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 507-520

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.

NORWAY

1. Legal Sources

The measures available for blocking, filtering and take-down of illegal Internet content in Norway are **not governed by legislation or rules specific to the Internet**. Instead, such measures may be taken in accordance with provisions laid down in general or sector specific legislation such as the Penal Code and the Copyright Act.

With regard to **Intellectual Property rights**, right holders may rely on injunctions from a court to block access to a website where material is being made available that evidently infringes copyright or other protected rights (Section 56c of the Act relating to copyright in literary, scientific and artistic works, etc. (*Lov om opphavsrett til åndsverk m.v.*)).

The general **Penal Law provisions on confiscation and seizure** also apply to illegal Internet content and domain names. Thus, illegal Internet content may be confiscated following a court decision in accordance with Section 69 and 76 of the Penal Code (*straffeloven)*. Section 76 specifically addresses the confiscation of electronic data. Seizure of illegal Internet content may be carried out under Section 203 in the Criminal Procedure Act (*Straffeprosessloven)*.

Websites containing child abuse material illegal under the Penal Code, may be blocked by an access Internet Service Provider (ISP) through the use of the **Child Sexual Abuse Anti-Distribution Filter** (CSAADF); this body is a **voluntary cooperation** between the major ISPs and the Police. The filter and blocking procedure is **not foreseen in any law**.

The provisions in the **Penal Code**, for example on unlawful threats, hate speech, sexual harassment, etc., also apply when a **criminal offense is committed on the Internet**.

Finally, it is worth noting that significant blocking/filtering and take-down of Internet content is carried out by the ISP by means of their general terms and conditions, applicable to all of their customers. In this manner, the ISPs seek to protect themselves from liability in any controversy regarding Internet content.

Many **International standards** contained in conventions relating to illegal Internet content have **been transposed** into the domestic regulatory framework. The Council of Europe's ***Convention on Cybercrime*** entered into force 1 October 2006 and the ***Additional Protocol to the Convention on Cybercrime*** entered into force 1 August 2008.

Further, the Council of Europe's ***Convention on Prevention of Terrorism*** entered into force 1 June 2010 and the ***Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*** entered into force 1 October 1985. The Council of Europe's ***Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse*** is signed but not ratified. The EU's ***Data Protection Directive 95/46/EC*** is transposed into Norwegian law through the Personal Data Act (*Lov om behandling av personopplysninger 14.4.2000 no 1).*

2. Legal Framework

2.1. Blocking and/or filtering of illegal Internet content

The measures available for blocking and filtering of illegal Internet content in Norway are **not governed by legislation specific to the Internet**. Provisions are instead laid down in general or wider area specific laws.

As will be described below, there is a legal framework for blocking or filtering in order to protect copyright and other intellectual property. Further, and although not foreseen in law, blocking and filtering is also carried out by ISPs by employing the Child Sexual Abuse Anti-Distribution Filter and by means of the particular ISP's general terms and conditions (as regards the latter, see section 2.2.3 below).

2.1.1. Protection of copyright and other intellectual property

Intellectual property rights are protected *inter alia* under the **Act relating to copyright in literary, scientific and artistic works, etc. (Copyright Act)** (*Lov om opphavsrett til åndsverk m.v.*).[1] In a 2013 amendment to the law, a new chapter – chapter 7 a - was introduced dealing specifically with measures in relation to infringements of copyrights and other related rights on the Internet.

Section 56c of the Act provides that upon a petition from a rights holder, the court may order a provider of electronic communication services who transfers, provides access to or saves content, to **hinder access to a website** where, material is being made available to a great extent, that evidently infringes copyright or other rights in accordance with the Act.

A **test of proportionality** shall be carried out, by which the court deciding on the injunction shall weigh the interests and the inconveniences of the blocking measure. Section 56 C of the Copyright Act provides that in the balancing act the court shall consider the interests motivating the blocking of access to the website on the one hand, and on the other hand, other interests affected by such order, including, primarily, the interest of the subject that is directly concerned by the order (i.e. the access ISP) and the owner of the website. According to the preparatory works to the law, the court shall in this regard take into account considerations such as gravity, scope and damaging effects of the infringement and whether legitimate third parties including consumer are affected.[2] Further, the court shall **take into consideration the freedom of information and expression** and the possibility of using alternative and less restrictive measures. As regards the freedom of information and expression, the preparatory works to the Copyright Act state that the court shall consider *inter alia* whether the measure will affect lawful content and, if that is the case, how worthy of protection the affected lawful material is.[3]

In a recent decision from the Oslo District Court, the **court ordered several ISPs to block access to their customers to seven websites where copyrights were infringed**, among others the file sharing website the **Pirate Bay**.[4] The decision was taken following a petition by a number of film and music companies and organizations. The court based its decision on section 56c of the Copyright Act (see description above of the provision). The court initially found that reasonable measures had been taken by the rights holders to first identify and address the owners of the websites in questions.

