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 180-192

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.

DENMARK

1. Legal Sources

There is **no specific overall legislation** in Denmark on the blocking, filtering or take-down of illegal internet content. Instead, regulation is fragmented over various areas of law and illegal content is generally prevented through three different channels: criminal law provisions preventing disorder and crime, civil law provisions protecting the reputation or rights of others and, lastly, administrative rules that authorize the relevant authorities to act in particular areas.[1]

The criminal law provisions are contained in the **Danish Criminal Code**.[2] Online content can also be illegal under other statues, for example, the **Danish Copyright Act**[3]**,** the **Danish Trade Marks Act**[4]**,** the **Danish Designs Act**[5] and the **Danish Act on Gaming**[6].

On 21 June 2005, Denmark ratified the **Cybercrime Convention of the Council of Europe**[7] and it entered into force in Denmark on 1 October 2005. The Cybercrime Convention is relevant to crimes committed on the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography, hate crimes, and violations of network security; its rules are now reflected in Danish national law.[8] Denmark has also assented to the **Additional Protocol** concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems.[9]

International standards such as the **EU Directive on Electronic Commerce**[10] have resulted in soft law and voluntary agreements in this area.

Illegal online content is primarily controlled by means of DNS- or IP-address blocking by the access service providers and, as a result, most regulation in the area concerns Internet access providers.[11] Blocking measures by Internet access providers are generally carried out following an injunction from a court. A voluntary agreement ensures that a court decision to block a website directed at one

---

1 See the memorandum from the Danish Ministry of Business and Growth, Oversigt over juridiske og tekniske håndhævelsesmetoder I Denmark og EU (June 2012), available at http://www.ft.dk/samling/20111/almdel/eru/bilag/300/1138525.pdf (18.02.15), p. 1.

2 Lovbekendtgørelse (LBKG) 2014-07-04 nr. 871, Straffeloven.

3 Ophavsretsloven, LBKG 2014-10-23 nr 1144 om ophavsret.

4 Varemærkeloven, LBKG 2016-03-01 nr. 192.

5 Designloven, LBKG 2016-03-01 nr. 189

6 Spilleloven, Lov 2010-07-01 nr. 848 om spil.

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

8 C.f. the OSCE, Report, Freedom of Expression on the Internet: Study of Legal Provisions and Practices Related to Freedom of Expression, the Free Flow of Information and Media Pluralism on the Internet in OSCE Participating States (2010), available at http://ssrn.com/abstract=1906717 (18.02.15), pp. 49-50.

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

10 Directive 2000/31/EC of The European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce).

11 See the memorandum from the Danish Ministry of Business and Growth, Oversigt over juridiske og tekniske håndhævelsesmetoder I Denmark og EU (June 2012), available at http://www.ft.dk/samling/20111/almdel/eru/bilag/300/1138525.pdf (18.02.15), p. 8.

Internet access provider shall be complied with by other members to the agreement (resulting in an effective “one stop shop” system).

2. Legal Framework

2.1. Blocking and/or filtering of illegal Internet content

2.1.1. Criminal Law Provisions

Under the Danish Criminal Code, **child pornography** is illegal.[12] Denmark also participated as a leading country in the Internet Related Child Abuse Material Project (CIRCAMP), which was a project mandated by the European Police Chiefs and launched in 2004. The objective of CIRCAMP was to improve and increase co-operation between law enforcement agencies in relation to child abuse material through increased sharing of information, reduced duplication of efforts, better quality work practices, and ultimately less drain on law enforcement resources. In the fall of 2006, Action Plan II for CIRCAMP was accepted, establishing a comprehensive mechanism which gave law enforcement authorities the ability to control and disrupt illegal child abuse websites. The CIRCAMP Action Plan II had a three-phase approach: first, the project introduced blocking technology and other technical means aimed at stopping the distribution of child abuse images and material using a system called “Child Sexual Abuse Anti Distribution Filter” (CSAADF); second, the project analyzed sites and identified legal elements on the business side, e.g., targeting “payment systems” and disrupting the capacity to make a profit from abusive content. Thirdly, the project investigated the people that benefit from the commercial distribution of child abusive material.[13] Although the CIRCAMP project is no longer active, a number of its initiatives have been integrated in the corresponding EMPACT projects.[14]

In Denmark, the Danish National Police, “Save the Children” Denmark and the service providers entered into a **voluntary agreement** in 2005 to prevent child pornography through a **child pornography filter**. The National Police assesses the webpages together with Save the Children and then sends a list of webpages that contain illegal material to the service providers. On the basis of this, service providers block webpages with illegal content. Private individuals can report allegedly illegal content to either the National Police or Save the Children.[15]

The Danish Criminal Code also lays down general provisions concerning liability for acts of **defamation**.[16] Generally, anybody who offends another person's honor by insulting words or actions or by stating or disseminating charges, that can be considered to reduce the insulted person in the

---

12 C.f. the Danish Criminal Code, Sections 234-235.

13 C.f. the OSCE, Report, Freedom of Expression on the Internet: Study of Legal Provisions and Practices Related to Freedom of Expression, the Free Flow of Information and Media Pluralism on the Internet in OSCE Participating States (2010), available at http://ssrn.com/abstract=1906717 (18.02.15), pp. 140-142.

