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 425-444

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.

LUXEMBOURG

1. Sources

Luxembourg has no specific legislation on the blocking, filtering and removal of unlawful Internet content. However, these problems can be dealt with through the application of the ordinary civil and criminal law.[1]

First and foremost, it must be stressed that Luxembourg has a body of legislation that enables it to assess the lawfulness of Internet content.

In connection with computer-related offences, the Criminal Code was amended in 1993[2] to criminalise attacks on computer systems. Although it signed the Budapest Convention in 2003, Luxembourg ratified it only in 2014 in an Act of 18 July.[3] The Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, opened for signature in Strasbourg on 18 January 2003, was ratified at the same time.[4] The 2014 Act was intended to fine-tune the domestic legislation in this area.[5] Regarding the dissemination of unlawful content, the development and use of malicious software of all kinds, such as viruses, phishing sites and malware, are prohibited under Article 509-4 of the Criminal Code.

The Criminal Code also establishes offences in connection with child pornography (in particular, Articles 383 and 384), violent content or content that is likely to pose a serious threat to human dignity (Article 383), or incite hatred (Articles 454 et seq.) or terrorism.[6] In connection with the latter, Luxembourg has ratified the Council of Europe Convention on the Prevention of Terrorism of 15 May 2005,[7] and the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, opened for signature in Lanzarote on 25-26 October 2007.[8]

---

1 All the legislation referred to in this note can be consulted on the Internet site: www.legilux.lu; consolidated legislation may be found under the heading Mémorial A, Textes coordonnés.

2 Act of 15 July 1993 to strengthen measures to combat financial and computer crime.

3 Act of 18 July 2014 to 1) approve the Council of Europe Convention on Cybercrime, opened for signature in Budapest on 23 November 2001, 2) approve the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, opened for signature in Strasbourg on 28 January 2003, 3) amend the Criminal Code, 4) amend the Criminal Investigation Code, 5) amend the amended Act of 30 May 2005 on the protection of privacy in the electronic communications sector.

4 Since the protocol's provisions were already covered by legislation in force, no further changes to the law were necessary.

5 Braun M., *La ratification de la Convention de Budapest sur la cybercriminalité par le Luxembourg*, Journal des Tribunaux Luxembourg (JTL), Larcier, No. 35, pp. 121 et seq.

6 n accordance with the conditions laid down in Articles 135-1 et seq. of the Criminal Code (legislation on terrorism).

7 Act of 26 December 2012 to approve the Council of Europe Convention on the Prevention of Terrorism, signed in Warsaw on 16 May 2005, and to amend the Criminal Code, the Criminal Investigation Code, the amended Act of 31 January 1948 on the regulation of air traffic, the amended Act of 11 April 1985 to approve the Convention on the Physical Protection of Nuclear Material, opened for signature in Vienna and New York on 3 March 1980, and the amended Act of 14 April 1992 to establish a maritime disciplinary and criminal code.

8 Act of 16 July 2011: 1. to approve a) the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, opened for signature in Lanzarote on 25-26 October 2007, and b) the Optional Protocol to the United Nations Convention on the Rights of the Child on the

Intellectual property and personal data also enjoy legal protection.[9]

As a member of the European Union, Luxembourg applies the Community regulations, directives and framework decisions, including 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 (the E-Commerce Directive), Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, and Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, as well as the various directives on data protection.[10]

From the procedural standpoint, we would refer to:

- the Criminal Investigation Code (hereafter the CIC),
- the new Code of Civil Procedure (hereafter the NCCP),
- the Act of 18 April 2001 on copyright, related rights and data bases (hereafter the Copyright Act), and more specifically Sections 76 et seq. on prohibitory injunctions against breaches of copyright,
- the Act of 2 August 2002 on protection of the public in connection with personal data processing (hereafter the Data Protection Act).

Since civil relationships are based on freedom of contract (Article 1134 of the Civil Code),[11] the parties to an agreement may define the content that they consider to be lawful in connection with performance of their obligations. However, this freedom may not be exercised in breach of fundamental rights, which include freedom of expression and of enterprise.

2. Applicable regulations

Since blocking, filtering and removal of unlawful content are not covered by specific provisions, we will consider these concepts from the standpoint of ordinary Luxembourg law.

It should be noted first that there is no central body or authority responsible for drawing up “black lists” of sites that need to be blocked. Nor is there any body to determine the filters that Internet service providers and web hosts are required to apply.

Content is monitored on a case-by-case basis. A distinction is made between orders to make content temporarily unavailable and those that, following a detailed examination of the case, require its permanent removal. The former are defined as “blocking” and the latter as “removal”. The term “filtering” does not reflect current national procedures, so we will confine consideration of this process to the sub-sections on copyright (2.2.2.1) and the urgent procedure (2.1.3).

---

sale of children, child prostitution and child pornography; 2. to amend certain articles of the Criminal Code and the Criminal Investigation Code.

9 Luxembourg also approved the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, signed in Strasbourg on 28 January 1981, in the Act of 19 November 1987.

10 For a summary of directives transposed into Luxembourg law see the National Data Protection Commission’s site: http://www.cnpd.public.lu/en/legislation/droit-europ/index.html.

11 “*Agreements legally entered into operate as law for those who have concluded them. They may be revoked only by mutual consent, or for reasons specified in law. They must be performed in good faith*”.

The application of blocking and removal measures is subject to the distinction made between content publishers, in the strict sense of the term, and intermediary service providers.[12] The latter include "mere conduit" and "hosting" service providers.[13] When it transposed the E-Commerce Directive into Luxembourg law,[14] parliament incorporated the specific liability systems laid down for intermediary service providers in the Directive.

Mere conduit services consist in the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network. More specifically, they concern Internet access providers. Such service providers are not liable for the information transmitted, on condition that they do not initiate the transmission, select the recipient of the transmission or modify the information transmitted (Section 60 of the E-Commerce Act).

Web hosting consists of the provision of an information society service involving the storage of information provided by a recipient of the service (Section 62).

Under the legislation, hosting service providers shall not be liable for the information stored, on condition that:

- they do not have actual knowledge of unlawful activity or information and, as regards claims for damages, are not aware of facts or circumstances from which the unlawful activity or information is apparent; or
- upon obtaining such knowledge or awareness, they act expeditiously to remove or to disable access to the information.

However, these provisions do not apply when the recipient of the service is acting under the authority or the control of the provider.

