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 218-235

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.

FINLAND

1. Legal Sources

What are the legal sources for measures of blocking, filtering and take-down of illegal Internet content?

Finland has a new general Code regulating the information society ("Tietoyhteiskuntakaari" Information Society Code), which entered into force on 1 st January 2015. The substantive contents of the Information Society Code were largely codified in previous acts already in force in Finland. The new legislation covers issues related to electronic communication networks and services. One of the core aims of the Information Society Code is to provide safe communication networks and services. Its also seeks to ensure privacy and confidentiality of electronic communications. Moreover, the Code regulates the liabilities and obligations of service providers in the information society. These were previously regulated (as of 1 July 2002) in a different act. The measures and procedures of blocking, filtering and take-down of illegal internet content, targeted at Internet Service Providers, are codified in the Information Society Code. However, the legal sources, which define the material basis for these actions (i.e. defining illegality of content), are fragmented. The overall regulation of the area in question is also fragmented, at least to some extent, as explained below in more detail.

Some examples of the relevant international instruments and their incorporation into Finnish legislation include the following:

- Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography has been implemented into Finnish legislation through Decree 41/2012 (Treaty Series).
- The Council of Europe Convention on Protection of Children against Sexual Exploitation and Sexual Abuse has been implemented into Finnish legislation through Decree 88/2011 (Treaty Series).
- Council of Europe Convention on the Prevention of Terrorism has been implemented into Finnish legislation through Act 49/2008 (Treaty Series).
- The Convention on Cybercrime has been implemented into Finnish legislation through Decree 60/2007.
- The Convention on Data Protection has been implemented into Finnish legislation through Decree 36/1992 (Treaty Series) and Act 269/92 (Law).

International treaties to which Finland is a contracting party have been implemented into Finnish legislation typically through so-called *blanco decrees* (or acts) in the Treaty Series. The decree or act merely restates the text of the international treaty and states when the decree or act (the substantive contents of the treaty behind the decree or act) enters into force in Finland as applicable law. As a legislative measure, a decree is below an act in the hierarchy of legal sources. This means that if there is a conflict between an act and a decree, the norm of an act shall prevail over that of a decree, under the *lex superior* standard. Yet, in addition to such *blanco* decrees/acts, some international treaties have been partly implemented through changes in other legislation, when deemed necessary. Moreover, Finnish legislation must be interpreted in the light of international treaty obligations binding Finland, when applicable, to avoid conflicts between domestic norms and international law.

Relevant legal sources in this area, in addition to the legal instruments mentioned above, consist of the Copyright Act, the Patent Act, the Trademark Act, Criminal Code, and Code of Judicial Procedure.

The provisions of the Finnish Constitution also affect the interpretation of many provisions of the laws addressed in this questionnaire, and may also become individually applicable. Similarly, the Act on the Exercise of Freedom of Expression in the Mass Media regulates the freedom of expression of journalists and mass media and the Coercive Measures Act regulates many relevant procedures.

2. Legal Framework

2.1. Blocking and/or filtering of illegal Internet content

2.2. Take-down/removal of illegal Internet content

The relevant legal instruments do not specify the manner in which Internet Service Providers (ISPs) need to prevent access to illegal content. Blocking, filtering, take-down and removal are not typically mentioned separately in the relevant legislation as specific prevention mechanisms. Under some circumstances, there is a general obligation to remove or disable access to information, but the relevant law does not specify just one available action. Therefore, questions 2.1. and. 2.2. are answered together.

In addition, the relevant law at times does not distinguish between access and hosting providers, but uses more general terms such as *intermediary* to cover both (e.g. in the Copyright Act). Yet, the Information Society Code, in specific instances, requires hosting providers to take actions. Access providers are exempted from liability under Section 182 of the Information Society Code, but they can be requested to take action based on a court order or by some other competent authority. Internet providers (and caching operators) are exempted from liability under a specific provision (Sections 183-184 of the Information Society Code), but they have broader general obligations than access providers to take action concerning illegal content.

The Finnish legislation seeks to implement 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).

Exemption from liability in data transfer and network services

Information Society Code (Section 182) regulates exemption from liability in data transfer services and network services. The main features of the exemption are the following.

When an information society service consists of *transmission* in a communications network of information provided by a recipient of the service, or the provision of *access* to a communications network, the service provider is not liable for the content or transfer of the information transferred if it does not: 1) initiate the transfer; 2) select the receiver of the transfer; and 3) select or modify the information contained in the transfer. The Section further provides that the acts of transfer and provision of access referred to in the provision include the automatic, intermediate and temporary storage of the information transferred in so far as storage takes place for the sole purpose of carrying out the transfer in the communications network, and provided that the information is not stored for any period longer than is reasonably necessary for the transfer.

The provision in question implements Article 12(1)-(2) of the Directive on Electronic Commerce as such, referred to above. It is interpreted in conformity with the said Directive and its interpretations by the CJEU.

Exemption from liability for caching

Section 183 of the Information Society Code regulates the exemption for caching. When an information society service consists of the transfer in a communications network of information provided by a recipient of the service, the service provider is not liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request, if the service provider:

1) does not modify the information;
2) complies with the conditions on access to the information;
3) complies with rules regarding the updating of the information, specified in a manner widely recognised and used in the industry;
4) does not interfere with the lawful use of technology, widely recognised and used in the industry, to obtain data on the use of the information; and
5) acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact:

   a) that the information at the initial source of the transmission has been removed from the network;

   b) access to it has been disabled; or

   c) a court or an administrative authority has ordered such removal or disablement.

The provision of the Information Society Code implements Article 13(1) of the Directive on electronic commerce as such, referred to above. It is interpreted in conformity with the Directive and its interpretations by the CJEU.

Exemption from liability in hosting services

Section 184 of the Information Society Code regulates the exemption from liability in hosting services. The main features of the exemption are the following.