14 In 2015 the Danish Police participated in the following EMPACT projects: Facilitation of Illegal Immigration, Trafficking in Human Being, Cocaine, Cybercrimes regarding online and payment card fraud, cybercrimes which regarding Child Sexual Exploitation, Cybercrimes regarding cyber-attacks, Illicit Firearms Trafficking and Organised Property Crime.

15 See the press release regarding the child pornography filter, available at http://om.tdc.dk/publish.php?id=7610 (12.02.15).

16 See The Danish Criminal Code, Sections 267-275. Defamatory offenses are subject to private prosecution, cf. the Danish Criminal Code, Section 275 (1).

esteem of fellow citizens, may be held liable. The provisions apply equally to defamatory actions over the Internet.[17]

Blasphemy is also forbidden under the Danish Criminal Code and anybody who publicly mocks or insults any domestic legally existing religious community, tenets of faith or worship is liable to a criminal offence.[18]

The Danish Criminal Code further prohibits **hate speech and racism**; the provision can be invoked to punish anyone who publicly, or with intention to disseminate in a larger circle, makes statements or other pronouncements by which a group of persons is threatened, derided or degraded because of their race, color of skin, national or ethnic background, faith or sexual orientation.[19] These rules are equally applicable in relation to crimes committed over the Internet.[20]

Where it is necessary to **prevent further crime** or otherwise **required due to special circumstances**, the Danish Criminal Code provides that the following objects (including websites) may be confiscated following a court order:

1) objects used or intended to be used in a criminal act,
2) objects produced by a criminal act,
3) objects in respect of which a criminal offense has otherwise been committed.[21]

Within the last two years, the Danish State Prosecutor for Serious Economic and International Crime (*SØIK)* has **seized a large number of domain names** on the ground that the websites in question **infringed intellectual property rights**.[22] Such seizure may only be carried out following a decision from a court and in accordance with the rules on seizure laid down in Chapter 74 of the Administration of Justice Act[23]. Recently, the Prosecutor, in accordance with the orders made by the Copenhagen City Court, seized 423 domain names allegedly used for selling counterfeit products to Danish consumers.[24] The measure was directed at the corporation DK Hostmaster A/S - responsible for the distribution and registration in Denmark under the .dk-domain - which was thus ordered by the Court to transfer the .dk domain names in question to the Prosecutor (see a description of DK Hostmaster A/S below in section 2.1.4).[25]

Infringements of intellectual property rights of a particularly serious nature can be tried as criminal cases in accordance with the rules laid down in Chapter 28 of the Danish Criminal Code.[26] Intellectual property rights will be discussed immediately below in section 2.1.2.

---

17 See e.g., the cases U.2002.2767 and FED 2001.1723.

18 C.f. the Danish Criminal Code, Section 140.

19 Cf. the Danish Criminal Code, Section 266.

20 See e.g. the case U.2003.751/2Ø where the Eastern High Court found an editor of a website guilty of violating Section 266 of the Danish Criminal Code by publishing an article named "Behind Islam" which included several degrading statements about Muslims. The court also regarded the publication of the article on the Internet as propaganda.

21 Cf. the Danish Criminal Code, Section 75 (2).

22 http://www.anklagemyndigheden.dk/nyheder/Sider/statsadvokat-beslaglaegger-423-falske-hjemmesider.aspx (13.04.2016). This paragraph in the present report was added in April 2016 following input from the Danish Ministry of Business and Growth via The Council of Europe.

23 Consolidated Act. No. 1255 of 16 November 2015 with subsequent amendments, Retsplejeloven.

24 http://www.anklagemyndigheden.dk/nyheder/Sider/statsadvokat-beslaglaegger-423-falske-hjemmesider.aspx (13.04.2016).

25 *Ibid*.

26 Cf. the Danish Criminal Code, Section 299 b, cf. Section 305.

2.1.2. Civil Law Provisions

In relation to civil law provisions protecting the reputation or rights of others, the economic and moral interests to **intellectual property** are protected under several laws, for example the Danish Copyright Act[27], the Danish Trade Marks Act[28] and the Danish Designs Acts.[29] An aggrieved party can apply for the Enforcement court ("*fogedretten*") to assist with the **enforcement of an injunction against a service provider**, in accordance with the Danish Administration of Justice Act[30] Chapter 57.

