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 494-506

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.

NETHERLANDS

1. Legal Sources

There is **no specific regulation of the issues of blocking, filtering, and take-down of Internet content in Dutch law**. However, **a wide body of case law** exists, primarily based on the liability exemption for information society service providers as laid down in Article 196c book 6 Civil Code (implementation of EU Directive 2000/31/EC on E-commerce). It should be noted that the relevant case law in the Netherlands dates back to March 1996 when in a law suit between Scientology and XS4all, a judge in The Hague ruled (in summary proceedings) on the circumstances in which Internet providers should act:

> "A responsibility might be assumed in a situation where it is unequivocally clear that a publication of a user is wrongful and where it can be assumed with reason that such is known to the access provider, for instance because someone has notified the provider of this. In such cases, Internet access providers might be requested to take steps against the user in question."[1]

The criteria that the wrongfulness must be unequivocally clear or known to be wrong were basically what the E-commerce Directive later determined. Hugenholtz[2] even claimed that the 1996 decision was a precedent with worldwide (or at least EU-wide) exposure that was ultimately codified in the E-commerce Directive. This case is also known as the first case (and remains one of the few cases) in which freedom of speech outweighed copyright protection.

Since August 31, 1954, the Netherlands has been a contracting party to the European **Convention for the Protection of Human Rights and Fundamental Freedoms**. According to Article 10 ECHR, any access to or use of services and applications through electronic communications networks that is liable **to restrict** fundamental rights or freedoms may only be imposed if they are appropriate, **proportionate and necessary within a democratic society**, and their implementation is subject to adequate **procedural safeguards**. On November 16, 2006, the Netherlands ratified the **Convention on Cybercrime** (CETS No. 185) and it entered into force in the Netherlands on March 1, 2007. On July 22, 2010, the Netherlands ratified the Additional Protocol to this Convention (CETS No. 189). The Protocol has been in force in the Netherlands since November 1, 2010 and includes an extension to cover offences of racist or xenophobic propaganda.

Further, on August 24, 1993 the Netherlands ratified the **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data** (CETS No. 108) (entry into force on December 1, 1993). On September 8, 2004, the Netherlands ratified its Additional protocol regarding supervisory authorities and trans border data flows (entry into force on January 1, 2005).

Restrictions on access to the Internet are considered a restriction to the constitutional rights of **freedom of expression and information**, which are laid down in Article 7 of the Dutch Constitution (DC). A **restriction** to this right, by blocking, filtering or taking down content otherwise available on the Internet, is possible **if based on formal legal grounds** ("*without prejudice to the responsibility of every person under the law*", Article 7(1) DC), such as anti-discrimination laws, defamation, slander or intellectual property laws.

Since Internet access as a general right does not have a central place in Dutch law, neither does the restriction to this access. Measures for taking down, blocking or filtering of illegal content can be

---

1 Court of The Hague 12 March 1996, <http://kspaink.home.xs4all.nl/cos/verd1eng.html>.

2 Annotation on the Appeal case, *AMI* 2003-6, p. 222-223.

found in different laws, including the Dutch Civil Code (DCC, *Burgerlijk Wetboek*), Dutch Criminal Code (DCrC, *Wetboek van Strafrecht*) and the Dutch Copyright Act (*Auteurswet*).

Related to the right to Internet access is **the principle of Internet neutrality**. In 2012, the Netherlands was the first European country to introduce Internet neutrality, in Article 7.4a(1) of the Dutch Telecommunication Act (*Telecommunicatiewet*), thereby prohibiting providers of public electronic communications networks via which Internet access services are delivered, and providers of Internet access services, from discriminating Internet traffic based on the service or application being transferred. The Article includes four exceptions that legitimize discriminatory measures if (i) they are necessary to prevent or diminish congestion, (ii) security matters require it, (iii) spam is filtered, or (iv) an obligation to do so is based on a legal act or court order. This right shall, however, be governed by the forthcoming EU Regulation on Connected Continent.[3]

2. Legal Framework

In general, illegal content can be taken-down, blocked or removed **based on a court order**, which – under Article 196c(5) book 6 (6:196c) DCC – does not have to take into account the different "roles" of the Internet service provider, meaning the ISPs that fall under the *mere conduit* provision also have to obey such an order. Notably, the hosting provider is the most common ISP asked to take down material.

Civil liability exemptions of ISPs' liability are regulated in art. 6:196c DCC. As in the E-commerce Directive, mere conduit providers are exempted from liability (cf. art. 6:196c(1) DCC) if they do not: (a) initiate the transmission, (b) determine who receives the information, and; (c) select or change the information. Caching providers are not liable (cf. art. 6:196c(3) DCC) if they: (a) do not change information, (b) respect access conditions, e.g. information behind pay walls should not be cached and offered for free, (c) information is updated according to generally recognized procedures, (d) do not change tracking and tracing software, and (e) remove the cached information promptly once it is known that the original information is no longer there or if competent authorities have ordered removal of the original information or that it be made inaccessible. Hosting providers are exempted (cf. art. 6:196c (4) DCC) if they have no knowledge of unlawful content and if they remove or make inaccessible the information as soon as they do acquire this knowledge.

