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 665-678

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.

SWEDEN

1. Legal sources for measures of blocking, filtering and take-down of illegal internet content

The blocking, filtering and take-down of illegal Internet content in Sweden is, as a rule, **not governed by legislation specific to the Internet**. Instead, legislation, but also various forms of soft laws and contractual terms by private actors that directly or indirectly relate to Internet content are to be found in numerous general or sector/matter-specific instruments.

In cases **of copyright or other intellectual property infringements**, the owners of such rights have the possibility to benefit from **injunctions** from the court in order to hinder Internet service provision to file-sharing websites that are violating such rights (Section 53 b of the Act on Copyright in Literary and Artistic Works (*Lag (1960:729) om upphovsrätt till litterära och konstnärliga verk*).

The legal tools available for **take-down/removal** of illegal Internet content are very limited, however, such measures can be imposed in certain circumstances according to the rules laid down in the **Act on Responsibility for Electronic Bulletin Boards**.[1] Electronic bulletin boards are services for mediation of electronic messages in the form of text, images, sound or other information, thus for example a website or a blog offering space for others to express themselves. According to the Act, the supplier of an electronic bulletin board **must remove a message**, or in some other way make it inaccessible, if it is obvious that the message is in breach of certain criminal offenses, for example agitation against an ethnic group or another group of persons with allusion to race, colour, national or ethnic origin, religious belief or sexual orientation, unlawful depiction of violence, etc.

The provisions in the **Penal Code** also apply when a **criminal offense is committed on the Internet**. Thus, the Internet is not a safe haven for criminal offenses such as defamation, unlawful threats, hate speech, sexual harassment, etc. The same applies for criminal offenses regulated in specific laws such as the Act on Sanctions for Terrorist Offences and the Personal Data Act.[2] There is, however, no specific law regulating the blocking, filtering or take-down of Internet content following criminal offenses. The Penal Code's rules on forfeiture of property may be relied on **to confiscate servers which have been used for illegal activities** such as unlawful file-sharing of copyright protected property.

The blocking of websites with **child sexual abuse** content is carried out in a **voluntary cooperation** between the Police and the ISPs: the so called Child Sexual Anti Distribution Filter.

Most blocking/filtering of Internet content is carried out by the Internet Service Providers ("ISP") in a **self-regulating** manner by means of their general terms and conditions applicable to their customers. Thus, in the absence of a legal framework Sweden has, in practice, to a large extent left blocking issues to **private actors**.

There are some relevant **international standards** contained in conventions relating to illegal Internet content which have **not yet been transposed** into the domestic regulatory framework. Sweden signed the Council of Europe's ***Convention on Cybercrime*** in 2001, but has not yet ratified it,

---

1 Lag (1998:112) om ansvar för elektroniska anslagstavlor, available in English (non-updated version) at http://www.government.se/content/1/c6/02/61/42/43e3b9eb.pdf (05.05.2015).

2 In Swedish: Brottsbalk (1962:700), Lag (2003:148) om straff för terroristbrott and Personuppgiftslag (1998:204).

although most provisions in the Convention are already covered by Swedish law.[3] Sweden has also signed but not yet ratified the ***Additional Protocol to the Convention on Cybercrime***. A Government-appointed Public Inquiry (SOU) presented in May 2013 the remaining legislative amendments necessary to permit ratification of the convention and its additional protocol by Sweden.[4]

The Council of Europe's ***Convention on Prevention of Terrorism*** and the ***Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse*** are, however, ratified and entered into force in 2010 and 2013 respectively. The Council of Europe's ***Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*** was ratified in 1985 and the EU's ***Data Protection Directive 95/46/EC*** was **transposed into Swedish law by enacting the Personal Data Act**, which replaced the Swedish Data Act from 1973 previously in force.

2. Legal framework

2.1 Blocking and/or filtering of illegal Internet content

2.1.1 Overview

There is **no law explicitly providing for blocking and/or filtering of illegal content on the Internet**. Indeed, a general legal obligation to block websites which contain illegal content would be likely to conflict with the constitutional protection of the freedom of expression and information. This is due to a large extent to the fact that it is not technically possible to block only the illegal information that is the aim of the measure; realistically, legitimate information that anyone has the right to procure would be blocked at the same time. Therefore, the problem with illegal Internet content has been addressed by other measures than legislation that specifically allows for blocking and/or filtering of websites. Thus, *in practice*, there are measures available to block/filter illegal Internet content, but the kind of measures available depend on the illegal content and/or the persons and bodies concerned.

In cases **of copyright or other intellectual property infringements**, the owners of such rights have the possibility, in accordance with the Act on Copyright in Literary and Artistic Works (*Lag (1960:729) om upphovsrätt till litterära och konstnärliga verk)*, to benefit from injunctions from the court in order to hinder access providers from providing Internet services to file sharing websites violating such rights. Hence, in technical terms it is a blocking of the provision of Internet access services rather than blocking of illegal Internet content. The question of whether intellectual property owners may also benefit from an injunction from a court to force an access ISP to block access to websites found to infringe copyright is currently being examined in a pending case at Svea Court of Appeal.[5]

The blocking of websites with **child sexual abuse** content is carried out in **voluntary cooperation** between the Police and the ISPs: the so called Child Sexual Anti Distribution Filter.

