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 410-424

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.

LITHUANIA

1. Legal Sources

Blocking, filtering and take-down of illegal internet content is partially regulated in Lithuania. There are only a few specific content regulations for the Internet in Lithuania mostly covering issues related to take-down of illegal internet content. For the most part, existing regulation is fragmented over various areas of law. A significant part of applicable legal provisions are not specific to the Internet.

A number of international conventions relating to illegal internet content have been transposed into the domestic Lithuanian regulatory framework. These conventions are:

The Council of Europe Convention on Cybercrime of 2001 and its Additional Protocol of 2003, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems;

- The United Nations International Convention on the Elimination of All Forms of Racial Discrimination of 1969;
- The Council of Europe Convention on the Prevention of Terrorism of 2005;
- The Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse of 2007;
- The United Nations Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography of 2000;
- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 1981.

The main statutory and legislative sources that permit or allow for the blocking, filtering and take-down of illegal internet content in Lithuania are as follows:

- The Constitution of Lithuania[1] which is on the top of the hierarchy of the Lithuanian law and prohibits seizure of government and its institutions,[2] grants the right to privacy,[3] prohibits degrading of humans,[4] grants freedom of expression,[5] prohibits discrimination based on sex, race, nationality, origin, social status, religion, beliefs or views,[6] grants protection to children;[7]
- The above-mentioned international agreements ratified by Lithuania;
- The applicable EU law, in particular the EU Directive on electronic commerce 2000/31/EC;
- The Civil Code[8] which establishes protection of commercial secrets,[9] privacy,[10] against defamation,[11] as well as rules of civil liability,[12] including general diligence standard applicable to anyone;[13]

---

1 The Constitution of the Republic of Lithuania. *Lietuvos Aidas*, Nr. 220; 1992, Nr. 33-1014.
2 Ibid., Article 8.
3 Ibid., Article 22.
4 Ibid., Article 21.
5 Ibid., Article 25.
6 Ibid., Article 29.
7 Ibid., Articles 38 and 39.
8 The Civil Code of the Republic of Lithuania. *Valstybės žinios*, 2000, Nr. 74-2262.
9 Ibid., Article 1.116.
10 Ibid., Articles 2.20-2.23.
11 Ibid., Article 2.24.
12 Ibid., Article 6.245-6.255.
13 Ibid., Article 6.246(1).

- The Criminal Code[14] which establishes criminal liability for public incitement to break the sovereignty or territorial integrity of Lithuania,[15] racist content, xenophobic and hate speech,[16] denial of Holocaust and international crimes, including those committed by the USSR or Nazi Germany against Lithuania,[17] inciting of terrorism,[18] dissemination of pornographic materials, including child pornography,[19] piracy,[20] libel,[21] disclosure of private information[22] or state secrets;[23]
- The Civil Procedure Code[24] which enables courts to issue any sort of injunction as both interim measures[25] and final decisions, [26] as well as rules for allocation of costs incurred by parties in legal proceedings;[27]
- The Law on Provision of Information to the Public[28] that sets forth which information cannot be published in mass media;[29]

  The Law on the Protection of Minors Against the Detrimental Effect of Public Information[30] that sets out the nature of information that cannot be made available to minors, unless marked with indications of target audience;[31] this law also requires internet providers to install and operate, at access points to the Internet, measures for filtering harmful content having a detrimental effect on minors;[32]
- The Law on Information Society Services[33] that determines circumstances under which providers of e-commerce services become liable for information transmitted or stored on behalf of users,[34] as well as sets forth a take-down obligation;[35]
- The Law on Copyright and Related Rights[36] which grants protection of copyright;[37]
- The Procedure for the Control of Forbidden Information on Public Use Computer Networks and the Distribution of Restricted Public Information[38] (the "Internet Information Regulation") which prohibits publishing and distributing unlawful information on the Internet (Article 5) and directs hosting service providers and internet service providers to terminate access to the information

---

14 The Criminal Code of the Republic of Lithuania. *Valstybės žinios*, 2000, Nr. 89-2471.
15 Ibid., Article 114.
16 Ibid., Articles 169, 170 and 170^1.
17 Ibid., Article 170^2.
18 Ibid., Article 250^1.
19 Ibid., Article 309.
20 Ibid., Article 192.
21 Ibid., Article 154.
22 Ibid., Article 168.
23 Ibid., Article 125.
24 The Civil Procedure Code of the Republic of Lithuania. *Valstybės žinios*, 2000, Nr. 36-1340.
25 Ibid., Articles 145(1)(6), 145(1)(12) and 145(1)(13).
26 Ibid., Articles 265 and 273.
27 Ibid., Article 93.
28 The Law on Provision of Information to the Public of the Republic of Lithuania. *Valstybės žinios*, 1996, Nr. 71-1706; 2006, Nr. 82-3254.
29 Ibid., Articles 13, 14, 17, 19.
30 The Law on the Protection of Minors against the Detrimental Effect of Public Information of the Republic of Lithuania. *Valstybės žinios*, 2002, Nr. 91-3890; 2009, Nr. 86-3637.
31 Ibid., Articles 4 and 7.
32 Ibid., Article 7(3).
33 The Law on Information Society Services of the Republic of Lithuania. *Valstybės žinios*, 2006, Nr. 65-2380.
34 Ibid., Articles 12-14.
35 Ibid., Article 15(3).
36 The Law on Copyright and Related Rights of the Republic of Lithuania. *Valstybės žinios*, 1999, Nr. 50-1598; 2003, Nr. 28-1125.
37 Ibid., Article 77 in particular.
38 Adopted by Order No 290 of 5 March 2003 of the Government of the Republic of Lithuania.

stored on servers (1) upon court orders or (2) once providers become aware that illegal information is stored on their servers, and if the termination of access is technically possible;[39]

- The Description of the Procedure for Terminating Possibility to Access Unlawfully Acquired, Created, Modified or Used Information[40] (the "Access Termination Procedure") which determines when internet intermediaries are considered to be aware of unlawful content which they store on behalf of customers for the purposes of the gauging liability.