---

1 Lov om opphavsrett til åndsverk m.v. 1961-05-12-2, available in Norwegian at https://lovdata.no/dokument/NL/lov/1961-05-12-2?q=%C3%A5ndsverklove (06.10.2015).

2 Prop.65 L (2012-2013), p. 91.

3 Ibid.

4 Oslo tingrett decision 2015-09-01 in case TOSLO-2015-67093.

According to the court it was not necessary for the rights holders to first request that the Pirate Bay's service providers stop the infringement. The reasoning was that such a measure would be complicated and burdensome for the rights owners and presumably not effective considering that the Pirate Bay easily could have changed service providers. In this finding, the court stressed the fact that it was a foreign website and that the operator of the website had not provided contact information in accordance with the rules set out in the E-Commerce Directive.[5]

As regards the **protection of freedoms of information and expression** in the Constitution and in Article 10 of the European Convention on Human Rights (ECHR), the court found that the blocking would not violate those rights. The court reasoned that the material in question was far from what is to be considered as the core of which the rules on freedom of information and expression are supposed to safeguard. In that regard it held that about 90 % of the material on the Pirate Bay website was estimated to be unlawful and noted that the material was available lawfully on other websites.[6] The court limited the injunction to 5 years.[7] To our knowledge, the decision has not been appealed.

In an earlier case from 2010, a Norwegian Court of Appeal rejected a request to order an ISP to block access to the Pirate Bay website.[8] The requesting rights holders argued that the ISP was contributing to the illegal file sharing carried out by its customers. The court, however, found that **the ISP could not be considered as contributing to the infringement** under the rules in Copyright Act. Further, the court found that the implementation of the Directive 2000/31/EC (E-Commerce Directive) in Norwegian law did not provide for any obligation of ISPs and other providers of electronic communication services to block illegal content. Amendments to the law allowing for such injunctions were subsequently adopted in 2013. It explains how the Oslo District court in a similar case from 2015 could order the blocking of the Pirate Bay and similar websites.

2.1.2. Blocking/filtering of child abuse content

Possession, access, distribution and exhibition of material containing child abuse content are unlawful under Article 311 of the Norwegian Penal Code (*Straffeloven)*. There is however **no specific legislation on the blocking of websites** containing child abuse content. It may be noted that the general Penal Law rules on confiscation and seizure apply and may be relied on and thus, to some extent, limit the spreading of child abuse material (see commentary on those rules below in section 2.2.1).

The solution chosen to deal with the issue is, however, similar to other Nordic countries, primarily the use of a filter to isolate websites containing child abuse content. In 2004, the major ISP access provider Telenor and the National Criminal Investigation Service (*den nasjonale enhet for bekjempelse av organisert og annen alvorlig kriminalitet - Kripos*) (NCIS), the Norwegian police agency that deals with organized and other serious crimes, began cooperating in order to limit the amount of child abuse material on the Internet. This work resulted in the so called **Child Sexual Abuse Anti-Distribution Filter** (CSAADF). Today, all major Norwegian access ISPs take part in this **voluntary cooperation** between the ISPs and the NCIS.[9]

---

5 Ibid, p. 11.

6 Ibid, p. 9.

7 Ibid, p. 14.

8 Borgarting lagmannsrett decision 2010-02-09 in case LB-2010-6542 - RG-2010-171.

9 Information from the Kripos website: https://tips.kripos.no/cmssite.asp?c=1&h=41&menu=2 (06.10.2015).

The filter is a blacklist of DNS addresses maintained and distributed by the NCIS. The blacklist is established by the NCIS in accordance with its assessment of the kind of material that is unlawful under Article 311 of the Norwegian Penal Code.[10] The ISPs implement the blacklist in their DNS servers by redirecting attempts to access blacklisted websites to a page with a warning message.[11]

The blacklist and the voluntarily cooperation between the Police and the ISPs are **not based or foreseen in legislation nor in any other kind of regulation**, but merely defined in a written contract between the participating ISPs and the NCIS.[12] In 2008, the Norwegian Minister of Justice sent a letter to all Norwegian ISPs stating that unless participation to the voluntary filtering scheme became universal, the minister would consider adopting legislation making the filter mandatory.[13] The blacklist is thus generated without judicial control. Furthermore, it is kept secret by the NCIS and the ISPs using it.[14] A list of supposedly blocked addresses was posted to Wikileaks in March 2009, containing 3,518 DNS addresses. According to Wikileaks, many of the websites on the Norwegian list had no obvious connection to child pornography.[15]

2.1.3. Calls for reforms and discussions in the doctrine

In 2002, the Norwegian Government commissioned a study on cybercrime conducted by a Data Crime Committee.[16] In this study, presented in 2007, the Committee discussed *inter alia* the feasibility of adopting rules allowing for **filtering of foreign websites that contain unlawful material**. The Committee recognized that the rules on confiscation, a tool used for websites based in Norway, could not be used for foreign websites.[17] The conclusion of the majority of the members of the Committee was that no rules on filtering of foreign websites should be adopted. There appeared to be three main arguments for this finding. first; because of the risk that such rules would not be compatible with Article 10 ECHR, second; that there would be an obvious risk that lawful material may be blocked, and third; that the measure in any case would be easy to circumvent and thus not effective.[18]