As noted above, infringements of intellectual property rights of a particularly serious nature can be tried as criminal cases.[31]

Before the access provider can be required to block illegal online activities, an **injunction must be issued against the actual infringing party**, i.e., the initial source that makes the illegal information available.[32] For an injunction to be issued, certain **requirements** must be met, namely: i) the party seeking the injunction must have a right, which is sought to be protected by the injunction, ii) the conduct of the other party must necessitate that an injunction is issued, and iii) there must be urgency in the sense that the opportunity of the party seeking the injunction to protect his right will be wasted if that party must await the decision in the underlying legal dispute.[33] Further, if it has not already happened, the party seeking the injunction must initiate court proceedings against the alleged actual infringer concerning the underlying legal dispute within two weeks of the decision to grant the injunction becoming final.[34]

Danish service providers do not play a role in establishing whether illegal activities have occurred. This is determined in proceedings between the aggrieved party and the assumed infringer. In Danish cases where the courts have issued injunctions against service providers requiring them to take down or block access to specific webpages, service providers have always complied with the injunctions.[35]

In certain circumstances, the Enforcement court can order a **search to preserve relevant evidence** in respect of an alleged infringement of intellectual property rights. In so far as it is found necessary to preserve the relevant evidence, items can be seized and copies can be made of documents, information on computers, computer programs or other relevant materials.[36]

2.1.3. Administrative Rules

In Denmark, administrative authorities may be authorized to take measures in order to prevent illegal Internet content within their field.

---

27 Ophavsretsloven, LBKG 2014-10-23 nr 1144 om ophavsret.

28 Varemærkeloven, LBKG 2016-03-01 nr. 192.

29 Designloven, LBKG 2016-03-01 nr. 189.

30 Consolidated Act. No. 1255 of 16 November 2015 with subsequent amendments, Retsplejeloven.

31 Cf. the Danish Criminal Code, Section 299 b, cf. Section 305.

32 C.f. the Administration of Justice Act, Chapter 40 (Sections 411-430).

33 Cf. the Danish Administration of Justice Act, Section 413.

34 Cf. the Danish Administration of Justice Act, Section 425.

35 See the report from the Danish Ministry of Culture, Rapport fra møderækken om håndhævelse af ophavsretten på internettet (2009), p. 35, available at http://kum.dk/uploads/tx_templavoila/Rapport%20fra%20moderakken%20om%20handhavelse%20af%20ophavsretten%20pa%20internettet.pdf (19.02.15).

36 C.f. the Administration of Justice Act, Chapter 57 a (Sections 653-653 d).

Gambling is subject to government control and as a starting point, all **gambling activities** require a license from the Danish Gaming Authority.[37] According to the rules, transmission of funds to and from an unlicensed organizer as well as transmission of information via a communication network to an illegal game system is prohibited.[38]

The provision makes it **illegal for the Internet service provider to facilitate access to unlicensed game systems** and this can form the basis for an injunction. The rule applies to service providers, who provide Internet access to a wide range of customers, whereas businesses such as hotels, restaurants and educational institutions, that provide access to only a limited or closed circle of people, are not covered by the provision.

If an organizer does not put an end to the unlicensed gambling when the Danish Gaming Authority contacts them with a request to do so, the Danish Gaming Authority will contact the relevant payment services, issuers of electronic money or the Internet service providers to have the transaction or internet page blocked. Internet service providers are **not obliged to check** continuously whether service is being made available to organizers who do not comply with the Danish legislation; the Danish Gaming Authority therefore actively informs the particular service providers which Internet domains that, in their opinion, are unlicensed. It is then up to the Internet service provider to block the illegal activity. The information from the Danish Gaming Authority is provided in the form of a **request** and the Internet service provider can avoid infringing the regulation by establishing a **DNS-blocking of the Internet domain** in question. The DNS-blocking may be repealed when the Danish Gaming Authority informs the service provider that the activities on the webpage no longer infringe Danish law.[39]

If a request from the Danish Gaming Authority to block either internet access or financial transactions is not observed by the Internet access provider, the Danish Gaming Authority can have a preliminary **injunction** issued in accordance with the Danish Administration of Justice Act Chapter 57.[40]

Historically, Danish law specifically prohibited Internet service providers from facilitating access to webpages from which medicines were sold to consumers in conflict with the Danish Medicines Act, and the Danish Health and Medicines Authority could request the service providers to block access to the webpages in question.[41] However, the provision has now been repealed.[42]

2.1.4. Soft Law and Voluntary Agreements

The **Danish E-commerce Act**[43] implements the European Directive on Electronic Commerce[44] and contains rules concerning liability of intermediary Internet service providers.

---

37 C.f. Spilleloven, Lov 2010-07-01 nr. 848 om spil, Section 3 (1) and Pokerloven, Lov 2009-12-27 nr. 1504 om offentligt hasardspil i turneringsform, Section 6.