2. Legal Framework

2.1. Blocking and/or filtering of illegal Internet content

A result of a lack of comprehensive regulation, there is no exhaustive statutory list of grounds that may lead to blocking and/or filtering. In general, one can request for blocking and / or filtering of any information that violates any Lithuanian law. Possible grounds for blocking and/or filtering of illegal internet content could include:

- The protection of national security, territorial integrity or public safety;[41]
- The prevention of racist content, xenophobic and hate speech;[42]
- The prohibition of pornography, including child pornography;[43]
- The prohibition of promotion of adult services and sexual perversion;[44]
- The prohibition of defamation;[45]
- Privacy[46] and personal data;[47]
- Health;[48]
- The protection of state secrets;[49]
- The presumption of innocence and impartiality of judiciary;[50]
- Children's interests;[51]
- Intellectual property rights;[52]
- The confidentiality of information;[53]

---

39 Ibid., Article 14.

40 Adopted by Order No 881 of 22 August 2007 of the Government of the Republic of Lithuania.

41 In relation to Article 122 of the Criminal Code, Articles 19(1)(1) and 19(1()(2) of the Law on Provision of Information to the Public.

42 In relation to Articles 169, 170 and 170[1] of the Criminal Code, Article 19(1()(3) of the Law on Provision of Information to the Public.

43 In relation to Article 309 of the Criminal Code and Article 19(1()(4) of the Law on Provision of Information to the Public.

44 In relation to Article 19(1()(4) of the Law on Provision of Information to the Public.

45 In relation to Article 154 of the Criminal Code, Article 2.24 of Civil Code and Article 19(2) of the Law on Provision of Information to the Public.

46 In relation to Articles 2.20-2.23 of the Civil Code, Articles 13-14 of the Law on Provision of Information to the Public, Article 168 of the Criminal Code.

47 In relation to the Law on Legal Protection of Personal Data of the Republic of Lithuania. *Valstybės žinios*, 1996, Nr. 63-1479; 2000, Nr. 64-1924; 2003, Nr. 15-597; 2008, Nr. 22-804.

48 In relation to Article 19(1)(5) of the Law on Provision of Information to the Public.

49 In relation to Article 125 of the Criminal Code, Article 5 of the Internet Information Regulation.

50 In relation to Article 19(3) of the Law on Provision of Information to the Public.

51 In relation to Article 4 of the Law on the Protection of Minors Against the Detrimental Effect of Public Information.

52 In relation to Article 192 of the Criminal Code, Article 77 of the Law on Copyright and Related Rights.

53 In relation to Article 1.116 of the Civil Code.

- The compliance with gambling regulation;[54]
- Any other interests protected by Lithuanian laws that could be violated by illegal internet content.[55]

Another consequence of a lack of comprehensive regulation is that there are no specific requirements to be fulfilled or safeguards to be followed for blocking and/or filtering. Conditions relating to blocking and/or filtering of illegal internet content can be imposed by way of an interim measure in civil proceedings or a final decision in civil proceedings, subject to general requirements of the Civil Procedure Law of Lithuania

Internet content can be blocked by way of an interim measures under general provisions of the Civil Procedure Code: prohibition for a defendant to take certain actions,[56] obligation to take actions preventing damages or increase thereof[57] or any other measure necessary to ensure enforceability of future final court decisions.[58] A party requesting for such blocking bears a general burden to prove that such an action is necessary and a court can pass such an order *ex officio* only where required by public interest.[59] Any blocking of internet content would have to be in compliance with general principles and safeguards applicable to interim measures, such as principles of economy,[60] equity, proportionality, balance of interests and protection of public interest (as established in the Lithuanian case law).

If requested by parties, blocking of internet content can also be the result of a final decision under general provisions of the Lithuanian Civil Procedure Code, which obliges a court to resolve all of requests presented by parties[61] and entitles a court to oblige a defendant to perform certain actions or cease certain actions.[62] In a final decision in civil proceedings, blocking of internet content can be permitted if the plaintiffs met their burden of proof and demonstrated that such action was necessary.[63]

As a matter of general procedure, a copy of a request for blocking of internet content injunction is forwarded to a defendant, as well as third parties to the case, who are granted a period to file their responses.[64] As any final decision, the decision to block internet content would have to be lawful, reasoned and based on the circumstances of the case.[65] Blocking of internet content would have to be in compliance with general principles and safeguards applicable to final decisions, such as principles of economy,[66] equity, proportionality, balance of interests and protection of public interest (as established in the Lithuanian case law).