Publishers are, firstly, any individuals or legal persons who, as their principal or regular activity, design and develop a publication, carry out editorial control, decide to make it available to the general public or a section of the public using a particular medium, and order that it be reproduced or circulated for that purpose (Section 3.3 of the Freedom of Expression in the Media Act of 8 June 2004). In order to distinguish publishers from web hosts – whose role is essentially a technical one – the definition in the Freedom of Expression in the Media Act has to be extended to any person who publishes information on the Web, and therefore also those who publish content privately or sporadically.[15]

The publisher is therefore the one who appoints the person that chooses to disseminate the content to the public.[16] Subject to the requirements of freedom of expression and of the press, publishers are liable for published content.

---

12 Defined in Article 2 of the E-Commerce Directive as "*any natural or legal person providing an information society service*".

13 Section 61 of the E-Commerce Act specifies a third category of intermediary service – so-called *caching* – which will not be considered in this paper. As far as we are aware, this type of service has never come to the attention of the Luxembourg courts.

14 In the E-Commerce Act.

15 The distinction between "publishers", who come within the scope of the Freedom of Expression in the Media Act, and the other persons concerned is particularly important from the standpoint of determining the applicability of the reduced limitation period of three months from the first time that the contested content is made available to the public (see, in particular, Luxembourg district court (TA Lux.) 22.05.2008, No. 1693/2008).

16 For a detailed analysis of this issue, see Monteiro E., "Les responsabilités liées au web 2.0" in *Revue du droit des technologies de l'information (RDTI)* – No. 32/2008, pp. 363 ff.

The distinction between publishers and web hosts is crucial for determining the liability of the person concerned. The Court of Justice of the European Union (hereafter the CJEU)[17] has clarified these conception in a number of judgments,[18] and we would also draw attention to a judgment of the European Court of Human Rights (hereafter the ECHR) of 16 June 2015, *Delfi AS v. Estonia*, which ruled on the liability of an Internet news portal for comments posted on it by third parties.[19]

Consideration of the case-law of the Luxembourg courts shows that the liability conditions established by the E-Commerce directive have had a practical influence on the proceedings brought by applicants. Broadly speaking, it can be seen that:

- web hosts are called on to ensure that content found to be unlawful is made inaccessible: the procedures selected are those that enable courts to reach a rapid decision,
- publishers' civil and criminal liability are determined in proceedings on the merits of the case – if necessary such proceedings are preceded by criminal law seizures or urgent proceedings.

Insofar as we have not found any judgments ordering measures concerning Internet access providers, we will confine ourselves in the remainder of this paper to the situation regarding web hosts.

2.1. Blocking and/or filtering of unlawful Internet content

Web hosts' obligation to remove unlawful content expeditiously from their systems, to avoid any liability, means that they have to deal with requests for blocking formulated by interested third parties. In certain cases, web hosts decide themselves to remove content stored on their systems (2.1.1).

Blocking may also be ordered in the course of criminal (2.1.2) or civil (2.1.3) proceedings.

2.1.1. Blocking on the host's initiative

The limits placed on web hosts' liability by Section 62 of the E-Commerce Act are accompanied by the requirement that once these service providers become aware of the unlawful content stored in their systems they must act promptly to remove it or make it inaccessible.

The Act creates a substantial problem for web hosts, namely that of deciding what content should be deemed unlawful. What makes the matter still more complex is the fact that the Internet is accessible throughout the world and that the same content may be perfectly legal in one country and prohibited in another.

Broadly speaking, hosts block content that is manifestly unlawful in the countries of the European Union. This includes, in particular, child pornography and open incitements to hatred (particularly racial hatred)[20] or to the commission of terrorist acts.

---

17 For an assessment of the Court's case-law concerning the Internet, see Jääskinen N., *Internet et la Cour de justice*, in Liber Amicorum Vassilios Skouris, Bruylant 2015, pp. 253 ff.

18 See, in particular, CJEU, judgments of 23.03.2010, Google France and Google, nos C-236/08 to C-238/08; CJEU 12.07.2011, L'Oréal v. Ebay, No. C-324/09; CJEU 16.02.2012, Sabam v. Netlog, No. C-360/10; CJEU 11.09.014, Sotiris Papasavvas v. O Fileleftheros Dimosia Etaireia Ltd, ea., No. C-291/13.

19 ECHR 16.06.2015, Delfi AS v. Estonia, No. 64569/09; for an assessment of this judgment see Spielmann D., Internet: libertés et restrictions (available in French only) on http://www.echr.coe.int/Documents/Speech_20150626_Observatoire.pdf (accessed on 17 August 2015).

20 For a practical example, see TA Lux. 12.11.2014, No. 3019/2014.

To ensure greater legal certainty, numerous web hosts define unlawful content in their general terms and conditions. Establishing such a legal framework in their private law contracts enables them to block artistic works that are placed on line in breach of copyright or the dissemination of malware through their computer systems.

Web hosts may become aware of unlawful content by means of spot checks or following complaints from concerned persons. Reference is made here to the BEE SECURE Stopline service,[21] to which anyone can report content relating to child pornography, racism, revisionism, other forms of discrimination and terrorism. As part of the system for managing the reporting of unlawful content, BEE SECURE Stopline has a co-operation agreement with the police[22] under which it acts as a specialist body for receiving and analysing information which it then transmits to the relevant police authorities.[23] The final decision on the legality or illegality of a content signalled to the BEE SECURE Stopline and the decision to inform the host located in Luxembourg belongs to law enforcement, namely the Grand-Ducal Police and the prosecutor's office. Generally the BEE SECURE Stopline will not contact the host for the removal of illegal content unless requested by the Grand-Ducal Police.

When content is blocked as a result of co-operation between the police and the private sector, this is generally carried out on the basis of the host's general terms of contract, which expressly authorise the latter to remove unlawful content from its systems. When it is not clear whether the content is unlawful, the web host must rely on the courts to rule on the matter.[24] If necessary, the state prosecutor may order content to be blocked under Articles 33.5 and 66.3 of the CIC (see sub-section 2.1.2).

Article 62 of the E-Commerce Act requires hosts to remove the information or make it totally inaccessible. This provision also authorises web hosts to permanently erase the files in question. In practice, they erase the information in their systems that can be accessed by the public, but retain a back-up copy. They then block the relevant data.