When an information society service consists of the storage of information provided by a recipient (content provider) of the service upon his request, the service provider is not liable for the content of the information stored or transmitted at the request of a recipient of the service if the following conditions are fulfilled: it acts expeditiously to disable access to the information stored upon: 1) obtaining knowledge of a court order concerning it or if it concerns violation of copyright or neighbouring right upon obtaining the notification referred to in section 191 of the Information Society Code, treated below; 2) otherwise obtaining actual knowledge of the fact that the stored information is clearly contrary to certain crimes related to **hate speech** (regulated in Section 10 and 10(a) of Chapter 11 of the Criminal Code) or against making available a picture of child pornography, sexual violence or intercourse with an animal (regulated in Section 18 and 18(a) of Chapter 17 of the Criminal Code). However, this exemption is not available for the hosting provider if the content provider acts under the authority or control of the hosting provider.

The provision in question implements Article 14 of the Directive on electronic commerce, referred to above. Finland also utilized the opportunity under Article 14, section 3, to implement more detailed measures for removal of and blocking access to information. According to the preparatory materials, the measures provided are considered not to infringe **freedom of expression** (Government bill HE 194/2991). It is possible to interpret the provision in conformity with the CJEU's interpretation e.g. in *L'Oreal v eBay* (C-324/09), where the Court established the standard of a diligent economic operator used to determine when illegality should have become apparent for the hosting service. Moreover, case C-324/09 and joined cases C-236/08-C-238/08 (*Google*) define that the exemptions are available only when the service provider has not played an active role of a kind to give it knowledge of or control over the information stored. The cases of the CJEU have been referred to in the government

bill concerning the Information Society Code (Government bill HE 221/2013). This seeks to ensure that interpretations of the CJEU are followed in Finland.
Yet, the Finnish courts have *not* accepted in copyright peer-to-peer (P2P) file sharing network-cases that the exemption in question would apply to the operators of these services. Typically, the awareness of operators over the illegal nature of content available in the service has been presumed easily. In cases, where liability is not exempted under the provision, normal rules of civil and criminal liability apply (Government bill HE 194/2001). Consequently, in these situations, the hosting service's own liability depends on rules on primary and secondary liability, e.g. copyright law. In the Supreme Court decision *Finreactor* (KKO:2010:47), operators of torrent P2P-services faced ***primary*** **copyright liability** by merely providing the facility and being aware of infringing activities, whereas in Sweden in *Pirate Bay* courts based their verdicts in similar situations in aiding and abetting a principal offence.

ISP obligation to act even before court order – specific procedure

There exists a specific procedure under which ISPs are obliged to act to prevent access to material infringing copyright or neighbouring rights, even before court order. The procedure is regulated in the Information Society Code. A holder of a copyright or his/her representative may, according to section 189 of the Information Society Code, request a hosting provider (referred to in section 184 of the Code) to prevent access to material that infringes copyright. The same applies to a holder of a neighbouring right and his/her representative if it concerns material that infringes this right. A request must first be presented to the content provider whose material the request concerns. If the content provider cannot be identified or if he/she does not remove the material or prevent access to it expeditiously, the request may be submitted to the hosting provider by notification, as prescribed in section 191 of the Code.

The hosting provider is obliged to give a contact point where the notification referred to above (section 191 of the Code) and the plea referred to below (section 192 of the Code) may be delivered. The contact information of the contact point must be easily and continuously accessible. The notification referred to above shall be made in writing or electronically so that the content of the notification cannot be unilaterally altered and so that it remains available to the parties. The more detailed contents of the notification are intended to be sufficiently precise and adequately substantiated, as also required by CJEU case law, notably *L'Oreal v eBay* referred to above.[1]

After notification, the material goes offline. The hosting provider must immediately notify the content provider of **prevention of access** to the material supplied by him/her and to supply the content provider with a copy of the notification on the basis of which prevention was made. If the content provider considers that prevention of access is **groundless**, he/she may get the material returned (online) by delivering to the notifying party a plea in writing or electronically within 14 days

[1] In more detail, the notification must include: 1) the name and contact information of the notifying party; 2) an itemisation of the material, for which prevention of access is requested, and details of the location of the material; 3) confirmation by the notifying party that the material which the request concerns is, in its sincere opinion, illegally accessible in the communications network; 4) information concerning the fact that the notifying party has in vain submitted its request to the content provider or that the content provider could not be identified; 5) confirmation by the notifying party that he/she is the holder of copyright or neighbouring right or entitled to act on behalf of the holder of the right; 6) signature of the notifying party. A notification that does not meet these requirements is invalid. If the shortcomings in the notification solely concern itemisation of the material, for which prevention of access is requested, and details of the location of the material, the information referred to in 2) above, the information society service provider shall, however, take reasonable steps to contact the notifying party and to communicate the shortcomings discovered.

of receiving the notification. A copy of the plea shall be delivered to the service provider.[2] If the **plea**, meeting the applicable requirements, is delivered within the time limit, the hosting provider must not (according to section 193 of the relevant Code) prevent the material specified in the plea from being returned (online) and kept available (unless otherwise provided by an agreement between the hosting and the content provider, or by an order or decision by a court or by any other authority). So, after the plea of the content provider the material goes online again.

A person who gives false information in the notification information referred to above is liable to compensate for the damage caused. However, there is no liability to compensate, or it may be adjusted if the notifying party had reasonable grounds to assume that the information is correct, or if the false information is only of minor significance, when taking into account the entire content of the notification or the plea. Liability to compensate is regulated in section 194 of the Code.

In addition, hosting providers are obliged to act based upon their knowledge and even before a court order when the material in question is about **hate speech** or making available a picture of child **pornography**, sexual violence or intercourse with an animal. In these situations the hosting provider must notify the content provider and the notification must state the reason for prevention and information on the right of the content provider to bring the matter for court hearing.