Interim measures in civil proceedings such as the obligation to take actions preventing damages or increase thereof[67] or other measures necessary to ensure enforceability of future final court

---

54 In relation to the Law on Gambling of the Republic of Lithuania. *Valstybės žinios*, 2001, Nr. 43-1495.
55 In relation to, *inter alia*, Article 5 of the Internet Information Regulation.
56 Article 145(1)(6) of the Civil Procedure Code.
57 Ibid., Article 145(1)(12).
58 Ibid., Article 145(1)(13).
59 Ibid., Article 145(1).
60 Ibid., Article 145(2).
61 Ibid., Article 265.
62 Ibid., Article 273.
63 Ibid., Article 178.
64 Ibid., Article 142(1).
65 Ibid., Article 263.
66 Ibid., Article 7.
67 Ibid., Article 145(1)(12).

decisions[68] can be imposed on any natural and legal persons, not only parties to the proceedings. Thus, internet access providers are fully exposed to internet filtering orders that arise from interim measures in civil proceedings, as illustrated by the case law cited below. For an internet blocking order to be imposed on an internet access provider arising from a final decision in the civil proceedings, it must be determined that the provider is a proper defendant that committed a violation of laws, a contract or a general obligation to act diligently.[69]

There are no notable soft-law instruments in this field in Lithuania.

The Lithuanian courts have not developed extensive case law on blocking and/or filtering of internet content. The most notable internet content blocking case to date is *Association Alliance of Betting Operators, UAB TopSport & UAB Orakulas v. bwin International Ltd., Unibet International Ltd., et al*., where Lithuanian betting operators sought to prohibit major foreign online betting companies from providing online betting services to the Lithuanian market in absence of betting licenses issued by the Lithuanian regulator. The Vilnius County Court adopted an interim measure requested by plaintiffs and prohibited all possible access to the defendants' websites from Lithuania, thus, imposing an obligation to block certain internet content without specifying whom this obligation applied to.[70]

The Lithuanian Court of Appeals upheld this interim measure.[71] The Vilnius County Court confirmed its previous decision noting that the obligation applied to all persons providing access to the defendants' websites in Lithuania.[72] All major Lithuanian internet service providers were included in the case as third parties. The Lithuanian Court of Appeals upheld the decision of the Vilnius County Court and, in additional, rejected the internet service providers' request to refer the case to the Constitutional Court regarding the alleged unconstitutionality of the provisions of the Code of Civil Procedure based on which the blocking obligation was imposed.[73] However, the Vilnius County Court *ex officio* cancelled the internet blocking obligation noting that such measure was excessive and disproportionate, since Lithuanian users can be prevented from accessing the defendants' websites by imposing obligations on defendants themselves (i.e. obligation not to allow the Lithuanian users to use their websites), not internet service providers.[74] The Lithuanian Court of Appeals upheld the said decision, noting that technic inefficiency and implying that it was costly and can violate users' privacy and freedom of information.[75]

Another noteworthy attempt to impose an obligation to block internet content, although in a very different context, was examined by the Lithuanian Supreme Administrative Court in 2012.[76] The Lithuanian State Gaming Supervisory Commission initiated administrative liability proceedings against one of the heads of an internet service provider, holding that he violated a prohibition of gambling advertising by not blocking access from Lithuania to foreign online betting sites containing advertisements that violate Lithuanian laws, although such blocking was technically possible. The Vilnius City 1st District Court terminated the case stating that the defendant did not take any actions related to dissemination of unlawful betting advertising. The Supreme Administrative Court upheld

68 Ibid., Article 145(1)(13).
69 Article 6.246 of the Civil Code.
70 Decision of 2010-07-02 in Case No 2-6458-578/2010.
71 Decision of 2010-12-30 in Case No 2-1585/2010.
72 Decision of 2011-03-10 in Case No 2-2961-823/2011.
73 Decision of 2011-07-14 in Case No 2-1579/2011.
74 Decision of 2011-08-18.
75 Decision of 2011-12-27 in Case No 2-2534/2011.
76 Decision of 2012-12-05 in Case No N575-641/2012.

the said position, noting that Lithuanians laws do not oblige internet service providers to terminate access to information that is hosted on foreign networks.

2.2. Take-down/removal of illegal Internet content

There is also a lack of comprehensive regulation with respect to take-down/removal of illegal internet content. In this case too, there is no exhaustive statutory list of grounds that may lead to take-down/removal. Internet host providers and other internet intermediaries can become liable for any unlawful information if they do not take it down.[77] Persons whose rights are violated by the unlawful internet content hosted or transmitted by internet intermediaries can request a court to issue an injunction against the host to terminate or prevent violation, *i.e.* to take-down, notwithstanding whether or not the host is liable for that unlawful internet content.[78] In general, one can request for take-down/removal of any information that violates any Lithuanian laws. Thus, theoretically it is possible that the grounds for take-down/removal of illegal Internet content could be the same as for blocking and/or filtering, as set out above.

The Access Termination Procedure outlines the specific procedure for taking-down information, narrows the scope of unlawful information to the information violating the Lithuanian Law on Provision of Information to the Public and intellectual property laws. Thus, civil liability can only be imposed on internet intermediaries for the content they host or transmit, or, certain take-down/removal procedure used subject to the grounds set out in the response to Question 2.1 above.

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 is defined by national statutory provisions implementing the EU Directive on electronic commerce 2000/31/EC.

The Information Society Services Law[79] establishes safe harbours for hosts caching the information: the host is not liable for the transmitted information as long as it:

1) does not modify the information;
2) complies with the terms of access to the information;
3) complies with the rules regarding the updating of information, specified in a manner widely recognized and used by industry;
4) does not interfere with the lawful use of technology, widely recognized and used by industry, to obtain data on the use of the information;
5) acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been disabled, or that a court or an administrative authority has ordered such removal or disablement.

