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 302-322

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.

HUNGARY

1. Legal Sources

What are the legal sources for measures of blocking, filtering and take-down of illegal internet content?

This area is **satisfactorily and exhaustively regulated**. Hungary has a wide variety of legal measures (criminal law, administrative law, civil law) concerning blocking, filtering and take down of illegal internet content focusing on the most current illegal contents.

Hungary has, moreover, transposed into domestic law **every relevant convention**, as well as **measures of EU law**. [1] As the Organization for Security and Co-operation in Europe (OSCE) published a report[2] under the title "Freedom of Expression on the Internet", which contains the most relevant issues and fields in which internet content regulation could emerge, I am primarily focusing on the list concerning the transposal of international standards and conventions; therefore I would like to underpin the status of harmonization. The most relevant and transposed sources are:

a. The Convention of Cybercrime (of the Council of Europe) has been ratified by the Act LXXIX. of 2004;
b. The Council of Europe Convention on the Prevention of Terrorism has been ratified by the Act II of 2011;
c. The Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse has been ratified by the Act XCII of 2015;
d. Council of Europe Convention on the counterfeiting of medical products and similar crimes involving threats to public health has been ratified by the Act CCVIII of 2013;
e. 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') implemented into the national law with the Act CVIII. of 2001.

Most regulation is governed by the Criminal Code, and Criminal Procedure Act, and other particular acts. **There is no Internet Code** (or such specific Act) concerning blocking, filtering and take down procedures in Hungary.

A short overview of the legal sources (in which the activities of blocking, filtering and take-down of illegal internet content are regulated):

Blocking/Filtering:

- Act XIX of 1998 on Criminal Proceedings Act (hereinafter: CPA) 158/B-158/D and 596/A. regulates "**rendering electronic data temporarily inaccessible**" and **"the temporary prevention of access to**

[1] With respect to the EU Framework Decision on combating racism and xenophobia on 28 November 2008 the Hungarian Criminal Code Art 465 (3) was amended by the Art. 35 of the Act LXXVI of 2015. The Art. 26 (2) and the XIX. Chapter of the Hungarian Criminal Code fulfils the obligation of implementation concerning 2011/93/EU Framework Decision. The Art. 399-400. fulfils the implementation duty of the Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing.

[2] OSCE, Freedom of Expression on the Internet (report), available at http://www.osce.org/fom/80723 (11.08.15), pp. 35-133.

electronic data" as a subcategory of the former. The Art. 596/A. regulates the **"order to render electronic data permanently inaccessible performed by disabling access irrecoverably".**

- Act XXXIV of 1991 on the Organization of Gambling (Art. 36/G.-36/J.) **temporary blocking** of unauthorized gambling sites by the National Tax and Customs Administration.
- Act CLXXXV of 2010 on Media Services and on the Mass Media (Art. 188-189.) **suspending or terminating the conveyance of media services and online press products**.
- Preventive measures (Filtering):
  - Act CXL of 1997 Art 55. (1a) defines software installing obligations of public libraries.
  - Act CXC of 2011 on National Public Education Art 9. (11) defines software installing obligation of public education institutes;
  - Act C on 2003 on electronic communication Art 144. (2a): ISPs shall make and publish on their websites information about the use and accessibility of filtering software or similar services which can protect the minor's physical, emotional and mental health, and notice the costumer about formers every quarter. Art 149/A. (1) ISPs shall provide the free downloading and free usage of abovementioned software;
  - Act CVIII of 2001 on certain issues of electronic commerce services and information society services Art. 4/A.: service provider shall sign the harmful (sexual or violent) content before it can be accessed, and inform about the possible risk of minors, this content shall be detectable by the filter software determined in the Act C. on 2003 on electronic communication Art. 149/A (1).

Removal/Take down:

- Act C of 2012 on Criminal Code (hereinafter: CC) Art 63. (1) g) lists and Art 77 regulates **"irreversibly rendering electronic information inaccessible"**, which is not only applicable for specific crimes. (It is a general measure.)
- Act. XIX of 1998 on Criminal Proceedings Act (hereinafter: CPA) 158/B-158/D and 596/A. regulates "**Rendering electronic data temporarily inaccessible**" and **"the temporary removal of electronic data"** as a subcategory of the former.
- Act XCV. of 2005 on Medicinal Products for Human Use and on the Amendment of Other Regulations Related to Medicinal Products (the "Medicines Act") 20/A. § **temporary removal of electronic data concerning fake and unauthorized medicines** by National Institute of Pharmacy and Nutrition.
- Act CVIII of 2001 on certain issues of electronic commerce services and information society services Art. 13 so called **"notice and take down" procedure** concerning intellectual property and personality rights of minor children.

2. Legal Framework

What is the legal framework regulating?

2.1. Blocking and/or filtering of illegal Internet content

2.1.1. "Rendering electronic data temporarily inaccessible"

CPA regulates these measures in Articles 158/B-158/D. This means a temporary restriction of a person's rights of use of data posted via electronic communication systems (hereinafter: electronic data) and temporarily disabling access to data. Proceedings instigated due to criminal acts that **warrant public prosecution** and **require that electronic data be rendered permanently inaccessible**

also in order to **prevent the criminal act from continuing**, an order may be issued to render electronic data temporarily inaccessible. **Courts are authorised** to issue an order to render electronic data temporarily inaccessible. Under the Art. 158/B. (4) of CPA, there are two different types of the abovementioned measure in a graduated system: a) **the temporary removal of electronic data (hereinafter: temporary removal)** (As the obliged party is the web hosting providers and the subject of this procedure is removal, this will be discussed under the Section 2.2.1), and b) **the temporary prevention of access to electronic data (hereinafter: temporary prevention of access)**. By issuing an order, the courts oblige **electronic communications providers**[3] (first of all: ISPs) to temporarily disable access to electronic data. The courts shall issue the order, if

- **a web hosting provider fails to comply** with its obligation of temporary removal, **or** where a **letter rogatory by a foreign government agency** seeking the temporary removal of electronic data fails to achieve its intended purpose within a period of thirty days after being sent, and
- criminal proceedings have been instigated to combat
  - **Drug Trafficking** (Art. 176-177 of the CC),
  - **Inciting Substance Abuse** (Art. 181. of the CC),
  - **Aiding in the Manufacture or Production of Narcotic Drugs** (Art. 182 of the CC),
  - **Criminal Offenses with Drug Precursors** (Art. 183 of the CC),
  - **Illegal Possession of New Psychoactive Substances** (Art. 184-184/A. of the CC),
  - **Child Pornography** (Art. 204 of the CC),
  - **Criminal Acts Against the State** (Chapter XXIV of the CC),
  - **Terrorist Act** (Art. 314-316 of the CC),
  - **Terrorist Financing** (Art. 318 of the CC),

and the electronic data are connected to these forms of criminality.

The courts shall immediately send electronic notification to the **National Media and Infocommunications Authority** (hereinafter: NMIA) about its orders. The NMIA organises and supervises the execution of orders to render electronic data temporarily inaccessible (It will be discussed in Section 3, and in particular, in 3.6.2 and 3.6.3.)