As regards child abuse material, the **Committee suggested maintaining the current situation whereby filtering is carried out under the Child Sexual Abuse Anti-Distribution Filter**. It held that the voluntary collaboration between the authorities and the ISPs in this field is a procedure that functions well, despite the fact that not all ISPs participate. The introduction of a **system where a prosecutor must apply to a court for the blocking of websites containing illegal Internet content would be impractical and costly** according to the Committee and it was therefore not recommended to introduce such a legal framework.[19]

---

10 NOU 2009:1 Individ og integritet - Personvern i det digitale samfunnet, p. 230.

11 Information from the Kripos website: https://tips.kripos.no/cmssite.asp?c=1&h=41&menu=2 (06.10.2015).

12 Global Alliance Against Child Sexual Abuse Online – 2014 Reporting Form, Norway, 2014, p. 11, available at http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/global-alliance-against-child-abuse/docs/reports-2014/ga_report_2014_-_norway_en.pdf (18.11.2015).

13 http://www.nrk.no/nyheter/1.6220557 (30.10.2015).

14 R. Deibert *et al.*, Access Controlled - The Shaping of Power, Rights, and Rule in Cyberspace, 34 b&w illus 2010, 34 p. 330. The text is also available at https://opennet.net/research/regions/nordic-countries (06.10.2015).

15 Ibid.

16 NOU 2007: 2 Lovtiltak mot datakriminalitet – Delutredning II.

17 Ibid, p. 120.

18 bid, p.121.

19 Ibid, p.122.

The relevant literature has discussed how violation of privacy on the Internet can more effectively be addressed. One author, *Sunde*, has addressed the issue of protection of privacy in social media and the **problem with ecosystem effects**.[20] By ecosystem effects she refers to the fact that expressions in social media can spread to other places both within and outside the social network and thereby reach a wider public. A violation of privacy may thus in many cases be difficult to stop. In order to safeguard the respect for privacy protected under Article 8 of the ECHR, she advocates for enabling the Prosecution Authority to actively filter illegal Internet content.[21] She also argues[22] that the state's positive obligation to protect the rights of its citizens is particularly important in relation to children and refers to the ECtHR's judgements in cases K. U. v. Finland[23], M.C. v. Bulgaria[24] and X and Y against v. Netherlands[25]. In practice, it is suggested that filtering is carried out by placing the filter on the ISP level or on the server to a host provider. The blocking will then be carried out following a matching of data files against a database which contain unlawful files already duly confiscated in accordance with the relevant provision in the Penal Code. The blocking may be carried out if the data files are duplicates (identical) or sufficiently similar to those already confiscated so that there can be no doubt of their illegality. According to the same author, the filtering would not require new legislation but can be carried out under the rules on confiscation provided for in section 69 in the Penal Code. [26] Further, sufficient legal safeguards would be awarded through the judicial review by courts.[27]

In 2007, the government appointed a Privacy Commission (Personvernkommisjonen) tasked with examining the legal framework related to the protection of privacy on the Internet. In its report *NOU 2009:1 Individ og integritet - Personvern i det digitale samfunnet* the Commission **proposed the establishment of a dispute settlement body**.[28] It was suggested that the body should be tasked with resolving conflicts resulting from expressions on the Internet and contribute to the development of ethical guidelines on expressions on the Internet.[29]

According to the Commission, the need for such a body was driven by the fact that many people use their expression on the Internet in order to harm others by bullying, harassment and diversion of personal information, hateful speech and copyright infringements etc. The authors of the report argued that the resolutions of disputes on these matters in courts are not satisfactory for a number of reasons. One of the main arguments was that **many of the conflicts related to expressions on the Internet concern youth and children and there is a need to act rapidly to limit the damages** for these persons. The comparably slow process in the ordinary judiciary system is not well suited for such rapid intervention. Furthermore, the person harmed by the expression may not have the means to bring legal action in court and the infringing party may not be able to pay compensation.[30]

According to the authors of the report, the dispute settlement body should be regulated in law, receive funding by the State and act in accordance with the Electronic Commerce Act. Furthermore,

---

20 I. Sunde, Økosystemeffekten - Om personvernet i sosiale medier, Lov og Rett 2013 nr. 1 s. 85-102.

21 I. Sunde, Økosystemeffekten - Om personvernet i sosiale medier, Lov og Rett 2013 nr. 1 s. 85-102.

22 I. Sunde, Økosystemeffekten - Om personvernet i sosiale medier, Lov og Rett 2013 nr. 1 s. 85-102, p. 97.

23 ECtHR, K.U. v. Finland, Judgement of 2 December 2008.

24 ECtHR, M.C. v. Bulgaria, Judgement of 4 December 2003.

25 ECtHR, X and Y v. the Netherlands, Judgement of 26 March 1985.

26 I. Sunde, Økosystemeffekten - Om personvernet i sosiale medier, Lov og Rett 2013 nr. 1 s. 85-102, p. 99.

27 I. Sunde, Økosystemeffekten - Om personvernet i sosiale medier, Lov og Rett 2013 nr. 1 s. 85-102, p. 99.

28 NOU 2009:1 Individ og integritet - Personvern i det digitale samfunnet. Available at https://www.regjeringen.no/no/dokumenter/nou-2009-1/id542049/ (30.10.2015).

