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 323-334

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.

ICELAND

1. Legal Sources

There is **no specific law** on blocking, filtering or taking down illegal Internet content in Iceland. Instead the area is regulated through penal law provisions preventing disorder and crime, civil law provisions protecting the reputation or rights of others and administrative rules where the relevant authorities are authorized to act in particular areas.

The penal law provisions are contained in the **Icelandic General Penal Code**.[1] Furthermore, content can be illegal under the **Icelandic Copyright Act**[2] and the **Icelandic Trade Mark Act**.[3] According to the **Icelandic Data Protection Act**[4] the Data Protection Authority can order the erasure or deletion of records that contain incorrect or misleading personal data. Provisions of the **Act on the Surveillance of Commercial Practices and Marketing**[5] allow for the Consumer Agency to take actions against certain infringements while the **Act on Electronic Commerce and other Electronic Services**[6] concerns inter alia the civil liability of different types of Internet service providers.

Iceland ratified the **Convention for the Protection of Individuals with regard to Automatic Processing of Personal data**[7] on 25 March 1991 and it entered into force on 1 July 1991. The Convention protects individuals against abuse which may accompany the collection and processing of personal data and seeks to regulate the transborder flow of personal data. On 29 January 2007 Iceland ratified the **Cybercrime Convention of the Council of Europe**[8] and it entered into force on 1 May 2007. The Cybercrime Convention regards crimes committed on the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography, hate crimes, and violations of network security and its rules are reflected in Icelandic national law. Furthermore, Iceland has signed (but not ratified) the **Additional Protocol** concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems.[9] On 20 September 2012 Iceland ratified the **Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse**[10] and it entered into force on 1 January 2013. **The Convention on the Prevention of Terrorism** has only been signed, but not yet ratified by Iceland.[11]

---

1 Almenn hegningarlög, nr. 19/1940.

2 Höfundalög, nr. 73/1972.

3 Lög um vörumerki, nr. 45/1997.

4 Lög um persónuvernd og meðferð persónuupplýsinga, nr. 77/2000. The Act incorporates into Icelandic law the provisions of Directive 95/46 EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data.

5 Lög um eftirlit með viðskiptaháttum og markaðssetningu, nr. 57/2005.

6 Lög um rafræn viðskipti og aðra rafræna þjónustu, nr. 30/2002.

7 The Convention for the Protection of Individuals with regard to Automatic Processing of Personal data, CETS no. 108.

8 The Budapest Convention on Cybercrime, CETS no. 185.

9 Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems, CETS no. 189.

10 Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, Lanzarote, 25.10.2007.

11 Council of Europe Convention on the Prevention of Terrorism, Warsaw, dated 16.5.2005.

The legal sources regulating the area are primarily through legal provisions granting injunctive relief against such illegal content. The injunctive relief is maintained by DNS- or IP-address blockings done by the access service providers.

2. Legal Framework

2.1. Blocking and/or filtering of illegal Internet content

2.1.1. Penal Law Provisions

According to the Icelandic General Penal Code it is illegal to produce, import or have in one's possession material, such as photographs, films or video files that shows **children in sexual or pornographic manner**.[12] The mere viewing of such content on the Internet or by any similar telecommunications technology is also punishable according to the Code.

Since 2001, Save the Children Iceland has participated in an international project to protect children against sexual abuse on the Internet. The National Commissioner of the Icelandic Police and Save the Children Iceland has operated **a hotline for the public to report online illegal content** on the internet, such as child sexual abuse content.[13] Information on reported webpages is analyzed by the National Police and can be shared within other hotlines through International Association of Internet Hotlines (INHOPE).[14]

Furthermore the Icelandic General Penal Code lays down general provisions concerning liability for acts of **defamation**.[15] Generally, anyone who ridicules or insults another person or presents a defamatory insinuation against that person, resulting in an injury of his personal honour, may be held liable. The provisions apply equally to defamatory actions over the Internet. Such offences are subject to private prosecutions unless a defamatory action is directed at a civil servant or if it is anonymous. In such cases an indictment is issued by the prosecutor if claimed by the injured person.[16]

The Icelandic General Penal Code prohibits **hate speech and racism** so that whoever publicly, or with intention to disseminate in a larger circle makes statements or other pronouncement, by which a group of persons is threatened, derided or degraded because of their race, color of skin, national or ethnic background, faith or sexual orientation, will be punished.[17] The provisions apply equally to any such offences committed by submitting such content on the Internet.