The case law could be examined through the central database (Hungarian abbreviation is "KEHTA") of the NMIA, but this is not public, and only the courts and specific authorities have access to it.[4]

The court lifts the obligation to prevent access temporarily if a) the web hosting provider complies with its obligation to remove electronic data temporarily, b) the reason for issuing the order has otherwise ceased to exist, or c) investigations have been terminated, except in cases with the option to issue an order to render electronic data irreversibly inaccessible under the Art. 77 of CC (see: 2.2.2.)

---

[3] Definitions of Act C of 2003 on Electronic Communications:
14. **Electronic communications service provider**: shall mean the operator of an electronic communications network or the provider of electronic communications service, which is a natural person or legal entity or a business undertaking without legal entity.
15. **Electronic communications activity**: shall mean the activity in the course of which signals, signs, texts, images, voice or messages of any other nature generated in any form that can be interpreted are transmitted via electronic communications networks to one or more users, including, in particular, the provision of electronic communications services, the operation of electronic communications networks and equipment, distribution of terminal equipment and related services.

[4] I have sent a letter to request statistic data of the database to NMIA in order to see the number of the order at least. This request has however been denied, with reference to the non-public status of the database.

The courts, acting ex officio or upon a motion to that effect by the prosecutor, may impose a **fine** between one hundred thousand and one million Hungarian Forints on electronic communications providers that fail to abide by the obligation to temporarily disable or to restore access to electronic data. Fines may be imposed repeatedly.

This Article came into force on 01.07.2013, with several other parts on 01.01.2014. There is therefore no public statistics on the number of orders.[5]

2.1.2. "Order to render electronic data permanently inaccessible performed by disabling access irrecoverably"

The CPA regulates in Art. 596/A. this kind of order. The courts, acting ex officio or upon a motion to that effect by the prosecutor, issue this order if

- an order to temporarily prevent to access to data (discussed in 2.1.1.) was in effect at the time criminal proceedings terminated and blocking access continues to be justified,
- the web hosting provider fails to comply with its obligation despite a fine,[6]
- the courts ordered to render electronic data permanently inaccessible due to acts of child pornography and the web hosting provider fails to abide by its obligation immediately despite being fined,
- a letter rogatory by a foreign government agency seeking to render electronic data permanently inaccessible fails to achieve its intended purpose within a period of thirty days after being sent.

The order shall be executed by **electronic communications service providers** within one working day after communication of the court ruling.[7]

The **NMIA** organises and supervises the execution of orders to render electronic data permanently inaccessible by irrevocably disabling access.

The courts, acting ex officio or upon a motion to that effect by the prosecutor, may impose a **fine** between one hundred thousand and one million Hungarian Forints whenever an obliged party fails to abide by its obligation to permanently disable or to restore access to electronic data. Fines may be imposed repeatedly. Rulings imposing a fine may be appealed with suspensory effect.

This Article came into force on 01.07.2013, with several other parts on 01.01.2014. There are therefore no public statistics on the number of orders.[8]

2.1.3. Temporary blocking of unauthorized gambling sites

The Act XXXIV of 1991 on the Organization of Gambling (Art. 36/G.-36/J.) regulates temporary blocking of unauthorized gambling sites by the National Tax and Customs Administration (hereinafter: state tax authority).

---

5 The website of the Prosecutor General and Prosecution Service contains data only till 2013 August. http://www.mklu.hu/cgi-bin/index.pl?text=22 (11.08.15)

6 Imposed under Art 324 (3) of Act 2013 of CCXL on the execution of punishments, criminal measures, certain coercive measures and confinement for administrative offences.

7 Art 324 (5) of Act 2013 of CCXL on the execution of punishments, criminal measures, certain coercive measures and confinement for administrative offences.

8 The website of the Prosecutor General and Prosecution Service contains data only till 2013. August. http://www.mklu.hu/cgi-bin/index.pl?text=22 (11.08.15)

The state tax authority shall order as temporarily inaccessible the rendering of information published by way of an electronic communications network (hereinafter: electronic information) the publication or disclosure of which constitutes **illegal gambling operations**. Rendering information temporarily inaccessible refers to when access to the information is blocked temporarily (hereinafter: **temporary blocking**). The state tax authority shall order the temporary blocking for a period of **ninety days**. The **NMIA** shall organize and monitor the execution of temporary blocking.

The state tax authority may impose a **fine** of not less than 100,000 forints and not exceeding 500,000 forints upon any provider of electronic communications services which fails to meet the obligations. (The fine may be imposed repeatedly during the period of non-compliance.)

The state tax authority **shall abolish the obligation** of temporarily rendering electronic information inaccessible, before it is terminated, if:

a) the grounds therefore no longer exist; or
b) it is based on a request made by the criminal court or authority, or upon information received from the NMHH that a procedure is in progress for adopting the sanction of temporarily rendering electronic information inaccessible or the measure of irreversibly rendering electronic information inaccessible stemming from illegal gambling operations or other criminal offenses involving the electronic information in question.

As for the relevant case law, the statistics on the announcements can be found on the site of the state tax authority.[9] 164 announcements were issued in 2013, 214 in 2014, and 303 in 2015 till now, but not all of these are connecting to blocking orders; there are lifting orders as well. According to press reports, the number of blocking orders issued was 82 in 2014, and 283 up until June 2015.[10]

2.1.4. Suspend or terminate the conveyance of media services and online press products.

This kind of measure can be ordered under the Act CLXXXV of 2010 Art. 188-189. The **Media Council**[11] can order the intermediary service provider[12] to suspend or terminate the conveyance for any infringement of media regulations, if the media service provider fails to fulfil the terms of the executable resolution of the Media Council following a request. (For the complete description of the procedure and the legal conditions see Section 3.7.)

As for safeguards: the time period of the suspension of dissemination or broadcasting must be **proportionate** to the **weight or gravity of the underlying legal sanction**, and it may not exceed the

9 http://nav.gov.hu/nav/szerencsejatek/hirdetmenyek/A_Szerencsejatek_Felu20150428.html?pagenum=1 (11.08.15)

10 http://www.vg.hu/vallalatok/szolgaltatas/tobb-szaz-szerencsejatek-oldalt-blokkolt-a-nav-454884 (11.08.15)

11 The Media Council is an independent body of the Authority reporting to Parliament, vested with legal personality. The Media Council is the successor in title of the Országos Rádió és Televízió Testület (National Radio and Television Board). Art 123 (1) of the Act CLXXXV of 2010.

12 Under the Art 203 (30.) of the Act CLXXXV of 2010 **"Intermediary service provider"** shall mean any provider of information society services: a) engaged in the transmission of information supplied by the recipient of the service through a telecommunications network, or who provides access to a telecommunications network (**mere conduit and network access**); b) engaged in the transmission of information supplied by the recipient of the service in a telecommunications network, performed for the sole purpose of making more efficient the onward transmission of information to other recipients of the service upon their request (**caching**); c) engaged in the storage of the information supplied by the recipient of the service (**hosting**); d) engaged in providing tools to the recipient of the service for the location of information (**location tool services**).

time limit specified in the final and executable resolution for the media service provider or publisher of online press products, including the time period required for the termination of suspension. The time period required for the termination of suspension by the broadcaster or intermediary service provider may not **exceed fifteen days**, covering also the notification of the broadcaster or intermediary service provider by the Media Council. **The costs incurred** by the broadcaster or intermediary service provider in connection with the termination or suspension of broadcasting and intermediation shall be covered by the media service provider or publisher of press products upon whom the legal sanction had been imposed.