In the case of child pornography content hosted in another country, the operational procedures of the BEE SECURE Stopline envisage to inform the Grand-Ducal Police and share the identified links with the relevant partner hotline, a member of the INHOPE (International Association of Internet hotlines). Note in this context that INHOPE banishes the term "child pornography" and prefers the terminology of " Child sexual abuse material " (or "content related to sexual violence against children").
The goal of the work of the BEE SECURE Stopline and members of the INHOPE network is to withdraw the prohibited content as fast as possible from the web, in order to avoid re-victimization of children and adolescents represented in the pictures or videos (Notice and Takedown).

2.1.2. Criminal law measures

The CIC contains no specific provisions on blocking, filtering or removal of unlawful content. However, these measures may be ordered under the general law on the seizure of assets which "*were used to commit the crime or were intended to commit it, and those which constituted the object of the crime*" (see Article 31 of the CIC).

---

21 https://stopline.bee-secure.lu

22 Namely the Youth Protection Section, the New Technologies Section and the Anti-Terrorist Unit.

23 https://stopline.bee-secure.lu/index.php?id=8.

24 Particularly under the urgent procedure, which is considered in sub-section 2.1.3.

Criminal law seizures are possible for all indictable offences. In particular, these include terrorism (Articles 135-1 et seq. of the Criminal Code), child pornography (see in particular Articles 383 and 384), and grooming (Article 385-2),[25] as well as incitement to hatred against various groups of persons (Articles 454 et seq. of the Criminal Code) or threats to cause bodily harm (Articles 327 et seq.).

With regard to privacy, Section 1 of the Protection of Privacy Act of 11 August 1982 establishes the principle that "*the courts may, without prejudice to a right to compensation for the damage sustained, order any measures, such as seizure, attachment and others, capable of preventing or causing to cease an interference with a person's privacy; in the event of urgency such measures may be ordered in urgent proceedings*". The infringements of privacy covered by the legislation, including in particular unauthorised audio and video recordings (Sections 2 to 4), montages using a person's words or images without his or her consent (Section 5) or unwanted harassment (Section 6), constitute lesser indictable offences.

Under Section 82 of the Copyright Act, copyright infringements are liable to criminal penalties.

The same applies to certain offences relating to data protection.[26] Indeed, just in the Data Protection Act, of a total of 45 articles, no less than 19 provide criminal sanctions for violations of these provisions.

If criminal law seizures are viewed in the traditional way, that is placing property or assets under the administration of the justice system,[27] unlawful content can be blocked by seizing the computer equipment on which it is stored. By removing this part of the data centre's equipment and disconnecting it from the Internet, all the content and services that it hosts become inaccessible.
There are two main drawbacks to this pragmatic approach:

- the data in question may be stored on a server that also holds the data of persons other than the one concerned by the judicial inquiries or investigation. This is particularly the case with shared web hosting services, where one server hosts the Internet sites of a multitude of clients. The seizure then affects not only the subject of the inquiry or investigation but also the web host and all the other persons whose sites are hosted by the server in question;[28]
- seizure of computer equipment results in a total blockage of all the content stored on it. As it is not a targeted measure, perfectly lawful content placed on line by the subject of the inquiry or investigation is also blocked.

The physical seizure of computer equipment may also be an answer to the exchange of child pornography material through peer-to-peer connections initiated by individuals.[29]

---

25 For the way these child-related provisions, introduced into Luxembourg law by the Act of 16 July 2011, have been applied in practice, see TA Lux. 19.03.2015, No. 914/2015; TA Lux. 30.04.2015, No. 1311/2015; and TA Lux. 28.05.2015, No. 1571/2015.

26 Offences specified in the Data Protection Act and in the Act of 30 May 2005 establishing specific provisions to protect persons with regard to the processing of personal data in the electronic communication sector and amending Articles 88-2 and 88-4 of the Criminal Investigation Code.

27 In French "*mettre un bien sous main de Justice" – see* Cornu G., *Vocabulaire juridique*, Presses Universitaires de France (PUF), 4th edition, 2003.

28 See also, on this subject, Losdyck B., *Les saisies et perquisitions de matériel informatique: les "garde-fous" entourant leur mise en œuvre*, RDTI No. 52, 3/2013, p. 36.

29 See in particular TA Lux. 23.03.2011, No. 1059/2011; TA Lux. 07.10.2008, No. 2822/2008; TA Lux. 24.06.2008, No. 2126/2008; TA Lux. 06.11.2008, No. 3150/2008.

The aforementioned Act of 18 July 2014[30] deals more specifically with the seizure of "*data stored, processed or transmitted in an automated data processing or transmission system"*.[31] Sections 31, 33 (indictable offences discovered during or immediately after their commission) and 66 (seizures ordered by an investigating judge) now provide expressly for the seizure of computer data "*either by the seizure of the physical carrier of the data, or by a copy of the data*" (Sections 33.5 and 66.3).[32]

In the first place, evidence of the allegedly unlawful content is gathered by the seizure of data.

Sections 33.5 and 66.3 of the CIC then authorise the deletion, and therefore the blocking, of these data on their physical carrier, on condition that:

- a prior copy of the data has been made,
- the data's physical carrier has not been seized,[33]
- the deletion has been ordered by an investigating judge, or by the state prosecutor in the case of offences discovered during or immediately after their commission,
- the holding or use of the data is unlawful or poses a threat to persons or property,
- the physical carrier (for example, the computer or server) carrying the data is located in the Grand Duchy of Luxembourg.

As well as satisfying evidential requirements, the condition that a prior copy of the deleted data be made means that the latter can be reconstituted if the decision to delete is set aside by a judge in chambers[34] or by a trial court, or in the event of a discharge or acquittal.[35] As explained in the parliamentary documents, "*the decision to delete data cannot be treated as an anticipated penalty of forfeiture. The purpose is to protect persons or property against further offences (particularly in the case of malware) or to avoid the dissemination of unlawful material, such as child pornography. In the event of an acquittal or a decision to discontinue proceedings, the seized data (their copy) can be restored. In the event of a prosecution, however, the data will be confiscated"*.[36]

It is clear from the parliamentary documents that the intention of the legislation is to make unlawful or dangerous content inaccessible, pending a judicial decision on the merits. The deletion measure has the effect of blocking the content.

Content that can be blocked includes, in particular, "child pornography, malware or incitement to hatred, or terrorism".