29 Ibid, p. 122.

30 Ibid.

it should be authorized to order the rectification, cancellation and the take-down of material.[31] To our knowledge, the report has **not resulted in any legislative reforms in order to establish the proposed dispute settlement body**.

2.1.4. Restrictions on the use of electronic communications networks under the Electronic Communications Act

Although it does not technically provide for blocking/filtering or take-down of illegal Internet content, it is relevant that the Electronic Communications Act (*Lov om elektronisk kommunikasjon LOV-2003-07-04-83*) Chapter 2 Section 5 states that the relevant Authority (which includes the King, the Ministry and the Norwegian Post and Telecommunications Authority) may order providers to implement restrictions on the use of electronic communications networks and services in the interest of national security or other important societal consideration. Providers shall implement necessary restrictions on Internet use in emergency situations that involve serious threats to life or health, safety or public order, or danger of sabotage against networks or services.

2.2. Take-down/removal of illegal Internet content

Similar to the situation for blocking and filtering, the measures available for take down/removal of illegal Internet content in Norway are **not governed by legislation specific to the Internet**. Provisions are instead laid down in general or sector specific laws such as the Penal Law and the Personal Data Act.

As will be described below, the legal tools available for take down/removal of Internet content are confiscation and seizure and, as regards data protection, the Data Protection Authority's order of removal. Further, take down/removal is carried out by the ISPs on their own initiative with reference to their general terms and conditions.

2.2.1. Penal law provisions on confiscation and seizure

Provisions on confiscation are laid down in chapter 13 of the Penal Code. Section 69 in that chapter provides that objects that have been produced by or been the subject of a criminal act may be confiscated *(inndragning)*. The same applies to objects that have been used or intended for use in a criminal act. It explicitly states that rights, claims and electronically stored information are considered to be objects under the provision. Hence, **illegal Internet content may be confiscated and thus effectively taken down/removed** on the basis of this provision. Illegal Internet content may, for example, be unlawful use of copyright protected material, incitement to terrorism, hate-speech, defamation, unlawful threats, sexual harassment, etc.

In addition to Section 69 in the Penal Code, there is a specific provision – Section 76 – that is only applicable to the **confiscation of a so called information carrier** (*informasjonsbærer)*. The third paragraph concerns information carrier of electronic data, for example a webserver or a website. The provision regulates *inter alia* how the confiscation shall be carried out when the offender does not own the information carrier where the illegal information is stored, which is often the case. In such cases there is a need for assistance from the ISP that made it possible to store and make available information on the information carrier (for example a website). Instead of closing the whole website and thereby make it inaccessible also to lawful users, the ISP will instead be ordered to hinder the offender to access the website and delete the unlawful content. In practice, this can be carried out by deleting the offender's user profile and account. If the offender is the rights holder of the

[31] Ibid, p. 123.

information carrier, the ISP may be ordered to make the whole information carrier (for example the entire website) inaccessible and delete the content.[32]

According to Section 70, confiscation of an information carrier can only be carried out if there is a risk of irreparable harm. If the offender owns the server where the illegal content is stored, the confiscation is carried out in the regular manner by physically taking the server from the offender.[33]

Domain names are also considered to be objects under the rules on confiscation and seizure. In 2009, the Supreme Court held that a **domain name may be seized** in accordance with the provision on seizure laid down in section 203 in the Criminal Procedure Act (*Straprosessloven)*.[34] According to the provision, objects that are deemed to be significant as evidence may be seized until a legally enforceable judgment is passed. The same applies to objects that are deemed to be liable to confiscation or to a claim for surrender by an aggrieved person. The websites in question were used for the advertisement of prostitution services, which are illegal in Norway. A decision to seize an object is generally taken by the prosecutor (in certain cases by the police or by court decision). A person who has had his or her object seized may challenge the decision in a court.[35]

2.2.2. Privacy law and the Data Protection Authority

The Norwegian Data Protection Authority (*Datatilsynet*) is tasked with the protection of privacy of individuals. It monitors whether the rules on data protection are being respected and it has the authority to render decisions and opinions.[36] The main rules are laid down in the Personal Data Act (*Lov om behandling av personopplysninger, Lov 2000-04-14-31*), which implements the requirements in the EU Data Protection Directive (95/45/EC).