The Information Society Services Law[80] and the Internet Information Regulation[81] establish safe harbours for hosts of information: the host is not liable for the information hosted on behalf of the customer as long as it:

1) does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of the facts or circumstances which prove the existence of illegal activity or information;

---

77 Articles 13 and 14 of the Information Society Services Law.

78 Article 15(3) of the Law on Information Society Services.

79 Ibid., Article 13.

80 Ibid., Article 14(1).

81 Ibid., Article 12.

2) upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

Any person or institution can file a detailed complaint of a regulated content to the host regarding the unlawful information.[82] Within 3 business days of the notification, the host must determine whether it indeed stores the notified information and whether the notification complies with the requirements thereto and, if so, to request within 1 more business day the customer owning the information to provide a response to the notification. If the owner of the information does not agree with the complaint, it must provide the host with a detailed response of regulated content[83] within 3 business days. In absence of the information owner's reply, the host must take down the unlawful information within 1business day following the expiry of the deadline for filing a reply and inform both the complainant and the information owner accordingly.[84] If the host determines that the information owner's reply is reasonable, it shall not terminate the access to the unlawful information and inform both the complainant and the information owner accordingly.[85] In case the host has any doubts regarding the reply provided by the information owner, the host can refer the matter to a competent state authority.[86] If the information owner's response does not comply with the requirements thereto, the information owner should be given an opportunity to rectify the non-compliance.[87] If the host determines that the reply by the information owner is not reasonable, the host must terminate, within 1 business day from the assessment of the reply, the access to the unlawful information and inform both parties accordingly.[88] If the host is not able to determine the identity of the information owner without incurring unreasonable costs, the host must determine itself whether the complaint is reasonable and, if so, terminate the access to the unlawful information under analogous procedure.[89]

The host is considered to be aware of the unlawful content if (1) it does not receive a proper reply from the information owner or determines that such answer is not reasonable; or (2) it is not able to determine the identity of the information owner, determines that the complaint is reasonable or fails to take any decision regarding the complaint in a timely manner; or (3) receives the notification from the competent authority and determines that it stores the information in question.[90]

In any case a person can make a request for the take-down/removal of illegal internet content before a court as a matter of injunction or a final court decision under the requirements of the Lithuanian civil procedure law as discussed earlier.[91]

In addition, pursuant to the Lithuanian laws, almost all governmental supervisory agencies are broadly entitled to issue mandatory orders to cease unlawful activities in their areas of competence. Functions and roles of these agencies vary significantly: from regulating a specific industrial sector, like the Inspector of Journalist Ethics (in charge of mass media's compliance with the Lithuanian Law on Provision of Information to the Public), the Bank of Lithuania (in charge of supervision of financial markets, including advertising of financial services), Lithuanian Drug, Tobacco and Alcohol Control Authority (tobacco and alcohol sectors, including alcohol and tobacco advertising), Lithuanian

82 Ibid., Articles 3-7.
83 Article 8 of the Access Termination Procedure.
84 Ibid., Article 9.
85 Ibid., Article 10.
86 Ibid., Article 11.
87 Ibid., Article 12.
88 Ibid., Article 13.
89 Ibid., Articles 15-19.
90 Ibid., Article 22.
91 Article 15(3) of the Law on Information Society Services.

Gambling Supervision Authority (gambling, including advertising of gambling), to regulating compliance of all sectors with one specific law, like the State Data Protection Inspectorate (compliance of data processing), Lithuanian Competition Council (competition law compliance, unfair competition, misleading and unpermitted comparative advertising), State Consumer Rights Protection Authority (consumer rights and unfair trading practices). Thus, it is possible for such supervisory authorities to also issue mandatory orders to take down content that violates requirements of Lithuanian laws. Such requests would have to comply with the general procedural regulations of these authorities as well as general requirements for administrative decisions, including the requirement to make a decision based on facts and statutory provisions, define the rights and obligations of persons, provide for grounds and appeal procedure, put a signature and a stamp on a document.[92]

There are no notable soft-law instruments in this field in Lithuania.

In the notable case *UAB Vedautos autotransportas v. S. G.*[93] the Lithuanian Supreme Court elaborated on obligations that an administrator of a website against whom a complaint had been made, to take down content allegedly defaming a company. Extensively citing the case law of the European Court of Human Rights and *Delfi* v. *Estonia* case in particular (the Chamber's judgement), the court held that online complaints pose great business risks, therefore, a higher diligence standard applies to hosts of such comments. The court stated that the host enabled anonymous comments, therefore, is subject to certain liability therefor. According to the court, the plaintiff cannot be requested to prove that anonymous complaints are false. On the contrary, the host must ground any refusal to take down the information or be requested to prove the accuracy of complaints. Pursuant to the court's decision, a general exercise of balancing freedom of information against protection of reputation shall be completed in order to determine that specific information is provided as a defamatory fact rather than opinion and, thus, should be taken-down. As the Lithuanian Supreme Court concluded that the court of lower instance had failed to conduct the said balancing exercise properly, the court of lower instance was ordered to re-examine the take down request.

In another notable Case *R. O., et al. v. UAB Interneto Vizija and A. U*.[94] the Supreme Court clarified the scope of the obligation of a blog owner to take-down the information posted on the blog and defaming the plaintiffs. The court noted that the hosts were not obliged to monitor the information they stored, however, they had to take actions upon receiving a notice on the unlawful information. The court dismissed the blog owner's arguments that he was not obligated to do so and was incompetent to assess lawfulness of the information at stake. The court cited the EUCJ's case *L'Oréal SA and Others v eBay International AG and Others* (C-324/09) to note that it is important whether a diligent economic operator should have identified the illegality. Since the blog owner did not respond to the "sufficiently informed" notice by the plaintiff under the Access Termination Procedure, the Supreme Court concluded that the courts of lower instance were right to impose civil liability on the blog owner for the defamatory posts.

