Procedure Code and Section 8(1)(d) of the State Control Act as well as the Copyright Act and the Plant Variety Act could be said to belong to the group of explicit legal basis.

The legal framework for website blocking and filtering in *intellectual property law* has not yet been tested before the national courts. The only available case-law in this respect originates from the Court of Justice of the European Union[42] or other Member States. The fact that even private parties do not consider website blocking in their litigation strategies is well-illustrated by the following high-profile lawsuit. In December 2011, a secret wiretap file revealing dealings of a local financial group with the political elite was leaked on the Internet.[43] When one of the main figures of the scandal, a financial tycoon, attempted to achieve the take-down of the wiretap file from the numerous foreign websites on the ground of his personality rights (Section 13 of the Civil Code), his lawyers sued[44] Google, Facebook and Wikidot, the platforms hosting the content, instead of attempting to sue local players, such as the Internet access providers, first.[45] This shows that a website blocking is not yet fully understood as an available remedy, despite the fact that the law could be arguably interpreted to support it.

As a temporary measure, website-blocking and filtering can be obtained based on Section 76(2) of the Civil Procedure Code. In the past, such injunctions were for instance used in the domain name disputes to oblige the domain name authority to prevent assignment of the disputed domain before the infringement proceedings is ended.[46] No cases are known where this legal basis would be invoked in order to achieve filtering or blocking of the content.

The orders based on the Section 90 of the Penal Procedure Code are subject to several *procedural safeguards* (see Part 3 of this report). Although they are primarily meant to prevent abuse of computer data seizures, the safeguards can be equally effective in the cases involving blocking of the access to data. According to the Penal Procedure Code, the orders may be served on the person who has possession of or control over such data, or on the provider of such services, who may be also imposed the duty to treat the measures set out in the order as confidential. Owing to under-regulation of the area, no specific safeguards are envisaged for other generally-worded provisions.

In the field of intellectual property, some of the safeguards were introduced by the Court of Justice of the European Union in its *UPC Telekabel* ruling.[47] The Court held that the *open-ended* website-blocking injunctions[48] must be (i) strictly targeted; (ii) must at least partially prevent and seriously discourage the access to a targeted website; (iii) must not lead to unbearable sacrifices for an access provider; (iv) must give a court in enforcement proceedings a possibility to assess their reasonableness; (v) must provide for a possibility for users to challenge the scope of the blocks once

---

42 Case C-314/12 (2014) *UPC Telekabel Wien* ECLI:EU:C:2014:192.

43 *See* <https://en.wikipedia.org/wiki/Gorilla_scandal>

44 M. Husovec, Posudzovanie právomoci slovenského súdu v prípade dištančných e-deliktov, 2012 (5) *Revue pro právo a technologie* p. 24 ff.

45 The lawsuit was eventually abandoned.

46 M. Husovec, Doménová čítanka: Výber zo slovenských doménových rozhodnutí, EISi 2012.

47 Case C-314/12 (2014) *UPC Telekabel Wien* ECLI:EU:C:2014:192.

48 Open-ended website blocking injunctions mean that they specify neither the exact IP address or domain name that ought to be blocked, nor the technical measures to be taken, but only identify the service. This allows then flexible adjustment of the order when the service moves to another location or technology changes, but at the same time increases the risk of abuse, since it narrows down the scope of the court oversight at the time of grant of the order.

the implementing measures are known; and (vi) must be transparent in their implementation. It is subject of the scholarly debate whether all these requirements equally apply to the measure-specific website blocking injunctions as opposed to only open-ended injunctions.[49] As will be pointed out in the Part 4, some of them certainly do anyway as a matter of the constitutional law.

Furthermore, Section 6(5) of the E-Commerce Act stipulates *prohibition of general monitoring obligation* that applies to mere conduits, such as access providers who might often face filtering and blocking efforts. Information society services providers that provide a service consisting of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, are exempted from liability for the information transmitted if they fulfil certain conditions (Section 6(1) of the E-Commerce Act). This liability exclusion, however, does not prevent the binding effect of the court orders that require the service provider to remove certain information from the infrastructure (Section 6(5) in fine of the E-Commerce Act). The prohibition of general monitoring, however, limits the potential scope of such orders by preventing imposition of orders to actively seek the facts or circumstances indicating illegal activity. After the recent CJEU ruling in *UPC Telekabel*, however, the scope of the prohibition based on Article 15 of the E-Commerce Directive appears to be rather narrow, applying only to cases of blanket and non-targeted measures rather than large-scale monitoring.[50] This is because of the CJEU's willingness to accept the blocking orders that might be implemented by the Internet access provider even by employing a filtering, such as deep packet inspections.