38 Cf. Spilleloven § 65.

39 Cf. SKAT, Den juridiske vejledning 2014-2, J.A. Spil, available at http://www.skat.dk/SKAT.aspx?oId=71002 (18.02.2015), section J.A.11.4.2.

40 See the Danish Administration of Justice Act, Consolidated Act. No. 1255 of 16 November 2015 with subsequent amendments, Chapter 57.

41 Cf. the Danish Medicines Act, LBKG 2011-05-18 nr. 464 om lægemidler, Section 39 b.

42 Cf. the current Danish Medicines Act, LBKG 2013-04-20 nr. 506 om lægemidler.

43 Lov 2002-04-22 nr. 227 om tjenester i informationssamfundet herunder visse aspekter af elektronisk handel.

According to Article 16 of the Directive on Electronic Commerce,[45] the Member States and the Commission shall encourage the drawing up of codes of conduct by trade, professional and consumer associations or organizations[46]. The preparatory works to the Danish E-commerce Act[47] establish that Article 16 of the Directive on Electronic Commerce does not necessitate enactment of any Danish legislation on the matter. However, **codes of conduct are encouraged** both on a national level and on a Community level through the already existing Nordic work and by support of the EU Commissions's eConfidence-group.[48]

Furthermore, the legislature specifies that it, in relation to the provisions in the Directive on Electronic Commerce, it may be relevant for trade organizations to provide guidelines concerning commercial communications and liability exemptions, e.g., regarding the application of a "notice-and-take-down-system".[49] This has given rise to a number of **soft law instruments** in the form of voluntary agreements and codes of conduct.

The corporation **DK Hostmaster A/S** is responsible for the distribution and registration in Denmark under the .dk-domain. DK Hostmaster is entirely owned by the organization Danish Internet Forum (DIFO). The **general terms and conditions** of DK Hostmaster[50] provide that the managing director of DK Hostmaster and the chairman of the board of directors of DIFO in agreement can decide that a domain can be suspended if: 1) the registrant's use of the domain clearly is intended to create a risk of confusion with the domain, name or trademark rights of a third party or other intellectual property rights and 2) the circumstances, e.g., highly offensive content, attempts of phishing, attempts to install malware etc., justify proceeding without waiting for a decision from The Complaints Board for Domain Names or the courts.[51]

A domain may also be **suspended and subsequently blocked** or deleted by DK Hostmaster due to significant safety or other public interest reasons when the domain is used for manifestly illegal acts or omissions or, in the case of typo squatting, where a nearly identical domain name is registered with the risk that internet users by a simple typing error or spelling mistake are directed to this domain.[52] Moreover, a domain may be suspended, blocked or deleted if it infringes a third party's name- or trademark rights or other intellectual property rights and The Complaints Board for Domain Names in at least two previous cases has determined that the registrant has acted against good practice in the field of domain names, cf. the Danish Act on Internet Domains[53] Section 12.[54]

---

44 Directive 2000/31/EC of The European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce).

45 Directive 2000/31/EC of The European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce).

46 See also the Directive in electronic Commerce, Recitals 40 and 46-48.

47 Lov 2002-04-22 nr. 227 om tjenester i informationssamfundet herunder visse aspekter af elektronisk handel.

48 See the preparatory works to the Danish E-commerce Act, LFF 2002-01-29, no. 61, section 13.

49 See the preparatory works to the Danish E-commerce Act, LFF 2002-01-29, no. 61, section 13.

50 Generelle vilkår for tildeling, registrering og administration af .dk-domænenavne, Version 08, 31 January 2016, available at https://www.dk-hostmaster.dk/fileadmin/generelle_vilkaar/Generelle_Vilkaar_08.pdf (12.04.2016).

51 Cf. the DK Hostmaster General Terms and Conditions, Section 8.3.1.

52 Cf. the DK Hostmaster General Terms and Conditions, Sections 8.3.2. and 8.3.3.

53 Lov 2014-02-26 nr. 164 om internetdomæner.

Furthermore, Teleindustrien (TI), which is the **professional organization for the Danish telecom industry**, has as of September 2014 entered into a **voluntary agreement** regarding the blocking and take down of Internet content.[55] The TI Code of Conduct has been established to make the implementation of decisions on DNS-blockings more simple and efficient. The agreement ensures that court decisions on **DNS-blocking** of a webpage against one TI-member must be complied with by the other members of TI within 7 days. Additionally, TI-members will block other DNS addresses if the infringed party shows that it is the exact same webpage as was subject to the court decision, but with another web address.[56] In this regard, the infringed party is required to accept economic responsibility for the service provider, if an unwarranted blocking happens on the basis of the provided information and the owner of the webpage subsequently holds the service provider liable.

This means that a rights holder who has obtained an injunction etc. from the courts must **notify the TI Secretariat** of the decision. TI members thus avoid being met by a possible large number of court proceedings, and the infringed party avoids the need to bring proceedings against all service providers separately.