In another notable Case *J. K. and UAB CAN2 FASHION v. S. G.*[95] the Supreme Court separated and clarified the nature of take-down obligations and the Access Termination Procedure. The court noted that in order to satisfy a requirement to take down illegal internet content stored or transmitted by an internet intermediary, three circumstances have to be determined: (1) illegality of the information; (2) the fact that the information at stake is stored or transmitted; and (3) the fact that a

---

92 Article 8 of the Law on Public Administration of the Republic of Lithuania. Valstybės žinios, 1999, Nr. 60-1945; 2006, Nr. 77-2975.

93 Decision of 19 February 2014 in Case *UAB Vedautos autotransportas v. S. G.* (No 3K-3-30/2014).

94 Decision of 27 February 2014 in Case *R. O., et al. v. UAB Interneto Vizija and A. U*. (No 3K-3-49/2013).

95 Decision of 21 December 2012 in Case *J. K. and UAB CAN2 FASHION v. S. G.* (No 3K-3-586/2012).

defendant is an internet intermediary. The internet intermediary can be obligated to take down the unlawful internet content notwithstanding whether or not it actively monitored the internet content, whether it acted in compliance with the Access Termination Procedure, irrespective of who the owner of the internet content is and what is the owner's opinion regarding the take-down request. As noted by the court, the Access Termination Procedure does not provide for mandatory pre-trial procedure for settling disputes regarding the unlawful internet content and is applicable when determining the awareness of the internet intermediaries' liability and, accordingly, their liability for the illegal internet content, and not when imposing take-down obligations.

Another noteworthy case is *Microsoft Corporation v. UAB N5 & K. E.*[96] In this case the claimant requested that a court prohibit the defendant who operated the major Lithuanian torrent website from providing intermediary services to persons who download, via the website, unlawful copies of the plaintiff's software. The Vilnius County Court satisfied the said request stating that the defendants indirectly, knowingly and publicly reproduced the plaintiff's software and thus, violated the Law on Copyright and Related Rights and a diligence standard applicable thereto. The said decision was annulled and the case was closed at the Lithuanian Court of Appeals by way of a settlement agreement between the parties, terms of which are not publicly available.

3. Procedural Aspects

No specific bodies have been granted authority to take decisions regarding blocking, filtering and take-down of illegal internet content in Lithuania. Thus, it is mostly for the judiciary to take such decisions, both as interim measures and as final decisions issued under the general requirements of the Lithuanian civil procedure law overviewed in the answer to Question 2.1 above.

There is no specific procedure for implementing judicial decisions on blocking, filtering and take-down of illegal internet content in Lithuania. Thus, the final judicial decisions on blocking, filtering and take-down of illegal internet content areimplemented under the general procedure set forth by the Civil Procedure Code. A decision issued by a court of the first instance would become binding upon the parties concerned following the expiry of the appeal period, if the decision is not appealed against.[97] Certified copies of the court's decision are handed to the parties present in a hearing and, within the following three days, are sent to all of the other parties to the case.[98]

An appeal against the decision that has not come into effect can be lodged with a court of a higher instance within 30 days following the issuance of the decision[99] by any party to the case.[100] In the appeal proceedings, courts review the lawfulness and reasonableness of a decision and can annul the decision if it was issued in material procedural violation,[101] substantial laws were interpreted or applied inappropriately[102] or the essence of a case was not disclosed.[103] In case the decision is appealed against and not annulled, it immediately becomes binding. The decisions issued in the appeal proceedings become binding immediately as well.[104]

---

96 Resolution of 2 June 2014 of the Lithuanian Court of Appeals in Case *Microsoft Corporation v. UAB N5 & K. E.* (No 2-742-262/2012).

97 Article 279(1) of the Civil Procedure Code.

98 Ibid., Article 275(1).

99 Ibid., Article 307(1).

100 Ibid., Article 305.

101 Ibid., Articles 327(1)(1) and 329.

102 Ibid., Article 330.

103 Ibid., Articles 327(1)(2).

104 Ibid., Article 279(1).

The decisions issued in the appeal proceedings can be appealed against at the Lithuanian Supreme Court[105] by parties to the case[106] within three months following the issuance of the decision.[107] The Supreme Court can examine the case only (1) upon violation of substantial or procedural provisions having material importance to the revised decision and the whole uniform case law, (2) where a court deviated from the case law of the Lithuanian Supreme Court, or (3) where the case law of the Lithuanian Supreme Court in the given area is not uniform.[108] The Lithuanian Supreme Court reviews the decisions only from the legal perspective and is bound by facts determined by courts of lower instances.[109] The decisions issued by the Lithuanian Supreme Court become binding immediately and cannot be appealed against.[110]

If a party fails to implement a decision issued by a court on blocking, filtering and take-down of illegal internet content in Lithuania, such decision can become subject to enforcement upon coming into force, unless a court decides that a decision must be enforced urgently.[111] Court decisions are enforced by bailiffs – private persons performing state functions – who can issue binding requests to enforce a decision, provide information on the debtor's financial status or refrain from actions that can impede enforcement.[112] If a bailiff is impeded in enforcing decisions, police can be called to eliminate impediments. A fine of up to EUR 289 can be imposed by a court for each day a person does not comply with a bailiff's requests or impedes the enforcement.[113] Bailiff's activities are supervised by a judge of a county court.[114]