Additional and general safeguards could be inferred from the Constitution. Although the Constitutional Court so far never had an opportunity to address the instances of website blocking and filtering, in its recent *Tankman II* case,[51] the Court stressed that the court-approved remedies to a copyright-infringement should be reviewed independently for their constitutional admissibility. This, in line with the case-law of the CJEU and ECtHR, opens doors to constitutional moderation of remedies, whether granted on request of the state authorities or private parties.

The Constitutional Court already has a track record of moderating use of Section 90 of the Penal Procedure Code (data seizures), when it held that a production order, an order to a person to submit specified computer data in that person's possession or control, is to be preferred before seizure or search orders related to computer data. The court also considered wholesale copying of the electronic data disproportionate and illegitimate, thus requiring that the relevant data are isolated first, and the irrelevant data are immediately destroyed.[52]

It is clear from the previous section that *explicit* freedom of expression safeguards with respect to website blocking and filtering are virtually non-existent. The Constitutional Court might develop them in response to the first cases, but until then, it is not even clear whether: (1) the courts or authorities are able to rely on merely generally worded provisions to obtain website blocking or filtering, (2) an independent review is required, (3) the users or targeted websites have a possibility to challenge over-blocking or (4) how limited the measures have to be in time and their reach (more on the opinion of the author in section 5). So far, the only body of governing principles can be

---

49 M. Husovec, CJEU allowed website-blocking injunctions with some reservations, 2014 9 *Journal of Intellectual Property Law & Practice* p. 631-634 (for more debate).

50 This decision shows that even website-blocking might be considered a permissible specific monitoring obligation (see Art. 15 of the E-Commerce Directive).

51 Decision of the Constitutional Court of the Slovak Republic, *Tank Man II* (2014) Case No. II. ÚS 647/2014 – reported in IIC 2015, 729.

52 Decision of the Constitutional Court of the Slovak Republic (2010) II. ÚS 53/2010; Decision of the Constitutional Court (2013) II. ÚS 270/2013.

inferred from the case-law of two institutions: (i) CJEU[53], hearing privately litigated Internet enforcement cases in the field of intellectual property and (ii) ECtHR[54] hearing complaints against mostly state-imposed website blocking measures. Although the two courts do not always speak one voice, the basic set of common requirements could be summarized as follows:

- *The orders have to respect "quality of the law" requirement*: sufficient and predictable legal basis for orders; precise formulation of orders;
- *The orders have to follow legitimate purpose:* balancing against the rights of others; weighing against the (public) interests;
- *The orders have to be proportionate in order to minimize the interference:* judicial review is required; orders should be specifically targeted in order to prevent "collateral censorship"; wholesale website blocking is not acceptable; the state has a positive obligation to prevent abuse of rights;

After the CJEU issued its *UPC Telekabel* ruling, it became questionable in the Slovak Republic how to achieve that private parties (users) could have an ex-post possibility to challenge over-blocking when they were not party to the initial proceedings. It is submitted that the solution could be either in the contractual legal relationship regarding Internet access, or tortious legal basis.[55] In the former case, the contract between the Internet subscriber and the Internet access provider could be read in the light of subscriber's right to freedom of expression so as to safeguard him/her an entitlement to access also unjustifiably blocked websites.[56] In the latter case, the subscriber or owner of a targeted website could rely on some of the existing tortious provisions in order to obtain the access to unjustifiably blocked websites. Tort and contract rules in both cases would serve a medium to provide fundamental rights in the horizontal relationships. A set of clear rules enabling such remedy for users and owners of targeted websites would be welcome, especially because some of the over-blocking might also originate from the voluntary initiatives, such as subscription to unsupervised IWF list on child pornography[57] (see Part 2.1 and discussion in Part 3). A specific problem is posed by injunctions that are issued by the courts in the neighboring countries (e.g. Austria), but have an (unintended) legal effect also for the subscribers in Slovakia[58].