If the intermediary service provider fails to fulfil the abovementioned provisions, the Media Council shall open ex officio administrative proceedings against it and shall have powers to impose a **fine.**

There have been no orders issued by the Media Council under the abovementioned Articles, so it can be stated that there has not yet been relevant case law concerning the suspension or termination of the conveyance of media services and online press products.[13]

2.1.5. Preventive measures (of filtering)

The Act CXL of 1997 Art 55 (1a) regulates the obligation of public libraries to install easy to use Hungarian language software on the computers which have an internet connection to protect the **mental, emotional and physical health of children.** The same obligation of public education institutes can be found in the Act CXC of 2011 on National Public Education Art 9 (11).

Act C. of 2003 on electronic communication Art 144 (2a) states that ISPs shall make and publish on their websites information about the use and accessibility of filtering software or similar services which can protect the **minor's physical, emotional and mental health**.. Under Art 149/A (1) ISPs shall provide for the free downloading and free usage of the abovementioned software.[14]

Act CVIII. of 2001. on certain issues of electronic commerce services and information society services Art. 4/A.: the service provider shall **sign for** the harmful (sexual or violent) content before it can be accessed, and inform of the possible risk to minors. This content shall be detectable by the filter software determined in the Act C. of 2003 on electronic communication, Art. 149/A (1).

As for the **soft law instruments**, the Internet Roundtable for Child Protection has recommendations on Harmful Internet Contents and Applicable Filtering Software concerning Child Protection.[15] Moreover, the **Association of Hungarian Content Providers** (MTE) as a self-governing body has an **Ethics Code**.[16]

2.2. Take-down/removal of illegal Internet content

2.2.1. Temporary removal (under CPA)

---

13 I have sent a particular request for information concerning this measure.

14 Under a short examination the randomly chosen ISPs fulfil this kind of obligation:

a) UPC Magyarország Kft.: http://www.upc.hu/rolunk/tarsadalmi-felelossegvallalas/szuroszoftver/

b) Magyar Telekom Nyrt.:http://www.telekom.hu/rolunk/vallalat/fenntarthatosag/tarsadalom/tarsadalmi_szerepvallalas/gyermekvedelem/tudatos_internetezes

c) DIGI Távközlési és Szolgáltató Kft: http://digi.hu/gyermekvedelem

d) Vidanet Zrt.: http://vidanet.hu/pages/tartalomszuro.

15 http://nmhh.hu/tart/index/850/Ajanlasok (11.08.15).

16 http://mte.hu/in-english/ (11.08.15).

In section 2.1.1. above, the CPA, Art. 158/B. (4) was mentioned. This regulates the ”Rendering electronic data temporarily inaccessible”, which can also result in temporary removal. Where the obliged parties are the **web hosting providers,**[17] they shall have **one working day** to give effect to the temporary removal of electronic data after the communication of the court order.

The court lifts the obligation of temporary removal and issues an order to restore electronic data if

a) the reason for the order to render electronic data temporarily inaccessible ceases to exist, or
b) investigations have been terminated, except in cases with the option to issue an order to render electronic data permanently inaccessible (see 2.2.2.).

Otherwise the obligation is lifted upon the termination of criminal proceedings. If a court refrains from issuing an order to render electronic data temporarily inaccessible, it shall require the web hosting provider to restore electronic data.

The courts, acting ex officio or upon a motion to that effect by the prosecutor, may impose a **fine** between one hundred thousand and one million Hungarian Forints whenever an obliged party fails to abide by its obligation to remove data temporarily or to restore electronic data. (Fines may be imposed repeatedly.)

This Article came into force on 01.07.2013, with several further parts on 01.01.2014. There are therefore no public statistics on the number of orders.[18]

2.2.2. Irreversibly Rendering Electronic Information Inaccessible (under CC)

This kind of action is regulated in Art. 77 of Hungarian Criminal Code as a measure. Art. 63 (1) of the Code states it can be ordered independently, or in addition to a penalty or measure.

It can be applied for **every crime** (crimes mentioned above in 2.1.1.**,** but even in other cases, such as **defamation, invasion of privacy, mail fraud, breach of business secrecy, plagiarism, infringement of Copyright and Certain Rights Related to Copyright as well**)[19] under one of the following conditions:

a) **the publication or disclosure of** which constitutes a criminal offence; or
b) which is actually **used as an instrument** for the commission of a criminal act; or
c) which is **created by** way of a criminal act.

The order for irreversibly rendering electronic information inaccessible shall be issued even if the perpetrator cannot be prosecuted for reasons of minority or insanity, or due to other grounds for exemption from criminal responsibility, or if the perpetrator had been given a warning. The obliged party is the **web hosting provider.**[20]

---

17 Defined in the aforementioned Act on Electronic Trading Services and Certain Issues Concerning Services Related to Information Society.

18 The website of the Prosecutor General and Prosecution Service contains data only till 2013. August. http://www.mklu.hu/cgi-bin/index.pl?text=22 (11.08.15).

19 The possible crimes can be predicted and grouped: 1) crimes committed via unauthorized disclosure or share of content; 2) crimes infringing the security and authentication of transmission; 3) computer crimes; 4) crimes against intellectual property. J. Verebics, Az információs bűncselekmények és az elektronikus adat ideiglenes hozzáférhetetlenné tételének lehetősége az új Btk.-ban, 2013 (2) Gazdaság és Jog p. 3 seq, p. 3.

20 The Act refers to the definition of the Act CVIII of 2001 on certain issues of electronic commerce services and information society services. Concerning the Art. 2 (lc) of the cited Act the web hosting

As for the relevant case law, the official collection of court orders does not contain any record concerning Art. 77. of the CC. There were rumours in the media regarding one decision of the Metropolitan Court in January of 2015; however it has not yet been published in the official collection. This is about the kurucz.info website, which disclosed an article on Holocaust denial in 2013. The court ordered the American web hosting providers to irreversibly render this Article (thus only one page of the site) inaccessible.[21]

2.2.3. Notice and take down procedure

Act CVIII of 2001 on certain issues of electronic commerce services and information society services Art. 13 regulates the so called "***notice and take down***" procedure concerning **intellectual property rights** and **personality rights of minor children** under the title: "notice on an unlawful information society service".

Holders of **intellectual property rights** (protected by the Copyright Act, established on any copyrighted work, performance, recording, audio-visual work or database, or of an exclusive right arising from trademark protection under the Act on the Protection of Trademarks and Geographical Indications of Origin) (hereinafter: "rights holders") which have been infringed by the information made accessible by the **service provider**[22] – excluding the standardised address of the access to the information – may **request the removal** of the information infringing their right by way of sending a **notice in the form of a private document with full probative force or a notarised deed**[23] to the service provider.

The service provider shall arrange for **disabling access to or removal of** the information identified in the notice, **within 12 hours** of receiving the notice, specifying the rights holder whose right was infringed based on the notice; and shall concurrently give **written notice** to the affected recipient of the service who had provided the information that infringes the right of the rights holder (hereinafter: "affected recipient of the service") **within three working days**. The service provider shall refuse to disable access to, or remove the information pursuant to the notice, if the service provider has already previously taken the abovementioned measures in relation to the same information based on the notice of the same rights holder, unless the removal of, or disabling access to the information was ordered by a court or authority.