According to the Icelandic General Penal Code it is prohibited to **disclose private affair** of another person without sufficient reasons justifying such an act.[18] Same accounts for private affairs relating to the work of a civil servant and which are to be treated as confidential.[19]

Acts of terrorism can be penalised with up to life imprisonment and any incitements and support of such punishable activities or the support of an association having the aim of committing such violations is subject to imprisonment for up to 6 years.[20]

---

12 Art. 210 a of the Icelandic General Penal Code.

13 www.barnaheill.is/TilkynnaologlegtefniReportillegalcontent/

14 http://www.inhope.org/gns/home.aspx

15 Chapter XXV of the Icelandic General Penal Code.

16 Art. 242 of the Icelandic General Penal Code.

17 Art. 233 a of the Icelandic General Penal Code. Cf. Art. 27 of the Icelandic Media Act (*Fjölmiðlalög nr. 38/2011*) where hate speech and racism in media is prohibited.

18 Art. 229 of the Icelandic General Penal Code.

19 Art. 230 of the Icelandic General Penal Code.

Where it is necessary to **prevent further crime** the Icelandic General Penal Code provides that objects used or intended to be used in a criminal act may be confiscated. Same applies to objects produced by a criminal act, such as child pornographic content, and objects in respect of which a criminal offense has otherwise been committed.[21] It is possible that the ownership of a webpage hosting an illegal content could be confiscated with reference to Art. 69 a of the Icelandic Penal Code. Up to date there are however no clear precedents of rules on confiscation being used in relation to illegal internet content.

2.1.2. Civil Law Provisions

In relation to civil law provisions protecting the reputation or rights of others, the economic and moral interests to **intellectual property** is protected under the Icelandic Copyright Act.[22] Infringements of intellectual property rights as further stipulated in the Act can be tried either as criminal cases or by filing a civil law suit.[23] Furthermore both rightholders themselves and legal collective rights management societies can apply for an injunction against the illegal use of a work protected by the Icelandic Copyright Act.[24] Such an injunction can be directed at the service provider[25] as being the party providing access to the content subjected to the general requirements of the Icelandic Act on Seizure, Injunction etc. to be met.[26]

Injunction procedure is often the only reasonable remedy in practice in cases of infringement of copyright since such procedure allows for the rightholders to enforce their rights faster than by initiating normal civil case proceedings. For an injunction to be awarded, certain **requirements** must be met, such as that the injunction is directed at an act that has begun or is pending and that the petitioner proves or shows that it is probable that the act infringes, or will infringe, upon his rights that are protected by law. Furthermore it is required that the respondent has already initiated the act or will do so and that his rights will be forfeited, or will be subject to notable harm if he is forced to wait for a judgment. An injunction will however not be granted if it is concluded that laws concerning penalties or damages for the disturbance of the interests of the petitioner will secure these rights in a sufficient manner. Same applies if it is shown that there is a vast difference between the interests of the respondent in the act taking place and the interest of the petitioner of preventing it, provided that the respondent may by held to place a guarantee for the losses that the act will result in for the petitioner.[27]

An injunction is granted by the district magistrates on a preliminary basis and must be followed by the filing of a suit for a **confirmation of the courts** within one week from the date of the finalization of the injunction order.[28]

According to the **Icelandic Trade Mark Act** it is possible to demand injunctive relief against any activity which has already commenced or is pending and violates or will violate a trade mark right.[29]

---

20 Art. 100 a – 100 c of the Icelandic General Penal Code.

21 Art. 69 a of the Icelandic General Penal Code.

22 The Icelandic Copyright Act (*Höfundalög nr. 73/1972*).

23 Art. 59 of the Icelandic Copyright Act.

24 Art. 59 a and 59 b of the Icelandic Copyright Act.

25 As the term is defined in the Act on Electronic Commerce and other Electronic Services No. 30/2002.

26 The Icelandic Act on Seizure, Injunction etc. (*Lög um kyrrsetningu, löggeymslu og lögbann nr. 31/1990*).

27 Art. 24 of the Icelandic Act on Seizure, Injunction etc.

28 Art. 36 of the Icelandic Act on Seizure, Injunction etc.

29 Art. 41 of the Icelandic Trade Mark Act (*Lög um vörumerki nr. 45/1997*).

The Icelandic Trade Mark Act generally prohibits the use of identical signs for goods or services that are for their part identical to those for which the trade mark enjoys protection; signs that might cause confusion, such as the conclusion that there is a connection between them or signs for other goods and services if the trade mark is well known in the country and the use would comprise misuse or lessen the distinctive nature of the characteristics or reputation of the known mark.[30]