---

3 C. Kirchberger et al., Kluwerlaw online Cyber Law National Monograph Sweden, 2014, p. 237.

4 Government-appointed Public Inquiry SOU 2013:39 - Europarådets convention om it-relaterad brottslighet available at http://www.regeringen.se/content/1/c6/21/81/01/a83091f6.pdf (05.05.2015).

5 Case T 11706-15 at Svea Court of Appeal. (Following an appeal of the Stockholm District Court's judgment in case T 15142-14.) For further description and comments on the case see below section 2.1.5.

Most blocking/filtering of Internet content is carried out by the Internet Service Providers ("ISP") by means of the general terms and conditions applicable to their customers. Thus, in the absence of a legal framework Sweden has, in practice, to a large extent left these issues to **private actors**.
As regards **online gambling**, a Government-appointed Public Inquiry suggested that foreign online websites should be blocked for Swedish users. The proposals in the report were however subject to criticism on various grounds and did not lead to amendments to the current legislation.

2.1.2 Protection of copyright and other intellectual property

Intellectual Property rights are protected *inter alia* under the Act on Copyright in Literary and Artistic Works (*Lag (1960:729) om upphovsrätt till litterära och konstnärliga verk*).[6] There is no provision in this Act or any other law that obliges an ISP to block access to a website that contains copyright material. However, article 53 b of the Act states that upon a petition by the author or by a party that, on the basis of a license, has the right to exploit the work, the **Court may issue an injunction** prohibiting, on penalty of a fine, a party that commits, or contributes to, an act constituting an infringement or a violation of the protected copyright. The provision **implements Article 8(3) of the Directive 2001/29/EC** ("Infosoc Directive") which states that Member States shall ensure that right-holders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right.[7]

The question of an **Internet service provider's contribution (from a civil point of view) in its customers' infringement of the protected copyright has** been subject to considerable discussion in two cases in Swedish courts: the so-called Black Internet case and the so-called Portlane case.[8] In both cases, the plaintiffs demanded injunctions to prohibit the concerned ISPs from providing Internet service for Bit-Torrent trackers, which are servers that assist in communication between peers using the BitTorrent protocol.

In the **Black Internet case**, copyright holders filed a request for an injunction to prohibit the ISP Black Internet from providing Internet access services to **The Pirate Bay**. Both the District Court and the Court of Appeal held that since Black Internet provided Internet service to The Pirate Bay, and that it was established in the case that Black Internet was well aware of the copyright infringement conviction in the criminal proceedings against people behind The Pirate Bay, Black Internet objectively **contributed to the copyright infringement**, for which the copyright holders had shown probable cause. Therefore, the Court **prohibited by penalty of a fine Black Internet from providing Internet services to The Pirate Bay.**[9]

In the **Portlane case**, copyright holders filed a similar injunction to prohibit the ISP Portlane from providing Internet access services to one or more BitTorrent trackers connected with the domain name tracker.openbittorrent.com. The Court of Appeal held that the copyright holders had shown a probable cause that Portlane had objectively contributed to the copyright infringement and

---

6 Lag (1960:729) om upphovsrätt till litterära och konstnärliga verk available at http://www.riksdagen.se/sv/Dokument-Lagar/Lagar/Svenskforfattningssamling/Lag-1960729-om-upphovsratt-_sfs-1960-729/ (17.03.2015).

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

8 Decision of Svea Court of Appeal 21 May 2010 in case no Ö 7131-09 (Black Internet) and Decision of Svea Court of Appeal 21 May 2010 in case no Ö 10146-09 Portlane).

9 Decision of Svea Court of Appeal 21 May 2010 in case no Ö 7131-09.

therefore prohibited, by penalty of a fine, Portlane from providing Internet services to BitTorrent trackers.[10]

There is currently a case pending at the Svea Court of Appeal concerning an **ISP's alleged contribution (from a civil point of view) to infringements of the protected copyright on websites, accessed by their customers**[11] The case was brought by several music and film companies against Bredbandsbolaget, one of the major access ISPs in Sweden, following Bredbandsbolaget's refusal of their request to block the Pirate Bay website and the streaming portal Swefilmer. Bredbandsbolaget claims that Swedish law does not require ISPs to prevent their subscribers from accessing websites that may contain illegal material. It argues that placing this responsibility on the ISP risks hampering the principle and social policy of an open and free exchange of information on the Internet.[12] The case is pending at the Svea Court of Appeal following the plaintiffs' appeal of the District Court of Stockholm's ruling that Bredbandsbolaget could not be considered to have contributed to the copyright infringements on the websites in questions.[13] In its judgment, the District Court held that, generally, additional elements than mere provision of internet access services are required for holding an intermediary liable for contribution to an infringement.[14] It then noted that Bredbandsbolaget did not have any particular relationship with the Pirate Bay and Swefilmer and that only a very limited number of the ISP's customers had accessed those websites.[15]

2.1.3 Blocking of domain name

The non-profit **organization *Internetstiftelsen i Sverige* (IIS) controls the Internet Swedish top-level domain .se**. Since July 1, 2006, *IIS'* operations have been governed by the Act concerning National Top-level Internet Domains for Sweden.[16] Section 14 of the Act provides that if Sweden is in a state of war or in danger of war, the government may adopt regulations about the administration of a national top-level domain for Sweden to the extent that is necessary with regard to national security. The National Post & Telecom Agency (PTS) is the supervisory authority for IIS and thereby contributes to safeguarding the stable operation of the Swedish domain name system.