The request to block, filter or take-down can be **based on many different substantial law articles** that include, but are not limited to, the most important ones mentioned briefly below. To begin with, instead of a variety of torts Dutch law has one **general article on civil liability** (Article 6:162(1) DCC): someone who acts wrongfully is obligated to compensate the damages the victim suffered because of his act. This article is not only used if damages have already occurred, but also in case of preventive measures. These preventive measures concern, e.g. restraining orders, and often cases about people wanting to prevent programs from being broadcast. In the context of Internet content, the preventive measure is always in the context of something that has already occured. So, for instance, where a party has uploaded defamatory material that had to be taken down and is ordered to never do that again. To our knowledge, ISPs never receive this kind of order.

Article 240b of the Dutch Criminal Code deals with content related to **child-pornography**; criminalizing not only the possession, but also the transfer of and access to such content. This Article has included the incriminations set out in the 2010 Lanzarote Convention and the incrimination of

[3] Regulation of the European Parliament and of the Council laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent - COM(2013) 627.

the Convention on Cybercrime of 2002, criminalizing watching (without possession) of such content and adding virtual child-pornography to the Article. The criminal code also knows a number of content related crimes. In civil proceedings these crimes are often used to prove the wrongfulness of the content, e.g. discriminatory acts (Articles 137c-e DCrC), insults (Article 261 DCrC on libel, Article 262 DCrC on defamation, Article 266 DCrC on insults in general and "mean" expressions directed to the King (Articles 111-113 DCrC)), etc.[4] In particular, in the event that it is not clear who uploaded material qualifying as one the above crimes, parties can go to the ISP to request personal details of the uploader and/or ask the ISP to remove the material.

The Dutch Code of Criminal Procedure (DCCP) has a special section for **terrorist crimes**. For instance, Article 126zi DCCP indicates that suspicion is not necessary, rather mere indications of terroristic crimes suffice for an investigating officer to request that an ISP provide information such as name, address, ZIP code, and residence. Regarding filtering, the government has indicated that this does not work adequately, since in case of terrorism unlawful content is not as evident as compared to e.g. child-pornography, resulting in a disproportionate interference with the right to freedom of speech.[5]

Finally, Article 26d Dutch Copyright Act provides for the Dutch implementation of Article 11 of Directive 2004/48/EC on the enforcement of **intellectual property rights** (see also Article 8(3) Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society): "At the request of the author, the court can order intermediaries whose services are used by third-parties to infringe on copyright, to stop providing the services that are used to infringe."[6]

2.1. Blocking and/or filtering of illegal Internet content

Filtering of illegal content is regarded a more severe measure than taking-down or blocking content after a request or order. On blocking and/or filtering, there is not much case law in the Netherlands. For instance, section 5.2 on blocking and filtering of the recently published Dutch Internet case law book 2009-2015[7] covers relevant EU cases (Scarlet/SABAM, SABAM/Netlog, UPC Telekabel Wien, ACI/Thuiskopie) but from Dutch courts specifically, it only mentions the Pirate Bay case discussed below.

Filtering is regarded as a severe form of censorship, also due to the technical aspects such as the inaccuracy and ineffectiveness of filters: as a result, the measure is strongly criticised.[8] The obvious difference between taking down and blocking access is that in case of take-down the ISP is aware of

---

4 See for an overview Lodder, A.R. and Murray, A.D., A Primer on the Law of Internet Communication and Content: From the UK and Dutch Perspective. *Diálogos de Saberes, Investigaciones en Derecho y Ciencias Sociales*, no. 41, Julio-Diciembre de 2014, p. 173-188. Available at SSRN: http://ssrn.com/abstract=2616497.

5 Parliamentary records: *Tweede Kamer* 2007-2008, 28684, nr. 133.

6 Translation via http://cyberlaw.stanford.edu/page/wilmap-netherlands where they add: It thus provides a basis for a particular type of injunction that is independent from any liability under tort law. According to the Explanatory memorandum to this article, courts do have to take into account the degree in which the intermediary is involved in the infringement, and the proportionality between the court order's aim and the loss or damage that is suffered by the intermediary as a consequence of the court order. If the copyright-holder can just as well sue the infringer, then the court should reject the request.

7 Linden-Smith, M. van der and Lodder, A.R. (2015), *Jurisprudentie Internetrecht 2009-2015*, Deventer: Kluwer.

8 Most strongly expressed by E. Dommering (2008), Filteren is gewoon censuur, en daarmee basta, *Tijdschrift voor Internetrecht*, 2008-5, p. 124-125.

what content it concerns, whereas in case of filtering or blocking the focus is on the future. The exact content normally is not known but criteria are used to decide what Internet traffic is allowed to pass through and what is filtered. This process easily leads to both false positives (content being filtered out that should not have been) and false negatives (illegal content slipping through).