The Code of Conduct does not prevent TI-members from reserving the right to try the case independently, if it is necessary in the specific circumstances, and TI cannot be held liable for the member's compliance with the agreement. The steps of the "one stop shop" blocking process are described in an Annex to the Code of Conduct and are, due to the purpose of the Code of Conduct, **not made public**.[57]

The Danish Ministry of Culture has recently presented a **Memorandum of Understanding concerning a new Code of Conduct; the** "Code of Conduct to promote lawful behavior on the internet".[58] The participants to the agreement are inter alia the Ministry of Culture, the Rights Alliance and other rights holders, ISPs, payment processors (Diners, MasterCard and Nets), advertising companies, web hosting companies, domain registrars, Google and Microsoft. The new agreement builds on the earlier more limited Code of Conduct from 2014 described above. Under the new Code of Conduct, it appears as if an injunction against a specific ISP to block a specific domain name could be **extended with voluntary blocking in other areas than Internet access services**, for example in the area of advertising networks and payment processors.[59] Further, the ISPs will continue their current practice of voluntary blocking once an injunction has been issued against a single ISP. The blocked websites will display a notice which encourages the consumer to search for legal alternative at a website called "Share With Care" (www.sharewithcare.dk).[60]

2.2. Take-down/removal of illegal Internet content

Internet host providers in Denmark generally have individual terms of service concerning the use of the particular website and which material may be made available on the website. These specific terms of service will not be discussed in the following.

---

54 Cf. the General Terms and Conditions, Section 8.3.4.

55 A list of the TI-members is available at; http://www.teleindu.dk/om-ti/medlemmer-af-ti/ (12.02.15).

56 A list of blocked webpages, Oversigt over blokeringer 20 januar 2015, is available at http://www.teleindu.dk/brancheholdninger/blokeringer-pa-nettet/ (19-02-15).

57 See TI's statement regarding the Code of Conduct available at http://www.teleindu.dk/wp-content/uploads/2014/10/TI-code-of-conduct-blokeringer.pdf (12.02.15).

58 http://kum.dk/nyheder-og-presse/pressemeddelelser/nyheder/bred-opbakning-til-faelles-kamp-for-et-lovligt-og-trygt-internet-paa-ophavsretsomraadet/1/1/ (23.07.2015).

59 https://edri.org/danish-culture-ministry-danes-regulated-by-google/ (23.07.15).

60 https://edri.org/danish-culture-ministry-danes-regulated-by-google/ (23.07.15).

There is no Danish legislation particularly directed at the Internet host providers.

2.3. Relevant Case Law

Most case law regarding illegal Internet content concerns intellectual property rights.

One of the most important cases in the area is U.2010.2221H,[61] where the Danish Supreme Court confirmed an injunctive order against the service provider Telenor, requiring the service provider to disable the access to the web-page www.thepiratebay.org, from which information protected by intellectual property rights was being transmitted. The Court upheld the finding of the High Court that, by giving its subscribers access to the Pirate Bay, Telenor contributed to the illegal copying of works protected by copyright and to the making of such works available to the public. Finally, it stated that the requested relief was precise enough to be granted and that there was no basis for assuming that an injunction would harm Telenor in a way that would be obviously disproportionate to the right holders' interest in the injunctive relief.[62]

In the case U.2006.1474H,[63] the service provider TDC was exempt from liability under the Danish E-commerce Act. Here, the Supreme Court likewise found that the liability exemption did not prevent issuing an injunction ordering the service provider to disable access to illegal information.

In case U.2013.2873Ø,[64] the Eastern High Court held that an injunctive order should first be directed against the claimed initial infringer and not the service provider. The owner of copyrights and trademarks to certain designer furniture applied for an injunction against TDC A/S, who it argued as an Internet service provider should be prohibited from transmitting access to the webpage www.voga.com. The webpage offered and sold Slavic copies of a great number of design furniture and other artifacts. The service provider only transmitted the illegal information and the service provider had no obligation or real possibility of obtaining knowledge to assess whether the transmitted information was legal. Only once illegality had been established by the courts, or if the information was manifestly illegal, could the injunctive order initially be directed against the service provider. These requirements were not met in this case and the injunctive order was therefore not issued against the service provider.

The recent case U.2015.1049.S[65] concerned a blocking injunction of a website distributing illegal tangible goods (copyright protected Danish design furniture). In this case, the Danish Maritime and Commercial Court ordered a Danish ISP (Telia Danmark) to block access to the UK based online store Interior Addict. The judgment was based on both Article 8(3) of the InfoSoc Directive and Article 11 of the Enforcement Directive and relied on **copyright infringement** as the central issue. The blocking ruling was also based on the fact that a prior ruling had convicted the owners of the Interior Addict website of illegal distribution and marketing of replica products that infringe the copyrights of Danish right holders.