In a recent judgment from the Stockholm District Court, the **court ordered the forfeiture of the domain names thepiratebay.se and piratebay.se** on the grounds that they were used for copyright infringements.[17] The case is unique since it is the first time that a prosecutor requested forfeiture of a domain name in accordance with the relevant rules on forfeiture (*förverkande)* of property laid down in the Swedish Penal Code. The organisation *IIS*, however, opposed the prosecutor's demand to prohibit any future use of the two domain names. The court conceded that it could not force IIS to block certain domain names, but by the forfeiture it effectively ensured that the rights to the domain names are now property of the state. In practice, it means that IIS no longer can grant those domain names to a third party. The judgment has been appealed by the prosecutor and the case is currently pending before the Appellate Court.[18]

---

10 Decision of Svea Court of Appeal 21 May 2010 in case no Ö 10146-09..

11 Case T 11706-15 at the Svea Court of appeal. The paragraph in the present report concerning Case T 11706-15 and appealed Case T 15142-14 was revised and updated in April 2016

12 Bredbandsbolaget's reply in Case T 15142-14 at the District Court of Stockholm, aktbilaga 23, p. 6.

13 Case T 15142-14 at the District Court of Stockholm.

14 *Ibid*, p. 26

15 *Ibid*, p. 27.

16 Lag (2006:24) om nationella toppdomäner för Sverige på Internet.

17 Judgment of Stockholms Tingsrätt 19 May 2015 in case B 6463-13.

18 Svea Hovrätt (Appeal Court) Case nr T B 5280-15.

2.1.4. Blocking/filtering of child abuse images

Possession, access, distribution and exhibition of child abuse images are all unlawful actions under the Swedish Penal Code.[19] Such images shall be forfeited in accordance with the general rules on forfeiture in the Penal Code. The Act on forfeiture of child abuse images (*Lag (1994:1478) om förverkande av barnpornografi*) provides that images of child abuse shall nevertheless be forfeited in cases where the provisions on forfeiture in the Penal Code do not apply.

However, there is no specific legislation on the *blocking* of websites containing child abuse images. The government has expressed that legislation which provides that an authority shall block websites with certain content, or impose that the relevant ISPs block such websites, is difficult to reconcile with the freedom of information and the freedom of speech protected by the constitution.[20] In relation to this, the government has acknowledged the voluntary collaboration between the authorities and the ISPs.[21]
Thus, the **blocking of websites with child sexual abuse content** in Sweden is carried out in **voluntary cooperation** between the Police and the ISPs: the so called Child Sexual Anti Distribution Filter.[22] The cooperation is regulated by an agreement between the Police and the participating ISPs: the "Agreement on the limitation of access and distribution of child pornography on the Internet" (*Avtal om samarbete för att begränsa åtkomsten och spridningen av barnpornografi på Internet*). There are currently 13 ISPs that have signed the agreement.[23] It has been estimated that over 90% of subscribers to the Internet in Sweden are captured by this voluntary cooperation.[24] The agreement between the Police and the ISPs is not foreseen in legislation nor in any other kind of regulation.[25] Hence, there is no explicit legal basis for the agreement.

The cooperation operates in the following way: the Police receive information about websites that contain sexual abuse content from different channels such as Europol, Interpol, child right organisations or the general public. Information is also collected by the Police themselves. The information is scrutinized by the Police, who list all websites containing child abuse images (that are, as mentioned previously, deemed unlawful to possess, access, distribute and exhibit by the Penal Code). This assessment is made by the Police in accordance with the applicable law and case law.[26] The listed websites are then shared with the ISPs who make the technical arrangements for blocking access to the websites. Websites with child sexual abuse content will be blocked and made inaccessible in Sweden regardless of where in the world the site is located.[27]

---

19 Penal Code (*Brottsbalk (1962:700)*) chapter 16, section 10a.

20 Faktapromemoria 2008/09:FPM114 Rambeslut om bekämpande av sexuellt utnyttjande av barn, m.m., p. 10.

21 Yttrande 2008/09:KU7y Ett område med frihet, säkerhet och rättvisa i allmänhetens tjänst p. 14 and Faktapromemoria 2008/09:FPM114 Rambeslut om bekämpande av sexuellt utnyttjande av barn, m.m., p. 10.

22 https://polisen.se/Om-polisen/Olika-typer-av-brott/Brott-mot-barn/Barnpornografibrott/Test-av-barnpornografifiltret/ (17.03.2015).

23 Information from the Swedish Police Authority, email dated 25.09.2015.

24 http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/global-alliance-against-child-abuse/docs/commitements/ga_commitment_-_sweden_en.pdf, p 11 (17.03.2015).

25 Information from the Swedish Police Authority, email dated 25.09.2015.

26 The Agreement on the limitation of access and distribution of child pornography on the Internet (*Avtal om samarbete för att begränsa åtkomsten och spridningen av barnpornografi på Internet*), section 1.

27 http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/global-alliance-against-child-abuse/docs/commitements/ga_commitment_-_sweden_en.pdf, p. 12 (17.03.2015).