The Dutch Criminal Code (DCrC) provides a general **legal ground for making illegal content inaccessible, to seize criminal offences or prevent new offences**. Making inaccessible could mean blocking and/or filtering, but also the taking down of content. Article 54a DCrC reads:

> "An intermediary which provides a telecommunication service that consists of the **transfer or storage of data from a third party**, shall not be prosecuted in its capacity as intermediary telecommunication provider if it complies with an order from the public prosecutor to be rendered **to take all measures** that can be expected of it within reason, **to make these data inaccessible**, **which order shall be issued by the public prosecutor** after he has applied for and received a **written authorisation from the examining magistrate**."

The above implementation of Article 15 Directive 2000/31/EC on E-commerce was included in the DCrC, but the legislator failed to include a corresponding competence in the DCCP. The long awaited legislative reform regarding computer crimes will place the competence of law enforcement to give out such an order in the Dutch Code of Criminal Procedure (DCCP), suggested Article 125p DCCP, since the dual purpose (both substantial and procedural) of the Article was deemed confusing in existing legal procedures.[9] The amendment results in "better appliance" of the competences, but will not broaden the reach of the attributed competences.[10]

One interesting interpretation of Article 54a DCrC can be found in a case of the Court of Appeal Leeuwarden from April 20, 2009.[11] The ISP was asked to cooperate under Article 54a DCrC, but was also prosecuted for committing the crime of racist speech because of the content concerned. The judge ruled that Article 54a DCrC is meant for intermediaries, and this excludes those that commit crimes. If someone is a suspect he cannot be asked to assist in the same case as an intermediary.

The required authorisation of an examining magistrate should provide a balance of interests, including the interference with the fundamental right to freedom of information and expression. Currently, intermediates are exempted from criminal liability if an order to take down any illegal content is not properly authorised by an examining magistrate. The mere notice of an investigative officer directing to block the access to illegal content is therefore not enough for criminal liability. Inaction could, however, result in civil liability of the ISP concerned. In 2014, the Dutch Supreme Court decided that ISPs that comply with a request of the prosecutor based on Article 54a DCrC cannot file a complaint (cf. Article 522 DCCP) against this order.[12]

Previous attempts of the Dutch National Royal Police Department (*KLPD*) and the national Internet Access Providers (IAP) to agree on a 'black list' of websites that contained, facilitated or proliferated child pornography and that therefore had to be blocked by the IAPs, failed in 2008. The Dutch police aimed to contractually bind ISPs with the duty to block child porn material. The police assembled a black list of websites that the ISPs would not see (so a black box) but had to use to block traffic

---

9 District Court Assen 22 July 2008, ECLI:NL:RBASS:2008:BD8451; Court of Appeal Leeuwarden 20 April 2009, ECLI:NL:GHLEE:2009:BI1645; District Court Assen 24 November 2009, ECLI:NL:RBASS: 2009:BK4226.

10 Memorie van Toelichting Wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verbandmet de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (computercriminaliteit III), p.

11 ECLI:NL:GHLEE:2009:BI1643

12 Dutch Supreme Court 14 April 2014, ECLI:NL:HR:2014:908.

coming from the particular websites on the list. In a research by Stol *et al.* (2009)[13] it appeared that the list was poorly updated and the police also did not have the time to maintain it effectively. More importantly, Stol *et al.* concluded:

> "The confidentiality of Internet traffic is protected by article 8 of the European Convention on Human Rights and Fundamental Freedoms (ECHR) and the corresponding provisions of the Dutch Constitution (Article 13). Therefore, **infringement of this fundamental right by filtering and blocking information requires an explicit legal basis**. **Today, such a basis is lacking in The Netherlands**. **Filtering and blocking of internet traffic without permission of the persons concerned cannot be undertaken by the police or other government body**."[14]

Even today, Dutch law does not contain the necessary explicit legal basis. It is possible for ISPs to develop filtering technology, without government intervention. ISPs such as Google[15] and Microsoft[16] have developed a **form of self-regulation** regarding child-pornography by applying filters to their services.

BREIN is the Dutch anti-piracy organization, a foundation which aims to enforce intellectual property rights for, basically, the entertainment industry. They are active in court. In 2007 they obtained a court order to block an ADSL-connection.[17] The torrents on the website mostly involved copyright protected content, and by uploading these torrents these copyrights are infringed. KPN (the IAP) did not deny this. A number of copyright holders of the content on the website were represented by *Stichting Brein*, arguing that the website owner facilitated the infringements. The argument that users will just go to another website was not accepted by the court. Respecting the difficult position of an IAP, the court ruled that in principle the provision of the personal details would be sufficient. However, **because the actions of the subscriber were evidently infringing, KPN had to block access to the website**.

In 2012 BREIN obtained **several court orders that forced ISPs to block access to the Pirate Bay**.[18] In the July 30th, 2009 verdict, the court ordered the Pirate Bay to:

1. Stop copyright infringements in the Netherlands;
2. Make websites thepiratebay.org, piratebay.se, etc. inaccessible to Dutch users.