An interim injunction imposing internet blocking, filtering or take-down obligations can be issued under the general requirements of the Civil Procedure Code in any phase of civil proceedings,[115] as well as prior to filing a claim if an applicant provides reason demonstrating why he / she was not able to submit a claim.[116] Such measures can be imposed by courts of the first instance. Requests for interim measures are examined by a court as soon as possible and no later than within 3 business days. A court notifies a defendant of a request for interim measures if it deems necessary.[117] Persons who are subject to interim measures are notified of these interim measures and are provided with explanation on liability for non-compliance with the imposed measures.[118] A court can change or annul *ex officio* the imposed interim measures at any phase of the civil proceedings upon request of a party or if is required to do so by public interest.[119] The decisions imposing interim measures are enforced urgently[120] by bailiffs under the general procedure for enforcing court decisions overviewed above.[121] Decisions regarding interim measures can be appealed against in a court of a higher

105 Ibid., Article 340(1).
106 Ibid., Article 342.
107 Ibid., Article 345(1).
108 Ibid., Article 346(2).
109 Ibid., Article 353(1).
110 Ibid., Article 362(1).
111 Ibid., Article 588(1)
112 Ibid., Article 585(1).
113 Ibid., Article 585(2).
114 Ibid., Article 594(1).
115 Ibid., Article 144(3).
116 Ibid., Article 147(3).
117 Ibid., Article 147(1).
118 Ibid., Article 150(1).
119 Ibid., Articles 148 and 149.
120 Ibid., Article 152(1).
121 Ibid., Article 152(6).

instance. The filing of an appeal does not suspend the enforcement of the decision imposing interim measures.[122] Decisions on interim measures cannot be reviewed in a cassation (third) instance.[123]

In addition to the judiciary, as noted in the answer to Question 2.2 above, basically all governmental supervisory administrative bodies are broadly entitled to issue mandatory orders to cease unlawful activities within their area of competence, including violations that are committed by way of illegal internet content. Thus, it is possible for numerous supervisory authorities to issue mandatory orders to take down the information which violates the requirements of the Lithuanian laws. There is no specific procedure for implementing decisions issued by administrative bodies on blocking, filtering and take-down of illegal internet content in Lithuania. Thus, the administrative orders on blocking, filtering and take-down of illegal internet content would be implemented under the general procedure set forth by the Law on Public Administration and regulations of each of the said supervisory authorities. An administrative decision must be brought to the notice of any person who is the addressee of the decision or whose rights and obligations are affected thereby, within 3 business days following the issuance of such decision.[124]

An administrative take-down order can be appealed against in Lithuanian administrative courts under the general procedure for settling administrative disputes set forth in the Lithuanian Law on Administrative Proceedings[125] (unless specific laws provide otherwise)[126] by any person whose rights were violated by such order.[127] An appeal against an administrative take down order can be lodged within one month after the decision was notified to an applicant.[128] Most supervisory administrative authorities that are able to issue take-down orders are considered to be central administrative authorities whose decisions can be appealed against in the Vilnius County Administrative Court.[129] Decisions issued by county administrative courts can be further appealed against in the Lithuania Supreme Administrative Court as a matter of final instance.[130]

Non-compliance with administrative take-down orders issued by supervisory authorities can result in monetary penalties, since a number of articles of the Lithuanian Law on Administrative Offences[131] provides for administrative liability for non-compliance with administrative orders issued lawfully by various supervisory authorities.

4. General Monitoring of Internet

There are no entities in Lithuania that are specifically authorized to monitor the internet content and assess its compliance with legal requirements, including human rights.

As noted in the answer to Question 2.2. above, there are a number of supervisory authorities in Lithuania that supervise the compliance of the market with various Lithuanian laws that provide for restrictions on information (please see the answer to Question 2 above). Activities of these

122 Ibid., Article 151(1).
123 Ibid., Article 151(2).
124 Article 8(4) of the Law on Public Administration.
125 The Law on Administrative Proceedings of the Republic of Lithuania. *Valstybės žinios*, 1999, Nr. 13-308; 2000, Nr. 85-2566.
126 Ibid., Article 15(1)(1).
127 Ibid., Article 22(1).
128 Ibid., Article 33(1).
129 Ibid., Article 19(1).
130 Ibid., Article 20(1)(1).
131 The Law on Administrative Offences of the Republic of Lithuania. *Vyriausybės žinios*, 1985, Nr. 1-1.

institutions are regulated by numerous specific laws and institutions' regulations.Typically no information medium is excluded from supervisory functions of such institutions. As a result, these institutions are entitled to assess, based on complaints or *ex officio*, the compliance of certain internet information with specific legal requirements. Such institutions will be granted rights to issue administrative orders, conduct on-site investigations, engage experts, obtain information that is necessary to perform their functions, and initiate administrative liability proceedings for determined violations or impose penalties themselves.