Within 8 days of receiving the notice specified above, the affected recipient of the service may lodge an **objection**[24] with the service provider, in the form of a private document with full probative force or a notarised deed, regarding the removal of the relevant information. Upon receiving the objection

---

provider is - by definition - an intermediary service provider, which stores information supplied by the recipient of the service (hosting).

21 http://atlatszo.hu/2015/01/17/mar-a-csata-elott-nyert-a-kuruc-info-a-bunteto-igazsagszolgaltatassal-szemben/ (11.08.15).

22 Service providers are **cache providers**, **search providers**, and **web hosting providers** as well under the Art. 2 (lb)-(ld), Art. 9-11. and therefore under Art 13, which is referring to the formers.

23 The notice shall contain the following: a) the subject of the infringement and the establishment of the facts that provide reasonable cause to believe that infringement has taken place; b) the data needed to identify the unlawful information; c) the name, address of residence or head office, phone number and electronic mail address of the rights holder.

24 The objection shall indicate the following: a) identification of the information removed or made inaccessible, including the network address where formerly the information had been available, as well as the identification data of the affected recipient of the service; b) a statement with detailed explanation that the information provided by the recipient of the service does not infringe the right of the rights holder specified in the notice.

the service provider shall expeditiously make the relevant information accessible again and notify the rights holder thereof by sending the objection to the rights holder, unless the removal of, or disabling access to the information was ordered by a court or authority. Should the affected recipient of the service admit to the infringement of the rights of the rights holder or does not lodge an objection within the time frame specified above, or the objection does not contain necessary data and statement, the service provider shall maintain the effect of disabling access to, or removal of the information.

Should the rights holder enforce his claim related to the infringement of right specified in the notice within **10 working days** after receiving the notice detailed above through a request of injunction for abandonment and prohibition or an order of payment or file a criminal report with the police within 12 hours of receiving the court decision ordering interim measures to that effect, the service provider shall once again disable access to, or remove the information identified in the notice. The service provider shall notify the affected recipient of the service of the measure that it has been taken within one working day by supplying a copy of the court decision. The rights holder shall advise the service provider of the final material decisions delivered in the course of the former procedure including an order for interim measure or the dismissal of the claim – without delay. The service provider shall expediently obey such decisions.

Under the Art. 13 (11) the rights holder and the service **provider may conclude a contract on the application of the "notice and take down" procedure**. In the contract the parties may not derogate the law, but may agree on issues not regulated by law.

The service provider shall not be liable for the successful removal of, or disabling access to the relevant information, when the service provider has acted in good faith to ensure removal or disabling access thereto.

The "notice and take down procedure" has been extended in order to protect personal right of minors on 01.01.2014. The abovementioned rules with the following exceptions shall be applied to the "notice and take down" procedure, if **personal rights of minors** – in its opinion – have been infringed by the information made accessible by the service provider:

a) the service provider shall give the **written notice** to the affected recipient of the service who had provided the information that infringes the right of the rights holder (hereinafter: "affected recipient of the service") **within one working day;**
b) the service provider shall keep up the disabling or removal even if the written notice could not be addressed because of the lack of data for identification;
c) the service provider shall disable the access or remove the information once again even if the minor or its representative send the order of the investigation received from the police;
d) the service provider shall not give information about the rights holder, whose claim was the reason of the disabling or removal;
e) The service provider could refuse to disable access to, or remove the information pursuant to the notice, if it considers it to be unsubstantiated because of the reasoning of the notice.

If the service provider does not abide by its abovementioned procedural obligations concerning the personal rights of minors or it refuses the notice on the ground specified in point e), the minor or its representative can **appeal** to the Internet Roundtable for Child Protection.

Statistical data cannot be provided concerning the number of notice and take down procedures, but it can be said that this kind of procedure is common in Hungarian practice.[25] The constitutional relations of this procedure, and the most recent and focal decision of the Constitutional Court of Hungary will be discussed in Section 5.

2.2.4. Temporary removal of electronic data (under Medicines Act)

Act XCV of 2005 on Medicinal Products for Human Use and on the Amendment of Other Regulations Related to Medicinal Products (the "Medicines Act") Art. 20/A. regulates **temporary removal of** electronic data concerning **fake and unauthorized medicines** by National Institute of Pharmacy and Nutrition (hereinafter: government body).

The government body shall order as temporarily inaccessible, by way of a decision, the rendering of information published by way of an electronic communications network (hereinafter: electronic information), the publication or disclosure of which constitutes **the provision of access to fake or unauthorized medicinal products**. The government body shall order by means of a decision **the temporary removal of electronic information** so as to render such electronic information temporarily inaccessible.

The party bound by the obligation imposed by the resolution of the government body shall be the **service provider and intermediary service provider**[26] (hereinafter referred to collectively as "service provider").

The government body may impose a **fine** of not less than 100,000 forints and not more than 1 million forints upon any service provider who fails to fulfil the obligation.[27] (The fine may be imposed repeatedly during the period of non-compliance.)

The obligation of temporarily rendering electronic information inaccessible shall cease **ninety days** after the date when ordered.

The government body shall abolish the obligation of temporarily rendering electronic information inaccessible, before it is terminated, if a) the grounds therefore no longer exist; or b) in criminal proceedings opened upon charges filed by the government body for pharmaceuticals on the grounds

---

25 Á. Kőhidi, A polgári jogi felelősség digitális határai Európában. A P2P rendszerekben megvalósuló szerzői jogi jogsértések felelősségtani vonatkozásai, available at http://www.doktori.hu/index.php?menuid=193&vid=10230&lang=EN (11.0815), p. 108-110.

26 Under the Art. 2 (k-ld) of Act CVIII of 2001 on certain issues of electronic commerce services and information society service **service provider,** means the natural or legal person or organisation without legal personality providing information society services. **Intermediary service provider** means the information society service provider which la) forwards the information supplied by the recipient of the service via the telecommunications network or ensures access to the telecommunications network (**simple data transmission and provision of access**); lb) forwards the information supplied by the recipient of the service via the telecommunications network, which principally serves to enhance the efficiency of information transmission originated by other recipient of the services (**caching**); lc) stores information supplied by the recipient of the service (**hosting**); ld) provides tools to the recipient of the services facilitating the search for information (**search functions**).

27 The amount of the fine shall be determined with regard to the severity of the infringement, repeated occurrence of the infringement and the extent of injury caused by the infringement, as well as other material circumstances weighing on the gravity of the infringement. The fine shall be payable to the account of the imposing government body for pharmaceuticals.

of falsification of health care products the court ordered in its binding peremptory ruling the obligation to render as temporarily or irreversible inaccessible electronic information.
As for the relevant case law, this Article came into force on 01.01. 2015. It is therefore a relatively new measure. The government body publishes the actual list of blocked sites on its website; there are at present 18 orders.[28]

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?

3.1. "Rendering electronic data temporarily inaccessible" (Articles 158/B-158/D. of CPA).