On October 22nd, 2009, the judge ordered:[19]

1. Pirate Bay to delete all torrents that refer to material that infringes copyright material relevant to BREIN;
2. that the relevant IAPs block access of Dutch internet users to the various Pirate Bay websites providing the torrents described at 1 above.

The Pirate Bay did not follow the court orders. As a result, BREIN moved on to the access providers. Based on the just discussed verdict, BREIN asked Dutch providers to filter out Pirate Bay Internet traffic. This appeared to be Ziggo, naturally, the biggest provider in the Netherlands. On principle grounds, XS4ALL joint Ziggo as a defendant in this case.[20]

---

13 Stol, W.PH., Kaspersen, H.W.K., Kerstens, J., Leukfeldt, E.R. & Lodder, A.R. (2009), Governmental filtering of websites: the Dutch case, *Computer Law & Security Review* 25 (3) 251 – 262.

14 Ibidem.

15 http://nos.nl/artikel/576732-google-gaat-kinderporno-filteren.html

16 https://www.security.nl/posting/436575/Microsoft+gaat+wraakporno+uit+zoekresultaten+verwijderen,

17 Court of The Hague 5 January 2007, ECLI:NL:RBSGR:2007:AZ5678.

18 This part is based on Lodder & Van der Meulen 2013.

19 Court of Amsterdam 22 October 2009, ECLI:NL:RBAMS:2009:BK1067.

20 Court of The Hague 19 July 2010, ECLI:NL:RBSGR:2010:BN1445.

In summary proceedings, BREIN applied Article 26d Dutch Copyright Act, **the Dutch implementation of Article 11 of Directive 2004/48/EC on the enforcement of intellectual property rights** (see also Article 8(3) Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society): *"(…) rightholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe an intellectual property right (…)"*

The judge ordered Ziggo and XS4ALL to block a list of 24 websites (of which several where out-dated at the moment of the verdict, and others later became out-dated), as well as three IP addresses.

On the subsidiarity question, the judge in the summary proceedings indicated that at least suing some consumers, i.a. because they could then have the opportunity to defend their position, could be requested from BREIN. Now the judge indicated this was not necessary, and that after the lawsuits against the Pirate Bay and the hosting providers, asking access providers was the logical next step.
On the proportionality question, the judge indicated that given the amount of illegal as opposed to legal content, the interests of the copyright holders outweigh the interests of the Internet users.
Based on the verdict, BREIN asked other ISPs to voluntarily start blocking The Pirate Bay. Since the ISPs refused, BREIN started new proceedings against other big providers, viz. KPN, UPC, T-Mobile, and Tele2.[21]

The **Court of Appeal of The Hague** handed down a decision on January 28th, 2014.[22] The court took into account several practical researches that demonstrated that the Internet traffic related to infringing material hardly showed any difference before and after the blocking. As a result, the court concluded that the blocking had not been effective. Despite the fact that the measures by the providers did not cost much or take much effort, being forced to block infringed on the freedom to act at its discretion. **Taking into account the ineffectiveness and the consequence that the measure could not contribute to what it was aimed at, the court found that the hindering of free entrepreneurship by ordering the blocking of Internet traffic is disproportional**.

2.2. Take-down/removal of illegal Internet content

Restricting access to illegal content via take-down procedures (**Notice-and-Take-Down**, NTD), entails the restriction of access to content following an order or request of a third party directed to the ISP. Adequately following this procedure is a prerequisite for the ISP to avoid civil or criminal liability, pursuant to Article 12-14 of the Directive 2000/31/EC. These Articles of the Directive are implemented in Dutch national law in Article 6:196c Civil Code and for criminal content in Article 54a Criminal Code. For the ISP to follow a NTD-request, **it should be unequivocally clear that the content is illegal**, which refers to various kinds of content infringing the reputation or rights of others. Article 125o of the Dutch Code of Criminal Procedure (DCCP) sees to the temporary measure of inaccessibility of illegal content that is found during an ongoing investigation. Other than the cases referred to in the previous section there are only few court cases on taking down material in a criminal law context. The reason is that ISPs normally cooperate if they are ordered to do so by the public prosecutor.

The taking-down of illegal content relating to copyright can be court ordered based on a claim by the rights holder, pursuant to Article 26d of the Dutch Copyright Act, an implementation of Article 11 of Directive 2004/48/EC on the enforcement of intellectual property rights. **Most take-down requests are based on copyright**. In the Netherlands there is no formal take-down procedure as, e.g.