If weighty considerations relating to protection of privacy so warrant, the Data Protection Authority may decide that rectification shall be effected by **erasing or blocking the deficient personal data**. This is provided for in section 27 of the Personal Data Act which regulates the rectification of deficient data. Section 28 deals with prohibition against storing unnecessary personal data. According to this provision, the data subject may demand that data which is strongly disadvantageous to him or her shall be blocked or erased if this is not contrary to another statute, and is justifiable on the basis of an overall assessment of, inter alia the needs of other persons for documentation, the interests of the data subject, cultural historical interests and the resources required to carry out the demand.

The Data Protection Authority may order a change or cease of unlawful processing of data **subject to a fine** (Personal Data Act section 46 and 47). Decisions made by the Data Protection Authority pursuant to sections 27 and 28 may be appealed to the Privacy Appeals Board. The Privacy Appeals Board consists of seven members who are appointed for a term of four years with the possibility of reappointment for a further four years. The chairman and deputy chairman are appointed by the Parliament. The other five members are appointed by the King (Personal Data Act section 42 and 43).

---

32 Preparatory works to the amendment of the Penal Code (*Ot.prp.nr.22 (2008-2009) Om lov om endringer i straffeloven 20. mai 2005 nr. 28 (siste delproposisjon - sluttføring av spesiell del og tilpasning av annen lovgivning*)), p. 399.

33 Ibid.

34 Decision by the Supreme Courts Appeal Committee (Høyesteretts ankeutvalg) 29.08.2009 in case HR-2009-1692-U - Rt-2009-1011.

35 Criminal Procedure Act (Lov om rettergangsmåten i straffesaker (Straffeprosessloven)) 1981-05-22-25, section 205 and 208.

36 https://www.datatilsynet.no/Om-Datatilsynet/Oppgaver/ (20.10.2015).

2.2.3. Take-down/removal by ISPs in accordance with their general terms and conditions

As a member of the European Economic Area (EEA), Norway has implemented the Directive 2000/31/EC **(E-Commerce Directive)** into Norwegian law by the adoption of the 2003 Electronic Commerce Act (*Lov om visse sider av elektronisk handel og andre informasjonssamfunnstjenester*). Although the Directive regulates the non-liability of service providers, the general interpretation of the directive in Norway is that **ISPs may be responsible for illegal content** (for example unlawful use of copyright protected material) on their servers if the provider, upon obtaining knowledge or awareness that such content is present, does not act expeditiously to remove or disable access to the content.[37] The measures can thus be either **removal or blocking**.

Following the implementation of the E-Commerce Directive, some ISPs have devised **user agreements that allow for the ISP to remove any controversial content, including content that is not illegal**, in order to protect themselves from liability in any controversy regarding content.[38] By way of example, one author refers to an incident in February 2008 where the Norwegian ISP Imbera removed images of the Danish ''Muhammad cartoons'' from the websites of one of their customers, an organization called Human Rights Service. The grounds for the removal were that Imbera's user agreement prohibited users from uploading controversial content to Imbera's servers.[39]

As regards the access ISPs specifically, their general terms and conditions generally allow them to block access to Internet services for non-complying customers. For example, the major Norwegian ISP access provider Telenor General Terms and Conditions provide that Telenor may block further use of its services if the customer acts contrary to applicable law or statutory regulations relating to electronic communication services, or in any other way grossly breaches the agreement, grossly misuses the services or equipment, grossly violates Telenor, Telenor's representatives or others.[40] Since this is a private matter between the access ISPs and their customers it is difficult to know how those conditions are applied in practice.

3. Procedural Aspects

3.1. Protection of copyright and other intellectual property

Section 56c of the Act relating to copyright in literary, scientific and artistic works, etc. (Copyright Act) provides that upon a petition from a rights holder, the **court may order** a provider of electronic communication services who transfers, provides access to or saves content, to hinder access to a website where material is being made available to a great extent, which evidently infringes copyright or other rights under the Act.

Section 56 d of the Copyright Act states that a petition for injunction shall be filed at the Oslo District Court (*Oslo Tingrett)*, which is thus the competent court. The request must contain the grounds for the request and clearly state against which ISP(s) it is directed. Further, the owner of the website in question must be indicated. Both the **ISP(s) and the owner of the website are parties to the case**.

---

37 R. Deibert *et al.*, Access Controlled - The Shaping of Power, Rights, and Rule in Cyberspace, 34 b&w illus 2010, 34 p. 330. The text is also available at https://opennet.net/research/regions/nordic-countries (06.10.2015).

38 Ibid.

39 Ibid.

40 Telenor Norway AS General Terms and Conditions applicable from 01/03/2015 available in English at http://www.telenor.no/privat/vilkar/subscription_terms_and_conditions.jsp (30.10.2015).

The ISPs to whom the request is directed and the owner of the website in question shall have the opportunity to submit their comments to the court before the case is decided. If the owner of the website is unknown or has an unknown address, the case can be decided even though the owner has not had the opportunity to be heard (section 56 e of the Copyright Act). Should the court decide without hearing a defending party in accordance with the rules laid down in section 56 e of the Copyright Act, that party may request subsequent proceedings in relation to the court order. Following these proceedings, the court shall make a new decision which replaces its previous decision (section 56 g of the Copyright Act).