2.2. Take-down/removal of illegal Internet content

All the provisions mentioned in the previous section could also serve to support content *take-down orders*. Additional legal basis can be found in Section 415 of the Civil Code, which if read in connection with individual legally protected interests of private parties, extends duties of care to protect third party rights also to intermediaries such as webhosting providers, social networks and user-generate content websites.[59] The potential legal liability is limited by the E-Commerce Act, which in its Section 6, incorporates set of three Union safe-harbours for *mere conduits* (Section 6(1)), *hosting* (Section 6(4)) and *caching activities* (Section 6(3)). The safe harbours, however, do not apply to orders of the courts. This set of liability exclusions is complemented by the prohibition of general

53 Cases C-5/08 – Infopaq International (Infopaq International A/S v. Danske Dagblades Forening) and C-275/06 – Promusicae (Productores de Música de España v. Telefónica de España SAU).

54 *Ahmet Yildrimi v. Turkey* App no 3111/10 (blocking of Google Sites; by an owner of a site); *Akdeniz v Turkey* App no 20877/10 (blocking of Last.fm; by a mere user of a service).

55 The Austrian Supreme Court presented a similar opinion in OGH (2014) Case No. 4 Ob 71/14s.

56 This assumes, however, that the Internet access that was contracted by the subscriber would be of unlimited nature.

57 *See* <https://en.wikipedia.org/wiki/Internet_Watch_Foundation>

58 *See* < https://torrentfreak.com/austrian-pirate-bay-blockade-censors-slovak-internet-accidentally-151203/?utm_source=dlvr.it&utm_medium=twitter>

59 M. Husovec, Zodpovednosť na internete: podľa českého a slovenského práva, CZNIC, 2014 p. 73 ff.

monitoring (Section 6(5)), which limits the type of measures that the courts can order. The hosting safe harbor in Section 6(4) of the E-Commerce Act shields from liability the kind of services that consist of the storage of information provided by a recipient of the service on the condition that the provider does not have actual knowledge of illegal activity or information. According to the case-law of the CJEU,[60] the hosting provider qualifies for the liability exclusion only if its activity is of passive nature.

The Slovak transposition of the E-Commerce Directive is marked with many legislative misunderstandings.[61] Probably the most important of all is whether the provision on liability exclusion also serves as an independent legal basis for the liability. According to the literal wording of Section 6(5) of the E-Commerce Act, each safe-harbour-covered intermediary, including hosting providers and mere conduits, would have to act expeditiously upon obtaining a notice. This would be not only against the mere conduit safe harbour (Art. 12 of the E-Commerce Directive), since mere conduits do not have to react to notices, but also undermine the idea that passive hosting providers should be afforded better treatment than active hosts that never qualify for the liability exclusion. The correct interpretation in light of the European Union law is nevertheless possible,[62] although it was not relied upon by the courts yet. Another problem of the wording relates to Section 6(5) that not only outlaws that general monitoring is imposed on intermediaries, but also that the mere conduit, caching and hosting intermediaries "are not allowed to search information, which they transmit or store". This is a clear mistake in the transposition of the E-Commerce Directive, which can be hardly defended as a justified interference with the right to conduct business. Hence its "constitution-conform" interpretation in light of the Article 15 of the E-Commerce Directive is also necessary.

According to the correct "euro-conform interpretation" of the hosting safe harbour (Section 6(4)), the intermediary proving service consisting of storage of third party information may not face liability, other than for injunctive relief, prior to acquisition of knowledge about the wrongful information. According to the Slovak transposition, the knowledge obtained must be always "actual" because the "constructive knowledge" standard was left out. The standard of "actual knowledge", according to the case-law of the CJEU,[63] requires awareness of illegal *nature* of the information. Actual knowledge is triggered always when the intermediary is faced with sufficiently precise and adequately substantiated notice.[64] Because the transposition of the Union safe-harbours is almost verbatim, the E-Commerce Act does not specify any specific procedures of notification or counter-notice. The decision how specifically to implement this procedure on the service is left entirely up to the intermediaries. Until today, no best-practice rules or guidelines are known to be developed locally to tackle the procedure of notice and take-down. The intermediaries seem to be largely dealing with the issue on their own and from the publicized information it seems that when the potentially criminal content is involved, they usually act upon mere notification of the authorities/third parties, without requiring any formal orders.