In the cases referred to above, the courts, when deciding on the injunction, balanced the interest of the right holders to prevent copyright infringements with the harm an injunction would cause the

---

61 Judgment from the Danish Supreme Court of 27 May 2010.

62 See for example S. Sandfeld Jakobssen abd C. Salung Petersen, Injunctions Against *Mere Conduit* of Information Protected by Copyright – A Scandinavian Perspective, I I C - International Review of Intellectual Property and Competition Law, Volume 42, 2011, p. 9.

63 Judgment from the Danish Supreme Court of 10 February 2006.

64 Judgment from the Eastern High Court of 3 June 2013.

65 Case A-38-14 of Sø- og Handelsretten i Kobenhavn 11 December 2014.

Internet access providers. The courts did not, however, carry out any assessment of the compatibility with the fundamental freedom of expression.

In relation to illegal gaming activities, case SKM.2014.307BR[66] may be mentioned. Five webpages offered online gaming activities in Denmark without authorization and were therefore illegal. Subsequently, it was illegal for the service provider to facilitate access to the webpages in question, and the court thus granted the request of the Danish Gaming Authority and issued an injunction against the service provider to block the webpages.

3. Procedural Aspects

An **injunction** can be issued by either a Danish District court or the Maritime and Commercial Court. A request for an injunction shall be filed at the court that has jurisdiction under the general rules in the **Danish Administration of Justice Act**.[67] If the application for an injunction meets the formal requirements, the application will be evaluated in a hearing where the necessary evidence is put forward. The court can exclude evidence which is irreconcilable with the advancement of the case.[68]

Assistance in the enforcement of an injunction is provided by the Enforcement court in accordance with the rules in Chapter 57 of the Danish Administration of Justice Act.[69]
A court decision to issue an injunction may be appealed to the High Courts in accordance with the rules in the Danish Administration of Justice Act, Chapter 53. An appeal does not have a suspensory effect on the injunction.[70]

If a party has obtained an injunction on the basis of rights that are later found not to exist, this party must indemnify the counterparty and compensate any damages suffered.[71]

The injunction is **valid until it is repealed or cancelled**. An injunction can be repealed, in part or in full, if:

1) the requirements for issuing the injunction are no longer present,
2) the party that obtained the injunction adversely delays the case, or
3) if court proceedings are not initiated concerning the rights in question within 2 weeks of the injunction being issued, or if the case is discontinued or rejected by the court.[72]

If possible, the party who obtained the injunction should be given an opportunity to be heard before the injunction is repealed.[73] A request for repeal of the injunction can be submitted in writing to the court that first issued the injunction.[74]

If the injunction has not already been repealed, it will be cancelled when a judgment has been given in the case concerning the rights in question and the judgment has not been appealed.[75]

---

66 Decision from the district court, Retten på Frederiksberg, of 31 March 2014.
67 C.f. the Danish Administration of Justice Act, Section 412.
68 See the Danish Administration of Justice Act, Sections 416-417.
69 C.f. the Danish Administration of Justice Act, Section 424.
70 C.f. the Danish Administration of Justice Act, Section 427.
71 C.f. the Danish Administration of Justice Act, Section 428.
72 C.f. the Danish Administration of Justice Act, Section 426 (2).
73 C.f. the Danish Administration of Justice Act, Section 426 (6).
74 C.f. the Danish Administration of Justice Act, Section 426 (5).
75 C.f. the Danish Administration of Justice Act, Section 426 (4).

An organizer of gambling activities can bring **decisions from the Danish Gaming Authority** before the Tax Appeals Agency ("*Landsskatteretten*").[76]
The administration of the Tax Appeals Agency screens all complaints and an organizer must therefore submit the complaint to the administration.[77] The complaint must be submitted in writing, be motivated and the decision from the Danish Gaming Authority must be submitted together with the complaint. Furthermore, the complaint must be received by the Tax Appeals Agency within three months of the organizer receiving the decision from the Gaming Authority. If the organizer has not received the decision, the complaint must be received by the Tax Appeals Agency four months after the Danish Gaming Authority has send out the decision in question.[78] If the complaint is received after the **set time periods**, the Tax Appeals Agency generally rejects the complaint.[79]

During the proceedings, the agency obtains all relevant information, the plaintiff is given the opportunity to submit his comments and the Tax Appeals Agency may request for the Danish Gaming Authority to be present.[80] Decisions by the Tax Appeals Agency cannot be tried by other administrative authorities.[81]

A decision from the Danish Gaming Authority can also be brought before the courts within three months of the decision being handed down. If a complaint is not submitted within three months, the decision of the Danish Gaming Authority is final and cannot be challenged.[82] The organizer can bring the case directly before the courts and is not required to have it tried by the Tax Appeals Agency first.