Courts are authorised to issue such coercive measures. One can **appeal** against the order to the higher court (as discussed in 3.1.1 and 3.1.2. and 3.2.) as well, but the appeal does not have suspensory effect.[29]

3.1.1. Temporary removal of electronic data (hereinafter: temporary removal)

The obliged parties are the **web hosting providers.**[30] They shall have **one working day** to give effect to the temporary removal of electronic data after the communication of the court order. Entities subject to a court order issued to render electronic data temporarily inaccessible shall **notify users** of the legal grounds of removing, or preventing access to, the affected content and shall cite the name of the court and the number of the court order in such notices.

The ruling on the termination of temporarily inaccessibility to electronic data and on restoring such data shall be communicated to the obliged party immediately. Web hosting providers shall have **one working day to restore** electronic data after the communication of the court ruling. It is the **duty of the bailiff** to give effect to orders issued to remove temporarily or to restore electronic data.

3.1.2. Temporary prevention of access to electronic data (hereinafter: temporary prevention of access).

By issuing an order, **the courts** oblige **electronic communications providers**[31] (e.g. IPSs) to temporarily disable access to electronic data. **If the person with the right to use the electronic data**

---

28 http://www.ogyei.gov.hu/hozzaferhetetlenne_tett_weboldalak_listaja/ (11.08.15).

29 Under the Art. 215 (5) of CPA.

30 Defined in the aforementioned Act on Electronic Trading Services and Certain Issues Concerning Services Related to Information Society.

31 Definitions of Act. C of 2003 on Electronic Communications:
14. **Electronic communications service provider**: shall mean the operator of an electronic communications network or the provider of electronic communications service, which is a natural person or legal entity or a business undertaking without legal entity.
15. **Electronic communications activity**: shall mean the activity in the course of which signals, signs, texts, images, voice or messages of any other nature generated in any form that can be interpreted are transmitted via electronic communications networks to one or more users, including, in particular, the provision of electronic communications services, the operation of electronic communications networks and equipment, distribution of terminal equipment and related services.

is unknown, court rulings shall be served to recipients by posting an announcement. Such announcements shall be posted on the bulletin board of the court for a period of fifteen days and on the central website of courts. The party holding the right to use electronic data has **eight days to appeal** against the ruling after it is served.

The courts shall immediately send an electronic notification to the NMIA of its orders. The NMIA organises and supervises the execution of orders to render electronic data temporarily inaccessible. With reference to electronic notifications received from the courts, the NMIA records the obligation to render electronic data temporarily inaccessible in a **central database (Hungarian abbreviation is KEHTA)** of court rulings issued to render electronic data inaccessible and **shall immediately notify electronic communications providers about court rulings**. Electronic communications providers have one working day to temporarily disable access to electronic data after the notice is served. The NMIA notifies the courts immediately of any failure by an electronic communications provider to comply with this obligation.

If the court lifts the obligation to prevent temporary access, the courts shall immediately notify the NMIA of the lifting of the obligation and the NMIA removes the obligation from the central database of court rulings ordered to render electronic data inaccessible and shall immediately notify electronic communications providers of the termination of the obligation by electronic means. Electronic communications providers have one working day to provide access to electronic data after the notice is served. The obligation is lifted upon the termination of criminal proceedings. When the courts have refused the order to render electronic data permanently inaccessible, the courts shall immediately notify the NMIA of the lifting of the obligation to render electronic data temporarily inaccessible, and the NMIA in turn shall remove the obligation from the central database of rulings and shall simultaneously notify electronic communications providers of the termination of the obligation by electronic means. Electronic communications providers have one working day to provide access to electronic data after the notice is served. The NMIA notifies the courts immediately of any failure by an electronic communications provider to ensure access once again.

3.2. "Order to render electronic data permanently inaccessible performed by disabling access irrecoverably". (CPA Art. 596/A)

The courts, acting ex officio or upon a motion to that effect by the prosecutor, issue an order to render electronic data permanently inaccessible by having access irrecoverably disabled.

The order shall be executed by **electronic communications service providers** within one working day after communication of the court ruling.[32]

The period for appealing a ruling issued to render electronic data permanently inaccessible by irrevocably disabling access, shall be open for **eight days**, respectively, for prosecutors after the date the ruling is communicated, for electronic communications providers after the related notice is served and for parties, including unknown parties, holding the right to use electronic data after the ruling is communicated, including communication by posting an announcement. Upon a request to that effect by the prosecutor, the court will terminate the order to render electronic data permanently inaccessible by disabling access irrecoverably in case the web hosting provider performs its obligation to remove the electronic data temporarily.

The courts shall immediately **notify** the NMIA by electronic means of court orders issued to render electronic data permanently inaccessible by irrevocably disabling access and of any rulings that lift

[32] Art 324 (5) of Act 2013 of CCXL on the execution of punishments, criminal measures, certain coercive measures and confinement for administrative offences.

such an obligation. **The NMIA organises and supervises** the execution of orders to render electronic data permanently inaccessible by irrevocably disabling access.

3.3. Irreversibly Rendering Electronic Information Inaccessible (Art. 77 of CC)

The execution of "Irreversibly Rendering Electronic Information Inaccessible" is regulated in Art 324 of Act CCXL of 2013 (on the execution of punishments, criminal measures, certain coercive measures and confinement for administrative offences). It is the **duty of the bailiff** to give effect to orders issued to the abovementioned measure. The **web hosting provider**[33] is obliged to comply with orders irreversibly rendering electronic information.[34] If the web hosting provider fails to abide by its obligation despite the first fine, the judge of penal execution will immediately send the documents to the court which rendered electronic information inaccessible in the first instance to "order to render electronic data permanently inaccessible performed by disabling access irrecoverably".

The verdict, which contains the order irreversibly rendering electronic information inaccessible, **can be appealed** against by several parties of the criminal procedure.[35]

3.4. Temporary blocking of unauthorized gambling sites

The state tax authority (National Tax and Custom Administration) shall order the rendering of information published by way of an electronic communications network temporarily inaccessible. The state tax authority shall deliver the resolution on temporarily rendering electronic information inaccessible by way of **public notice**.[36] The public notice shall be posted on the **state tax authority's website** for a period of **fifteen days**.

The decision of the state tax authority is **addressed to all providers of electronic communications services**, without having to indicate them in the decision by name.
The NMIA shall organize and monitor the execution of temporary blocking in accordance with the Act on Electronic Communications.

The state tax authority shall - in order to ensure compliance with the law and for the protection of players - **publish** the name of the website affected by the binding order of temporarily rendering electronic information inaccessible during the period of execution of the measure prescribed in the present subheading.

---

33 The Act refers to the definition of the Act CVIII of 2001 on certain issues of electronic commerce services and information society services. Concerning the Art. 2. (lc) of the cited Act the web hosting provider is - by definition - an intermediary service provider, which stores information supplied by the recipient of the service (hosting).

34 Except the in 2.1. mentioned case of *"Order to render electronic data permanently inaccessible performed by disabling access irrecoverably"* (if an order to (the abovementioned) temporarily prevent to access to data was in effect at the time criminal proceedings terminated and blocking access continues to be justified).

35 Under the Art. 323 (1) of CPA the following parties shall be entitled to lodge an appeal against the verdict of the court of first instance: the accused, the prosecutor, the counsel for the defence, the heir of the accused, the legal representative and the spouse of an accused of legal age, the private party (against a disposition adjudicating a civil claim in its merit, those against whom a disposition has been made in the verdict, in respect of the relevant order.