The liability prior to take-down of the content from user-generated content platforms is the main subject of the still pending case *Stacho v Klub Strážov*. In this case, a private individual sued an operator of a local media platform for allowing third parties to post anonymous libelous comments in its comments section below one of the articles. The first[65] and second instance[66] court held the

---

60 Cases C-236/08 to C-238/08 *Google France and Google* [2010] ECLI:EU:C:2010:159, para 113 ff.

61 M. Husovec, Zodpovednosť na internete: podľa českého a slovenského práva, CZNIC, 2014 p. 94 ff.

62 M. Husovec, Zodpovednosť na internete: podľa českého a slovenského práva, CZNIC, 2014 p. 96 ff.

63 Cases C-236/08 to C-238/08 *Google France and Google* [2010] ECLI:EU:C:2010:159, para 109.

64 Case C-324/09 *L'Oréal and Others* [2011] ECLI:EU:C:2011:474, paras 121-122.

65 M. Husovec, Zodpovednosť poskytovateľa diskusného fóra za údajne difamačné príspevky tretích osôb, 2012 (6) *Revue pro právo a technologie* p. 45 ff.

operator liable, although the second instance rejected to award any damages, but only obliged to removal of certain expressions from the comments. The case was recently re-opened after the Supreme Court cancelled the decision of lower courts on the basis that they did not sufficiently examine the applicability of the safe harbours in the E-Commerce Act.[67] In an another case concerning the Slovak domain name authority, SK-NIC, the Supreme Court held that SK-NIC is not liable for third-party registrations of the domain names and thus cannot be successfully sued to de-register the disputed domain names.[68]

Last but not least, Section 76(2) of the Civil Procedure Code might be often invoked in order to achieve a (preliminary) take-down of the data before the legal proceedings is resolved. This provision can be especially useful when the addressee of a take-down request is not sued as a defendant in the main proceedings. These provisions apply to all civil matters.

Following the *Google Spain* decision of the CJEU, citizens of the Slovak Republic started also applying for the newly created *right to be delisted* from search engines. According to the statistics, until today only 1318 requests were filed by person associated with the Slovak Republic.[69] Similarly as the European data protection laws, the Slovak data protection law does not provide for any safe guards against abuse of this type of requests or intermediaries' over-compliance. The search engine is under no obligation to notify the source website, which is about to be delisted. Moreover, the source does not have a possibility to challenge the decision of the search engine or to force it to re-include the content at the later stage when the grounds for delisting cease to exist.

Similar lack of safeguards arises also in the situation of take-down notices based on rights and interests of third parties other than delist-requests addressed to search engines. Intermediaries can freely choose whether they forward the notice to the author of the content. Often, they are even discouraged from doing so by the brief time-frame before the liability is imposed and rather evaluate the content only on its own. Even after the decision on take-down is taken, there is no recourse or possibility of independent review for the affected parties. Since the liability scheme in the private disputes can hardly mandate these types of safe-guards, it would be advisable to at least encourage them in the design of the liability scheme for intermediaries, so that these practices appear as a rational choice for the intermediaries at stake. Unfortunately, again the decision of the ECtHR in *Delfi* does not mandate these safe guards as a part of the European minimal standard. However, already in the past, some European courts did encourage various other models,[70] which can be of inspiration

---

66 *Ibidem*.

67 The Decision of the Supreme Court (2013) Case No. 7 Cdo 141/2012.

68 The Decision of the Supreme Court (2007) Case No. 3 Obo 197/06, reported in M. Husovec, Doménová čítanka: Výber zo slovenských doménových rozhodnutí, EISi 2012.

69 *See* <https://www.google.com/transparencyreport/removals/europeprivacy/>

70 An example of such an approach can be found in the jurisprudence of the German Federal Supreme Court (BGH). In the *Blogger* case (BGH *Blogger* (2011) ZR VI 93/10), Google was sued for a content posted by a third party on one of the blogs hosted and operated by it. The BGH held that a careful balancing exercise between a right to private life and the freedom of expression needed to be carried out. As a result, the BGH required the following before any liability could be imposed: "Taking of an action by a hosting provider is only prompted when the notice is so sufficiently specific that an infringement can easily be established based on the claims of the affected person, i.e. without any in-depth legal or factual review. [..] Regularly, the compliant of the affected person should be forwarded to a person who is responsible for the blog so he can react to it. If no reaction is received within a reasonable time limit, legitimacy of an objection should be presumed and the objected entry should be removed. Should the person responsible for the blog reply with a substantiated denial of the objections, so that legitimate doubts arise, the provider can basically hold and communicate this to the affected person, also requiring possible proof of the alleged infringement. Should the reaction or the necessary evidence not be delivered by the affected person, any further review is not needed. If

also for the Constitutional Court of the Slovak Republic. Even after the *Delfi* decision, the Constitutional Court is free to set the standards for the freedom of expression higher, as long as a positive obligation to respect the right to effective remedy of injured third parties is guaranteed, which does not seem to preclude a counter-notice procedure in any way.