---

30 Act of 18 July 2014 to 1) approve the Council of Europe Convention on Cybercrime, opened for signature in Budapest on 23 November 2001, 2) approve the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, opened for signature in Strasbourg on 28 January 2003, 3) amend the Criminal Code, 4) amend the Criminal Investigation Code, 5) amend the amended Act of 30 May 2005 on the protection of privacy in the electronic communications sector..

31 Since the Act of 15 July 1993 to strengthen measures to combat financial and computer crime, which incorporated computer-related offences into the Criminal Code, the relevant criminal legislation has used the term "automated data processing or transmission systems" to signify "computer systems" (the term used in the Budapest Convention).

32 For the seizure of data before this legislation was enacted see Court of Appeal (CA) 09.07.2013, No. 375/13; 16.11.2012, No. 752/12; CA 21.12.2011, No. 931/11.

33 Which necessarily entails a total blocking of all the data recorded on the server, thereby excluding any selective deletion of data.

34 For procedural matters, see sub-section 3.2.

35 This problem was raised by the *Conseil d'Etat* in its first opinion of 16.04.2013, Parliamentary documents (doc. parl.) 6514-2, p. 6, section 4.

36 Doc. parl. 6514-7, p. 12.

The measure is accompanied by significant safeguards, since it has to be ordered by the state prosecutor, in the case of offences discovered during or immediately after their commission, or by an investigating judge in other circumstances. These decisions may be the subject of an application to set aside and for the recovery of property.[37]

2.1.3. Civil law measures and urgent applications

Urgent applications are the subject of Part XV of the NCCP. In urgent cases, urgent applications judges can order any measure to which there is no serious objection[38] or that is justified by the existence of a dispute (urgent applications – Article 932). They may also order such interim measures as are necessary either to prevent imminent damage or to put an end to a manifestly unlawful infringement (urgent applications, infringement of rights – Article 933).

The advantage of the urgent applications procedure is that orders are issued rapidly. The judge may even agree to hear an application "*at the time specified, even on public holidays or non-working days, either in chambers or at his or her own home*" (Article 934.2).

However, in principle, urgent applications orders do not constitute *res judicata* (Article 938.1). Decisions of urgent applications judges are therefore purely provisional, pending consideration of the merits of the case.

To ensure that urgent applications judges' decisions are implemented, they may be accompanied by a coercive fine (*astreinte)*.[39] This may be defined as an order to pay a sum of money issued as an ancillary measure by the judge to exert pressure on the person liable to ensure that the latter implements the court's decision.[40] In principle, any court decision, other than sentences to pay a sum of money, may be accompanied by such a coercive fine.

One fundamental aspect of the urgent procedure (Article 938.3), is that the orders are enforceable immediately notwithstanding any appeal, though at the risk of the person implementing them.[41]

The speed with which such urgent orders can be issued makes this procedure particularly appropriate for content published online. It makes it possible not only to rapidly obtain a writ of execution against the publisher of unlawful content but also to oblige the web host to block the content. The order gives the latter the necessary legal assurance that it can remove the content in question from its systems.[42] Although we have been unable to identify any decisions on this point, we consider that a filtering measure could also be ordered against an Internet access provider under the urgent applications procedure.

---

37 See sub-section 3.2.1.

38 Once there is a serious objection concerning a question of fact or law, the urgent applications judge no longer has jurisdiction to hear the case. For a practical example of an alleged infringement of a person's reputation and honour, see TA Lux. 22.05.2012, No. 363/2012.

39 For a detailed assessment of this procedure, see Thewes M., *L'astreinte en droit luxembourgeois*, Annales du Droit luxembourgeois 1999, No. 9, pp. 119 et seq.

40 P. Van Ommeslaghe, *Les obligations – examen de jurisprudence (1974 – 1982)*, Revue critique de jurisprudence belge 1986, p. 198, No. 94, quoted in Thewes M., *L'astreinte en droit luxembourgeois*, op. cit., No. 9, p. 119.

41 Established case-law, see in particular CA 16.04.1915, Pasicrisie 10, p. 510.

42 For an assessment of this issue, see Prum A., *Le commerce électronique en droit luxembourgeois*, Larcier 2005, p. 562, No. 680.

The urgent procedure can be lodged by persons who consider themselves to have suffered infringements of their privacy[43] or harm to their reputation. We can also cite a case in which a divorced father had posted photographs of his under-age daughter online, without the mother's agreement. When the judge was asked to rule on the matter, the father had already removed the photos from the social networks. The urgent applications judge nevertheless prohibited the father, subject to a penalty in the event of non-compliance, from posting in future any photos of the child in question on the Internet.[44]

2.2. Retrait de contenu illégal d'internet

In this section, we will consider the removal measures ordered by courts ruling on the merits of disputes. This includes criminal (2.2.1) and civil (2.2.2) proceedings, with particular reference to the specific procedures that can be used for data protection (2.2.3).

2.2.1. Removal ordered by the criminal courts

There are no specific provisions in Luxembourg legislation on the removal of online content. As described in sub-section 2.1.2, the situation can be summarised as follows: the state prosecutor or the investigating judge orders the seizure of the contested data in the form of a digital copy and their deletion on the original hardware. The content is therefore blocked. Following preliminary inquiries or the judicial investigation, the case comes before the criminal courts.
In the event of a conviction for an indictable offence, these courts order the forfeiture of the unlawful content. The intangible asset in question constitutes the direct object of the offence committed. Deletion of the content is therefore justified by the judgment against the person concerned.[45]

We would also refer to a judgment ordering the judicial closure of an Internet site.[46]

In child pornography cases, the courts naturally confiscate the unlawful material.[47] In doing so, they remove it not only from the convicted person but also from the distribution channels he or she has used.[48]

A practical problem may arise when convicted persons operate Internet sites abroad. It may then be difficult to enforce the judicial decision, particularly as domestic legislation does not currently provide for a coercive penalty in criminal matters.[49] One approach might be to hand down a suspended sentence with probation (Articles 629 et seq. of the CIC), subject to the obligation to remove the contested content within a certain period.

2.2.2. Removal ordered by the civil courts

---

43 See in particular CA 10.07.2013, No. 39634.

44 TA Lux. 29.07.2014, No. 463/2014.

45 Doc. parl. 6514-7, p. 12.

46 CA 14.02.2012, No. 101/12 V.

47 See in particular TA Lux. 05.03.2014, No. 715/2014; TA Lux. 07.11.2013, No. 2921/2013; TA Lux. 09.10.2013, No. 2574/2013.