If the servers containing the unlawful material are based in Sweden, the Police will start an investigation and use coercive measures, such as search warrants, in order to make the unlawful material inaccessible and in order to collect evidence for a possible criminal procedure against the person responsible. If the servers are based in another country, the Police will send the information about the unlawful material to the Police authority in that country.[28]

Some ISPs have put in place additional services or measures in order to block access to websites containing child sexual abuse content.[29]

2.1.5 Blocking/filtering by ISPs in accordance with their general terms and conditions

Blocking/filtering of Internet content is carried out by the ISPs **by means of the general terms and conditions** applicable to their customers. For example, the major Swedish ISP access provider TeliaSonera's general terms and conditions state *inter alia* that TeliaSonera may "discontinue or limit the service provided" if a customer's use of the service infringes copyright or other intellectual property rights or conflicts with law or a public authority's regulations or decisions.[30] The same applies if the use of the service "leads to damage or other inconvenience to TeliaSonera or any third party".[31] Since this is a matter between the ISPs and their customers, it is difficult to know how those conditions are applied in practice.

The power held by private parties - ISPs - to censor and block Internet content has been criticized by, *inter alia*, the organization *IIS*, a non-profit organisation responsible for the Swedish top-level domain .se and which has as its aim to "promote the positive development of the Internet in Sweden".[32] In a report about freedom of speech on the Internet, ***IIS* argues that the ISPs' general terms and conditions are too general, giving the ISP too much discretion** as to when and how to take measures against an allegedly non-complying customer.[33]

2.1.6 Blocking/filtering of online gambling websites

The Swedish legislation on **gambling** requires that an operator is granted a licence by the Swedish Gambling Authority (*Lotteriinspektionen*) in order to supply online gambling in Sweden. Article 38 of the Lotteries Act (*Lotterilag (1994:1000*)) states that it is not permitted, in commercial operations or otherwise, for the purpose of profit to promote participation in unlawful lotteries arranged within the country or in lotteries arranged outside the country.[34] In the Government-appointed Public Inquiry *En framtida spelreglering (SOU 2008:124)*, the authors suggested that, *inter alia*, foreign

---

28 Information from the Swedish Police Authority, email dated 25.09.2015.

29 Cf. for example TeliaSonera's service "Child Service" which is a collaboration between TeliaSonera, NetClean and IWF. The service is offered to ISPs in order to block access to websites with child sexual abuse content (https://www.telia.se/privat/om/anmalan-overtradelser (22.04.2015)).

30 TeliaSonera General Terms and Conditions as of 1 September 2014, available at http://www.telia.se/privat/om/villkor (22.04.2015).

31 TeliaSonera General Terms and Conditions as of 1 September 2014, available at http://www.telia.se/privat/om/villkor (22.04.2015).

32 https://www.iis.se/english/about-se/ (29.04.2015).

33 A. Olsson, Yttrandefriheten på nätet – En guide om gränserna för det tillåtna på nätet (2009), p. 21, available at https://www.iis.se/docs/Yttrandefrihet_pa_natet.pdf (29.04.2015).

34 Lotterilag (1994:1000) available at http://www.riksdagen.se/sv/Dokument-Lagar/Lagar/Svenskforfattningssamling/Lotterilag-19941000_sfs-1994-1000/ (17.03.2015).

online gambling websites should be blocked for Swedish users.[35] The proposal was referred to different bodies for consideration and it was subject to criticism for various reasons. Some of the criticism was related to concerns whether the proposed blocking measures would be compatible with the freedom of speech whereas other argued that the proposal on IP blocks would not be an appropriate and effective measure for other reasons. .[36] The Public Inquiry did not result in any amendments to the present legislation. Hence, there is currently **no legislation allowing for blocking of foreign online gambling websites**.

2.1.7 Monitoring of websites used for terrorist purposes

The Swedish National Security Service (*Säkerhetspolisen*) monitors, on a regular basis, websites that might contain terror-related messages. The activity of the Security Service is regulated in the ordinance containing instruction to the Security Service (*Förordning (2002:1050) med instruktion för Säkerhetspolisen)*. There are, however, no provisions in the ordinance specifically concerned with the monitoring of websites.

If a crime is detected, the Security Service can initiate a preliminary investigation, however it is **not authorised to take any measures in order to shut down the website**. The Security Service may, however, notify the provider of the website about its content. The provider may then be obliged to remove the message from the website if the Act on Responsibility for Electronic Bulletin Boards is applicable (see section 2.2.2 below).[37]

2.2 Take-down/removal of illegal Internet content

2.2.1 Overview

Similar to the case of blocking and/or filtering illegal Internet content, there is no law which lays down a general legal obligation as regards the take-down/removal of illegal Internet content. As mentioned in section 2.1.1 above, it is due to the fact that such a law is likely to conflict with the constitutional protection of the freedom of expression and information. Nevertheless, take down/removal of illegal Internet content may be imposed according to the rules laid down in the **Act on Responsibility for Electronic Bulletin Boards** (Lag (1998:112) om ansvar för elektroniska anslagstavlor).[38] It is important to note, however, that take-down/removal of illegal Internet content is an extraordinary measure and the legal tools to impose such a measure are therefore very limited.

The Swedish **Data Protection Authority** may declare that the content of a website is offensive according to the Personal Data Act and therefore demand that the person responsible for the website remove the content. However, the authority has no power to block access or remove

---

35 En framtida spelreglering (SOU 2008:124) available at http://www.regeringen.se/sb/d/108/a/117594 (17.03.2015).

36 A Olsson, Sökes: En teknisk lösning på ondskans problem - En guide om filtrering av innehåll på nätet, 2010 .SE:s Internetguide nr 17, p. 60, available at https://www.iis.se/lar-dig-mer/guider/sokes-en-teknisk-losning-pa-ondskans-problem/ (17.03.2015), see also for example H. Jordahl, Sveriges digital tillväxtbransch – Nya perspektiv på behovet av en omreglerad spelmarknad, 2011, available at http://www.ifn.se/
publikationer/policy_papers/policy_papers/50_1 (29.04.2015).