Finally the **Act on Electronic Commerce and other Electronic Services** allows for injunctive relief outside of a service provider's limited liability.[31] According to the Act, a service provider who hosts information provided by the recipient of the service is not liable for the information provided that it promptly removes it or disables access to it on receiving a knowledge that a district magistrate has placed an injunction on the hosting of the information or a court has ruled on its removal or disablement of access to it; the service provider has been notified of the violation of an alleged copyright infringement or if the service provider is aware of the information containing child pornography.[32] The Act therefore provides for an indirect notice and takedown procedure with regards to certain illegal content, such as copyright protected material and child pornography.

In Icelandic cases where the courts have ordered the district magistrate to issue injunctions against service providers requiring them to take down or block access to specific webpages, the service providers have complied with the injunctions.

2.1.3. Administrative Rules

Administrative authorities in Iceland may be enabled to prevent illegal Internet content within their field.

The **Icelandic Data Protection Act**[33] implements Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The Act imposes minimum requirements on every person or entity that process personal data and its purpose is to ensure the reliability and integrity of such data and their free flow within the internal market of the European Economic Area (the "EEA-Area").[34]

According to the Act the controller of personal data must **rectify, erase, delete or improve data that it has registered without the proper authorization, which is incorrect, misleading, incomplete**, or if the defect in question is liable to affect the interests of the data subject. If such erasure, deletion or alteration is not allowed according to provisions of other acts, then the Data Protection Authority may **prohibit the use of the data**.[35]

When there is **no longer an apposite reason to preserve personal data**, the controller must erase them. An apposite reason for preserving data may, for example, stem from a provision of law or from the fact that the controller is still processing the data in line with the original purpose of their collection.[36] The data subject may still demand that data relating to him, be erased or their usage prohibited, if that is considered justifiable, following a comprehensive assessment of the interests involved. In making such an assessment, the interests of others, general considerations of privacy, public interests, and the measures necessary for complying with the demand, shall be taken into

30 Art. 4 of the Icelandic Trade Mark Act.

31 Chapter V of the Act on Electronic Commerce and other Electronic Services.

32 Art. 14(1) of the Act on Electronic Commerce and other Electronic Services.

33 The Icelandic Data Protection Act (*Lög um persónuvernd og meðferð persónuupplýsinga, nr. 77/2000*).

34 The EEA-area consist of the EU-member states, Iceland, Lichtenstein and Norway.

35 Art. 25 of the Icelandic Data Protection Act.

36 Art. 26(1) of the Icelandic Data Protection Act.

account.[37] The Data Protection Authority may, in individual cases or by issuing a general ordinance, prohibit the use of such data or order that they be erased.[38]

As a preliminary measure, the Data Protection Authority can assign to the Chief of Police the task of halting temporarily a process violating provisions of the Act.[39]

If the instructions of the Data Protection Authority are not observed the Authority can, in certain instances, decide to impose daily fines upon the receiver of the instructions.[40]

The Data Protection Authority has rendered several decisions where a controller of certain processing of personal data is to cease the processing or erase data. Such processing has in some instances been carried out on the Internet.[41] Up to date the Data Protection Authority has not imposed daily fines on a controller and a processing has not been ceased by the Chief of Police halting the operations of the party in question as a preliminary measure.

According to the **Act on the Surveillance of Commercial Practices and Marketing** the Consumer Agency can resort to actions against unfair commercial practices such as by prohibiting them or by issuing instructions to the party in question.[42] Unfair commercial practices are illegal, if they affect the interests of competitors, consumers or other market actors.

The Act lists a broad range of examples of unfair commercial practices, such as misleading commercial practices, comparative advertising and unacceptable nuisance.[43] The Consumer Agency can apply administrative fines against a party violating the provisions of the Act or the rules and decisions of the Consumer Agency.[44] In the event of non-compliance with a decision taken in accordance with the Act the Consumer Agency may decide to impose daily fines on the party or parties at which the decision is directed until the decision is complied with.[45]

The Consumer Agency has issued several decisions regarding unfair commercial practices, such as in relation to **domain names**, advertisements and slogans.[46] By such decisions the party violating the Act is prohibited the use of a domain name and is ordered to cancel its registration with the Icelandic domain registry.