36 The public notice shall contain:
a) the subject matter and a brief description of the case;
b) the data required for temporarily rendering electronic information inaccessible;
c) information as to the venue and the time when and where the documents of the case are to be made available to the parties concerned for inspection.

The order of the state tax authority is **appealable** within fifteen days after posting the public notice.[37]

3.5. Temporary removal of electronic data concerning fake and unauthorized medicines

The party bound by the obligation imposed by the resolution of the government body for pharmaceuticals (National Institute of Pharmacy and Nutrition) shall be the **service provider**[38] **and intermediary service provider** provided for in the Act on Electronic Commerce and on Information Society Services (for the purposes of this Section hereinafter referred to collectively as "service provider"). The obligated party shall remove the electronic information temporarily within **one working day** from the time of delivery of the decision.

The obligation of temporarily rendering electronic information inaccessible shall cease **ninety days** after the date when ordered.

The government body for pharmaceuticals shall - in order to ensure compliance with the law and for the protection of patients - **publish the name of the website** affected by the binding order of temporarily rendering electronic information inaccessible during the period of execution of the measure prescribed in the present subtitle.

The order of the government body is **not appealable**, but a petition for the **judicial review** of the decision may be lodged at the court of jurisdiction for administrative actions.[39]

3.6. Common rules of Rendering Electronic Published Information Inaccessible Temporarily or Permanently under Act C of 2003 on Electronic Communications

3.6.1. General rules of execution.[40]

Electronic communications service providers functioning as intermediaries of **mere conduit** and **network access services**[41] (hereinafter referred to as "electronic communications service provider of access") shall execute the court order adopted in criminal proceedings, or as ordered by an authority referred to in specific other legislation, **immediately** upon receipt thereof, **at the latest within one working day**, on rendering temporarily or permanently inaccessible information published by way of an electronic communications network , by means of disabling access to such information.

NMIA, if it finds that the electronic communications service provider of access fails to comply with the abovementioned obligation, shall **order** the given service provider to comply with the obligation without delay.

---

37 Under the Art. 7/A of Act XXXIV of 1991 on the Organization of Gambling and Art. 99 (1) of Act CXL of 2004 on the General Rules of Administrative Proceedings and Services.

38 See: footnote no. 26.

39 Art. 26 (6) of Act XCV of 2005 on Medicinal Products for Human Use and on the Amendment of Other Regulations Related to Medicinal Products Art. 109 of Act CXL of 2004 on the General Rules of Administrative Proceedings and Services.

40 Under Art 92/A of Act C of 2003 on Electronic Communications.

41 In accordance with the Act on Electronic Commerce and on Information Society Services, defined above.

If the electronic communications service provider of access refuses to comply despite being ordered to do so, **NMIA shall inform** the court of competence, or the authority of competence referred to in specific other legislation, thereof. The court shall have the option to impose a **disciplinary fine** upon the electronic communications service provider of access in the amount specified in the CPA. The authority referred to in specific other legislation (e.g. National Tax and Custom Administration, National Institute of Pharmacy and Nutrition) shall have the option to impose a **financial penalty** upon the electronic communications service provider of access in the amount specified in said other legislation (See sections 2.1.3., 2.2.4. of this country report).

The electronic communications service provider of access shall **inform the users**, disclosing the name of the court of competence or of the authority of competence referred to in specific other legislation and the number of the ruling, as to the legal basis for disabling access to the content in question temporarily or permanently.

The electronic communications service provider of access shall move to disable access to electronic information temporarily or permanently if so ordered by the court or by the authority referred to in specific other legislation before the time of starting up the provision of services in Hungary.

3.6.2. The NMIA's role in Rendering Electronically Published Information Temporarily or Permanently Inaccessible

NMIA shall arrange and monitor the execution of rendering illegal information published via the electronic communications network temporarily or permanently inaccessible, as ordered in criminal proceedings, or rendering illegal information inaccessible, as ordered by an authority referred to in other specific legislation, and shall, to this end, operate the **central database** of court orders on disabling access to electronic information, and shall cooperate in providing the technical environment necessary for rendering such information inaccessible.[42]

Upon receipt of notice from the court or the authority referred to in specific other legislation by way of electronic means, NMIA shall **communicate exclusively by electronic means** to the electronic communications service providers of access the relevant court order, or the order of the authority referred to in other specific legislation for rendering of electronic information inaccessible.

For this purpose NMIA shall operate the **central database** of rulings on disabling access to electronic information (hereinafter referred to as **"KEHTA"**), and shall process the data entries to that end. **The data contained in the KEHTA are not considered public information**.[43]

3.6.3. Obligations of electronic communications service providers of access.[44]

---

42 Under Art 10 (1) 28. and 159/B of Act C of 2003 on Electronic Communications.

43 It may be accessed only by the courts, public prosecutors, investigating authorities and by members of the competent Parliament committees if rendering electronic information inaccessible temporarily or permanently was ordered by a court or by the authority referred to in specific other legislation. Upon receipt of notice from the court or from the authority referred to in specific other legislation by way of electronic means, NMIA shall record in the KEHTA in the form of an entry:
a) the name of the competent court or the authority referred to in specific other legislation, and the case number;
b) the court order for disabling access to the electronic information, and for restoring access to such information;
c) data for the identification of, and access to, the electronic information in question.

44 Under Art 159/C of Act C of 2003 on Electronic Communications.

Electronic communications service providers of access and providers of browsing and caching services are **required to join the KEHTA** so as to be able to comply with the court order or the order of the authority referred to in other specific legislation on rendering electronic information inaccessible, and for restoring access to such information, and for providing assistance for execution by way of disabling access to the results of any search made in connection with information that has been rendered inaccessible or by way of disabling access to the stored version of such information.

Providers of public Internet access shall not be required to join the KEHTA if connected to the Budapest Internet Exchange (BIX) and to other international internet exchange points exclusively through another electronic communications service provider that has already joined the KEHTA.[45]

Data exchange between the KEHTA and electronic communications service providers of access or providers of browsing and caching services shall take place by way of electronic means, through a secure data link. Electronic communication between the courts or the authority referred to in specific other legislation and NMIA shall take place by means of **secure delivery service**. NMIA shall - to the extent that technical means are available - participate in providing the technical environment necessary for the execution of court orders when so requested by electronic communications service providers of access and providers of browsing and caching services.

NMIA shall **conclude an agreement** with the electronic communications service providers of access and providers of browsing and caching services affected. Within the framework of such cooperation the Authority shall provide access - by way of the methods and under conditions set out in an administrative agreement - for the electronic communications service providers of access and providers of browsing and caching services affected to technical support with facilities for rendering electronic information inaccessible.

NMIA may **publish recommendations** regarding the best practices for the methods of execution of disabling access under this Section, and shall offer assistance to the courts, electronic communications service providers of access, and providers of browsing and caching services for the use of KEHTA.[46]

3.7. Suspend or terminate the conveyance of media services and online press products

This kind of measure can be ordered under the Act CLXXXV of 2010 Art. 188-189. The **Media Council** can order the intermediary service provider[47] to suspend or terminate the conveyance of media services and online press products for any infringement of media regulations if the media service provider[48] fails to fulfil the terms of the executable resolution of the Media Council after it is requested by the Media Council or the Office of NMIA (hereinafter: Office).