48 For peer-to-peer exchanges, see TA Lux. 23.03.2011, No. 1059/2011; TA Lux. 07.10.2008, No. 2822/2008; TA Lux. 24.06.2008, No. 2126/2008; TA Lux. 06.11.2008, No. 3150/2008.

49 However, the criminal courts may attach such a penalty to the civil dimension of their judgments; see CA 14.12.1970, Pasicrisie 21, p. 434.

In this sub-section we will consider traditional civil law proceedings (2.2.2.2), with a more detailed examination of requests for an injunction to be served in connection with copyright infringements (2.2.2.1).

2.2.2.1. Actions for injunctions for breach of copyright

Sections 76 et seq. of the Copyright Act provide for actions for injunctions[50] against any breaches of copyright, a related right or a *sui generis* database right. Such actions are defined by parliament as rapid substantive actions, lodged and heard in accordance with the urgent procedure, that enable those concerned to request the cessation of any violations of copyright or related rights. The civil courts have jurisdiction to order compensation to be paid to one or more rights holders whose rights have been violated.[51] It should be noted that this action is a substantive one, but in which the court rules "in accordance with the urgent procedure".[52] Unlike the urgent procedures provided for in articles 932 et seq. of the NCCP, the immediate enforceability of the decision is optional.

Injunctions handed down may be accompanied by a coercive penalty.

Any interested party, including collective management organisations, can apply to the courts to order the cessation of a breach of copyright. Such actions may be brought against any persons, since the law does not limit the range of potential defendants to the direct and principal authors of breaches.

Under Section 76 of the Copyright Act, which in this respect replicates Article 8.3 of Directive 2001/29/EC of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, the court applied to may also issue an injunction against intermediaries whose services are used by a third party to infringe a copyright.

Applications for injunctions against intermediaries are not subject to any prior formalities and can be lodged in the absence of any previous action against the perpetrator of the copyright breach.[53]

Still in accordance with the case-law of the CJEU,[54] the domestic courts have applied the status of intermediary to intermediary service providers, within the meaning of the E-Commerce Act, including Internet access providers and web hosts.

In two cases between a copyright collective management organisation and a web host,[55] the court ordered the cessation of the infringements identified on the Internet sites stored on the web hosts' computer facilities. The court did not attach any details to the injunctions, having noted that the Copyright Act did not authorise the court to order specific technical measures. It was the responsibility of the party that had been ordered to cease the copyright breaches to comply with the decision by taking all appropriate measures.

---

50 For more details on such actions see Putz J-L., *Le droit d'auteur*, Promoculture-Larcier 2013, pp. 281 et seq.

51 Doc. parl. No. 4431, Explanatory memorandum, *Renforcement des sanctions de la contrefaçon* .

52 CA 25.04.2012, No. 38033.

53 Putz J-L., *Le droit d'auteur*, op. cit., p. 304, No. 701a.

54 See the judgments CJEU 24.11.2011, Scarlet Extended, No. C-70/10 and CJEU 16.02.2012, Netlog NV, No. C-360/10.

55 See TA Lux. 11.05.2011, No. 349/2011 and TA Lux. 11.03.2014, No. 54/2014.

To ensure that its decision was enforced, the court ordered that the infringements identified cease within three working days of the notice of the decision, subject to a coercive penalty for non-compliance of €2,000 per violation, per day.[56]

We have been unable to identify any decisions to order an Internet access provider to filter or block content. In the light of the case-law of the CJEU,[57] however, we consider that such an action could be based on Sections 76 et seq. of the Copyright Act.

2.2.2.2. Procedures under ordinary law

The civil courts ruling on the merits of cases can of course hear applications for the removal of unlawful content. However, given the speed with which information is disseminated on the Internet, this procedure is not very appropriate.

It is essentially viewed as operating in parallel with the urgent applications procedure to offer a formal basis for the urgent applications judge's decision. Another potential situation is one in which a victim claims damages from the civil court and at the same time asks for the removal of the contested content.

Decisions taken on the merits of cases may also be accompanied by coercive penalties (Article 2059 of the Civil Code).

2.2.3. Data protection

Personal Data protection is governed by the Data Protection Act, and by the Act of 30 May 2005 establishing specific provisions to protect persons with respect to the processing of personal data in the electronic communication sector and amending Articles 88-2 and 88-4 of the Criminal Investigation Code.

These laws establish a strict regulatory and procedural framework governing all processing of personal data. Failure to comply with the obligations imposed on data controllers and data breaches are accompanied by penal and administrative sanctions[58].

We will consider actions for injunctions – which are comparable to those applicable to copyright protection – and then look at the administrative penalties that can be handed down by a public body, the National Data Protection Commission (hereafter the NDPC).[59]

2.2.3.1. Actions for injunctions

Actions for injunctions consist in applying to the courts for an order to cease acts in violation of the Data Protection Act.[60] One particular feature of the procedure introduced by Section 39 of the Act is that it can be used only by:

- state prosecutors who have initiated proceedings for violation of the Data Protection Act,

---

56 With regard to coercive penalties for non-compliance, see section 2.1.3.

57 CJEU 24.11.2011, Scarlet Extended, No. C-70/10.

58 See the table setting out the various offences concerned in Pierre-Beausse C., La protection des données personnelles, Promoculture 2005, p. 287.

59 For more information, see the NDPC's Internet site: www.CNPD.lu.

60 For more information on this procedure see Pierre-Beausse C., *La protection des données personnelles*, op. cit., p. 282 ff.

- the NDPC in cases where a disciplinary sanction handed down under Section 33 of the Act has not been complied with,
- injured parties, but only if they have previously submitted a request to the NDPC concerning the data controller's respect for their fundamental rights and freedoms or requesting a check on the lawfulness of the data processing, following the controller's decision not to grant them right of access or to limit that right.

The scope of such actions is limited in that it covers only the "controller", defined as "*the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by legal provisions, the controller shall be designated in accordance with specific criteria, laid down in law"* (Section 2 of the Act), and his or her "processor", defined as "*a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller*" (Section 2).