If the Internet service provider does not comply with a request from the Danish Gaming Authority to block illegal online activities, an injunction is issued against the service provider in accordance with the Danish Administration of Justice Act Chapter 57.[83] Thus, if the service provider wishes a review of the decision it must be done in accordance with the abovementioned rules concerning injunctions.

Decisions from DK Hostmaster concerning suspension and subsequent blocking or deletion of an Internet domain can be appealed to The Complaints Board for Domain Names. The appeal does not have suspensory effect.[84] A complaint must be brought within two weeks after the decision from DK Hostmaster.[85]

The **Complaints Board for Domain Names** is an independent board appointed by the Minister of Business and Growth. The chairman and vice-chairman of the board are judges and the board further consists of two members with theoretical and practical legal expertise as well as two members representing consumer- and business interests respectively.

A complaint is submitted to the secretariat of the Complaint Board for Domain Names and must meet the formal requirements set forth in the Rules of Procedure of the Complaint Board for Domain

---

76 C.f. Spilleloven, Section 50 and Skatteforvaltningsloven, LBKG 2011-02-23 no 175, Section 35 b (3).

77 C.f. Skatteforvaltningsloven, LBKG 2011-02-23 no 175, Section 35 b (4).

78 C.f. Skatteforvaltningsloven, LBKG 2011-02-23 no 175, Section 35 a (3).

79 C.f. Skatteforvaltningsloven, LBKG 2011-02-23 no 175, Section 35 a (6).

80 C.f. Skatteforvaltningsloven, LBKG 2011-02-23 no 175, Section 35 e.

81 C.f. Skatteforvaltningsloven, LBKG 2011-02-23 no 175, Section 35 f.

82 C.f. Spilleloven, Section 55.

83 See the Danish Administration of Justice Act, LBKG 2014-12-09 no. 1308 Retsplejeloven, Section 57.

84 C.f. the Dk Hostmaster general terms and Conditions, Sections 8.3.1.-8.3.4.

85 C.f. the Complaints Board for Domain Names' Articles of Association Section 2, available at https://www.
domaeneklager.dk/fileadmin/user_upload/dokumenter/Klagenaevnet/Vedtaegt_2014.pdf
(23.03.2015).

Names Section 2.[86] The secretariat then notifies the respondent of the complaint and asks the respondent to submit a comment as soon as possible and within two weeks at the latest.[87] The secretariat may try to settle the matter and the case is ended if the plaintiff withdraws the complaint or the case is settled. Cases that are not ended in this matter will be presented to the Complaints Board for Domain Names on the basis of the material provided by the secretariat.[88]

If a case between the parties is pending before the courts, the board can either reject the complaint or stay the case.[89]

Decisions from the Complaint Board for Domain Names are given in writing, together with the reasoning of the board. The parties and DK Hostmaster are notified about the decision and generally have four weeks to comply with the decision. The parties must furthermore be informed about the possibility of bringing the matter before the courts.[90]

The chairman of the Complaint Board for Domain Names may decide that a case is to be resumed if one of the parties requests so within 8 weeks after the board has delivers its decision. A case can only be resumed if special circumstances are presented, in particular if one of the parties were legitimately absent and did not have the opportunity to comment on the matter, or if new information has been obtained, which would have changed the decision had the information been available at the time.[91]

Decisions from the Complaints Board for Domain Names are published at the Board's webpage.[92]

4. General Monitoring of Internet

Denmark has **no entity in charge of monitoring** Internet content.

From 2007, Danish service providers were obliged to log and store information concerning the telecommunication traffic of the end users, e.g., information on Internet sessions and which webpages the end user visited.[93] The information was intended to be used in the investigation and prosecution of criminal activities. However, as the rules proved not to be suitable for achieving the stated purpose, they were abolished as of 22 June 2014.[94]

---

86 C.f. FORRETNINGSORDEN fastsat af Klagenævnet for Domænenavne i henhold til § 3 i Vedtægt for Klagenævnet for Domænenavne, jf. Lov nr. 164 af 26. februar 2014 (domæneloven), available at https://www.domaeneklager.dk/fileadmin/user_upload/dokumenter/Klagenaevnet/Forretningsorden_2014.pdf (23.03.2015).

87 C.f. the Rules of Procedure of the Complaint Board for Domain Names, Section 5 (4).

88 C.f. the Rules of Procedure of the Complaint Board for Domain Names, Sections 6 and 7.

89 C.f. the Rules of Procedure of the Complaint Board for Domain Names, Section 3.

90 C.f. the Rules of Procedure of the Complaint Board for Domain Names, Section 15.

91 C.f. the Rules of Procedure of the Complaint Board for Domain Names, Section 16.

92 The webpage is www. Domaeneklager.dk. C.f. the Complaints Board for Domain Names' Articles of Association, Section 5.

93 See the administrative order on logging, BEK nr 988 af 28/09/2006 om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik (logningsbekendtgørelsen), available at https://www.retsinformation.dk/Forms/R0710.aspx?id=2445 (23.03.2015).