---

37 Art. 26(2) of the Icelandic Data Protection Act.

38 Art. 26(3) of the Icleandic Data Protection Act.

39 Art. 40(2) of the Icelandic Data Protection Act.

40 Art. 41 of the Icelandic Data Protection Act.

41 Cf. Case No. 2004/529 where a controller was to cease the publishing of the personal data of alleged drug dealers on his website, available at http://www.personuvernd.is/efst-a-baugi/urskurdir-og-alit/2004/greinar/nr/134 (12.08.2015). Case No. 2004/158 where a webmaster of certain webpage was ordered to delete a data subjects Social security number from the webpage, available at http:// http://www.personuvernd.is/efst-a-baugi/urskurdir-og-alit/2004/greinar/nr/130 (12.08.2015). Case No. 2014/1078 where a controller of a certain webpage was ordered to delete all personal data of a data subject from the website, available at http:// http://www.personuvernd.is/efst-a-baugi/urskurdir-og-alit/2014/greinar/nr/1912 (12.08.2015).

42 Art. 21 b(2) of the Act on the Surveillance of Commercial Practices and Marketing.

43 Capter II-V of the Act on the Surveillance of Commercial Practices and Marketing and Regulation No. 160/2009 on Commercial Practices which shall in all circumstances be regarded as unfair.

44 Art. 22 of the Act on the Surveillance of Commercial Practices and Marketing.

45 Art. 23 of the Act on the Surveillance of Commercial Practices and Marketing.

46 Cf. Case No. 31/2010 where a company was prohibited the use of the domain name “stoð.is” and the slogan “Ég styð við þig“, available at http://www.neytendastofa.is/library/Files/Neytendarettarsvid-/akvardanir/akv2010_31.pdf (22.10.2015).

The **Electronic Communications Act**[47] applies to electronic communications, electronic communications service and electronic communications networks and is to ensure cost-efficient and secure electronic communications in Iceland.[48] The Post and Telecom Administration (PTA) is the supervisory authority regulating the electronic communications affairs. The PTA is not responsible for regulating the content being hosted on or sent through the electronic communications networks but rules and regulations in the area concern *inter alia* the safety and quality of such networks and therefore apply to the access to the networks.[49]

2.1.4. Domain Rules

The corporation **Internet á Íslandi hf. (ISNIC[50])** administers the distribution and registration of domain names in Iceland under the .is-domain. ISNIC is a public limited liability company and its operation is based on a decision of IANA[51]/ICANN[52] and an agreement between ICANN and ISNIC on the administration of the .is-domain.

According to ISNIC's **domain rules** (.is naming policy) a registrant is responsible for ensuring that the use of a domain is within the limits of Icelandic law.[53] The **general terms and conditions** of ISNIC allow for ISNIC to cancel all business relation with a customer and to stop the supply of service without notice, if the material on the customer's web or if the product offered on his behalf grossly and in a decisive manner contravenes with Icelandic law, subjected to a ruling from the Icelandic judicature and/or the police authorities has been presented.[54]

Disputes regarding a registration of domains can be submitted to a Board of Appeals which can issue decisions on the transfer of domain, such as if trademark rights are violated, the registrant has no legitimate interests for the use of the domain and when a domain was not registered in good faith.[55]

A bill was put forward in the Icelandic Parliament in 2012 which aimed at legalising the .is-domain and shift the governance of the .is-domain to the Icelandic government.[56] The aim of the bill was to ensure safe and efficient access to the Icelandic domain names. The bill did however not pass through the Parliament and the .is-domain regulatory environment therefore remains unchanged under the governance of ISNIC.

2.2. Take-down/removal of illegal Internet content

There is no Icelandic legislation particularly directed at Internet host providers and their role in content take-down/removal measures. Their operation needs to be in conformity with relevant legislation, such as the Icelandic Data Protection Act, where such host providers would in general have the role as a processor within the controller-processor relationship.