When these provisions were enacted, the Government and the Constitutional Committee of the Parliament evaluated the impact of the proposed measures on **freedom of expression** and freedom to conduct business. Section 12 of the Finnish Constitution secures freedom of expression, and does not permit restrictions by *ex ante* measures.[3] In most situations, removal and blocking orders are decided by a court. Only in very precisely delineated situations actions can be taken without court orders. Moreover, it was taken into account that the provisions do not contain any *ex ante* preventive measures, but all the actions are taken afterwards.

For materials infringing **copyright**, it was considered in the Government bill that these situations often relate to piracy or infringement of copyright where freedom of speech issues are not relevant, and there is no uncertainty of copyright infringement.[4] Yet, the procedure is designed to ensure content providers' right to **due process**, as they can challenge the grounds of removal and get the material returned online. The compensation scheme for wrongful information was also considered to prevent groundless notifications.

Situations concerning **hate speech** or making available a picture of child pornography, sexual violence or intercourse with an animal, could relate to freedom of expression. Yet, because the measures are taken afterwards, and there is the possibility to appeal the decision to a court, the legislation is thought to secure the content providers' due process rights (Government Bill HE 194/2001).

The Constitutional Committee of the Parliament (report 60/2001) considered that even though the notification procedure for copyright infringements is based on subjective evaluation when initiating the removal procedure, the legislation fulfils the requirements of **preciseness** and **limited nature**, due to the objective criteria used in the legislation. For actions taken as a result of suspected crimes,

---

2 The plea must include: 1) the name and contact information of the content provider; 2) the facts and other reasons under which prevention is considered groundless; 3) an itemisation of the material for which prevention is considered groundless; 4) signature by the content provider.

3 The Finnish Constitution is in this respect stricter than the European Convention on Human Rights, as the Finnish Constitution does not enable preventive measures at all. See for example *Tiilikka, Päivi*: Journalistin sananvapaus, p. 63 WSOYpro 2008.

4 This assumption in the Government Bill might not hold water.

the Constitutional Committee required actions to be based on the criteria that the material is *clearly* against said provisions of the criminal code. This was due to the principle of legality in criminal procedure and the presumption of innocence until proven guilty. The Constitutional Committee also analysed the requirement of **proportionality**. Treating specific crimes under a different procedure was considered acceptable, as the crimes under the different treatment related to particularly objectionable material, and as preventing the dissemination of such materials protected the fundamental rights of others. The measures concerning copyrighted materials were considered to fulfil the proportionality requirement, as there is due procedure after the removal of the material.

ISP's obligation to take action to implement a decision by the authorities

Section 188 of the Information Society Code regulates information society service provider's obligation to take action to implement a decision by the relevant authorities. The provisions treated above (Sections 182–184), regulating information society service provider's exemption from liability, will not apply to the service provider's obligation to take necessary action, under any other law, to implement an order or a decision by a court or by any other competent authority. If the information is clearly of such nature that keeping its content available to the public or its transmission is punishable, or constitutes a basis for civil liability, the access can be disabled under Section 185 of the Information Society Code. The procedure for this is described below under title 3.

Court orders concerning infringements of copyright or neighbouring rights under the Copyright Act

The norms treated here concerning court orders related to materials infringing copyright or neighbouring rights under the Copyright Act apply similarly to both copyright and neighbouring rights.

Section 60 b of the Copyright Act defines the actions available when allegedly copyright infringing material is made available to the public. For the purpose of prohibiting continued violation, the author or his/her representative has the right to take legal action against the person who makes the allegedly copyright-infringing material available to the public. A court (Market Court in practice) may order that the availability of the material to the public must cease.

The role of the ISPs in copyright infringements is regulated by Sections 60 a, c and e of the Copyright Act. Section 60(a) of the Copyright Act regulates information requests on the subscribers behind IP addresses. As has become clear from the relevant CJEU case law, e.g. *Promusicae* (C-275/06) and *Bonnier Audio* (C-461/10), Member State courts may validly under EU law obligate ISPs in civil law processes to give copyright holders such information, in alleged cases of infringements of copyright. According to the principles established in these cases, as far as the national norms enable the national court to weigh the conflicting interests involved in each case and to evaluate the application for an order for disclosure of personal data from the viewpoint of the proportionality principle, the legislation likely secures a fair balance between the protection of intellectual property rights enjoyed by copyright holders and the protection of personal data enjoyed by Internet subscribers or users.

According to Section 60 a of the Copyright Act, an author or his/her representative is entitled, by a court order, to obtain contact information from the service provider acting as an intermediary about its customer who, unauthorised by the author, makes material protected by copyright available to the public to a significant extent from the perspective of the protection of the author's rights. The author or his/her representative, who has obtained the contact information, is bound by the Information Society Code's provisions on confidentiality and privacy, the handling of messages and identification data, information security, guidance and supervision, coercive measures and sanctions. An author or his/her representative must defray the costs incurred from the enforcement of an order to supply information and recompense the maintainer of the transmitter, server or other similar device or other service provider acting as an intermediary for possible damage.

For a long time, Finnish courts granted such orders essentially without any critical evaluation of the significance of making the material available to the public from the perspective of the copyright holder and without considering opposing interests, such as privacy of customers. Only in one case out of more than hundred did the court decline such an information request after performing a weighing operation. This case law was hardly in line with *Promusicae* and *Bonnier Audio* and the requirement of weighing the applicable interests and proportionality in individual cases to the situations has recently begun to change, after legal scholars in Finland paid attention to this inadequacy,[5] and the treatment of such requests in Finland is now the responsibility of the Market Court rather than of regular district courts.