---

21 Court The Hague 17 April 2012, ECLI:NL:RBSGR:2012:BW3596.

22 Court of Appeal The Hague 28 January 2014, ECLI:NL:GHDHA:2014:88.

the US DMCA, but often ISPs take down material after claims about copyright infringements, even if they are unjustified. A clear example in the last respect is the so-called Multatuli-project from 2004. What people in the UK did in 2003 with the Mill text *On Liberty* (in relation to which copyright had obviously expired), was repeated in the Netherlands with the famous book Max Havelaar (from 1871). Of the 10 ISPs receiving a take-down request, seven proceeded with the take down.[23]

In a public-private cooperation a **voluntary code of conduct for Notice and Take-down** has been formulated, describing how online service providers deal with illegal online content, such as child-pornography, plagiarism, discrimination and copyright infringement. In 2008, government, businesses and interest groups delivered this NTD code of conduct.[24] It was presented on October 9th, 2008 to the then secretary of state for Economic Affairs Heemskerk.[25] The code of conduct provides clarity for online services providers and provides **guidelines on how to decide when a complaint is legitimate and which steps to follow in order to comply with legal obligations**. Even though the NTD-procedure can be regarded a form of self-regulation, non-compliance with the legal procedure will lead to civil or criminal liability placing the provider under the formal regulatory framework.

The NTD-procedure is also relevant in a criminal law context. Firstly, law enforcement informs the intermediaries of such illegal content and will only resort to an order based on Article 54a DCC when the procedure is not sufficient.[26] The NTD code of conduct is subscribed by organizations as the premier ISP XS4all, Foundation for domain name registration SIDN, and the Dutch Hosting Provider Association DHPC. It is however, not easy to find this code of conduct on the Internet. The link ECP provides leads to a webpage[27] containing some information about the code of conduct but not the text of NTD-procedure. Also the Dutch IT Law consultancy firm ICTrecht is involved and supports people in this area, and they provide information on a special webpage but not the actual text of the code.[28] It can be retrieved on websites of subscribers to the code, but only in Dutch.[29]

There have been many "take-down incidents", and most of them do not make it to court. Still, over the years, dozens of cases have dealt with the taking down of infringing material, mainly based on copyright but also privacy, insult, threats, defamation, etc. Below we discuss the most important ones. We will indicate for each case to which of the legal categories introduced above (DCC, Copyright, DCrC) it belongs.

As already mentioned in the introduction, the first and longest running relevant case (spanning almost ten years in court) was between Scientology and ISP XS4all. Scientology demanded Karin Spaink and the provider XS4all to take down various Scientology documents under copyright law.[30] Karin Spaink had published on her website hosted by XS4all the so-called *Fishman Affidavit*. As Karin Spaink explains on her website:[31]

---

23 S. Nas (2004), *The Multatuli Project. ISP Notice & take down*. http://docplayer.nl/1397728-The-multatuli-project-isp-notice-take-down.html

24 https://ecp.nl/werkgroep-notice-and-takedown

25 For some background P.B. Hugenholtz (2009), Codes of Conduct for ISPs: Pragmatism v. Principle, in: A.R. Lodder & A. Oskamp (eds.), *Caught in the Cyber Crime Act*, Deventer: Kluwer, p. 45-47.

26 See Memorie van Toelichting Computercriminaliteit III, p 44. http://www.internetconsultatie.nl/computercriminaliteit.

27 https://www.dhpa.nl/vertrouwen-ntd/.

28 https://ictrecht.nl/factsheets/notice-and-takedown/.

29 https://www.oypo.nl/media/**ntd_gedragscode**.pdf.

30 For a historic overview of all the cases, see the website by Karin Spaink, <http://kspaink.home.xs4all.nl/fishman/>.

31 <http://kspaink.home.xs4all.nl/fishman/index2.html>.

> "The case file for Church of Scientology International v. Fishman and Geertz contains over 700 documents. This web page presents a declaration filed by Steven Fishman on April 9, 1993 in which he included the OT (Operating Thetan) materials as exhibits."

The Court of the Hague handed down its decision on June 9th, 1999,[32] and the Court of Appeal of the Hague on September 4th, 2003.[33] The Court of Appeal decided that **in balancing copyright against the freedom of expression the latter should (at least in this case) prevail**. Before the Supreme Court decided, Scientology withdrew their appeal. As a consequence the Supreme Court could not judge the case but only indicated that the appeal was withdrawn and the Court of Appeal decision remained in force.[34]

Another landmark case is Supreme Court case Lycos/Pessers.[35] This case is about civil liability (DCC) and was about Pessers, who next to his normal job earned about 350.000 euro per year by trading in postage stamps on eBay. Lycos is an ISP and hosted amongst others the website "Stop the fraud" on which in 2003 amongst others the following text could be found:

> "Have you ever been ripped off by [naam verweerder]@home.nl on E-bay, join our quest for justice!!

On 1 August 2003 Pessers asked Lycos to remove (amongst others) the above information, and the personal details of the owner of the website. On August 4 Lycos removed the material and placed the following text: "Site removed to avoid legal actions!!"

The Court of Appeal of Amsterdam defined on June 24th, 2004 the following rules of thumb. The provider may be forced to hand over the personal details (name, address, etc.) of subscribers if:

1. It is plausible that the information is unlawful in respect to the third person ordering the personal details;
2. The third person has a legitimate interest in obtaining the personal details;
3. It is plausible that in the specific case there is no less radical way to obtain the personal details;
4. The concerned interests of the third party outweigh the interests of the ISP and the owner of the website.