Internet host providers in Iceland have individual terms and conditions of their service concerning the use of the particular website and which material may be made available on the website. If such

---

47 The Electronic Communications Act (*Lög um fjarskipti nr. 81/2003*).

48 Art. 1 of the Electronic Communications Act.

49 Cf. Regulation on protection, functionality and quality of IP communications services No. 1223/2007.

50 IS Network Information Center.

51 Internet Assigned Numbers Athority.

52 Internet Corporation for Assigned Names and Numbers.

53 Art. 9 of the ISNIC Domain Rules.

54 Art. 10(3) of the ISNIC Terms and Conditions.

55 Chapter IX of the ISNIC Domain Rules.

56 Cf. parliamentary document No. 528 – Case No. 421 in the 141st Parliamentary session, available at http://www.althingi.is/altext/141/s/0528.html (12.08.14).

terms are violated Internet host providers can cancel the service agreement in place with the customer in question.

As an example the terms and conditions of Síminn (Iceland Telecom) with the regards to Internet and hosting service refer to the prohibition of broadcasting illegal, indecent or defamatory content on a website and that Iceland Telecom reserves the right to block access to websites that contain such content (Art. 14). According to Article 21 of the terms Iceland Telecom reserves the right to protect its customers from spam, viruses and fraudulent or other inappropriate content. Iceland Telecom also reserves the right to cancel the service agreement in place if the service or equipment is misused (Art. 24). [57]

2.3. Relevant case-law

Case law in Iceland regarding illegal internet content concerns mainly intellectual property rights.

In the Supreme Court Case No. 214/2009[58] the Icelandic Supreme Court confirmed an injunctive relief against the operation of a website that allowed its users to share content protected by the Icelandic Copyright Act. The Supreme Court noted that the plaintiff had proven that the main purpose of the website was to facilitate its users to share copyright protected content without the consent of the rightholders. The Supreme Court applied the same reasoning when it concluded that the limits on liability of intermediaries as stipulated in Chapter V of the Act on Electronic Commerce and other Electronic Services No. 30/2002, would not apply to the operators of the website.

In the District Court case No. K-8/2013[59] the district magistrate was ordered to issue an injunctive relief against an Internet service provider's act to allow its customers to gain access to the webpages www.deildu.net, www.deildu.com, www.thepirateby.se, www.thepiratebay.sx and www.thepiratebay.org.[60] The court stated that the structure and purpose of the websites in question was to facilitate the sharing of copyright protected content without the prior consent of the rightholders. The injunction was based on Art. 59 a of the Icelandic Copyright Act which states that an injunctive relief can be issued against a service provider independent of its responsibility of the sharing of the illegal content.

The Internet service provider claimed that an injunctive relief would restrict the freedom of expression according to Article 73 of the Icelandic Constitution and Article 10 of the European Convention of Human Rights (ECHR), which was enacted into law in Act No. 62/1994. The freedom of expression would include the right to share information and ideas with any legitimate resources, as is the right to receive such information. The operation of providing customers access to the Internet would apply to such sharing of information and would be interpreted as an expression within the meaning of these provisions. The service provider also pointed out that the websites in question did not contain mere copyright protected content.
The judge ruled that the service provider's, or its customers', freedom of expression would not be considered to override the legitimate interests of the contents' rightholders. In this respect any copyright protected material on these websites could be easily accessed by other lawful means.

---

57 Cf. Terms and conditions of Síminn (Iceland Telecom) with regards to Internet and hosting service, available at https://www.siminn.is/siminn/verslanir-thjonusta/skilmalar/internet-og-tolvuthjonusta/ (22.10.2015).

58 Judgment from the Icelandic Supreme Court in case No. 214/2009 of 11 February 2010, available at http://haestirettur.is/domar?nr=6419 (12.08.2015).

59 Judgment from the District Court of Reykjavik in case No. K-8/2013 of 14 October 2014, available at http://domstolar.is/domaleit/nanar/?ID=K201300008&Domur=2&type=2&Serial=2 (12.08.2015).

60 https://www.rt.com/news/196684-iceland-block-pirate-bay/ (22.10.2015).

Article 59 a of the Icelandic Copyright Act was considered to be a legitimate restriction to freedom of expression and to fulfil the conditions set out in Article 73(3) of the Icelandic Constitution.[61] The injunctive relief was to be issued despite the fact that the customers of the Internet service provider could easily get around such blocking, such as by using proxy services. The Performing Rights Society (STEF) and five Icelandic service providers reached an agreement in September 2015 regarding the blocking of access to the websites iirespective of the domain names used by their representatives and without the need to have a new injunctive relief in place.[62]

3. Procedural Aspects

The **Icelandic Data Protection Authority** can decide on the processing of personal data to be ceased or such data to be deleted if it is thought to violate data protection rights, cf. under section 2.1.3. of this report. Such decisions are directed at the controller of the processing but the Icelandic Data Protection Authority has no general resources to implement such decisions unless by imposing daily fines upon the party violating the Authority's instructions.[63] Decisions of the Data Protection Authority can be referred to the courts of law for an annulment.