When trying a case the court may, according to section 60 c of the Copyright Act and also upon request of the author or his/her representative, order the service provider acting as an intermediary to discontinue, on pain of fine, the making of the allegedly copyright-infringing material available to the public (injunction to discontinue), unless this can be regarded as unreasonable in view of the rights of the person making the material available to the public, the intermediary, the recipient of the material and the author. When considering such a request, the court must reserve an opportunity to be heard for both the person against whom the injunction is sought and the person making the allegedly copyright-infringing material available to the public. The order may not endanger a third person's possibilities to send and receive messages.

Section 60 c of the Copyright Act implements Article 8(3) of the Information Society Copyright Directive, which obliges Member States to provide an opportunity for copyright injunctions against intermediaries. Recital 59 of the Directive states that the conditions and modalities are to be determined in national legislation. In the statement (15/2006, 2) by the Constitutional Law Committee of the Parliament, it was noted that giving such an order is possible provided it is not unreasonable for the parties. According to the Law Committee (5/2005 10) the principle of proportionality also requires that the order must not affect communication to the public more than strictly necessary for protecting copyright. The Law Committee also held that third parties must not suffer from the dispute, and that the prohibition on endangering legal communications is inviolable. It has been evaluated in the relevant legal scholarship that Finland is one of the few examples of rather detailed legislation on the implementation of Article 8(3) of the Information Society Copyright Directive.[6]

Helsinki district court has issued an interim injunction to discontinue based on section 60 c of the Copyright Act (decision 11/41552, 26th of October 2011). The decision was issued against Elisa Corporation, which is one of the biggest companies in Finland providing telecommunication services. The court ordered Elisa Corporation to prevent access to Pirate Bay webpages. Elisa Corporation was ordered to delete domain names used by the Pirate Bay, and prevent access to the IP addresses used by the Pirate Bay's service. The court considered whether the injunction was unreasonable from the perspective of fundamental rights, namely freedom of speech and copyright owner's right to property. It was considered that the decision should not interfere more with the making available of material than what is necessary in order to protect copyright.

Helsinki Court of Appeal affirmed the decision (decision number 1687, S 11/3097, 15th of June 2012). The Supreme Court of Finland did not grant parties the right of appeal.

---

5 Notably *Päivärinne, Jussi* in Defensor Legis 2013/2, p. 196.

6 *Savola, Pekka*: Internet Connectivity Providers as Involuntary Copyright Enforcers: Blocking Websites in Particular, IPR University Center 2015, p. 35.

There are similar decisions concerning TeliaSonera and DNA corporations (Helsinki District Court, 11.6.2012 H11/48307 and Helsinki District Court, 11.6.2012 H11/51544). These major companies also provide telecommunications services and in both cases, the orders also concerned Pirate Bay.

These decisions have been criticized in legal scholarship, as despite the function of the relevant norms being targeted at interim measures, the purpose of the proceedings was permanent blocking. Moreover, it has been argued that such measures constitute ex ante restriction of freedom of expression, as prohibited by section 12 of the Finnish Constitution.[7]

The interim injunctions can also be issued before the legal action is taken if the above-mentioned conditions are met, and provided that the rights of the author would otherwise be seriously jeopardized. Before the legal action is taken, a court may also order interim injunction without hearing the alleged infringer if this is deemed necessary due to the urgency of the case. Such an injunction will remain in force until further notice. After the injunction has been issued, the alleged infringer must be allowed an opportunity to be heard without delay. After hearing the alleged infringer, the court shall decide without delay whether it retains the injunction in force, or cancels it. The legal safeguards for the measures to discontinue are governed by Chapter 7 of the Judicial Procedure Code, which regulates precautionary measures.

The new provision of Copyright Act, section 60 e, enables a court to order an intermediary (ISP) to discontinue the making available of allegedly copyright infringing material when the claimed infringer is unknown. This is possible provided that the making available of allegedly infringing material takes place to a significant extent without the consent of the author or it is obvious that the protection of the author's right would be otherwise seriously jeopardized. The claimant/applicant must provide information on what actions it has taken in order to identify the alleged infringer. The order can be given on the condition that it is not considered unreasonable from the perspective of the alleged infringer, the intermediary, the recipient of the material and the author. The order may not jeopardize a third person's possibility to send and receive messages. The court treating the matter has to reserve the possibility for the intermediary to be heard before issuing the order. Such an order must be given for a fixed period of time and a maximum of one year at a time. It is possible to continue such an order for reasonable grounds. If the original reason ceases to exist, the court must cancel the order upon request by the concerned party.

There is not yet any case law applying section 60 e of the Copyright Act.

The provisions of the Copyright Act referred to above, and the provisions of the Patent and Trademark Acts referred to below, also implement Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the Enforcement of Intellectual Property Rights.

Court orders in patent cases

Section 57 b of the Patent Act covers court orders in patent cases. When trying a case, the court may also upon request of the patent holder order the service provider acting as an intermediary to discontinue, on pain of fine, the allegedly patent-infringing usage (injunction to discontinue), unless this can be regarded as unreasonable in view of the rights of the claimed infringer, the intermediary, and the patent holder. The interim injunctions can also be issued before the legal action is taken if the above-mentioned conditions are met, and further provided that the rights of the patent holder would otherwise be seriously jeopardized. The court must reserve an opportunity to be heard for both the person against whom the injunction is sought and the claimed infringer. Before the legal

[7] *Pihlajarinne, Taina*: Internet-välittäjä ja tekijänoikeuden loukkaus, Lakimiesliiton kustannus 2012, p. 140 and 149. Pihlajarinne also considers that filtering measures might constitute restrictions of freedom of expression as prohibited ex ante measures (at p. 51).

action is taken, the court may also order an interim injunction without hearing the alleged infringer, if this is deemed necessary due to the urgency of the case. The injunction will remain in force until further notice. After the injunction has been issued, the alleged infringer must be reserved an opportunity to be heard without delay. After hearing the alleged infringer, the court must decide without delay whether it retains the injunction in force or cancels it. The order may not jeopardize a third person's possibility to send and receive messages. The injunction to discontinue will enter into force when the applicant provides the security referred to in section 2 of Chapter 8 of the Enforcement Act (705/2007) to the execution officer, unless otherwise provided in section 7 of Chapter 7 of the Code of Judicial Procedure. The injunction to discontinue issued by virtue of this section shall expire, if a legal action has not been taken within six months from the issuing of the injunction. If the legal action is dismissed or ruled inadmissible or the case is discontinued due to the fact that the plaintiff has cancelled his legal action or failed to appear in court, the person requesting the injunction to discontinue must recompense the person against whom the injunction is issued, as well as alleged infringer for damage caused by the enforcement of the injunction.