37 Council of Europe's Committee of Experts on Terrorism, national policy brief for Sweden available at http://www.coe.int/t/dlapil/codexter/Source/cyberterrorism/Sweden.pdf (28.04.2015).

38 Lag (1998:112) om ansvar för elektroniska anslagstavlor, unofficial and non-updated English version of the law available at http://www.government.se/content/1/c6/02/61/42/43e3b9eb.pdf (06.05.2015).

content on a website and such decision is therefore merely a measure to put pressure on the responsible person in order for him or her to **voluntarily remove the content**.

The take-down/removal of illegal Internet content is in practice carried out by the ISPs in accordance with the general terms and conditions applicable to their customers. For further detail of how this is carried out see section 2.1.2 above.

2.2.2 Take-down/removal according to the Act on Responsibility for Electronic Bulletin Boards

The **Act on Responsibility for Electronic Bulletin Boards** (Lag (1998:112) om ansvar för elektroniska anslagstavlor) is the only legislation **specifically targeting content on the Internet**. Electronic bulletin boards are defined as a service for mediation of electronic messages in the form of text, images, sound or other information (section 1 of the Act). Examples of Electronic Bulletin Boards are services where users can perform functions such as uploading and downloading software and data, reading news and exchanging messages with other users. The aim of the law is that natural or legal persons who offer space to others to express themselves publicly (for example on a website, blog or social network) have a certain responsibility for those expressions.

When describing the Act on Responsibility for Electronic Bulletin Boards, it is important to mention that the rules on exemption of liability of service providers (*inter alia* host service providers) in Directive 2000/31/EC (**E-Commerce Directive)** has been transposed in a specific Act, namely the E-Commerce Act (*Lag (2002:562) om elektronisk handel och andra informationssamhällets tjänster)*. A potential contradiction between these two Acts as regards the responsibility of host service providers has, to our knowledge, not been subject to any substantial discussion or consideration in legal doctrine. However, it has been argued that it is difficult to assess the responsibility of host service providers in many situations and that the legislator therefore ought to act in this area.[39]

The main principles on liability in the Act on Responsibility for Electronic Bulletin Boards are found in sections 3 to 5. According to section 3, the supplier of an electronic bulletin board must notify each person who connects to the service of the identity of the supplier and to what extent messages posted will be available to other users. Section 4 provides that the supplier has an **obligation to supervise the service**, to an extent that is reasonable considering the extent and objective of the service.

According to section 5, the supplier **must remove a message**, or in some other way make it inaccessible, if it is *obvious* that the message is in breach of the following criminal offenses laid down in the Swedish Penal Code: **incitement of rebellion**, **agitation against an ethnic group or another group of persons** with allusion to race, colour, national or ethnic origin, religious belief or sexual orientation, portrayal or in any other way **making pornographic pictures of children available** to others, **unlawful depiction of violence**. Further, the supplier must also remove a message if it is *obvious* that the user, by submitting the message, has committed **copyright infringement.** In the preparatory works to the Act, the requirement that the breach shall be obvious to the supplier is motivated by the fact that it is not realistic to require the supplier to make difficult legal assessments.[40] Section 7 of the Act states that a person who intentionally, or through gross carelessness, violates Section 5 shall be sentenced to a fine or to imprisonment for not more than six months, or, if the offence is gross, to imprisonment for not more than two years.

---

39 L. Olsen, Näthat I form av hot – några reflektioner kring elektroniska tjänsteleverantörers ansvar, SvJT 2015 s. 297, 2015, p. 312.

40 Prop. 1997/98:15 s. 17.

The obligation to remove messages agitating against a group with certain sexual orientation has been subject to a ruling of the Swedish Supreme Court.[41] The **case concerned negative remarks about persons with homosexual preferences** that were posted on an electronic bulletin board (guestbook on a website) with reference to the Bible. The Court held that the messages objectively constituted agitation against an ethnic group in accordance with Chapter 16 section 8 of the Penal Code, but that this was not obvious to the supplier of the electronic bulletin board. The supplier was therefore released from all charges (see section 5 below for further comments on this case).[42]

The Act on Responsibility for Electronic Bulletin Boards does **not apply to services that are covered by the regulations in the Freedom of the Press Act or the Fundamental Law on Freedom of Expression**, such as the rule regarding databases found in Chapter 1 section 9 Fundamental Law on Freedom of Expression.[43] When those two fundamental laws are applicable, criminal charges can only be pressed for certain specific crimes that are specifically regulated or referred to in those laws. In such cases, there is always an assigned person, generally the editor of the media in question, who is primarily responsible for the illegal content.

A Committee of Inquiry has proposed that the criminal liability under the Act on Responsibility for Electronic Bulletin Boards should be broadened to cover unlawful threats and unlawful violation of privacy. The report, *Integritet och straffskydd* (SOU 2016:7), has been circulated for comments to relevant consultation bodies.[44] A Government Bill dealing with these issues is expected to be put before Parliament in the spring of 2017.