For instance, a notable part of internet content can be supervised by the Inspector of Journalist Ethics that is in charge of supervising the compliance of mass media, including internet mass media, with the requirements of the Law on Provision of Information to the Public overviewed in the answer to Question 2.1 above.[132] The Inspector of Journalist Ethics examines complaints regarding defamation, privacy and data protection violations, investigates violations of the Law on the Protection of Minors against the Detrimental Effect of Public Information, supervises compliance with the Law on Provision of Information to the Public and has other competences.[133] While performing his functions the Inspector of Journalist Ethics is entitled to initiate investigations on his own or forward collected materials to competent institutions for investigation, obtain from mass media and state institutions information that is needed to exercise his functions, establish working groups, engage experts etc.[134] The Inspector of Journalist Ethics can issue decisions to warn persons of violations and request the elimination of these violations, request for retraction regarding defamatory or damaging information, initiate administrative liability proceedings, impose penalties, as well as make other decisions.[135]

Certain institutions are granted competences related to the supervision of compliance with the Internet Information Regulation that prohibits publishing and distributing unlawful information in the Internet. The Police Department under the Ministry of the Interior must, upon determining any violation of the Internet Information Regulation, notify the Communications Regulatory Authority, the Inspector of Journalist Ethics and other competent institutions as appropriate.[136] Upon determining any violation of the Internet Information Regulation, the Criminal Police Bureau must conduct investigation within its competence.[137]

The Communications Regulatory Authority has established and operates internet hotline (http://www.draugiskasinternetas.lt/lt/main/report) which enables any person to report illegal internet content. The Communications Regulatory Authority examines the submitted complaints and forwards them to competent authorities, other members of INHOPE Association, as well as sends Notice and Takedown letters to internet service providers.

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

There are no notable authoritative local commentaries or doctrines providing comprehensive assessment of the national legal framework for blocking, filtering and taking down content of the Internet as to the case law of the European Court of Human Rights (the ***ECtHR***).

---

132 Article 49(1) of the Law on Provision of Information to the Public.

133 Listed under Article 50(1) of the Law on Provision of Information to the Public.

134 Listed under Article 50(2) of the Law on Provision of Information to the Public.

135 Listed under Article 50(3) of the Law on Provision of Information to the Public.

136 Article 16.2 of the Internet Information Regulation.

137 Article 17 of the Internet Information Regulation.

As explained in the answer to Question 1 above, to a large extent, blocking, filtering and take-down of illegal internet content is not regulated by specific provisions in Lithuania. As explained in the answer to Question 3 above, there is no specific procedure for implementing decisions on blocking, filtering and take-down of illegal internet content either. Thus, it will be Lithuanian courts that will have to decide, on a case-by-case basis and in accordance with the general legal requirements, on blocking, filtering and take-down of illegal internet content and ensure that such measures comply with the requirements of the European Convention for the Protection of Human Rights and Fundamental Freedoms (the ***ECHR***) and the case law of the ECtHR. The compliance of the national legal framework on blocking, filtering and take-down of illegal internet content with the ECHR will depend on whether a Lithuanian court has properly performed an exercise of balancing the freedom of information against competing values protected by the ECHR in line with the case law established by the ECtHR.

It should be noted that the case law of the ECtHR is extensively cited and usually followed as an authoritative legal source by the Lithuanian courts when balancing freedom of information against the prohibition of defamation and other values in general and when examining restrictions on the allegedly illegal internet content in particular. For instance, when deciding whether anonymous defamatory user-generated comments should be taken down from a website in the case *UAB Vedautos autotransportas v. S. G.,* the Lithuanian Supreme Court made extensive references to the ECtHR's case *Delfi* v. *Estonia* (the Chamber's judgement).[138]

As noted in the answer to Question 2.1 above, although Lithuanian laws do not specifically provide for provisions on internet filtering and blocking, it still provides for courts to issue measures to this end, as in the case of *Association Alliance of Betting Operators, UAB TopSport & UAB Orakulas v. bwin International Ltd., Unibet International Ltd., et al*.. In this case, Lithuanian courts applied very general statutory provisions on injunctions to impose an internet blocking obligation upon an indefinite circle of persons which was later enforced against particular internet service providers (such interpretation was confirmed by the Lithuanian Court of Appeals as a matter of the final instance). As it was later acknowledged by the Lithuanian Court of Appeals,[139] internet filtering measures raise concerns of technical possibilities, efficiency, costs, threats to freedom of information. The said concerns were not extensively assessed by the Lithuanian courts initially while imposing the internet blocking obligations. Moreover, the general provisions of Lithuanian civil procedure allow a court to impose such measures on internet service providers which are not even parties to the case and accordingly do not notify these internet service providers.

It can be argued that imposing internet blocking obligations by Lithuanian courts under the above circumstances did not meet the quality of the law requirements restricting freedom of expression (foreseeability, accessibility, clarity and precision) as developed by the ECtHR. As the ECtHR noted,[140] the expression "prescribed by law" in the second paragraph of Article 10 of the ECHR not only requires that the impugned measure should have a legal basis in the domestic law, but also refers to the quality of the law in question, which should be accessible by the person concerned and foreseeable as to its effects.[141] As the ECtHR's Grand Chamber noted in *Delfi* v. *Estonia,*[142] one of the requirements flowing from the expression "prescribed by law" is foreseeability. Thus, a norm cannot be regarded as a "law" within the meaning of Article 10 § 2 of the ECHR, unless it is formulated with

---

138 Decision of 19 February 2014 in Case *UAB Vedautos autotransportas v. S. G.* (No 3K-3-30/2014).

139 Decision of 2011-12-27 in case No 2-2534/2011.

140 Ahmet Yildirim V. Turkey (Application no. 3111/10), par. 57.

141 See, among other authorities, VgT Verein gegen Tierfabriken v. Switzerland, no. 24699/94, § 52, ECHR 2001-VI; Rotaru v. Romania [GC], no. 28341/95, § 52, ECHR 2000-V; Gawęda v. Poland, no. 26229/95, § 39, ECHR 2002-II; and Maestri v. Italy [GC], no. 39748/98, § 30, ECHR 2004-I.