Court orders in trademark cases

Section 48a of the Trademark Act (21.7.2006/680) contains an almost identical provision to section 57b of the Patent Act. Only the time limit for the legal action after an interim injunction is different: the injunction to discontinue issued by virtue of this section shall expire, if a legal action has not been taken within *one month* from the issuing of the injunction.

Coercive measures under Act on the Exercise of Freedom of Expression in Mass Media

The Act on the Exercise of Freedom of Expression in Mass Media applies to publishing and broadcasting in Finland. Operations consisting solely of the technical production, transmission, intermediation or distribution of publications or network messages are subject to the two provisions (sections 17 and 18 of the Act) treated below. Separate provisions explained elsewhere in this report apply to copyright and to the provision of information society services.

Section 17 of the Act regulates the release of identifying information for a network message. A private individual maintaining a web site is not subject to this obligation. According to Section 17, a court may order the intermediary to release the information required for the identification of the sender of a *network message*[8] to the requester, provided there are probable reasons to believe that the contents of the message are such that providing it to the public is a criminal offence. However, the identifying information may be ordered to be released to the injured party only in the event that he or she has the right to bring a private prosecution for the offence. The request must be filed with the district court of the domicile of the intermediary, or with the district court of Helsinki, within three months of the publication of the message in question. The court may reinforce the order by imposing a threat of a fine. A court order on the release of identifying information is open to appeal as a separate matter. The order cannot be enforced until it has become final, unless the appellate court orders otherwise.

Identifying information may be ordered to be released on the **request of the authorities of a foreign state**, if the provision of the relevant message to the public would constitute an offence in Finland under the prevailing circumstances, or if the release is based on an international agreement or on some other international obligation binding on Finland. The intermediary is entitled to compensation from state funds for the reasonable direct costs arising from the release of the identifying information. The decision to pay compensation is made by the police chief of the district where the

[8] A network message means information, an opinion or some other message provided to the public by means of radio waves, an electronic communications network or some other comparable technical arrangement.

investigation was carried out, or by the chief of a national police unit. The decision is open to appeal in an administrative court. However, the injured party must bear these costs when the information is being released to him or her in accordance with a court order.

Section 18 of the Act concerns an order to cease the distribution of a network message. At the request of the public prosecutor, the head of a pre-trial investigation, or the injured party, a court may order that the publisher, broadcaster or intermediary is to cease the distribution of a published network message, if it is evident on the basis of the contents of the message that providing it to the public is a criminal offence. The court deals with the request as a matter of urgency. Before issuing a cease order, the court reserves the intended addressee of the order and the sender of the network message an opportunity to be heard, unless the urgency of the matter necessitates otherwise. Notice of the cease order is served also on the sender of the network message referred to therein. If the sender is unknown, the court may order that the intermediary attends to the service.

A cease order lapses unless within three months of its issue a charge is brought for an offence arising from the contents of the relevant message, or a demand of forfeiture or destruction is made, or a tort action pertaining to the contents of the message is brought. The person having been issued with a cease order, as well as the sender of the network message, has the right to apply for the reversal of the cease order from the court that originally issued it. The network message shall not again be provided to the public while the reversal proceedings are pending, unless the court seized of the matter orders otherwise. Also the public prosecutor has standing to appeal against the reversal of a cease order. On the request of the public prosecutor or an injured party, the court may issue a cease order also when it is hearing charges based on the contents of a published message, a demand for a sanction of forfeiture or destruction, or a tort action pertaining to the contents of the message. Such a cease order is not open to appeal as a separate matter.

Voluntary measures targeted at foreign child pornography webpages

There is a specific law covering voluntary measures targeted at foreign child pornography webpages. The Act on preventive measures for spreading child pornography (Act 2006/1068) authorizes the police to keep records of child pornography webpages maintained abroad. The police request and receive information related to the issue from non-governmental organizations, private persons, public authorities and telecommunications operators. Telecommunication operators have the right to provide their services in a manner that access to child pornography webpages is prevented. The police are obligated to draft a notice, which becomes visible whenever access to the defined webpages is prevented. The information notice must contain the following information: 1) the fact that access to the webpages is prevented; 2) the reasons for the measure; 3) information to whom one can contact when necessary; 4) contact information. The records kept by police under this Act are confidential.

The Supreme Administrative Court decision (KHO 2013:136) concerned a list of foreign child pornography pages. A person provided on his webpages a list of foreign child pornography webpages. The police included this Finnish webpage in the list of foreign child pornography webpages. A previous Supreme Administrative Court decision (KHO 2010:53) had already established that one has the right to appeal the decision by the police to include something in the list, notwithstanding the Finnish *travaux prépatoires* stating that one cannot appeal the decision of the police on this issue. The reasons for this right related to the Constitution of Finland (section 21) and the European Convention on Human Rights (Article 13). The Helsinki Administrative Court then decided that the Finnish webpage had to be removed from the list, as the Act concerns foreign webpages only.