The **Consumer Agency** can resort to actions against unfair commercial practices such as by prohibiting such practices or by issuing instructions to the party in question.[64] The Consumer Agency can apply administrative fines against a party violating decisions of the Consumer Agency and in the event of non-compliance with a decision taken in accordance with the Act the Consumer Agency may decide to impose daily fines on the party or parties at which the decision is directed until the decision is complied with.[65] The decisions of the Consumer Agency can be appealed to the Appeals Committee for Consumer Affairs and cannot be referred to the courts of law until the Appeals Committee's conclusion has been issued.[66]

ISNIC's general terms and conditions and its domain rules allow for ISNIC to cancel all business relation with a customer and to stop the supply of service without notice, if the material on the customer's web or if the product offered on his behalf grossly and in a decisive manner contravenes with Icelandic law, subjected to a ruling from the Icelandic judicature and/or the police authorities.[67] Cases involving the registration of domains or refusal to register domains may be referred to the Board of Appeals.[68] Recently ISNIC did however cancel the supply of its service on the grounds that a customer's web material was violating Icelandic law even though a ruling from the Icelandic judicature or the police authorities had not been issued.
On 13 October 2014 ISNIC did suspend the domain names khilafah.is and Kilafah.is that were used for the website of a known terrorist organisation (Islamic State) since the content on the website was thought to be in violation of Icelandic law. According to ISNIC this act was unprecedented since ISNIC

---

61 Article 73(3) of the Icelandic Constitution: *Freedom of expression may only be restricted by law in the interests of public order or the security of the State, for the protection of health or morals, or for the protection of the rights or reputation of others, if such restrictions are deemed necessary and in agreement with democratic traditions*.

62 The agreement has however not been made public. Cf. http://www.visir.is/loka-a-vefsidurnar--ohad-hysingu-theirra/article/2015150919188 (22.10.2015).

63 Art. 41 of the Icelandic Data Protection Act.

64 Art. 21 b(2) of the Act on the Surveillance of Commercial Practices and Marketing.

65 Art. 22 and 23 of the Act on the Surveillance of Commercial Practices and Marketing.

66 Art. 4 and 25 of the Act on the Surveillance of Commercial Practices and Marketing.

67 Art. 10(3) of the ISNIC Terms and Conditions and Art. 9 of the ISNIC Domain Rules.

68 Art. 33 of the ISNIC Domain Rules.

has never closed down a domain name with reference to the material content of a website. The suspension was made with reference to Art. 9[69] of the ISNIC Domain Rules. [70]

In June 2009 two of the largest **individual service providers** in Iceland, Fjarskipti ehf. (Vodafone) and Síminn hf. (Iceland Telecom) blocked access to the webpage ringulreid.org. In September 2010 same action was taken against the webpage slembingur.org. These actions were taken with reference to the indirect notice and takedown procedure provided for in the Act on Electronic Commerce and other Electronic Services.[71] The Act stipulates that a service provider can be held liable for the information provided by the recipient of the service if it does not remove or disables access to the information, such as when it has the knowledge of the information containing child pornography. The service providers in question explained their actions of blocking the whole webpage of the customer by pointing out that the Act did not have special provisions banning such extensive blocking to reach the goal of blocking an illegal content. These measures were by the service providers thought to be extraordinary and made after appeals from several official and non-official organisations, such as The National Commissioner of the Icelandic Police, Save the Children Iceland and the Government Agency for Child Protection.

A customer of a service provider later filed a complaint to the PTA regarding the blocking of the service providers of these websites (Decision No. 8/2011).[72] In its complaint the customer referred to regulation on the protection of information in public communications networks No. 1221/2007, regulation on the functionality of public communication networks No. 1222/2007, regulation on protection, functionality and quality of IP communication services No. 1223/2007 and rules on general authorisation to operate electronic communications networks or services No. 345/2005. The customer maintained that by the blocking of the websites the service provider had infringed these rules and regulations issued by the PTA. The customer also maintained that these actions did limit freedom of expression and provide for censorship of service providers of content on the Internet.