In its decision, the court shall specify the measures to be taken by the ISPs and the time limit for the implementation of the measures. The court may decide that the order is limited in time (section 56 f of the Copyright Act).

The **defendants may request the court to annul the order** in accordance with the rules laid down in section 56 i of the Copyright Act. According to this provision, the court shall annul the order if it can be established that because of new evidence or other circumstances there is no longer any legal basis for the order. Section 56 l of the Copyright Act provides that an access ISP may only be liable to pay the applicant's legal cost if there is an appeal case and the ISP itself has appealed the decision.

A request for injunction shall be filed at the Oslo District Court (*Oslo Tingrett)* which is thus the competent court. A **decision of the Oslo District Court may be appealed** to the Court of Appeal (*lagmannsretten)*. Further, the Supreme Court (Høyesterett) may grant leave to appeal, thus allowing for the appeal of the Court of Appeal's decision.

3.2. Penal law provisions on confiscation and seizure

Section 69 in the Penal Code provides that objects that have been produced by or been the subject of a criminal act may be confiscated (*inndragning)*, including rights, claims and electronically stored information. The same applies to objects that have been used or intended for use in a criminal act. Illegal Internet content and domain names are considered to be objects under the provision. The **district court decides on the confiscation** of an object.

In case of confiscation of an information carrier (*informasjonsbærer)* (for example a website or a webserver), there is a specific provision applicable when the offender does not own the server where the illegal information is stored (Section 76 in the Penal Code). In such cases, the court may order the ISP to hinder access to the information carrier and the deletion of the unlawful content.

According to section 203 in the Criminal Procedure Act (*Straffeprosessloven)*, objects that are deemed to be significant as evidence may be **seized until a legally enforceable judgment is passed**. The same applies to objects that are deemed to be liable to confiscation or to a claim for surrender by an aggrieved person. A decision to seize an object is generally taken by the **prosecutor** (in certain cases by the police or by the district court). A person who has had his or her object seized may challenge the decision in a court.[41]

Decision by the district court on seizure or confiscation of an object may be appealed to the Court of Appeal (*lagmannsretten)*. Further, the Supreme Court (Høyesterett) may grant leave to appeal, thus allowing for the appeal of the Court of Appeal's decision.

[41] Criminal Procedure Act (Lov om rettergangsmåten i straffesaker (Straffeprosessloven)) 1981-05-22-25, section 205 and 208.

3.3. Measures taken under the Data Protection Act

The Data Protection Authority may decide on the erasure or blocking of deficient personal data. Such decision **may be appealed to the Privacy Appeals Board**. The Privacy Appeals Board consists of seven members and is an independent administrative body subordinate to the King and the Ministry (Personal Data Act section 42 and 43).

The Data Protection Authority may make an order on the erasure or blocking of deficient personal data subject to a coercive fine. The coercive fine shall not run until the time limit for lodging an appeal has expired. If the administrative decision is appealed, the coercive fine shall not run until so decided by the Privacy Appeals Board (Personal Data Act section 47).

3.4. Blocking/filtering of child abuse images

As described above, blocking of websites with a child sexual abuse content in Norway is carried out by way of a 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. A person trying to access a blocked website is redirected to a page with a warning message. The message contains information about the reasons for the redirection, a description of the unlawful material, a reference to the relevant provision in the Penal Code and contact **information and instructions on how to notify the Police in case of opposition to the blockage**.[42]

To our knowledge, the blacklist and the voluntarily cooperation between the Police and the ISPs are **not based or foreseen in legislation** nor in any other kind of regulation. Furthermore, the Police's list of websites containing child abuse material is **generated and managed without judicial control**.

4. General Monitoring of Internet

In Norway, 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, at least to some extent, by different bodies.

Norwegian secret services, the so called **EOS services**, monitor and collect information in order to carry out their tasks. This includes information on the Internet. The EOS services include the Norwegian Intelligence Service (NIS), the Norwegian Police Security Service (PST), the Norwegian National Security Authority (NSM), and the Norwegian Defence Security Agency (FSA).

The **Norwegian Intelligence Service** (NIS) collects information about situations and conditions outside the nation's borders. The primary tasks assigned to the NIS are conferred by statute in Section 3 of the Intelligence Service Act, which states that the service shall procure, process and analyse information regarding Norwegian interests viewed in relation to foreign states, organizations or private individuals, and in this context prepares threat analysis and intelligence assessments to the extent that this may help to safeguard important national interests.[43]

---

42 Information available at the website of the Norwegian Police (*Kripos*), https://tips.kripos.no/cmssite.asp?c=1&h=41&menu=2 (06.10.2015).