However, the Supreme Administrative Court in KHO 2013:136 decided that even though the *travaux prépatoires* of the Act suggest that the objective of the law is to prevent access to foreign child pornography webpages, the provision of the act does not prevent an interpretation according to which also a Finnish webpage can be included in the list recorded by the police, if a Finnish webpage enables access to foreign pages, and this way promotes distribution of child pornographic material. It was considered that since the child pornography Act does not provide *ex ante* censorship mechanism but only *ex post* preventive mechanism, the Act is not unconstitutional on this basis. In addition, it was considered that the protection of children prevailed over the freedom of speech arguments, when limited freedom of speech concerned child pornographic material. Moreover, there was a possibility to appeal, and thus possibility of court review. The regulation fulfilled, among others, the requirements of precision and legal safeguards.

It was also stated in the Supreme Administrative Court judgment that the decision to include the Finnish list in the police record did not prevent the person, providing the list, of other means for critical discussion (and freedom of speech), because it was deemed possible to engage in critical discussion concerning child pornography-related issues (and the Act in question) without including the list of foreign webpages in the same media. This decision has been criticized in the legal literature in Finland. The critique has highlighted that the law was clearly targeted at foreign webpages, but still the court held that even Finnish webpages listing foreign webpages qualify for the procedure. Second, the critique has pointed out that there are more effective measures available to address Finnish webpages. Consequently, the action against the Finnish webpages was not considered effective and proportionate with regard to the objective, namely the prevention of access to foreign webpages containing child pornography.[9]

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?

The Information Society Code describes in general the procedure and competent authorities for decisions to prevent access to illegal internet content. For copyright issues, the procedure is partly described under heading 2.1. above. The same applies for orders based on Act on the Exercise of Freedom of Expression in Mass Media.

Upon request from a public prosecutor, or a person in charge of inquiries, or on application by a party whose right the matter concerns, a court may order the information society service provider referred to in section 184 of the Information Society Code to disable access to the information stored by it if the information is clearly such that keeping its content available to the public or its transmission is prescribed punishable or constitutes a basis for civil liability. The court must process the application urgently. The application cannot be approved without reserving an opportunity for the service provider and the content provider to be consulted, except if the consultation cannot be arranged as quickly as the urgency of the matter so necessarily requires. The procedure is regulated in section 185 of the Information Society Code.

A court order must also be made known to the content provider. If the content provider is not known, the court may order the information society service provider to take care of the notification.

---

[9] *Savola, Pekka – Neuvonen, Riku* KHO 2013:136 – Verkkotunnusluettelon julkistamisen katsottiin edesauttavan lapsipornon levittämistä, Lakimies 1/2014, pp. 114-138.

An order ceases to be effective unless charges are raised for an offence based on the content or transmission of information referred to in the order or, when concerning a liability, action is brought within three months of issuing the order. On request by a public prosecutor, by an injured party or by an interested party within the time limit referred to above, the court may extend this time limit by a maximum of three months. The information society service provider and the content provider have the right to apply for reversal of the order in the court where the order was issued. When dealing with a matter concerning reversal of the order, the provisions of Chapter 8 of the Code of Judicial Procedure must be observed. However, the court takes care of the necessary procedures to hear a public prosecutor. The reversal must be applied for within 14 days of the date when the applicant was notified of the order. The information must not be made available again when the hearing of the case concerning the reversal is pending, unless otherwise ordered by the court dealing with the case. A public prosecutor also has the right to appeal the decision that reversed the order.

The Constitutional Committee (report 60/2001) considered that because court decisions for removal and other similar measures are given in order to prevent the dissemination of illegal material, there is justified reason for these provisions. Prevention of crime is one such justified ground. Moreover, for copyright infringement, it was elaborated that copyright receives protection under constitution (right to property). Even though the court decisions can sometimes be given without hearing a party beforehand, hearing is still the main rule. Moreover, there is the right to appeal. Consequently, the procedural measures were considered to secure adequate remedies for the affected parties.

The application referred to above (based on section 185 of the Information Society Code) is heard by the court of the information society service provider's domicile. However, the application may also be heard by the district court in Helsinki. The chairman of the court alone may also constitute a quorum, in line with Section 186 of the Information Society Code.

Section 187 of the Information Society Code provides legal safeguards for the content provider. If the information society service provider has prevented access to information under section 184(1)(2) of the Information Society Code, it shall according to section 187 of the Code immediately notify the content provider of this in writing or electronically so that the content of the notification cannot be unilaterally altered, and it remains accessible to the parties. The notification must state the reason for prevention as well as information on the right of the content provider to bring the matter for a court hearing. The notification must be made in the mother tongue of the content provider, in Finnish or in Swedish. The notification may also be made in another language agreed with the content provider. The content provider has the right to bring the matter concerning prevention to be heard by the court referred to in section 186 of the Information Society Code within 14 days from the receipt of the notification. The provisions of section 185(4) of the Information Society Code must be observed during the hearing of the case concerning prevention.

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?

There is no central Internet monitoring agency in Finland. There has been a Working Group under the Ministry of Defence, addressing among others the possibilities for intelligence on telecommunications and internet traffic. However, fundamental rights as protected by Finland's Constitution were seen as jeopardized by such legislation. The Working Group published its report on 14th of January 2015. The report and its proposals for broader monitoring possibilities received heavy criticisms in the media in Finland, as well as among scholars. However, the new government in

Finland includes the proposal in its government program. Legislating it may require changes in the Finnish constitution, which would require processing by two consecutive Parliaments. Legal scholars in Finland have criticized these plans, e.g. prof. *Juha Lavapuro*.[10] It is likely that the CJEU's *Schrems*-judgement (C-362/14), finding the Commission's safe harbour decision concerning the US invalid, affects the preparation and contents of the Finnish initiative.