Despite this, arguably, the freedom of expression standard should oblige the state to affirmatively protect speech of third parties from illegitimate take-down requests. When the requestor is the state, the application of such obligation is not problematic. It is more so when the dispute involves merely private parties, such as in intellectual property or personality rights disputes. The case for positive obligations is, however, admittedly weaker after the ruling of the Grand Chamber of ECtHR in *Delfi AS v Estonia,*[71] although the Slovak Constitution can naturally provide for higher safe-guards than the Convention. The Constitutional Court might be only more hesitant to do so.

The prohibition of general monitoring obligation in Section 6(5) of the E-Commerce Act can be also seen as a freedom of expression safe-guard. It prevents that safe-harbour-covered intermediaries are exposed to any obligations requiring general surveillance of the third party content. However, the scope of applicability of this prohibition is too narrow, because many intermediaries do not qualify for any of the safe-harbours. It is submitted that prohibition of general monitoring should, as a principle, enjoy more general application. Arguably, the use of the principle in order to advance the objectives of the freedom of expression pre-dates emergence of Internet intermediaries.[72]

3. Procedural Aspects

The private parties that are victims of tort of defamation, intellectual property infringements, misuse of their personal data or other wrongs can request intermediaries to remove the objected third-party information from their services. The intermediaries are usually obliged to act upon such requests if they are sufficiently clear and adequately substantiated. If they wish to achieve blocking of a particular website, they have to apply to the courts.
For the take-down, there is no obligation to pre-litigate the matter before the courts. On the contrary, most of the requests are made without consulting the courts first. Under the existing legal framework, the intermediary is also not generally excused to require the confirmation of illegality from the independent authority prior to the take-down. If it does not respond to a justified request

---

from the reaction of the affected person or from the presented evidence, and taking into account an eventual reaction of the person responsible for the blog, an infringement of personality rights is proven, the objected entry should be removed" (translation mine). Similar need for an appropriate defense was articulated also by the Advocate General in the above mentioned *L'Oréal v. eBay* case ("Obviously freedom of expression and information does not permit the infringement of intellectual property rights. These latter rights are equally protected by the Charter, by its Article 17(2). Nevertheless, it entails that the protection of trade mark proprietor's rights in the context of electronic commerce *may not take forms that would infringe the rights of innocent users of an electronic marketplace or leave the alleged infringer without due possibilities of opposition and defence.*"). Last but not least, the principle of counter-reaction before the take-down has also been endorsed by the English High Court in *Tamiz v. Google* [2012 EWHC 449 (QB)], which tolerated Google's response time of several weeks.

71 *Delfi AS v. Estonia*, App no. 64569/09 (ECHR, 16 June 2015)

72 In 1976, the BGH decided an important case (BGH *VUS* (1976) VI ZR 23/72) involving an importer of Yugoslavian newspapers to Germany that included untrue libelous statements. The BGH concluded in this case that imposing a general monitoring obligation would be unreasonable, though maybe technically feasible. An importer, said the BGH, should be obliged to control only a certain specific texts of specified newspapers, which were brought to his attention, and does not need to control content of all the imported newspapers before the import.

within a reasonable time from the delivery of the notice, it might face joint-liability for the content. Victims might also apply for preliminary injunctions to take-down or block the content prior to resolution of the case against the perpetrator. In the field of data protection and consumer law, they can also apply to the Slovak Data Protection Authority or Slovak Commercial Inspection to order the take-down or blocking of the content.

The state authorities investigating a crime of distribution of child pornography, defamation, unjustified interference with personal data, endangerment of confidential information, treason, distribution of extremist materials, denial of holocaust, instigation of racial hatred or other crimes, may request the court or prosecutor to order a take-down or blocking of a content in accordance with Section 90 of the Penal Procedural Code. Other state authorities might try to issue such orders in order to support their own operations.[73]

From the legal bases mentioned, only Section 90 of the Penal Procedure Code foresees specific statutory safeguards. Filtering, blocking and take-down orders have to be always time-limited, and their grant may not exceed 90 days (Section 90(2)). After this period, a new order needs to be issued for any extension of that period. If the reason for issuing the order ceases to exist, the order has to be reversed by the authority that granted it at the first place (Section 90(3)).