The E-commerce Directive does not specifically regulate the duty for ISPs to hand over personal details of their subscribers. Therefore, **the Supreme Court stated that the exemption of ISP liability does not prevent judges from take measures that can reasonably be expected from ISPs in respect of duties of care concerning detecting and preventing unlawful activities**. The Supreme Court referred to recital 48 of the Directive:

> "This Directive does not affect the possibility for Member States of requiring service providers, who host information provided by recipients of their service, to apply duties of care, which can reasonably be expected from them and which are specified by national law, in order to detect and prevent certain types of illegal activities."

The question of whether a hyperlink can be (e.g. Svensson) considered a communication to the public and therefore has to be removed upon request by the copyright holder has been addressed in a Dutch case that involved the unauthorized linking to nude pictures of a Dutch celebrity called Britt Dekker, which were to be published in the Playboy magazine later that month. Here the court tried the case according to the criteria: intervention, new public, and if the website that placed the

---

32 <http://kspaink.home.xs4all.nl/cos/verd2eng.html>.

33 Court of Appeal The Hague 4 September 2003, ECLI:NL:GHSGR:2003:AI5638.

34 Supreme Court 16 December 2005, ECLI:NL:HR:2005:AT2056.

35 Supreme Court 25 November 2005, ECLI:NL:HR:2005:AU4019.

hyperlinks was doing it for financial profit.[36] On appeal, the Amsterdam court judge ruled that the linking to "secret" information is not relevant from a copyright perspective but otherwise can be unlawful. The case is now with the Supreme Court, which has referred preliminary questions to the ECJ.[37]

The text Google selects to accompany the **search results** sometimes does not correctly reflect the content of the retrieved website. These cases are about civil liability (DCC). In one case the car dealer Zwartepoorte was incorrectly presented as bankrupt. If the search terms "Zwartepoorte" and "Bankrupt" were entered in Google, the first results phrased "Zwartepoorte. This company is bankrupt." If one clicked on the link of the Google search result, it became immediately clear that the combination was unlucky and that Zwartepoorte was not bankrupt. Zwartepoorte did not sue Google, but asked the website causing the first, confusing search result to **change their website**. The Judge in first instance defined a good standard for this type of situations:

> "if due to the design of a website search results cause damage for someone mentioned on this website, and this person asks the website owner to take a measure to prevent the damages, the freedom of expression should be weighed against the damage caused".

In this case, the website could take a very simple measure. The reason they did not was because they considered it principally unfair. The judge at first instance as well as the judge on appeal decided otherwise. The Court of Appeal confirmed the position.[38]

The company Stokke had tens of court cases in the Netherlands on intellectual property infringements. This case is about a particular children's chair they developed called Tripp Trapp. On Marktplaats, the Dutch online auction site owned by eBay, there is quite some trade in chairs under the name Tripp Trapp that actually are not genuine Tripp Trapp chairs. Marktplaats has offered Stokke a backdoor to the online auction site that allows them to take down infringing advertisements effectively. Stokke uses this backdoor, but claims that Marktplaats should carry out these Intellectual Property enforcement activities. Not only does Marktplaats offer the backdoor, but they also have as a general policy that all complaints are handled within 24 hours. The Court of Appeal Leeuwarden decided on May 22nd, 2012 that **Marktplaats cannot be held liable for the infringements, and that the measures already in place are sufficient**. The liability exemption for hosting providers was applied following the EU case L'Oreal/eBay.[39] One could doubt whether services such as the ones offered by Marktplaats fit into the category of classic hosting websites. However, even if the exemption would not be applied, under general tort law the outcome would still be that Marktplaats cannot be held liable. So, for the outcome the exact position taken in this case does not matter. The court of appeal does, however, seem to misunderstand the rationale of the liability exemption. They argued that exemptions become relevant if someone could be held liable. However, the safe harbor created by the liability exemption is meant to prevent someone from being held liable in the first place. If the conditions of the exemption are fulfilled, someone cannot be held liable.

---

36 District Court Amsterdam, 12 September 2012, CR 2013/7, m.nt. A.R. Lodder (Sanoma/Geenstijl). The District Court decided that the linking was a communication to the public in the copyright sense, and that permission was required. In appeal the court decided that only if the information was proven fully private, a link could be a communication to the public. Since the owners of Playboy could not prove it, the judge decided that the placing of the link was not a communication to the public.

37 District Court Amsterdam 12 September 2012, ECLI:NL:RBAMS:2012:BX7043; Court of Appeal Amsterdam 19 November 2013, ECLI:NL:GHAMS:2013:4019; Supreme Court 3 April 2015, ECLI:NL:HR:2015:841.

38 Court of Appeal Amsterdam 26 July 2011, ECLI:NL:GHAMS:2011:BR3418 (and District Court Amsterdam 13 May 2009, ECLI:NL:RBAMS:2009:BJ1595).

39 Court of Justice EU 12 July 2011, Case C-324/09 (*L'Oréal SA and Others/eBay International AG and Others*).

3. Procedural Aspects

From the legal framework discussed above, in particular the case law, it follows that in the Netherlands there is **no special authority that blocks, filters or removes illegal Internet content**. **The police and public prosecutor can take down material or make it inaccessible in case of criminal content**, e.g. child pornography.