The Copyright Information and Anti-Piracy Centre (CIAPC) in Finland represents its member associations, which consist of various Finnish copyright holder groups in the fields of music, literature and audio-visual industries. CIAPC can represent the relevant right holders in copyright infringement cases. CIAPC also conducts centralized surveillance of the Internet for the benefit of the right holders. The legality of such surveillance measures under Finnish or European standards is questionable.

The Police have a *Net tip* service for submitting non-emergency information to the Police for any suspicious material found on the Internet.[11] Save the Children Finland Association maintains "*Hotline Nettivihje*", as a member of INHOPE (International Association of Internet Hotlines) network. It strives to enhance the removal of Child Sexual Abuse Material (CSAM) from the Internet through national and international co-operation. Hotline Nettivihje sends the information of illegal online content (CSAM) located outside Finland to the Hotline in the country where the illegal material is hosted. When there is no Hotline in that country, the information is sent to Law Enforcement Authorities in Finland. The Finnish Hotline Nettivihje processed over 2300 reports in 2014. Of these, 1/5 was assessed to be illegal, typically pertaining to child sexual abuse.[12]

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

Background

In Finland, the Constitutional Committee of the Finnish Parliament (consisting of Members of Parliament and administrative personnel) bears the main responsibility for checking the constitutionality of laws and their conformity with basic rights as protected in the Finland's Constitution, as well as with international human rights binding Finland. In case potential constitutional conflicts are identified in a Governmental Bill, the Committee processes the Bill and may require changes to secure compatibility with the Finnish Constitution and/or International Human Rights standards binding Finland. Yet at times important laws under preparation, affecting for example the rights of Internet users and ISPs, may bypass the Committee due to work-overload, time-pressures and/or political manoeuvring. The Committee may also at times treat Governmental Bills superficially, or only concentrate on some potential problems identified by external experts.

In addition to the Constitutional Committee, regular courts – there is no constitutional court in Finland – may establish an apparent conflict between laws (or decrees) and the Finnish Constitution, especially with basic rights as protected in Finland's Constitution. They are also intended to interpret laws in conformity with the Constitution and international and European human rights standards binding Finland (including the European Convention on Human Rights and the EU Charter of Rights). The Supreme Court and the Supreme Administrative Court, in particular, may discuss the case law of the European Court of Human Rights (as well as that of the CJEU when applicable) at length. Yet at

---

10 *Lavapuro, Juha*: Finnish Government and the Desire to Constitutionalize Mass Surveillance: Toward Permanent State of Emergency?, 31 August 2015, available at (visited 4 October 2015): http://www.verfassungsblog.de/en/finnish-government-and-the-desire-to-constitutionalize-mass-surveillance-toward-permanent-state-of-emergency/.

11 See https://www.poliisi.fi/nettip.

12 See http://www.pelastakaalapset.fi/en/how-we-work/children-and-digital-media/finnish-hotline-nettivihje/.

times – especially at lower court levels – the treatment of constitutional conflicts may be superficial, one-sided or totally lacking.

Requirements of quality

The requirements for the limitation of basic rights in Finland are very similar to those developed by the ECtHR in its case-law for the limitation of rights in the European Convention. Limitations must thus be: 1) based on law,

2) precise and limited,

3) justified by an overriding interest,

4) not affect the core of the right,

5) proportionate,

6) secure adequate remedies, and

7) be in line with international human rights standards.

In major legislative renewals (such as the implementation of the Information Society Copyright Directive in Finland and the Information Society Code), conformity with international and European human rights standards is typically checked already at the stage of administrative preparation in the relevant Ministry. Yet, sometimes such analysis may be lacking or superficial.

Generally, the relevant Finnish legislation meets the requirements of foreseeability, accessibility, clarity and precision as developed by the ECtHR. Some specific problem-areas are highlighted in the following analysis.

The possibility to give an order for the intermediary, setting the requirement to block access to copyright-infringing material (section 60 c of the Copyright Act treated above), was not evaluated by the Constitutional Committee when enacting the Act, as the proposal to this effect was initiated in the Law Committee during the Parliamentary procedure. The legislation is based on the premise that the applicant is responsible for compensating the access provider's legal and enforcement costs only in exceptional circumstances. This has been criticized in the Finnish legal literature, as the law possibly conflicts with the property ownership and freedom to conduct a business of the access provider.[13] The remedies are not well secured either, among others, because according to the *travaux preparatoires* to section 60 c of the Copyright Act, the interim measure including the blocking order could not be appealed. Yet courts in Finland have established that the access to justice –principle requires that the order can be appealed.

Moreover, a blocking order based on section 60 c of the Copyright Act may not jeopardize the right of third parties to send or receive messages. Although the interpretation of this provision could be encompassing – e.g. covering the general technical impairment of communication systems, unintentional or necessary blocking of non-infringing web-sites, blocking of technical or administrative messaging, or blocking traffic outside the jurisdiction of Finland – the interpretation has been very narrow in practice. Legitimate traffic in the blocked site has not prevented the blocking measure, as long as there has been copyright infringing activity. Furthermore, technical or administrative traffic has not been specifically allowed, and finally the blocking orders could also according to their wordings result in an obligation to block in cases outside the jurisdiction of Finland. In practice, the obligation not to jeopardize the right of third parties to send or receive messages is restricted to the requirement that the blocking may not affect sites other than the blocked one, and it cannot for example be used to block an entire business corporation from the internet. This narrow interpretation of the rights of third parties has resulted in potential impediments for freedom of expression, although such risks have not yet entirely been realized.

---

[13] Most Notably by *Savola, Pekka*: Internet Connectivity Providers as Involuntary Copyright Enforcers: Blocking Websites in Particular, IPR University Center 2015.