43 An English version of the Intelligence Service Act available at the website of the Norwegian Parliamentary Intelligence Oversight Committee http://eos-utvalget.no/english_1/legal_framework/content_3/text_1401199215164/1401199218959/lov_19980320_011_eng.pdf (22.10.2015).

The **Norwegian Police Security Service** (PST) is tasked with collecting and analyzing information and implementing countermeasures against matters that threaten national security. The service is organized as a special police service parallel to the regular police, and the service reports directly to the Ministry of Justice. The PST key methods that are used to prevent and investigate crimes that may pose a threat to national security include gathering information on individuals and groups that may pose a threat, preparing various analysis and threat assessments, investigating relevant matters, and other operative countermeasures.[44] The PST's organization, tasks and use of coercive measures are regulated in chapter IIIa of the Police Act (*Lov om politiet, LOV-1995-08-04-53*).

The **Norwegian National Security Authority (**NSM) is a cross-sectoral professional and supervisory authority within the protective security services in Norway. One of its tasks is to gather and analyze information relevant for protective security services in accordance with the provisions laid down in the Security Act (*Lov om forebyggende sikkerhetstjeneste, LOV-1998-03-20-10*).

The **Norwegian Defence Security Agency's (**FSA) primary responsibility is the protective security service and operative security of the Armed Forces, including responsibilities related to the Armed Forces' security intelligence. The FSA shall, on behalf of the Chief of Defense, counteract security threats associated with espionage, sabotage, and terrorist acts that may affect military activities and/or national security.[45]

The **Norwegian Parliamentary Intelligence Oversight Committee** *(Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste*) is responsible for external and independent control of the above described EOS services.

The Committee's primary task is to make sure that the EOS services keep their activities within the legislative framework applicable to them, with a particular emphasis on matters that concern the **protection of civil liberties and due process of law** for private individuals. A central aspect of the Committee's oversight activities is thus to ensure that the services keep their activities within the particular legislative framework to which they are subject, as well as general provisions, particularly those contained in laws and regulations.[46] The responsibility for oversight does not include activities involving persons who are not resident in Norway or organizations that have no address in this country.[47]

The Committee is not authorised to order the services to take specific action on a matter, nor to make decisions to which the services are obligated to follow, but the Committee may express its opinion on matters or situations it investigates as part of its oversight duties and make

---

44 Information available at the website of the Norwegian Parliamentary Intelligence Oversight Committee *(Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste*), http://eos-utvalget.no/english_1/services/the_eos_services/pst_the_norwegian_police_security_service_/ (15.10.2015).

45 Information available at the website of the Norwegian Parliamentary Intelligence Oversight Committee *(Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste*), http://eos-utvalget.no/english_1/services/the_eos_services/fsa_the_norwegian_defence_security_agency/ (15.10.2015).

46 Information available at the website of the Norwegian Parliamentary Intelligence Oversight Committee *(Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste*), http://eos-utvalget.no/english_1/legal_framework/ (15.10.2015).

47 Information available at the website of the Norwegian Parliamentary Intelligence Oversight Committee *(Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste*), http://eos-utvalget.no/english_1/services/area_of_oversight_1/ (15.10.2015).

recommendations to the services, such as recommending that information on a person be deleted from the service's register, that a matter be reconsidered, or that a practice or measure ought to be discontinued.[48] Any individual who feels he has been subjected to unjust treatment by any of the EOS services may lodge a complaint with the EOS Committee.[49]

The NCIS within the Norwegian Police operates a national hotline for the reporting of child sexual abuse, trafficking in human beings, racism on the Internet and radicalization, violent extremism on the Internet and other matters.[50] The reports from the public are handled by police officers immediately when they arrive and by specialised police officers in the various crime types within office hours.[51]

Finally, it may also be mentioned that the Norwegian Media Authority (*Medietilsynet)* receives funding from the European Commission's Safer Internet Programme to coordinate the Safer Internet Centre in Norway. The Centre is tasked with helping children and young people to a safe life online. For example, in cooperation with the Red Cross' helpline "Kors på halsen", the Centre aims to ensure that children across Norway are empowered to take sensible choices in their everyday digital life.[52]

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

In addition to the protection under the European Convention on Human Rights (ECHR) which apply as domestic law since 1999[53], freedom of expression is protected by Article 100 in the Norwegian Constitution (*Kongeriket Norges Grunnlov)*. The statutory protection covers all kind of expressions, including expressions on the Internet.

As presented in this report, there are a **limited number of legal measures available to block, filter and take down illegal content** on the Internet. In the assessment as to the case law of the European Court of Human Rights, it should be noted initially that in the absence of a more developed legal framework, it is common that the ISPs on their own initiative take such measures in order to avoid risking liability because of illegal Internet content. This is carried out in accordance with the ISPs general terms and conditions applicable to their customers, without any legal safeguards in place.

Section 56c of the **Act relating to copyright in literary, scientific and artistic works, etc. (Copyright Act)** (*Lov om opphavsrett til åndsverk m.v.*) provides that upon a petition from a rights holder, the court may order an ISP to block access to a website. The scope of application of the provision is limited and clearly indicated; it applies only when material is being made available to a *great extent*, *evidently* infringing copyright or other rights in accordance to the Act.