ISPs sometimes voluntary cooperate to take down or filter, either in response to a request or on their own initiative. In the field of cyber security, ISPs have realized over the years that it is in their best interest to act. The same is true for spam. If ISPs did not use spam filters, probably no one would use e-mail any longer. The aim for these actions is to guarantee a properly functioning Internet, in particular to guarantee access that is not hindered by unwanted (spam) and the undesired (malware) activities of others. In 2013 Van der Meulen & Lodder introduced rules of thumb that could help in deciding whether an access provider should cooperate in case of a request.[40]

It remains a difficult position for ISPs, about when to take action or not. It is preferable that they remain neutral. The discussed code of conduct can help in their decision process.

There are cases in which it is obvious ISPs should act and cases in which it is obvious they should not: however, most cases are not so clear cut. In a recent court case, action was clearly required. Someone wanted from Facebook personal details of someone who created a fake account and uploaded sexually explicit material. The material was taken down, and also the account. The victim asked for the details of the person who created the account. Under these circumstances Facebook should have cooperated. They did not, but reacted in a standardized way: “we need a valid subpoena or court order.” Of course, in case of a court order it is clear for an ISP that they should act. But here it is arguable that Facebook should not have waited for the case to go to court.[41]

A special actor is the **Dutch Gaming Authority**. They can request the **blocking of advertisements for (foreign) illegal gambling websites, based on the prohibition of promoting illegal gambling** as laid down in Article 1 of the Dutch Gambling Act. The new law proposal on remote gambling provides the Gambling Authority with the additional competence to order the inaccessibility of illegal websites (Article 34n of the proposed law). This Article has been proposed in 2013 but is highly controversial and at the time of writing it is still not clear whether it will be enacted.

4. General Monitoring of Internet

Internet access is not monitored in the Netherlands. Monitoring of Internet content is only possible as part of a criminal investigation. Procedures of monitoring are similar to other surveillance measures.
ISPs are exempted from a general obligation to monitor the Internet under Article 15 of the Directive 2000/31 on E-commerce. ISPs can be forced by court order to either end or prevent an infringement (cf. implementation of Articles 12(3), 13(2), and 14(3) of the Directive 2000/31/EC on E-commerce.

---

40 See further A.R. Lodder & N.S. van der Meulen, Evaluation of the Role of Access Providers: Discussion of Dutch Pirate Bay Case Law and Introducing Principles on Directness, Effectiveness, Costs, Relevance, and Time, 4 *Journal of Intellectual Property, Information Technology and E-Commerce Law*. http://ssrn.com/abstract=2319494

41 District Court of Amsterdam 25 June 2015, ECLI:NL:RBAMS:2015:3984.

The EU data retention directive from 2006[42] forced ISPs to retain traffic data of their users. The Directive was declared invalid by the European Court of Justice in 2014,[43] and the related Dutch legislation was abolished by the Dutch Court in 2015. At both the EU and Dutch level, new data retention legislation is being drafted.[44]

In November 2007, the Court of Amsterdam ruled a case against the website of the Dutch association of paedophiles.[45] The judge stated that precautionary measures should be in place to prevent people who do not know the limits of the freedom of speech[46] from using the website to post material that infringes upon the rights of others. We would call this a special obligation to monitor. In a sense it is a general obligation, but the reason to call it a special one is that the reason the monitoring has to take place is because of the special nature of the website. The owner of the website was not exempted from liability because he actively selected the persons that could post on the forum. In general, an active moderator is a problem for applying exemptions.

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

Dutch case law is based on open norms. Almost all cases are about either copyright or other civil liability. **There is no strict legal criterion based on which the judge can decide whether or not an ISP should block, filter or take-down certain Internet content**. The central norm is our general tort Article 6:162 DCC. The ISP has to **balance interests**. In the event of a request to take down (almost all cases are about take-down requests) the claimant has to make clear why the ISP should take down the material in question.

Does the Dutch law meet the criteria developed under art. 10(2) ECHR? Authorities do not play a role, the ISP receives the request from either a company or a private person. As said, there is hardly any case law on blocking and filtering, almost all case law is on take-down of material. From a freedom of speech perspective, this is far less infringing. The set of criteria taken over in 2012 by the Dutch Supreme Court as were defined by the Court of Appeal of Amsterdam are meeting the requirements of exemptions on freedom of speech.[47] In a 2011 case about medical failures that were reported on a special website, the Court of Appeal Arnhem also used these criteria. The following rules of thumb determine whether the freedom of speech should outweigh, given all relevant circumstances of the case:

1. the nature of the suspicions;
2. the severity of the anticipated effects for those who are related to those suspicions;
3. the severity of the abuses that are communicated;
4. the degree to which the statements were rooted in the facts available at the moment of the communication;

---

42 Directive 2006/24/EC on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC OJ L 105/54 (Data Retention Directive).

43 Digital rights Ireland and Seitlinger and others judgement of 8 April 2014. Joined cases C-293/12 and C-594/12 I-18.

44 Court The Hague 11 March 2015, ECLI:NL:RBDHA:2015:2498.

45 Court of Amsterdam 1 November 2007 (Stichting Martijn), ECLI:NL:RBAMS:2007:BB6926.

46 As Article 10(2) European Convention of Human rights states “The exercise of these freedoms, since it carries with it duties and responsibilities (…)”.