---

45 The internet exchange points located in the territory of Hungary, such as the Budapest Internet Exchange (BIX), shall cooperate in carrying out the measures defined in this Section.

46 NMIA has not yet published such a recommendation.

47 See: footnote no. 12.

48 Under the Art 203 (41.) of the Act CLXXXV of 2010 “Media service provider” shall mean the natural or legal person who has editorial responsibility for the choice of the content of the media service and determines the manner in which it is organized. Editorial responsibility means the exercise of effective control both over the selection of the media content and over its organization, and does not necessarily imply any legal liability for the media services provided.

Where the Media Council or the Office applies - in case of linear,[49] on-demand[50] or complementary media services[51], online press products - either of several legal sanctions (impose a fine, order to publish a notice or the resolution on its website, suspend the exercise of the right to provide media services for a specific period of time)[52] against a media service provider or the publisher of press products, and it fails to fulfil the terms of the final and executable resolution on the relevant legal sanction when so requested by the Media Council or the Office, the intermediary service provider may be ordered to suspend the intermediation of the linear, on-demand or complementary media services or the press product to which the official resolution on the relevant legal sanction pertains, based on the official resolution issued by the Media Council in regulatory proceedings conducted ex officio.[53]

The time period required for the termination of suspension by the broadcaster or intermediary service provider may not exceed **fifteen days**, covering also the notification of the broadcaster or intermediary service provider by the Media Council.

No appeal can be lodged against the resolution of the Media Council. **The client may request to have the resolution reviewed** - alleging infringement of the law - **at a court** of jurisdiction for administrative actions within **fifteen days** of delivery of the official resolution. The court shall adopt a decision in non-contentious proceedings, upon hearing the parties if necessary, within fifteen days. Lodging a petition for non-contentious proceedings shall have no suspensory effect on the enforcement of the resolution. Suspension of the execution of the official resolution contested may not be requested from the court, and the court has no jurisdiction to order such a suspension. The resolution shall be executable with immediate effect, irrespective of the submission of a petition for non-contentious proceedings.

The provisions of suspension and termination shall not apply in respect of the suspension of enforcement requested in the petition for judicial review of the official resolution on the legal sanctions, until the court's decision in the first instance is delivered; moreover, they shall not apply until the final conclusion of the related administrative action if the court has suspended the execution of the official resolution on the said legal sanctions.

3.8. Notice and take down procedure

The procedural rules are exhaustively examined in 2.2.3.

---

49 Under the Art 203 (36.) of the Act CLXXXV of 2010 "**Linear media service**" shall mean a media service provided by a media service provider for simultaneous viewing of or listening to programs on the basis of a program schedule.

50 Under the Art 203 (35.) of the Act CLXXXV of 2010 "**On-demand media service**" shall mean a media service provided by a media service provider for the viewing of or listening to programs at the moment chosen by the user and at his individual request on the basis of a catalogue of programs selected by the media service provider.

51 Under the Art 203 (23.) of the Act CLXXXV of 2010 "**Complementary media services**" shall mean all services involving content provision, which are disseminated through a broadcast transmission system, other than media services or electronic communications services. Complementary media services shall, for example, cover electronic program guides.

52 Defined in Art. 187 (3) b)-d) of the Act CLXXXV of 2010.

53 Under the Art 189 (5) the Act CLXXXV of 2010 the resolutions shall specify the procedure and the conditions of termination and suspension, a reasonable deadline for compliance, the duration of termination or suspension, as well as the bearing of the costs the broadcaster or the intermediary service provider has incurred in connection with the termination or suspension of the dissemination or transmission of the media services, or with the intermediation of the press product, including any compensation.

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?

Hungary does not have an entity in charge of general monitoring of Internet content.

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

As for the primary legislation, the Hungarian law in this area actually fits the requirements of "quality of the law". This area is regulated in several Acts, found at the highest level of legal source. Therefore these Acts are obviously **accessible** (enacted, published) and they are **sufficiently clear and precise** to be **foreseeable** in their application. If we scrutinise the application of these legal measures, it can be stated that this field has been recently regulated. Therefore the relevant case law is absent or not yet reported. The **coercive measures of the CPA** (sections 2.1.1.-2.1.2., 2.2.1. of this country report) concerning blocking and filtering, and the **measure of CC** (2.2.2.) concerning removal are subjected to the principles of constitutional criminal law (e.g. nullum crimen sine lege, nulla poena sine lege, proportionality etc.) and criminal procedural law (e.g. right to a fair trial, officiality, the principle of accusation, rights of the defence, right to appeal etc.). Art. 10 (2) of ECHR meets the requirements and conditions specified in section 2.1.1 of this country report. The system of temporary and permanent blocking has been established as a graduated and coherent system. The only **critical point** of the regulation could be the general character of irreversible removal (see 2.2.2 of this country report), which can be applied for every crime (but as I have mentioned in 2.2.2, there is no relevant case law behind this Article). It should be emphasised that the abovementioned measures shall only be ordered by the **court** (which can be a **safeguard** of the protection of human rights).

Hungary regulates the **notice and take down** procedure in details concerning infringements of intellectual property rights and personal rights of minor. This is an important fact because of the following. Directive 2000/31/EC and the Act CVIII pf 2001 on certain issues of electronic commerce services and information society services deal with the liability of service providers. The Directive and the Hungarian Act state that the service provider is not liable for the information stored if it does not have actual knowledge of illegal activity or information, or upon obtaining such knowledge, acts expeditiously to remove or to disable access to the information; hence the notice and take down procedure absolves the service provider from liability. The service provider, after receiving the request of removal does not have any discretion; whether the infringement is real or not, it shall disable access to or remove of the information identified in the notice within 12 hours.[54] There is obviously a temporary (or without an objection: permanent) disabling or removal **without any court order**, which can last days (depends on the existence of an objection, request of injunction; see 2.2.3 of this country report), and it is **based only on the request of the rights holder**. This raises the possibility of an **abuse of rights** and the take down of non-infringing content. The Hungarian Act does not contain such a **misrepresentation clause**[55] as, for example, the Digital Millennium Copyright Act, which could provide a solution for this situation.[56]

---

54 Kőhidi, A polgári jogi felelősség.., *op. cit.*, p. 103., p. 166.

55 DMCA Art. 512. (f) „Misrepresentations": any person who knowingly materially misrepresents…that material or activity is infringing…shall be liable or any damages, including costs and attorneys' fees…"

56 P. Mezei, Digitális Sampling és fájlcsere, Szeged: Szegedi Tudományegyetem Állam- és Jogtudományi kar 2010, p. 217-218.