94 See the press statement from the Minister of Justice available at http://www.justitsministeriet.dk/nyt-og-presse/pressemeddelelser/2014/justitsministeren-oph%C3%A6ver-reglerne-om-sessionslogning (23.03.2015).

The Minister of Justice and the Danish National Police have, since the end of 2014, considered reintroducing rules on session logging, however no such new rules are in place yet.[95] Thus, there is currently no general monitoring of internet traffic in Denmark.

Additionally, the Directive on Electronic Commerce, Article 15 (1) provides that Member States shall not impose a general obligation on service providers, when transmitting information covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation to actively seek facts or circumstances indicating illegal activity. Accordingly, Danish law does **not impose a general obligation on the service provider to monitor** the information which is transmitted or stored, nor a general obligation to actively investigate activities or circumstances that may be illegal. There is also no obligation for the service provider to report illegal activities.

However, the Directive on Electronic Commerce Article 15 (2) leaves it to the Member States to decide whether to establish or sustain rules imposing a monitoring obligation in specific cases and Danish law imposes an **obligation to report illegal activities in certain specific cases**, e.g., if the service provider has knowledge of crime against national security, life and welfare or social values.[96]

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

Blocking, filtering and take down of Internet content raises certain concerns in relation to freedom of expression and the legal certainty of the public.

Doubts have been raised about whether monitoring and blocking of the Internet through filtering of the content is inconsistent with the freedom of expression in the Danish Constitution[97] Section 77, as well as Article 10 of the European Convention on Human Rights. As a result, such systematic filtering of Internet content has not been implemented in Denmark.[98]

Instead, blocking of illegal online content may only be carried out after the Danish courts have made an evaluation of the specific case and found it likely that the central server has been used to make illegal content available on the Internet. Hereby, the requirements for foreseeability, accessibility, clarity and precision as developed by the European Court of Human Rights are deemed to be met.[99] However, the issue of the fundamental rights and freedoms of the end users has not been considered particularly in relation to the legislation allowing such measures, e.g., the preparatory works to the Danish Act on Gaming (*Spilleloven*) does not mention these issues.

---

95 See the document from the Danish National Police of 5 December 2014 available at http://www.politiko.dk/sites/default/files-dk/node-files/142/8/8142095-ls-hele-notatet-fra-politiet-her.pdf (23.03.2015).

96 Cf. the Danish Criminal Code, LBKG 2014-07-04 no. 871, Straffeloven, Section 141.

97 Lov 1953-06-05 nr. 169, Danmarks Riges Grundlov.

98 See the report from the Danish Ministry of Culture, Rapport fra møderækken om håndhævelse af ophavsretten på internettet (2009), pp. 49-50, available at http://kum.dk/uploads/tx_templavoila/Rapport%20fra%20moderakken%20om%20handhavelse%20af%20ophavsretten%20pa%20internettet.pdf (19.02.15).

99 See the report from the Danish Ministry of Culture, Rapport fra møderækken om håndhævelse af ophavsretten på internettet (2009), p. 51, available at http://kum.dk/uploads/tx_templavoila/Rapport%20fra%20moderakken%20om%20handhavelse%20af%20ophavsretten%20pa%20internettet.pdf (19.02.15).

Furthermore, the Danish child pornography filter has generally been criticized, since the assessment of whether a webpage should be blocked is done administratively by the police and Save the Children and, thus, without neither a court order nor a judgment. This means that legal webpages risk being blocked due to mistakes or mere suspicions of illegal content. However, the procedure has not been held to be inconsistent with the assessment of necessity and proportionality of the interference with freedom of expression.[100]

Concerning the voluntary agreements and codes of conduct in the area, these are considered to create clarity and transparency regarding the procedures and guidelines of the service providers' handling of illegal online content and freedom of expression. Furthermore, the codes of conduct are designed to ensure consistency in the blocking of Internet content undertaken by different service providers.[101] The procedures do not seem to be inconsistent with the freedom of expression, as TI members only block subsequent to a court decision, and decisions by DK Hostmaster to block are subject to independent review by the Complaints Board for Domain Names.

Signe Vest, LL.M., Intern at the SICL
Henrik Westermark, Legal adviser at the SICL
29.09.2015

Revised on 03.05.2016 taking into consideration comments from Denmark on this report.

100 See Tholl, S., article „Børneporno er et argument, der trumfer alt andet" published in the Danish newspaper Information on 27 May 2011, available at http://www.information.dk/269346 (16.03.2015).

101 See the report from the Danish Ministry of Culture, Rapport fra møderækken om håndhævelse af ophavsretten på internettet (2009), p. 50, available at http://kum.dk/uploads/tx_templavoila/Rapport%20fra%20moderakken%20om%20handhavelse%20af%20ophavsretten%20pa%20internettet.pdf (19.02.15).