In its decision the PTA concluded that the Electronic Communications Act No. 81/2003 would not apply to content broadcast on electronic communications networks (cf. Art. 1(5) of the Act). Certain safety and quality requirements of the Electronic Communications Act, such as regarding electronic communications traffic, would however affect the access to the content on such communications networks (cf. Art. 21 of regulation No. 1223/2007). The Article reads as follows:

In order that customers may be aware of how their electronic communications traffic is transferred, electronic communications undertakings shall provide their customers with information on whether their traffic is sent via proxy transfer, and if so, what traffic is so sent; and whether the proxy transfer is transparent and the limitations it causes, such as possible rejection of traffic and censoring of customer data.

---

69 *An applicant designates the domain's registrant in the registration process in accordance with ISNIC's rules. The registrant is responsible for ensuring that the use of the domain is within the limits of Icelandic law as current at any time. The registrant is also responsible for the payment of any fees due regarding delegation and renewal of the domain. The registrant is obliged to comply with the decision of a special Board of Appeals for domains cf. Chapter IX of these rules. The registrant is under obligation to compensate ISNIC for any damage that the use of the domain may cause ISNIC.*

70 .Cf. http://www.isnic.is/en/news/index (12.08.2015) and http://www.visir.is/forsvarsmenn-isnic-tiltoku-ymsar-astaedur-fyrir-ad-loka-a-islamska-rikid/article-/2014141029931 (22-10-2015).

71 Art. 14(1) of the Act on Electronic Commerce and other Electronic Services. Cf. http://www.mbl.is/greinasafn/grein/1287123/ (12.08.2015).

72 Cf. PTA's decision No. 8/2011, available at http://www.pfs.is/upload/files/-Ákv_nr.8_2011_lokun_aðgangs_að_heimasíðu.pdf (12.08.2015).

The PTA pointed out that other requirements of the said regulation, such as regarding a guarantee of minimum basic level of service, could not be used as a constraint on the service providers to broadcast alleged illegal content (cf. Art. 27(5) of regulation No. 1223/2007). The Article reads as follows:

Electronic communications undertakings shall not block their customers' access to the Internet unless this is especially negotiated or is in accordance with this Regulation. Those who seek lawful service shall be enabled to provide equally.

The PTA noted that the reservation made in the Article regarding the service to be "lawful" was vital in this sense. Customers could therefore not have the right to access an illegal content since that would not be a "lawful" service.

An **injunction** is granted by the district magistrates as a preliminary remedy and must be followed by the filing of a civil suit for confirmation of the injunction unless the respondent declares that he will comply with the injunction without the filing of a suit.[73] Application for an injunction must meet the formal requirements set out in the Act on Seizure, Injuction etc. (cf. section 2.1.2. in this report). The petitioner will be ordered to put a guarantee in place for the injunction.[74] A guarantee can be of a considerable amount if the financial interests at stake are high. If the respondent does not take the necessary steps in order to comply with the injunction order, such as by acting in accordance with the injunction, *inter alia* by closing access to certain webpages, the district magistrate can himself act on behalf of the respondent.[75] If necessary the district magistrates can ask for the assistance of the police with the enforcement of an injunction.[76] A court decision confirming an injunction may be appealed to the Supreme Court in accordance with the provisions of the Act on Civil Procedure. If the conclusion of a confirmation case is that the injunction is rescinded, the petitioner may face liability in damages.[77]
There are quite limited resources to have an injunction order reassessed by the district magistrate but such a reassessment can occur in some instances, such as if both parties agree to have an reassessment, if the petitioner wants to relinquish his rights or if the respondent is acquitted of the petitioner's claim in a court case.[78]

Finally a blocking, filtering or take-down of illegal Internet content can be granted by a **judgment in a court of law**. A judgment on blocking of illegal Internet content can be appealed to the Supreme Court and will be enforced in accordance with the provisions of the Act on Enforcement Procedure.[79]

4. General Monitoring of Internet

Iceland does not have a special **entity in charge of monitoring** Internet content.

Icelandic service providers are obliged to **log and store** data concerning the telecommunication traffic of the end users, such as data on Internet sessions, which webpages the end user visited and the quantity of data transfer. Such data is to be retained by the service providers for six months.[80]

---

73 Art. 36 of the Act on Seizure, Injunction etc.
74 Art. 30 of the Act on Seizure, Injunction etc.
75 Art. 25(1) of the Act on Seizure, Injunction etc.
76 Art. 32(1) of the Act on Seizure, Injunction etc.
77 Art. 42 of the Act on Seizure, Injunction etc.
78 Art. 31(2) and 22 of the Act on Seizure, Injunction etc.
79 Act on Enforcment Procedure No. 90/1989.
80 Art. 42(3) of the Electric Communications Act.