The civil liability of intermediaries and the collision of the personality rights of others (right to reputation) and freedom of expression concerning infringing comments have been examined by the Constitutional Court of Hungary, which dealt with the liability question of the intermediary service provider for unmoderated and infringing comments in the decision No. 19/2014. (V.30.). The owner of the site cited Art 2 (lc) of the Act CVIII of 2001, was deemed to be an intermediary service provider (especially web hosting provider), as he only stored information supplied by others in this case. Therefore he is not liable for the infringing content of the comments of third parties. The abovementioned Act states[57] that an intermediary service provider **does not have a general obligation to monitor** the information which it transmits or stores, nor a general obligation actively to seek facts or circumstances indicating illegal activity. Hence, in his opinion, it can be applied to his status, as a comment can be disclosed without any permission, control or intervention on these kinds of sites (which contain blog parts as well). In a previous section of the case, the Supreme Court of Hungary (Curia) held that the comments are private disclosures and the owner of the site is liable, because he should have counted on the risk of disclosing illegal content by third parties if these kind of comments were made available to post without any control. The owner of the site filed a constitutional complaint against the decision of the Curia at the Constitutional Court. The decision of the Court was fundamental concerning the limits of the freedom of expression (and freedom of press) on the Internet. The Constitutional Court stated correctly that in the case of several internet activities the categories of intermediary services might be cumulative (in the case of sites containing own content and content of third parties as well), and the comments are not private disclosures; accordingly, the E-Commerce Directive and the implementing Act should be applied. However, the Constitutional Court qualified this kind of site as an online press product, and cited its former case law concerning freedom of press, and declined the exculpation clauses concerning the liability based on the E-Commerce Directive. The Court considered the possible liability as a constitutionally **legitimate aim** (protection of personality rights) of limitation of freedom of expression which **suits the requirement of proportionality**, and stated that **the liability of intermediaries is verified in the constitutional sense** (except in the case of certain sites, e.g.: Facebook, mere blog sites, because these do not have an editor). In my opinion the verification of liability for such cases is not the most moderate measure; the Constitutional Court did not take the notice and take down procedure into account, which is a much more proportional and moderate measure before the liability (and damages).[58] This opinion can be underpinned by the decision of Court of Appeal of Pécs from 2013,[59] in which the Court stated: "the owner of the website (as an intermediary service provider) shall be liable for the comments (infringing right to reputation) disclosed by third party only in the case if upon obtaining knowledge or awareness of illegal activity does not act expeditiously to remove the content." The decision of Constitutional Court held up the risk of liability of intermediary service providers for unmoderated content, which might infringe other rights (as soon as the comment is disclosed), thus evidently making the operation of these sites (which contain comments or blog elements) much more risky.

The temporal removal of electronic data under **Medicines Act** (2.2.4) and temporary blocking of **unauthorized gambling sites** (2.1.3.) can be ordered by **authorities**, but it can be appealed against or reviewed by court. In my opinion, such measures do not interfere with Human Rights (in the case of medicine its aim is protecting health, which suits Art 10 (2) of ECHR), rather than the freedom to provide services (but neither of them have been tested by the ECJ) in the case of gambling sites.

---

57 Art 7 (3) of Act CVIII of 2001 and Art 15 (1.) of Directive 2000/31/EC.

58 This argument can be found in the minority report of István Stumpf, member of the Constitutional Court. See: http://public.mkab.hu/dev/dontesek.nsf/0/4E4D071867671629C1257B0C00212E7F?OpenDocument (79-93.)

59 Pf.VI.20.776/2012/5. (March of 2013).

As a safeguard to prevent abuse of power and arbitrariness the right to appeal or for judicial review should be mentioned in all abovementioned cases, and the existence of the **central database** ("KEHTA") in which NMIA can record the relevant obligations of electronic communication providers; hence NMIA is able to **organize and supervise** the execution of orders, and remove the obligation from the database if the court lifts it. NMIA notifies the courts immediately of any failure by an electronic communications provider to ensure access once again.

As for the suspension or termination of the conveyance of **media services and online press products** under Media Act, it is questionable that the Media Council can apply this measure **for any infringement**[60] of media regulations;[61] however, there are procedural preconditions: if the media service provider fails to fulfil the terms of the executable resolution of the Media Council after it is requested by the Media Council or the Office of NMIA, the suspension or termination can be applied as **"ultima ratio"**[62] and relevant safeguards can be examined: **the time period of the suspension** of dissemination or broadcasting must be **proportionate** to the **weight or gravity of the underlying legal sanction**, etc. (see: 2.1.4.)[63] It is worth noting that the authorities' right of discretion is subjected to constitutional requirements as well (empowered by the law, respect the limits of discretion, duty of reasoning).[64] It is also worth noting that there are no orders issued by the Media Council, so it can be stated there is not yet any relevant case law concerning the suspension or the termination of the conveyance of media services and online press products.[65]

The abovementioned interferences are deemed **"necessary in a democratic society" and proportional** – except the blocking of unauthorized gambling sites –; from my point of view, all of these can be traced back to the Art. 10 (2) of ECHR. The only exception might be the aforementioned decision of Constitutional Court of Hungary. It might actually induce future case law of lower courts,[66] which set the limits of freedom of expression – establishing the liability of intermediaries – under a questionable proportionality test; however, the Grand Chamber of the European Court of Human Rights found the liability of the host provider in the similar Delfi case justified and proportionate.[67]

---

60 However, the Act defines the concept of "media regulation" under Art 203. (39.): ">>Media regulations<< shall mean this Act and Act CIV of 2010 on Freedom of the Press and on the Basic Rules Relating to Media Content, and any legislation published in respect of the implementation of the aforementioned acts, any directly applicable legislation of the European Union concerning the media, any broadcasting agreement, any administrative agreement entered into by and between the Media Council and the Office, and the resolutions adopted by the Media Council or the Office." See also: A. Koltay & A. Lapsánszky, Az új magyar médiaszabályozás alkotmányossági kérdései, 2011 (2) IAS p. 31 et seq, p. 121-123.

61 The concept of „media regulation" is regarded as ambiguous by some. See: G. Polyák: Végképp eltörölni – Adatszűrés és blokkolás a magyar jogban. http://www.jogiforum.hu/mediajog/108 (11.08.15)

62 See also: Koltay & Lapsánszky, Az új magyar médiaszabályozás.., *op. cit*., p. 123-126.

63 A. Lapsánszky: A médiaigazgatás szankciórendszere, in A. Koltay & L. Nyakas (eds.), Magyar és európai médiajog, Budapest 2012, p. 815 et seq, p. 830-831.

64 Koltay & Lapsánszky, Az új magyar médiaszabályozás.., *op. cit*., p. 116.

65 This information has been received after a particular request for information concerning this measure.

66 Several debated court decisions can be found before the cited decision of the Constitutional Court of Hungary as well, since approximately 2010 some courts have accepted the concept of host liability, notwithstanding the exclusion clause of the E-Commerce Act. See also: P. Nádori, Kommentek a magyar interneten: a polgári jogi gyakorlat, 2012 (2) In Medias Res. http://www.media-tudomany.hu/laparchivum.php?ref=28 (22.09.15).

67 Case of Delfi AS vs Estonia (64569/09), Final Judgement of the ECtHR, on 16.06. 2015. http://hudoc.echr.
coe.int/eng?i=001-155105 (22.09.15).

As **the relevant case-law** in Hungary is **not remarkable** (the only statistical data can be found in a few fields, concerning in particular the blocking of unauthorized gambling sites) it cannot be determined whether it is in line with the pertinent case law of the European Court of Human Rights.

Ákos Kőhidi[68]
14.08.15

[68] Senior lecturer, Széchenyi István University (Győr), attorney at law. **I would like my name to appear at delivery.**