2.2.3 Privacy law and the Data Protection Authority

The Swedish Data Protection Authority (*Datainspektionen*) cannot block access or remove content on a website. However, it may render decisions stating that the processing of personal data on a website is offensive according to the Personal Data Act and therefore order the person responsible to remove the content. Since it cannot make such an order subject to a fine, nor decide that damages shall be awarded, the decision is, in practice, a measure to **put pressure on the person in order for him or her to voluntarily remove the offensive content**.[45] It is, however, only the police that may investigate and pursue criminal offenses such as defamation.

The authority has a **specific website to inform and advise victims of offensive treatment on the Internet** on how they can deal with such problems.[46] For example, it informs on how to report offensive material on different social Medias such as Facebook and Twitter and how to apply to Google to have a search hit removed.

In May 2014, the government decided to mandate a **Government-appointed Public Inquiry** (*Ett modernt och starkt straffrättsligt skydd för den personliga integriteten, dir. 2014:74*), with the mandate of **examining the protection in penal law for privacy**, in particular as regards threats and offensive treatment on the Internet.[47] The Government considers that there is a need for such an

---

41 Decision by Supreme Court 7 Nov. 2007, in case NJA 2007 s. 805.

42 For comments on the decision see for example Kluwerlaw online Cyber Law National Monograph Sweden, C. Kirchberger et al., p. 197.

43 Government bill (Proposition) 1997/98 :15 Ansvar för elektroniska anslagstavlor, p. 12.

44 The report is available at http://www.regeringen.se/contentassets/207048837827439b9d1dce919d0dd6f9/integritet-och-straffskydd-sou-20167 (12.04.2016).

45 Information available at http://www.krankt.se/foer-dig-som-blivit-kraenkt-pa-internet (22.04.2015).

46 http://www.krankt.se/om-kraenktse (22.04.2015).

47 A description of the mandate is available in Swedish at http://www.regeringen.se/sb/d/18313/a/241321 (29.04.2015).

inquiry since the technical development has led to the negative effects that threats and offensive treatment have taken new forms while the penal law in the area is partly obsolete.[48] The results of the Public Inquiry were presented in February 2016 in the report, *Integritet och straffskydd* (SOU 2016:7)."

In a motion to the Parliament, several members of Parliament have proposed that the Government shall put in place an **Internet Ombudsman** (*nätombudsman*) as a new authority with the task of supporting victims of threats and offensive treatment on the Internet. According to the motion, the Internet Ombudsman shall be tasked to help victims to make website operators remove offensive material and to offer assistance to report criminal offences to the Police. Further, the Ombudsman shall also have the right to take civil actions before the courts in order to claim damages from the offending party.[49] The Parliament, however, rejected the motion. The majority noted that there is a Government-appointed Public Inquiry on the protection in penal law for privacy, in particular as regards threats and offensive treatment on the Internet (see above), and argued that it is important to wait for the results of that inquiry before taking legislative actions in the area.[50]

3. Procedural Aspects

3.1 Protection of copyright and other intellectual property

Article 53 b of the Act on Copyright in Literary and Artistic Works (Lag (1960:729) om upphovsrätt till litterära och konstnärliga verk) states that upon a petition by the author or by a party that, on the basis of a license, has the right to exploit the work, the **district court** may issue an **injunction** prohibiting, on penalty of a fine, a party that commits or contributes to an act constituting an infringement or a violation of the protected right. The provision implements Article 8(3) of the Infosoc Directive which states that Member States shall ensure that right-holders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right.

A **decision of the District Court may be appealed** to the Court of Appeal. Further, the Supreme Court may grant leave to appeal, thus allowing for the appeal of the Court of Appeal's decision.

3.2 Act on Responsibility for Electronic Bulletin Boards

Section 5 of the Act on Responsibility for Electronic Bulletin Boards provides that a supplier of an electronic bulletin board must remove a message or in some other way make it inaccessible, if it is obvious that the message is in breach of certain criminal offenses or constitutes a copyright infringement (see section 2.2.2 above). Section 7 of the Act states that a person who intentionally, or through gross carelessness, violates Section 5 shall be sentenced to a fine or to imprisonment for not more than six months, or, if the offence is gross, to imprisonment for not more than two years.

The **law enforcement authorities (police and prosecutor) investigate and prosecute** a person violating the law. A **judgment rendered by the District Court may be appealed to** the Court of Appeal and the Supreme Court may grant leave to appeal of the Court of Appeal's decision.

---

48 Ibid.

49 The motion to the Parliament is available at http://www.riksdagen.se/sv/Dokument-Lagar/Ovriga-dokument/Ovrigt-dokument/Natombudsman_H202189/?text=true (05.05.2015).

50 *Konstitutionsutskottets betänkande 2014/15:KU15*, p. 19, avaialble at http://data.riksdagen.se/fil/B10657D9-2B5E-4FD6-97DE-77D0FC8B53B2 (25.10.2015).

3.3 Blocking/filtering of child abuse images

As described above in section 2.1.3, blocking of websites with a child sexual abuse content in Sweden is carried out in voluntary cooperation between the Police and the ISPs. Websites containing child abuse content are listed by the Police and shared with the ISPs, who then make the technical arrangements for blocking access to the websites. The websites are then inaccessible in Sweden, regardless of where in the world the website is hosted.