---

48 Information available at the website of the Norwegian Parliamentary Intelligence Oversight Committee *(Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste*), http://eos-utvalget.no/english_1/services/area_of_oversight_1/ (15.10.2015).

49 Information available at the website of the Norwegian Parliamentary Intelligence Oversight Committee *(Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste*), http://eos-utvalget.no/english_1/services/processing_complaints/ (15.10.2015).

50 https://tips.kripos.no/cmssite.asp?c=1&nm=0&menu=-1 (18.11.2015).

51 Global Alliance Against Child Sexual Abuse Online – 2014 Reporting Form, Norway, 2014, p. 7, available at http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/organized-crime-and-human-traffick ing/global-alliance-against-child-abuse/docs/reports-2014/ga_report_2014_-_norway_en.pdf (18.11.2015).

52 http://www.medietilsynet.no/en/children-and-media/safer-internet-centre-norway/ (18.11.2015).

53 Human Rights Act (*Lov om styrking av menneskerettighetenes stilling i norsk rett, LOV-1999-05-21-30*), Article 2.

As described above in section 2.1.1, a **test of proportionality** shall be carried out where the court deciding on the injunction shall weigh the interests and the inconveniences of the blocking measure for the concerned parties. According to the preparatory works to the Copyright Act, the court shall take into account, for example, the gravity, scope and damaging effects of the infringement and whether legitimate third parties including consumer are affected.[54] Further, the court shall **take into consideration the freedom of information and expression** and the possibility of using alternative and less restrictive measures. As regards the freedom of information and expression, the preparatory works to the Copyright Act state that the court shall consider *inter alia* whether the measure will affect lawful content and, if that is the case, how worthy of protection the affected lawful material is.[55]

In a recent **decision from the Oslo District Court** (see section 2.1.1 above), the court held that the blocking of several websites, among others the Pirate Bay, did not amount to a violation of the freedom of information and expression in the Constitution and in Article 10 ECHR.[56] The court reasoned that the material in question was far from what is to be considered as the core of which the rules on freedom of information and expression are supposed to safeguard. In that regard it held that about 90 % of the material on the Pirate Bay website was estimated to be unlawful and noted that the material was available lawfully on other websites.[57] The reasoning of the Court reflects that the blocking of illegal Internet under Section 56 c of the Copyright Act shall be assessed taking due account of the fundamental right of freedom of expression.

Considering the limited scope of the provision, its clarity and the requirement of the test of proportionality, it is our opinion that **the law meets the requirements of foreseeability, accessibility, clarity, precision and proportionality as developed by the European Court of Human Rights**.

The penal law provisions on **confiscation and seizure** applicable to illegal Internet content and domain names have been presented in section 2.2.1 above.

Confiscation and seizure are coercive measures which are subject to **considerable limitations and safeguards**. Confiscation of so called information carriers (for example information on the Internet), may only be carried out if it is a risk of irreparable harm. In addition to the physically taking of a server, the rules on confiscation allows for the ordering of an ISP to make illegal Internet content inaccessible. A decision to confiscate an object shall be taken by the district court.

The seizure of objects (including electronically stored information) is carried out in accordance with the provisions in chapter 16 of the Criminal Procedure Act (*Straffeprosessloven)*. Objects may only be seized **until such time as a legally enforceable judgment is passed.** A decision to seize an object is generally taken by the **prosecutor** (in certain cases by the police or by the district court) and it may be challenged in court.

To our knowledge, it has not been argued that the rules and/or the application of the rules on confiscation and seizure in relation to Internet content, would not be in line with the case law of the European Court of Human Rights.

Although not based or foreseen in legislation nor in any other kind of regulation, a few comments may be made on the so called **Child Sexual Anti Distribution Filter** which aims to block websites with

54 Prop.65 L (2012-2013), p. 91.
55 Ibid.
56 Oslo tingrett decision 2015-09-01 in case TOSLO-2015-67093.
57 Ibid, p. 9.

a child sexual abuse content. As described in section 2.1.2 above, this is a voluntary cooperation between the Police and the ISPs. The list of unlawful websites is generated by the Police without judicial or public oversight and it is kept secret by the ISPs using it. Privacy and advocacy groups have raised concerns of the risk that the filter could be used to also filter websites that do not contain child sexual abuse content.[58]

Considering that the voluntary cooperation is **not based or governed by law and lacks judicial review**, it arguably raises questions about the responsibility of a state to intervene and put in place legal safeguards for compliance with freedom of expression and other related rights. The same concerns may be raised as regards the ISPs blocking and removal of Internet content in accordance with their general terms and conditions.

Henrik Westermark
05.11.2015

[58] R. Deibert *et al.*, Access Controlled - The Shaping of Power, Rights, and Rule in Cyberspace, 34 b&w illus 2010, 34 p. 328.