The actions for injunctions provided for in the Data Protection Act can therefore be brought only against persons who are deemed to be the "controllers" or "processors" of data processing held to be unlawful. In principle, these terms do not include web hosts or Internet access providers. Hosts – in the traditional sense of the term – simply store their clients' data. If they process data for their own purposes, they may then be designated as "controllers". In its Google Spain judgment, the CJEU states that "*the activity of a search engine consisting in finding information published or placed on the internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users according to a particular order of preference must be classified as "processing of personal data" within the meaning of Article 2(b) when that information contains personal data and, second, the operator of the search engine must be regarded as the "controller" in respect of that processing, within the meaning of Article 2(d)."*[61]

2.2.3.2. The administrative procedure before the National Data Protection Commission (NDPC)

The Data Protection Act grants the NDPC disciplinary powers that authorise it to "lock, delete or destroy" data that is being processed in breach of this Act or its implementing regulations (Section 33).[62]

Such powers can be exercised against a controller processing personal data unlawfully.

We have not identified any examples of the application of these provisions.

In case of violation of the security measures provisions, the NDPC can prescribe a warning or admonition (Articles 21 to24), and the temporary or permanent ban of the processing and where appropriate, the obligation to publish the prohibition decision. The NDPC also has the possibility to impose administrative fines not exceeding € 50,000 according to section 3 of the Act of 28 July 2011 on data protection in the electronic communications sector.

---

61 CJEU 13.05.2014, Google Spain v. Agencia Española de Protección de Datos (AEPD), No. C-131/12.

62 See also Pierre-Beausse C., *La protection des données personnelles*, op. cit., pp. 289 ff.

3. Procedural issues

Since there are no specific rules governing the blocking, filtering and removal of unlawful content, ordinary legal procedures apply. It is beyond the scope of this note to describe these in detail so we will confine ourselves to an outline of the main points.

3.1. Appeals against web hosts' blocking or removal decisions

As stated, web hosts are required to remove expeditiously from their systems unlawful content of which they are aware. As well as responding to court injunctions, hosts may also remove content on their own initiative. Their knowledge of such content may be the result of their own periodic checks or of notifications from interested third parties.

The publishers of blocked content may of course challenge the web host's decision.

In particular, they can make an urgent application for the disputed content to be reinstated online.[63]

3.2. Criminal law proceedings

A distinction should be drawn between proceedings during the preliminary – inquiry or judicial investigation – stages, when blocking is still not final, and hearings on the merits, in which permanent removal can be ordered.

3.2.1. Proceedings during inquiries or judicial investigations

As noted in sub-section 2.1.2, blocking measures may be ordered against web hosts that are not the publishers of the contested content or against the publisher himself or herself.

Other than in the case of offences discovered while they are being committed or immediately afterwards,[64] when police officers may carry out seizures, any seizure effected without the consent of the person concerned requires an order issued by an investigating judge. This may be issued in the course of a judicial investigation or after a mini-investigation, in accordance with Article 24-1 of the CIC. This latter procedure enables the state prosecutor to apply to the investigating judge to authorise a search, a seizure, the hearing of a witness or the ordering of an expert opinion, without the need to open a judicial investigation.

In practice, state prosecutors' or investigating judges' decisions are served and enforced by police officials.

Accused persons in inquiries or investigations and any interested third parties can challenge the lawfulness of decisions that adversely affect them and ask for them to be set aside. The CIC distinguishes between appeals to set aside decisions taken during inquiries (Article 48-2 of the CIC) and those applicable to decisions taken during judicial investigations (Article 126 of the CIC). We would also refer here to appeals against orders handed down by investigating judges under Article 24-1 of the CIC, which also specifies the relevant appeals procedure.

Appeals are lodged – through a simple application – to a judge in chambers of the district court for the area in question.

---

63 See in particular the discussion in sub-section 2.1.3.

64 Article 30.1 of the Criminal Code. Generally speaking, this applies to a period of up to 24 hours following commission of the offence.

As the concept of "any interested third party" is very broad, web hosts that have acted as intermediaries can also use this appeals procedure.

However, applications to set aside decisions must be lodged within very strict time limits:

- for decisions taken during inquiries, "any interested person" can ask for the decision to be set aside within two months of its execution, whether or not a preliminary investigation has been opened following the contested decision,
- also in the case of decisions taken during inquiries:
- if a preliminary investigation has been opened on the basis of the inquiry, accused persons have five days from the date they were charged to lodge an application,
- if no preliminary investigation has been opened, accused persons may lodge their application to set aside a decision with the trial court, before any request, pleading or objection, other than objections to jurisdiction.

The same rules apply to decisions taken on the basis of Article 24-1 of the CIC.

In the case of measures ordered by an investigating judge in the course of a judicial investigation, if it is not to be ruled out of time the application to set aside must be lodged with the same court that is conducting the investigation within five days of notification of the decision (Article 126 of the CIC).

Orders handed down by a judge in chambers may be appealed against to a judge in chambers of the Court of Appeal (Article 133 of the CIC).

Lastly, reference should be made to applications for restitution, which normally apply to cases of the seizure of computer equipment used to host contested content (Article 68 of the CIC).

3.2.2. Proceedings in trial courts

Contested content will probably have already been blocked during the inquiry or the investigation phases (see sub-section 2.1.2). If the blocking was effected by means of the seizure of the relevant computer equipment, this will be confiscated in the event of conviction and restored to its owner after an acquittal.

Based on the parliamentary documents on Sections 33.5 and 66.3,[65] it can be concluded that a conviction validates the deletion of the content. The copy of the deleted content of the original computer equipment is confiscated. In the event of an acquittal, this copy is restored to the accused.

All the decisions taken in criminal proceedings are subject to appeal (Articles 199 and 221 of the CIC). They can also be appealed against on points of law (Article 407 of the CIC).[66]

3.3. Civil law proceedings

In all the types of situation considered in section 2, we have assumed that applicants are taking action against the relevant content publisher and/or web host. For an application to be valid, the summons must be served through a bailiff. Depending on the procedure chosen, the summons must

---

65 Doc. parl. 6514-7, p. 12.

66 See also the Cassation Appeals and Procedure Act of 18 February 1885.

indicate either a date set for appearance in court or a date by which the defendant must have instructed counsel.[67]

If the defendant appears in court, the proceedings take place in the presence of both parties.