This self-regulating regime has been criticized in a report by the organisation IIS, arguing that this kind of censorship is carried out without support in law and that there are no legal measures available to a person whose website has been allegedly wrongfully blocked. It is true that **the decision to block a website cannot be appealed to an administrative body or a court.** Furthermore, no one can be held responsible if the blocking measure mistakenly censors a website that does not contain illegal content.[51]

Similar criticism has been expressed in relation to ISPs. As described in section 2.1.2 above, the ISPs may also limit their services, for example close down the Internet service provided to a customer following an alleged **non-compliance with the general terms and conditions** applicable to the customer. Such a measure cannot be appealed. The organization .SE has expressed concern that the ISPs' general terms and conditions are too general, giving the ISPs too much discretion as to when and how to take measures against an allegedly non-complying customer.[52]

4. General monitoring of Internet

In Sweden, there is **no entity in charge of general monitoring of Internet content**. However, monitoring of Internet content related to certain specific matters is carried out, to a greater or lesser extent, by different bodies.

The **National Defence Radio Establishment** (*Försvarets radioanstalt*) is the Swedish national authority for signal intelligence.[53] It is a civil authority subordinated to the Ministry of Defence and supplies intelligence to the Government, the Swedish Armed Forces and to other concerned authorities. It may not initialize any surveillance on its own and operates purely on instruction from the Government, the Government Offices (*Regeringskansliet)*, the Armed Forces (*Försvarsmakten)*, the National Operative Department of the Police (*Nationella operativa avdelningen inom Polismyndigheten*) and the Swedish Security Service (*Säkerhetspolisen*).

The National Defence Radio Establishment's **collection of information, for example which searches words that may be used, is subject to approval by the Defence Intelligence Court** (*Försvarsunderrättelsedomstolen*). The Defence Intelligence Commission (*Statens inspektion för försvarsunderrättelseverksamheten*) monitors that the National Defence Radio Establishment carries out its activities in accordance with applicable laws. Additional control as regards protection of personal data is carried out by the Swedish Data Protection Authority (*Datainspektionen*).[54]

---

51 A. Olsson, Yttrandefriheten på nätet – En guide om gränserna för det tillåtna på nätet (2009), p. 20, available at https://www.iis.se/docs/Yttrandefrihet_pa_natet.pdf (29.04.2015).

52 A. Olsson, Yttrandefriheten på nätet – En guide om gränserna för det tillåtna på nätet (2009), p. 21, available at https://www.iis.se/docs/Yttrandefrihet_pa_natet.pdf (29.04.2015).

53 Information about the authority available at http://www.fra.se/index.html (19.03.2015).

54 http://www.fra.se/omfra/myndighetenfra/tillstandkontrollochgranskning.86.html (19.03.2015).

Article 1 in the Act (2008:717) on signal intelligence within defence intelligence operations (*Lag (2008:717) om signalspaning i försvarsunderrättelseverksamhet)* states that signal intelligence is only permitted in order to assess (1) external military threats to the country; (2) conditions for Swedish participation in peace support operations and international humanitarian efforts or any threat to the security of national interests in the implementation of such efforts; (3) strategic matters regarding international terrorism or other serious transnational crime that could threaten important national interests; (4) development and proliferation of weapons of mass destruction, military equipment and items referred to in the law on the control of dual-use items and technical assistance; (5) serious external threats to the public infrastructure; (6) conflicts abroad with ramifications for international security; (7) foreign intelligence operations against national interests; or (8) foreign powers actions or intentions that are of vital importance to Swedish foreign policy or security and defence policy.[55]

As regards **child pornography**, the Police receive information from different channels such as Europol, Interpol, organizations for the protection of children and the general public. **Information is also collected by the Police themselves e.g. on the Internet**.[56] As mentioned in section 2.1.3 above, the information collected is listed by the Police and shared with the ISPs who then can make the technical arrangements for blocking access to the websites.

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

In addition to the regulation in the European Convention on Human Rights, which has applied as domestic law since 1995, freedom of speech is regulated in three different constitutional laws: the Instrument of Government (*Regeringsformen (1974:152)*), the Freedom of the Press Act (*Tryckfrihetsförordning (1949:105))* and the Fundamental Law on Freedom of Expression (*Yttrandefrihetsgrundlag (1991:1469)*). The Instrument of Government protects, in a general manner, freedom of speech and freedom of information (Chapter 2 section 1). Additional protection is granted for expressions in books or other kinds of media (including online press), which fall under The Freedom of the Press Act or the Fundamental Law on Freedom of Expression.[57]

Take-down/removal of illegal Internet content may be imposed in certain circumstances according to the rules laid down in the **Act on Responsibility for Electronic Bulletin Boards.** As mentioned in section 2.2.2 above, the obligation under this law to remove messages has been dealt with by the Supreme Court in case *NJA 2007 s. 805* that concerned negative remarks about persons with homosexual preferences posted on an electronic bulletin board (guestbook on a website) with reference to the Bible. In its judgment, the Court referred to Article 10 of the ECHR and the criteria developed in the case law of the ECtHR. The Court particularly discussed whether the restriction of freedom of speech in a hypothetical convicting judgment could be considered "necessary in a democratic society". It held that the margin of discretion to restrict the freedom of speech is particularly limited when the matter concerns political views or discussions of public interest and that not only the content itself of the expression matters, but all the circumstances in the specific case. In this regard, the Court noted that the expressions referred to bible texts and that they had been exchanged in the form of a discussion between persons who had actively chosen to visit the

---

55 Lag (2008:717) om signalspaning i försvarsunderrättelseverksamhet available at http://www.riksdagen.se/sv/Dokument-Lagar/Lagar/Svenskforfattningssamling/sfs_sfs-2008-717/ (05.05.2015).