47 Supreme Court 2 November 2012, ECLI:NL:PHR:2012:BX8122. Court of Appeal Amsterdam 5 July 2011, ECLI:NL:GHAMS:2011:BR0246; Court of Appeal Arnhem 18 April 2012, ECLI:NL:GHARN:2012:BX9224 confirmed in Supreme Court 20 December 2013, ECLI:NL:HR:2013:2072.

5. the framing of the suspicions;
6. the nature of the medium used for communication; and
7. the position of the one who the communications concerns.

What should also be mentioned is the fact that in the Netherlands judges are not allowed to evaluate the law in the light of the Constitution. The rationale behind this prohibition is that the legislator is assumed to have taken into account the Constitution and the fundamental rights that are part of it when issuing the legislation. Nevertheless, judges evaluate cases in the light of fundamental rights such as, e.g. privacy and freedom of speech. The Dutch judge then refers to the European Convention of Human Rights, and recently also to the EU Charter of fundamental rights, instead of the Constitution of the Netherlands.

How the judge uses the ECHR case law is illustrated by the following cases. First, a case before the District Court of Rotterdam, where the limits of the freedom of speech of Article 10 ECHR were applied.[48] The ISP had not taken down discriminatory content. The judge referred to the well-known phrase that freedom of speech also protects communication that is meant to "offend, shock or disturb". In this Jews were insulted, and the judge indicated that what had been said in no way contributed to discussion in society (often used as an argument in US cases), so that there was no "pressing social need" whatsoever to keep the insulting statements online.

A December 2014 case[49] about a website with content that was damaging for the government and civil servants concerned also analysed the borders of the freedom of expression:

> "The right to freedom of expression, after all, does not extend as far as to allow that individuals can be accused publicly, without valid grounds but in a way as if there was no doubt about the truth of the statements, let alone with especially strong value judgments as [plaintiff] has given in the texts."

In most cases related to freedom of speech Article 10 ECHR is used, in particular the criterion, "necessary in a democratic society". On May 29th, 2015 the Advocate-General at the Supreme Court advised in the discussed BREIN Pirate Bay. He balanced the interest of the copyright infringement against the freedom of information of the ECHR:

> The infringement of the freedom of information of Ziggo's subscribers cannot be regarded as necessary in a democratic society to protect the rights of others (cf. Art. 10(2) ECHR) and this would impermissibly undermine the goal of the Copyright Directive to promote the information society. It is of importance that a mere conduit provider such as Ziggo provides the internet access service to its subscribers.

In all the areas discussed in this chapter the balancing of the rights are in case law addressed with reference to Article 10 ECHR. For instance, the 2010 case about the website Geenstijl posting footage of a drunken student:[50]

> GeenStijl has the right "to shock, offend and disturb", but it has its limits. Those limits have been exceeded here. Besides the degrading and humiliating nature of the film, there was no compelling reason of public interest to putting the video (and the accompanying texts) online placing absence."

A 2012 case dealt with negative publicity about attorneys:[51]

---

48 District Court of Rotterdam 2 February 2009, ECLI:NL:RBROT:2009:BI1786.

49 Rechtbank Midden-Nederland 17 December 2014, ECLI:NL:RBMNE:2014:6596.

50 District Court of Amsterdam 14 July 2010, ECLI:NL:RBAMS:2010:BN4359.

51 District Court of Haarlem 2 August 2012, ECLI:NL:RBHAA:2012:BX9028.

> The restriction is lawful if it is provided by law and necessary in a democratic society, such as the protection of rights of others. A restriction is provided by law when statements on a website are unlawful within the meaning of Article 6: 162 BW. In the opinion of the judge this is the case in casu. The statements and the qualifications as "intimidating, cunning, self-interest prevails, unreliable liar, greedy, fantasist" are of a highly negative and defamatory nature. Moreover, given the domain name "badlawyers", it is likely that the website is intended to publish negative criticism of lawyers.

Finally, in conclusion, it is worth mentioning a 2015 case about the broadcasting organization AVROTROS that had put on their website allegations including personal details about suspects of fraud:[52]

The above implies that [plaintiff] has been exposed by AVROTROS to accusations and bad publicity about his person. The importance of [plaintiff] that bad publicity stops outweighs AVROTROS' right to freedom of expression.

A.R. Lodder & K.E. Sandvliet
Dep. Transnational Legal Studies, Center for Law & Internet
Vrije Universiteit Amsterdam
23.08.2015

[52] District Court of Amsterdam 5 February 2015, ECLI:NL:RBAMS:2015:740