If blocking or removal is ordered by the court, the applicant must notify this decision to the defendant. Only when the decision has been notified is the defendant obliged to implement it and enforcement of the decision becomes possible.
It should be noted that all interim orders (see sub-section 2.1.3) are immediately enforceable, notwithstanding any appeal or application to set aside. In the case of all decisions handed down by trial courts for which immediate enforcement is not expressly provided, the applicant must await expiry of the time allotted for lodging an appeal before the decision becomes final.

All civil court rulings on applications to block or remove content are liable to appeal (see Articles 571 and 939 of the NCCP) and can also be appealed against on points of law to the Court of Cassation (Section 1 of the Cassation Appeals and Procedure Act of 18 February 1885).

3.4. Data protection proceedings

The actions for injunctions provided for in Section 38 of the Data Protection Act follow the same rules as those set out in sub-section 3.3.

The disciplinary sanctions imposed by the NDPC under Section 33 of the Act may be challenged by an appeal to the (lower tier) Administrative Tribunal.[68] If, in response to such an appeal, the Tribunal declares the decision unlawful, it will also take the place of the administrative authority to remedy the initial shortcomings of the decision. As such, it acts as a judicial authority while also substituting for the power of the administrative body whose decision it has supervised.[69]

Decisions handed down by the Administrative Tribunal may be appealed against to the Administrative Court (Section 8.2 of the Organisation of Administrative Justice Act of 7 November 1996).

4. General Internet monitoring

Section 63 (1) of the E-Commerce Act[70] reads:

> *"when providing the services covered by Sections 60-62, providers shall not be under a general obligation to monitor the information which they transmit or store, nor a general obligation to actively seek facts or circumstances indicating unlawful activity."*

In the light of this provision, Internet access providers and web hosts cannot be made subject to any general monitoring obligation.[71][72] However, the legislation does not affect their duty to co-operate

---

67 For a very detailed assessment of civil law procedures in Luxembourg law, see Hoscheit T., *Le droit judiciaire privé au Grand-Duché de Luxembourg*, Paul Bauler 2012.

68 As laid down in Section 3 of the Organisation of Administrative Justice Act of 7 November 1996.

69 Feyereisen M., Guillot J., Salvador S., *Procédure administrative contentieuse*, Promoculture 2006, p. 78, No. 86.

70 Based on the wording of Article 15.1 of the E-Commerce Directive.

71 Article 88-1 CIC lays down strict legal conditions governing special surveillance measures ordered by an investigating judge.

with the prosecution authorities. As noted in sub-section 2.1.1, the police authorities can report content that they judge to be unlawful to web hosts. We would point out in this context that the police "new technologies" section, like its counterparts responsible for anti-terrorism, analyses and investigates unlawful content that it itself identifies or that is reported to it.

The CJEU has ruled on the scope of Section 63 (1) of the E-Commerce Act, particularly with regard to blocking requests by the rights holders of works protected by copyright.

In an initial decision, L'Oréal v. Ebay, the Court held that:

> *"it follows from Article 15(1) of Directive 2000/31, in conjunction with Article 2(3) of Directive 2004/48, that the measures required of the online service provider concerned cannot consist in an active monitoring of all the data of each of its customers in order to prevent any future infringement of intellectual property rights via that provider's website. Furthermore, a general monitoring obligation would be incompatible with Article 3 of Directive 2004/48, which states that the measures referred to by the directive must be fair and proportionate and must not be excessively costly."*[73]

In its judgment no C‑360/10, Sabam v. Netlog,[74] the Court of Justice stated that a fair balance had to be struck between protection of the fundamental right of property, of which intellectual property rights form part, and that of other fundamental rights. In connection with measures adopted to protect rights holders, national authorities and courts therefore had to strike a fair balance between the protection of the intellectual property right enjoyed by copyright holders and that of the freedom to conduct a business enjoyed by operators such as hosting service providers.

The Court of Justice concluded that the provisions of the E-Commerce Directive, together with those of Directives 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, and 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, as well as the various data protection Directives:

> *"are to be interpreted as precluding a national court from issuing an injunction against a hosting service provider which requires it to install a system for filtering:*
> - *information which is stored on its servers by its service users;*
> - *which applies indiscriminately to all of those users;*
> - *as a preventive measure;*
> - *purely at its own expense; and*
> - *for an unlimited period,*
>
> *which is capable of identifying electronic files containing musical, cinematographic or audio-visual work in respect of which the applicant for the injunction claims to hold intellectual property rights, with a view to preventing those works from being made available to the public in breach of copyright ('the contested filtering system')."*[75]

The ruling of the Court of Justice has not yet been applied in practice in Luxembourg case-law.

---

72 See also Reisch T., *Internet et les nouvelles technologies de la communication face au droit luxembourgeois*, Mike Koedinger 2008, p. 75.

73 CJEU 12.07.2011, L'Oréal v. Ebay No. C-324/09, paragraph 139.

74 CJEU 16.02.2012, Sabam V. Netlog No. C-360/10.

75 Ibid., para. 26.

5. Assessment in the light of the case law of the European Court of Human Rights

Freedom of expression, as enshrined in Article 10 of the European Convention on Human Rights (hereafter "the HR Convention"),[76] is also protected by Article 24 of the Luxembourg Constitution,[77] and in the Freedom of Expression in the Media Act of 8 June. The domestic courts abide by the case-law of the ECHR[78] and interpret freedom of expression very broadly. In particular, this includes satire and caricature,[79] a more extensive right to criticise politicians[80] and freedom to express political opinions, even if these are likely to cause offence.[81]

As noted above, Luxembourg legislation does not lay down specific procedures for the blocking, filtering and removal of unlawful content. Such measures are taken in the course of civil or criminal proceedings based on the ordinary rules of law.[82] The problem lies in applying these legal rules (5.1) to actual situations, according to the principles of "pursuit of a legitimate aim" (5.2) and "necessary in a democratic society" (5.3), as laid down in Article 10.2 of the HR Convention.

5.1. The requirement for a legal basis

All the measures described in section 2 above are provided for in law. The procedural rules are laid down in the CIC, with regard to criminal law, and the NCCP, for the civil domain. The other, special, laws are grouped together in a compendium of special laws, which can be easily accessed on the www.legilux.lu Internet site. This site now offers the public access to all the codes, compendiums of legislation and acts of parliament, together with their preparatory works and implementing regulations.

Blocking, filtering and removal are not decided on by bodies specially created for that purpose, but are ordered by the courts.

In criminal cases, blocking – based on the seizure of unlawful content – forms part of an established legal tradition. Seizure of the proceeds of crime, or of the means used to commit it, is a legal principle that is firmly rooted in the legal system.