56 http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/global-alliance-against-child-abuse/docs/commitements/ga_commitment_-_sweden_en.pdf, p. 12 (17.03.2015).

57 For further reading see for example Kluwer Law Online – IEL Constitutional Law National Monographs Sweden Part IV Human Rights and Judicial Review (2014).

website and its discussion forum. The Court finally ruled that the messages objectively constituted agitation against an ethnic group in accordance with Chapter 16 section 8 of the Penal Code, but that this was not obvious to the supplier of the electronic bulletin board and the supplier was therefore released from all charges.[58]

The reasoning of the Court reflects that the removal of illegal Internet content under the Act on Responsibility for Electronic Bulletin Boards shall be assessed taking due account of the fundamental right of freedom of expression. Further, it shall be noted that the scope of application of the law is limited (see section 2.2.2 above) and clearly indicated. Therefore, it is our opinion that **the law meets the requirements of foreseeability, accessibility, clarity and proportionality as developed by the European Court of Human Rights**.

There has not been any extensive discussion by the courts and/or legal scholars on the safeguarding of freedom of expression in relation to injunctions in order to protect **copyright protected material.** In the cases noted in section 2.1.6 above concerning injunctions to prohibit the ISPs in question to provide Internet service for Bit-Torrent trackers used for file sharing activities, the courts simply held that the injunctions were proportionate and in accordance with the freedom of speech as regulated in the Swedish Constitution and in the ECHR.[59]

As presented above, the possibilities to block, filter and take down illegal content on the Internet are very limited. In practice, removal and limitation on using Internet services to access illegal content are almost exclusively carried out by the ISPs in accordance with the general terms and conditions applicable to their customers. Some concerns have been raised by the organization *Internetstiftelsen i Sverige* (IIS) regarding this kind of self-regulating system carried out by private parties. In particular, IIS has in a report argued that the **ISPs general terms and conditions are too general, thereby giving the ISPs too wide margin of discretion** as to when and how to take measures against allegedly non-complying customers. Furthermore, it has criticized the fact that **the decision of the ISPs are not subject to legal review by an independent body or the court**s.[60] While the ISPs appear to be reluctant to resort to measures amounting to blocking, filtering or take down of Internet content, it is true that there are no legal rules and guarantees put in place in order to prevent potential general blocking activities.

The **blocking of websites with a child sexual abuse content** is carried out in a **voluntary cooperation** between the Police and the ISPs: the so called Child Sexual Anti Distribution Filter, covering some 90% of subscribers to the Internet in Sweden (see section 2.1.3 above). Some concerns have been expressed that there is no transparency and third party control as regards the maintenance of the list of blocked websites, and that there is no legal ground by which to appeal a list entry.[61]

Although the ISPs' margin of appreciation and the voluntary cooperation between the Police and the ISPs to block websites with child sexual abuse content have been subject to criticism for the reasons stated above, this criticism appears to be rather limited, in particular in legal literature. The view of this author is that the ISPs' margin of appreciation and the lack of judicial review could be problematic since it entails the need to rely on the ISPs' good will to not carry out unlawful censorship. It raises questions about the responsibility of a state to put in place legal safeguards for

---

58 For comments on the decision see for example Kluwerlaw online Cyber Law National Monograph Sweden, C. Kirchberger et al., p. 197.

59 Decision of Svea Court of Appeal 21 May 2010 in case no Ö 7131-09and case no Ö 10146-09.

60 A. Olsson, Yttrandefriheten på nätet – En guide om gränserna för det tillåtna på nätet (2009), p. 20, available at https://www.iis.se/docs/Yttrandefrihet_pa_natet.pdf (29.04.2015).

61 See reference to Marcin de Kaminski in Internet Policy Review – Journal on Internet regulation available at http://policyreview.info/node/127/pdf (05.05.2015).

compliance with freedom of expression and other related rights when these matters are left to private parties.

However, in support of the Swedish largely un-regulated system one may note that, to our knowledge, there are no indications that the State actively encourages the ISPs to block or take down Internet content. On the contrary, Sweden has a strong tradition of freedom of expression and the Swedish government takes an active role in promoting freedom on the Internet.[62] Furthermore, and as mentioned above, it appears as if the **ISPs themselves are reluctant to limit access to Internet content**. This may be illustrated by the pending case between several music and film companies on the one side and the major ISP *Bredbandsbolaget* on the other side, concerning the refusal of the latter to follow the request by the music and film companies to block the *Pirate Bay* website and the streaming portal *Swefilmer* to its customers.

Henrik Westermark
01.11.2015

Revised on 03.05.2016 taking into consideration comments from Sweden on this report

62 See for example The role of governments in protecting and furthering Internet freedom, report from the Ministry of Foreign Affairs of the Netherlands, p. 5, available at https://www.freedomonlinecoalition.com/wp-content/uploads/2014/04/Background-Paper-NL-The-Role-of-Goverments-in-Protecting-Internet-Freedom.pdf (27.07.2015) and Internet freedom and development - A qualitative study of Internet freedom and Sweden's global importance with respect to Internet freedom issues, report from the Swedish Institute (SI), p. 3, available at https://si.se/wp-content/uploads/2013/11/SI_Internet-freedom_A4_WEB.pdf (27.07.2015).