Although the Copyright Act and the relevant *travaux preparatoires* are silent, in applicable case law it has emerged that courts must evaluate the technical feasibility of the blocking order. However, this position was developed before the *UPC Telekabel* –case of the CJEU, where outcome prohibitions not specifying the measures in question were not only allowed, but possibly preferred over specific orders.

Prevention of abuse of power and arbitrariness

The Finnish legislation and in particular the enforcement and interpretation mentality of courts ensures relatively effectively, that abuse of power and arbitrariness are prevented. This is generally ensured by access to courts and judicial review, interpretation in conformity with basic rights and international and European human rights standards, as well as the substantive contents of the applicable laws. The Finnish constitutional and administrative law tradition emphasizes *Rechtsstaat* principles and legality. For example, shutting down whole services to block individual content (like in the facts of the *Yildirim* case reaching the ECtHR) or imposing large-scale filtering obligations for protecting copyright without any practical limits (like in the circumstances of the *Scarlet Extended* – case reaching the CJEU) would hardly be possible in Finland. In the latter case, freedom to conduct business and freedom of expression concerns would likely disable such measures.[14]

Although Finland has relatively often been found to overprotect the reputation and honour of politicians and other public figures by awarding compensations resulting in chilling effects for freedom of expression, it is not likely that national legal developments leading to the situation in the *Delfi* case in Estonia (reaching the Grand Chamber of the ECtHR) would take place in Finland either, as the legal responsibility of on-line news services for defamatory user comments is likely not as strict in Finland as it is in Estonia. However, the question of when on-line news services are liable for user comments posted on-line is yet unsettled under the Act on the Exercise of Freedom of Expression in Mass Media. For example, the extent of required modification and control triggering the liability of on-line news service is to be developed in subsequent case law.[15]

Implementation in practice

Implementation of human rights standards in practice has already become partially clear from the case law referred to above. One particular aspect of the Finnish legislation and case law is strong protection of copyright-related interests over other competing interests and values, such as freedom of expression.

The three cases against major intermediaries (Sonera, DNA and Elisa) to block access to Pirate Bay reflect the implementation and enforcement of the applicable laws treated above. In these orders, the courts accepted that the (not absolute) likely inefficiency of the intended blocking measure did not prevent giving the orders. It has been critically questioned in the Finnish legal literature how ineffective blocking measures must be to prevent the imposition of a blocking order.

The orders issued by the courts in these cases were detailed with regard to technical implementation, connoting that these aspects of the cases could also be appealed to higher courts. The standards established by the Finnish courts will be further evaluated below.

Self-regulatory frameworks

According to the *travaux preparatoires* to the Child Pornography Act, an access provider may – also in accordance with the freedom to conduct a business – offer their services substantively restricted, i.e. they may undertake self-regulatory measures to prevent their customers' access to illegal

---

14 See also *Pihlajarinne, Taina*, op. cit. at p. 61-63.

15 See more closely *Tiilikka, Päivi*, op. cit. at p. 31-33.

content. Intermediaries may thus include contractual provisions in their end-user agreements to this effect. In the absence of such provisions, it is deemed in legal literature that the access provider may also block illegal content when there is no question of illegality. However, it is more doubtful whether the access provider may reserve itself the right to block content that is merely potentially infringing. The contractual provisions used may also reserve the access provider the right to restrict access to content "*when the police or other competent public authority demands so*". The limits and the access providers' rights and obligations are not entirely clear with these respects, as there is no applicable case law or clear provisions of law.

As mentioned above, the Child Pornography Act also provides (section 3) that the access provider may – at its own cost – prevent access to web pages containing child pornography. The police maintain a secret list of such pages. Only foreign pages are to be included in the list (section 1). According to the Act, there is no decision subject to judicial review in such instances. This is problematic from the perspective of Article 6 of the European Convention, as also noted in the relevant Finnish legal literature. The Act did not go to the Constitutional Committee's review when enacted, nor was there any discussion about remedies in any other preparatory committee of the Parliament. However, the Supreme Administrative Court accepted in its decision referred to above that there must be judicial review. However, it later accepted in the same subject-matter that the inclusion of a Finnish web page in the list maintained by the Police, which merely linked to foreign pages as examples to protest and criticize the law, was in line with the Act and could thus be included in the list. This is hardly in line with the wording of the Act. It is also questionable, whether access providers can block access to such pages in an effective way. It is thus possible that the Act, despite setting a nominally voluntary regime of blocking, is proportionate as required by the European Convention and the Finnish Constitution. The legislation has been criticized from this perspective in the Finnish legal literature.

Conformity with the case-law of the European Court of Human Rights

There are no cases from the ECtHR or from Finnish courts that establish non-conformity of the laws addressed here with the standards of the European Convention. The Finnish courts have not imposed wholesale blocking orders shutting down entire services for restricting access to limited content. Furthermore, although the Finnish legislator has not always succeeded in securing judicial review, the Supreme Courts of Finland, in particular, have secured access to courts even in the absence of direct legislative support. Finally, the orders imposed have been rather specific.

The Finnish legislation and enforcement by courts may be criticized for taking a very narrow view of the freedom of third parties to send and receive messages in case of blocking orders. Therefore, the weighing between (intellectual) property ownership and freedom of expression tilts easily in favour of intellectual property ownership.

Similarly, the evaluation of the efficacy of the blocking measure as a condition for its justifiability has been very limited. This connotes that blocking measures may impair freedom of expression rights of third parties, but may not be effective in securing the purported aims. This could mean that the limitations test as developed by the ECtHR for freedom of expression is not fulfilled. However, in the absence of cases addressing this directly, this remains a mere possibility and argument in favour of changing the current legislation and practices.

Tuomas Mylly and Ulla-Maija Mylly[16]

09.11.2015

[16] Tuomas Mylly is professor of European economic law and Ulla-Maija Mylly is senior lecturer, both at the University of Turku, Faculty of Law.