142 *Delfi* v. *Estonia* (Application no. 64569/09), par. 128.

sufficient precision to enable the citizen to regulate his conduct; he must be able, if need be with appropriate advice, to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail.[143] It can be argued that an internet service provider is not able to foresee to a reasonable degree that, based on very general provisions of the Lithuanian Civil Procedural Code enabling courts to impose an injunction as a matter of interim measures, along with the relevant case-law, it may be obliged to implement internet blocking measures and, thus, be subject to interference with freedom of expression guaranteed under Article 10 of the ECHR. The said opinion is further supported by other Lithuanian case law acknowledging that Lithuanian laws do not obligate internet service providers to terminate access to information hosted on outside networks.[144]

It is worth noting that in the case *Association Alliance of Betting Operators, UAB TopSport & UAB Orakulas v. bwin International Ltd., Unibet International Ltd.* the internet service provider claimed that very general provisions of the Lithuanian Civil Procedural Code that allowed courts to impose the internet blocking obligation on the provider violated the provider's freedoms of expression and commercial activities protected by the Lithuanian Constitution (and similarly protected by the ECHR) and, therefore, requested the court to refer the case to the Lithuanian Constitutional Court to determine the constitutionality of these provisions. The Lithuanian Court of Appeals rejected the request noting that the internet service provider was virtually challenging the validity of the application of statutory provisions that had to be decided in the given case, rather than the provisions themselves.[145] The Lithuanian Court of Appeals *ex officio* cancelled the previously imposed internet obligation after assessing concerns of technical possibilities, efficiency, costs and threats to freedom of information caused by such obligation.[146] Thus, the Lithuanian Court of Appeals rectified the potential non-compliance with the ECHR and the ECtHR's case law. The reasoning of the Lithuanian Court of Appeals will bind the Lithuanian Court of Appeals itself and courts of lower instances in examining similar internet blocking questions in the future.

The above-listed concerns are likely to be considered in future cases regarding internet blocking. As a result, current Lithuanian regulatory framework on filtering and blocking down of illegal internet content cannot be considered *per se* non-compliant with the requirements for the quality of the law restricting freedom of expression (foreseeability, accessibility, clarity and precision) as developed by the ECtHR.

Lithuanian statutory obligations of taking down the illegal internet content does not seem to raise issues of legal quality, since it is precisely defined in the Lithuanian laws that publishing and distributing unlawful information in the Internet is prohibited;[147] the host can be requested to take down the unlawful content;[148] the Lithuanian Supreme Court has elaborated extensively on the foregoing obligation;[149] the liability of an internet intermediary for the stored or transmitted information is regulated by the Lithuanian Law on Information Society Services[150] and clarified by the case law of the Court of Justice of the European Union.

---

143 See, for example, Lindon, Otchakovsky-Laurens and July v. France [GC], nos. 21279/02 and 36448/02, § 41, ECHR 2007-IV, and Centro Europa 7 S.r.l. and Di Stefano, cited above, § 141.

144 The Decision of 2012-12-05 of the Lithuanian Supreme Administrative Court in Case No N[575]-641/2012.

145 The Decision of 2011-07-14 in case No 2-1579/2011.

146 The Decision of 2011-12-27 in case No 2-2534/2011.

147 Article 5 of the Internet Information Regulation.

148 Article 15(3) of the Lithuanian Law on Information Society Services.

149 For instance, the Decision issued on 13 November 2012 in case *J. K. and UAB CAN2 FASHION v. S. G.*

150 Articles 12-14 of the Lithuanian Law on Information Society Services.

As explained in the answer to Question 2 above, Lithuanian laws provide for very general, principle-based, however, workable safeguards for the protection of human rights (notably freedom of expression) and prevention of abuse of power and arbitrariness in line with the principles established in the case-law of the ECtHR in the cases on blocking, filtering and take-down of illegal internet content. These safeguards include principles of proportionality, economy, equity, public interest, uniformity of the case law, direct applicability of the Lithuanian Constitution and the ECHR granting the said rights. It is for a court to employ these general safeguards to ensure that human rights are protected in each individual case. These legal requirements are implemented in practice, as in most of the analysed internet content related cases. The courts applied tests for limiting freedom of expression in light of the ECtHR's case law. Although such legal framework does not seem *per se* incompatible with the ECHR and the ECtHR's case law, it increases the risk of violations of the ECHR by causing uncertainty for judges that have to perform the complex and sophisticated (and requiring technical knowledge) test of balancing freedom of expression against other values in the Internet pursuant to the very general criteria and in the absence of specific statutory guidance.

As noted by the ECtHR's Grand Chamber in the recent case *Delfi* v. *Estonia,*[151] some countries have recognised that the importance and complexity of the subject matter involving the need to ensure proper balancing of different interests and fundamental rights, call for the enactment of specific regulations for situations, such as those pertaining to the said case. Such action is in line with the "differentiated and graduated approach" to the regulation of new media recommended by the Council of Europe and has found support in the ECtHR's case-law.[152] Enacting such specific regulations would be useful for Lithuania too, as it would decrease the risk that blocking, filtering and take-down of illegal internet content on a case-by-case basis will not comply with human rights protected by the ECHR.

Julius Zaleskis
18.11.2015
Revised on 16.06.2016 taking into consideration comments from Lithuania on this report

151 *Delfi* v. *Estonia* (Application no. 64569/09), par. 128.

152 See, *mutatis mutandis*, Editorial Board of Pravoye Delo and Shtekel v. Ukraine, no. 33014/05, §§ 63-64, ECHR 2011.