The same applies to the removal of content, which amounts to confiscation.

Civil law measures can be taken only by a court, ruling after *inter partes* proceedings. The fact of having to remove from Internet servers, either temporarily or permanently, content found to be unlawful may be construed as an obligation for the losing party to the proceedings to perform a specific act. We consider that this satisfies the requirement of foreseeability.

---

76 We refer also to Article 11 of the Charter of Fundamental Rights of the European Union.

77 Article 24 of the Constitution reads "*Freedom of speech in all matters and freedom of the press are guaranteed, subject to the prosecution of offences committed in the exercise of these freedoms. No censorship may ever be introduced.*"

78 For an assessment of the European Court decisions concerning Luxembourg courts' application of Article 10, see Hirsch C., *Le Luxembourg et la Cour Européenne des Droits de l'Homme*, Larcier 2015, p. 325 et seq.

79 CA 21.06.2011, No. 325/11 V.

80 See in particular CA 24.05.2011, No. 274/11 V.

81 See in particular CA 09.03.2011, No. 126/11 X.

82 Note, however, that there is an administrative procedure before the NDPC for blocking and removal linked to the protection of personal data – see sub-section 2.2.3.2.

Another important factor is that all the decisions taken by the judicial authorities in this area are subject to appeal.

In criminal proceedings, judges in chambers monitor compliance of decisions with both domestic law and the HR Convention.[83] Alleged violations of freedom of expression or the proportionality principle may therefore be relied on in support of applications to set aside decisions, once they have been taken.

Urgent proceedings make it possible to secure a rapid judicial decision in all civil law disputes.

5.2. Pursuit of a legitimate aim

Article 10.2 of the HR Convention stipulates that freedom of expression may not be subject to restrictions other than ones that "*necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.*"

The authorities, and in particular state prosecutors and investigating judges, are responsible for ensuring that their activities are strictly in compliance with the provisions of this Article.[84] In practice, blocking measures are applied to the most serious offences:

- child pornography,
- incitement to racial hatred,[85]
- dissemination of malware,
- publication of personal data extracted from a computer system through a cyber attack,
- manifest violations of privacy.

The issue becomes more sensitive in the case of defamation, calumny and insults. The offence of calumny does not apply if the author can prove the truth of the statements made. Under the Freedom of the Press Act this is even more the case with publishers, who are not guilty of defamation or calumny if, provided that they have taken the requisite legal steps, they can show that they had sufficient reason to conclude that the accusations reported were accurate and that there was an overriding public interest in disseminating the information in question (Article 443 of the Criminal Code).

The absence of any manifest violations of the rights of others undermines the legal basis for any blocking measures. Such measures may also fail to satisfy the proportionality test, considered in sub-section 5.3.

We consider that, without the authorisation of a court, web hosts can take blocking and removal measures under Section 62 of the E-Commerce Act only if the content is manifestly unlawful.[86] This of course applies to content relating to child pornography or terrorism, that is contrary to human

---

83 See in particular CA 22.10.2012, No. 674/12; CA 21.01.2014, No. 44/14; CA 28.01.2014, No. 69/14.

84 For a strict application of this provision, see Administrative Court 11.12.2012, No. 31148C, JTL No. 28, p. 107, with the comments of T. Chevrier.

85 See in particular TA Lux. 10.05.2012, No. 1754/2012.

86 An issue discussed in Prum A., *Le commerce électronique en droit luxembourgeois*, op. cit., p. 560 et seq.

dignity or that incites to hatred. We also consider that technical aspects such as destroying viruses or malware disseminated by a web host's servers constitute legitimate aims.

The issue becomes more complex in the case of breach of copyright, where the locus standi of the person requesting its elimination may cause problems, or in the case of defamation of character. Regarding the latter point, the relevant legislation varies greatly from country to country, making it difficult for web hosts to determine whether or not content is lawful. They may also be faced with problems regarding the classification of the content (see the aforementioned example of defamation or calumny).

We therefore consider that those concerned must exercise a certain restraint at the blocking measures stage.[87]

The situation is different in the case of removal measures, which are ordered by trial courts. These measures result from a final conviction or conduct that is censurable in civil law.

5.3. The need for such measures in a democratic society

The Internet is not a virtual world but a means of communication. The rules that should apply are therefore the same as those that govern physical relations between persons. Certain types of content – such as child pornography – are unacceptable. They have to be blocked and removed.

Nor can information networks become areas outside the law where, under the cover of anonymity, anyone can infringe the rights of others. It must be possible to impose restrictions on abuses of freedom of expression on the Internet.

Given the scale of on-line communications, blocking and removing unlawful content are necessary measures that are regulated by legislation. Their use is subject to judicial review and all those concerned have substantial remedies at their disposal (see, in particular, sections 2 and 3).

The proportionality principle, which serves as a corrective to the application of rules of law, also makes it possible to ensure that the measures ordered are consistent with other legal rules.

First, the application of this principle may reveal that ordering the blocking or removal of content to deal with a particular offence is disproportionate, in the light of other fundamental rights. Second, the proportionality principle means that the planned measure has to be confined to what is strictly necessary.

Before the amendments to the legislation of 18 July 2014,[88] there were no specific provisions on the seizure and deletion of computer data. In order to block content, the authorities physically seized the computer equipment hosting the contested data. This measure could pose problems from the standpoint of proportionality, whenever it also affected perfectly lawful content.

Following the 2014 reform, domestic legislation now authorises the seizure of computer data in the form of a copy of the data, coupled with the deletion of data found to be unlawful on their original physical carrier. This makes it possible to target the data to be blocked and removed.

---

87 Defined as interim measures, as described in section 2.

88 For the changes brought about by this reform, see sub-section 2.1.2.

The judge in chambers monitors compliance of blocking measures with the principles embodied in the HR Convention.[89] Violations of the proportionality principle can then be identified very quickly following implementation of the contested measure.

In the case of civil proceedings, the courts can specify in detail the content to be blocked. Compliance with the proportionality principle can be monitored at all stages of the proceedings.[90]

Max Braun

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

89 See in particular CA 16.05.2012, No. 301/12; CA 22.10.2012, No. 674/12.

90 For a practical example, see TA Lux. 11.05.2011, No. 349/2011 and TA Lux. 11.03.2014, No. 54/2014.