The voluntary website blocking scheme related to child pornography is not subject to any safeguards. In case of over-blocking, the question is whether users and/or affected websites could object before the access providers and if so, whether they would feel obliged to re-include the unjustifiably blocked websites. At this point, no Slovak case of IWF list related over-blocking, apart from famous Wikipedia and Wayback-machine cases,[74] is known to us. As discussed above, it is possible that either tort law or contract on Internet access, aided by the "constitution-conform interpretation", could provide the necessary course of action to remedy the situation of collateral censorship.

4. General Monitoring of Internet

In the Slovak Republic, there is no authority in charge of proactive monitoring of the Internet. Since July 2013, the Computer Crime Department is active within the Criminal Police Bureau of the Presidium of the Police Force. One of the competences of the Computer Crime Department are attacks to computer systems, online child abuse and credit card fraud. The Department participates in the already mentioned project "Stoponline.sk" which is a part of the broader INHOPE network. Its aim is to operate a national centre for reporting of illegal and inappropriate content and activity on Internet. It makes available a form which can be used by the general public to report illegal or suspicious content, in particular, instances of child pornography, sexual exploitation, child prostitution, child trafficking or grooming, but also other activities with criminal character such as xenophobia and racism. Once the notification is received, the reports are distributed to individual INHOPE Member States. When it is established that the illegal content or activity originates from the Slovak Republic, the (Slovak) Police Force takes appropriate measures in order to prevent this activity. Work of the centre is based on the framework foreseen by the European Union and United Nations[75].

---

73 Section 8(1)(d) of the State Control Act; Section 65(1) of the Data Protection Act; Section 70 of the Confidential Information Act; Section 3 of the Penal Procedure Code; Section 15 of the Slovak Intelligence Service Act; Section 15 of the Army Intelligence Service Act (all requiring only own exercise of authority; no application to an independent authority is needed).

74 *See* https://en.wikipedia.org/wiki/Internet_Watch_Foundation.

75 European Commission's "Safer Internet Plus" project; the Council Decision to combat child pornography on the Internet (2000/375/JHA); the Council Framework Decision on combating the

In addition, to some extent, one could perceive the task of the Internet Watch Foundation, which compiles list of illicit child pornography websites, equivalent to these efforts. As was explained earlier, IWF is a charitable organization that was established by the internet industry in the UK in order to provide a hotline for the public to report criminal online content such as child pornography. In the meantime, some parts of its black-list database are used also in other countries. In the Slovak Republic, two major Internet access providers confirmed that they filter the child pornography based on the black-lists provided by the IWF. On the other hand, apart from the legislation on data protection, no legislation prevents the Internet intermediaries from actively monitoring the Internet content. So far, however, there is no case-law that would *require* them to carry out such task. This can partially be also caused by Section 6(5) of the E-Commerce Act, stipulating a *prohibition of general monitoring obligation*, which applies to mere conduits, caching and hosting providers within the meaning of the E-Commerce Directive.

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

In order to assess the legal framework two situations needs to be distinguished from the outset: (i) take-down of the content and (ii) website blocking or filtering.

As for *website blocking and filtering*, only few of the outlined legal provisions satisfy the basic constitutional safeguards required for a justified interference with the freedom of expression. The provisions are not sufficiently clear and foreseeable and thus fail to satisfy the requirement of the quality of the law. From the enumerated *provisions on powers of public authorities*, only Section 90 of the Penal Procedure Code, Section 8(1)(d) of the State Control Act, Section 76(2) of the Civil Procedure Code satisfy this important precondition. As a result the possibilities of authorities to request *blocking and filtering* measures are rather limited in the Slovak legal system.

The situation is slightly different for *private parties who want to request filtering and blocking* measures as a response to infringement of their rights. First of all, the ECHR[76] as well as the Constitution places upon the state a positive obligation to protect the rights of third parties with an effective remedy. Second, the legal consequences of the provisions related to enforcement of intellectual property rights, if read in the light of case-law of the CJEU, are more foreseeable. Because the personality rights provisions do not mention that the addressee of an injunctive relief has to be an infringer, it is accepted in the literature that the measures might also cover non-infringing intermediaries such as access providers. Hence, the legal basis in the field of intellectual property rights enforcement, but also personality rights enforcement, will most likely satisfy the conditions of the quality of the law.