The data can only be accessed with a prior issuance of a court order and in relation to an investigation and prosecution of criminal activities.[81]

According to the Regulation on protection, functionality and quality of IP communications services the service providers are to inform their customers of a **possible rejection of traffic and censoring of customer data**.[82]

Icelandic law does however **not impose any general obligation on service providers to monitor** the content which is transmitted or stored in electronic communication networks.

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

Blocking and filtering of Internet content has raised certain concerns in Iceland mainly in relation to freedom of expression and legal certainty.

Doubts have been raised about whether blocking of Internet content through filtering is inconsistent with the freedom of expression in the Icelandic Constitution.[83] The customer that complained to the PTA in case No. 8/2011 did criticize the fact that Internet content had been blocked by private actors in the field without either a court order or a judgment. Same concerns have been raised regarding the suspension of domain names.[84] Both when service providers decided to block certain websites (cf. PTA's decision No. 8/2011 under section 3 of this report) and when ISNIC decided to suspend domain names (cf. under section 2.1.4. of this report) , this was done without the possibility of the concerned parties, such as the representative of the website in question and the rightholder to the domain name, to defend such actions. No court order was in place and a judgment had not been rendered.

When the blocking of illegal content on the Internet is sought by way of applying for injunction or with a claim submitted before the courts it allows for an evaluation of the criteria set out in the Icelandic Constitution for limiting freedom of expression. Such evaluation is mandatory and all three conditions of Article 73(3) of the Icelandic Constitution need to be fulfilled.[85] This procedure does as well allow for the courts to interpret Article 73 of the Icelandic Constitution with regard to the provisions of the European Convention on Human Rights and the case law of the European Court of Human Rights.

---

81 Art. 47(7) of the Electric Communications Act.

82 Art. 21 of the Regulation on protection, functionality and quality of IP communications services No. 1223/2007.

83 Art. 73(3) of the Icelandic Constitution (*Stjórnarskrá lýðveldisins Íslands nr. 33/1944*). Cf. PTA's decision No. 8/2011 available at http://www.pfs.is/upload/files/%C3%81kv_nr.8_2011_lokun_a%C3%B0gang-s_a%C3%B0_heimas%C3%AD%C3%B0u.pdf (22.10.15).

84 Law professor at the University of Iceland said that the legal framework as it stands did not allow for the Icelandic state to instruct private actors, such as ISNIC, to suspend domain names or close undesireable websites. Cf. http://www.visir.is/haepid-ad-stjornvold-geti-farid-fram-a-lokun-vefsidna/-article-/2014141029897 (22.10.2015).

85 Cf. Art. 73(3) of the Icelandic Constitution: „Freedom of expression may only be restricted by law in the interests of public order or the security of the State, for the protection of health or morals, or for the protection of the rights or reputation of others, if such restrictions are deemed necessary and in agreement with democratic traditions." Cf. the District Court's decision in Case K-8/2013 (under section 2.3. of this report).

In the District Court Case No. K-8/2013 the service provider claimed that Article 59 a of the Icelandic Copyright Act was not a legitimate restriction to the freedom of expression according to Article 73(3) of the Icelandic Constitution and Article 10 of the ECHR. The Court rejected the argument and ruled that Article 59 a of the Icelandic Copyright Act was a legitimate restriction to freedom of expression and fulfilled the conditions set out in Article 73(3) of the Icelandic Constitution and Article 10 of the ECHR.

The fact that there is such limited case law existing in Iceland in the field of blocking, filtering or take-down of illegal internet content makes it difficult to draw conclusions of the possible effect of the case law of the European Court of Human Rights in that field. In general however, though judgments of the European Court of Human Rights do not have binding effect,[86] the Icelandic Courts have sought to observe the interpretation of the European Court of Human Rights, as far as possible.[87]

Ingvi Snaer Einarsson
28.10.2015

[86] Cf. Art. 2 of Act No. 62/1994.

[87] Cf. Supreme Court Case No. 248/2005, where the Court observed the interpretation of Art. 6(4) of the ECHR in its judgement. Available at http://haestirettur.is/domar?nr=3530 (22.10.2015).