The quality of the law requirement also influences *the form of the orders* in which the constitutionally acceptable legal orders can be granted.[77] For instance, even if website blocking is acceptable as a remedy, this does not mean that the order may leave any implementation of such blocking unsupervised and without safeguards. As was also stressed by the Advocate General in the *Sabam* case,[78] the wording of certain orders might be so complex that even though they can be

---

sexual abuse, sexual exploitation of children and child pornography; the United Nations Convention on the Rights of the Child.

76 *K.U. v Finland*, Application no. 2872/02 (2 December 2008), *Delfi AS v. Estonia*, App no 64569/09 (ECHR, 10 October 2013) [91]; *Delfi AS v. Estonia*, App no. 64569/09 (ECHR, 16 June 2015)

77 M. Husovec & M. Peguera, Much Ado About Little: Privately Litigated Internet Disconnection Injunctions, 2015 (10) *International Review for Intellectual Property and Competition* p. 10-37.

78 Case C-70/10 *Scarlet Extended* [2011] ECLI:EU:C:2011:255, Opinion of AG Villalón, paras 88-114.

proportionate, they just should not be granted on the basis of generally-worded provisions, such as one on injunctions. Since there is no filtering or blocking case-law, this aspect of application compliance cannot be evaluated at this point.

As was explained earlier, the situation with safeguards is particularly worrying. First of all, apart from Section 90 of the Penal Procedure Code, none of the legal bases for blocking and filtering foresees any explicit freedom of expression safeguards. All the safeguards, such as the strict targeting of the measures, their transparency, independent oversight or time limitation have to be introduced by the case-law.

Moreover, certain safeguards, such as the possibility to request the review of the scope of the issued measures or their practical implementation, have very uncertain grounds in the existing law. Especially in the situations of voluntary enforcement mechanisms like the IWF's black-listing, it is important that the users or the targeted websites have at least an ex-post possibility to challenge the instances of illegitimate over-blocking. Currently, the users could sometimes maybe object based on their contract with the access provider, while the affected websites might try to use the cause of action in tort law. However, these remedies are far from being generally accepted at the time.

Furthermore, the instances of legal actions against middle-man such as actions to disconnect users or block websites, suffer with a problem regarding the right to fair trial of the affected parties. Not only are these parties intentionally not included in the original lawsuit, but their outcomes cannot be easily challenged, despite the fact that they are binding at least upon the sued intermediary. Slovak courts so far did not recognize this problem. However, in the *rover.sk* case,[79] this consideration could have contributed to the rejection of direct cancellation claim against the domain name authority, since otherwise the plaintiffs could avoid arguing their case with the alleged infringers who registered the domain names.

The situation regarding the legal basis for the *take-down* requests seems to be more nuanced. The requests related to the right to be delisted are, following the *Google Spain* decision, firmly based on the data protection framework. Hence also the National Data Protection Authority cannot be said to face any difficulties when requesting such delisting on behalf of the natural persons. Similar is true for the take-down requests of private parties that are based on liability of the intermediary. The scope of protective duty of care has its explicit legal basis, which allows the extension of protective duties beyond the ordinary acts of infringements. Although the E-Commerce Act could surely accommodate more safeguards to protect the freedom of expression, its wording shielding from the liability, is also in line with the requirement of quality of the law given that it is not the legal basis of such requests, but rather serves as a clarification thereof.

The greatest problem of the E-Commerce Act is, however, again lack of articulated safeguards. In the absence of elaborate case law encouraging the intermediaries to ask for or process the counter-notices, the system can lead to incentives that are too one-sided and favor take-down of the third party content without any elaborate examination of its legitimacy. This should be remedied by allowing for proper response of the affected authors of the content in the less straightforward cases and encouraging the intermediaries to install informal dispute settlement system that could resolve the take-down disputes if they arise. When the intermediary liability is designed so that existence of such system mitigates the risk of liability for the third party content, it will become a rational choice for them to introduce it.

Martin Husovec
18.9.2015

[79] The Decision of the Supreme Court (2007) Case No. 3 Obo 197/06.

Revised on 07.04.2016 taking into consideration comments from Slovakia on this report