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 75-87

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.

BELGIUM

Belgium is one of the states which have legislation allowing the blocking or removal of certain illegal information on the Internet.

1. Sources

Belgium has ratified numerous international standards in the field of Internet governance. The Convention on Cybercrime, concluded in Budapest on 23 November 2001, came into force in Belgium on 1 December 2012 in accordance with the law of 3 August 2012 assenting to the Convention.[1] The Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, was signed by Belgium, but has still not been ratified. Belgium has also signed but not ratified the Council of Europe Convention on the Prevention of Terrorism. Finally, the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse came into force in the territory of Belgium on 1 July 2013, following various legislative acts giving assent to it according to the different federal and regional spheres of competence concerned.[2] Lastly, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data entered into force in Belgium on 1st September 1993 following the adoption of several legislative acts in this field.

The measures of blocking and removing content from the Internet are regulated in several statutory provisions of different kinds. However, with the recent codification of several laws in the Code of Economic Law, several of these provisions are found in different sections of the same code. Thus the Code of Economic Law comprises, in Title XII, the measures which transposed the provisions of directive EC/2000/31 on electronic commerce, and in Title XI the specific measures on protection of intellectual property rights. Moreover, special laws and the Code of Criminal Procedure provide for certain prerogatives as regards blocking and removal of content from the Internet.

1 Law of 3 August 2012 assenting to the Convention on Cybercrime, M.B., 21.11.2012.

2 Law of 7 February 2012 assenting to the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, done at Lanzarote on 25 October 2007, M. B., 21. 06.2013; Decree of 28 April 2011 assenting to the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, done at Lanzarote on 25 October 2007, M. B., 13.05.2011; Decree of 28 March 2011 assenting to the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, done at Lanzarote on 25 October 2007, M. B., 29.04.2011; Decree of 12 February 2010 assenting to the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, done at Lanzarote on 25 October 2007, M. B., 04.03.2010; Decree of 26 April 2012 assenting, in respect of the matters whose handling has been transferred by the French Community to the Walloon Region, to the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, done at Lanzarote on 25 October 2007, M. B., 22.05.2012; Order of 1 March 2012 assenting to the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, done at Lanzarote on 25 October 2007, M. B., 14.03.2012.

2. Regulations applicable to blocking and/or removal of illegal content from the Internet

Blocking and removal measures are considered in the same section given that the law deals jointly with the rules applicable to these measures.
Possibilities for blocking and/or removing content on the Internet differ depending on the content concerned. According to the fields involved, two different types of procedure allow blocking and/or removal to be applied to contents on the Internet: (a) an application by the prosecution, and (b) a decision of the judicial authority. These procedures must be combined, as appropriate, with specific rules linked relating to the responsibility of Internet service providers, adopted in pursuance of directive EC/2000/31 on electronic commerce.

2.1. Breach of public order and national security, and prevention of disturbances or crimes

Blocking measures are decided by the competent authority under criminal procedure, pursuant to the provisions of the Code of Criminal Procedure on seizure of computerised data. Indeed, to make up for the fact that the physical seizure of objects, in that it implies removing the object from the possession of the person concerned by the seizure, is not always desirable and/or possible when it applies to computerised data, the legislator has provided the possibility for the competent authority to carry out a **new form of seizure relating to computerised data**.

These measures are taken at the **stage of detecting criminal offences and their perpetrator(s)**, ie before the stage of the criminal court's decision as to the guilt of the person concerned under the Penal Code. They are taken by the **crown counsel** in the context of a criminal investigation (Article 39bis of the Code of Criminal Procedure ("CIC") **or by the examining judge** when an inquiry is opened (Article 89 CIC).

The inquiry is directed by the examining judge who performs his functions as regards independently establishing the true facts incriminating as well as exonerating the person concerned. It is obligatory in criminal cases and optional for lesser offences. The examining judge generally acts on referral by the crown prosecutor.

Conversely, **investigation** is directed by the crown counsel who comes under the state prosecution department. The crown counsel may prosecute either of his own motion or following a user's complaint lodged with the competent police offices.[3] Until lately the police made available to users a platform to report any offence committed on or via the Internet (www.ecops.be). Owing to the too-large number of complaints lodged in all areas, it was recently closed and a new reporting system is being developed. Until then, users are asked to apply to the ordinary police who will if appropriate pass the word to the police offices specialising in data processing, namely the *Federal Computer Crime Unit* at national level within the central directorate of serious and organised crime prevention (FCCU) or the regional *Computer Crime Units* (CCUs) in each judicial district under the authority of the judicial directors.

Under Article 39bis CIC (or Article 89 CIC), in principle **seizure of the material carrier of the data concerned** is performed or, if this seizure is not desirable, **the data are copied** on carrying media which belong to the authority (Article 39bis §2 CIC). Under this article, in addition to copying the data

[3] For certain offences, the legislator has made prosecution subject to a prior complaint by the injured person, as for example slander and libel (Article 450, Penal Code).

at issue – or instead of copying where this is not possible for technical reasons or because of the volume of data:

"[The crown counsel or the examining judge] also employ the appropriate technical means for **preventing access** to these data [which serve the same purposes as those envisaged in the case of seizure] in the computer system, as well as for preventing access to the copies of these data which are available to persons with permission to use the computer system, and likewise for guaranteeing their integrity."[4]

The measure to render the copied or seized data inaccessible constitutes a **blocking measure**. Either it is combined with the copying of data provided for in Article 39bis §2 CIC or, if such copying is not possible, it may be ordered on its own under Article 39bis §4 CIC.

All these measures – copying and/or inaccessibility of data – make it possible to ensure that the true facts are ascertained and preserved for the purpose of trial on the merits. The provision leaves some latitude for the **crown counsel or the examining judge: they may decide – without being obliged to do so –** to make the data inaccessible, or **to block access to them**. Thus, if the data and their utilisation by the suspected culprit of a criminal offence allow the suspect's guilt to be proven, access to them will probably not be blocked in order to collect evidence needed to expose the person implicated.

Again in the context of seizure of computerised data, the legislator has nevertheless gone further. Article 39bis para. 3 indent 2 CIC in fact provides that:

"If the data constitute the object of the offence or have been generated by the offence and if they are contrary to public order or morality or pose a danger to the integrity of computer systems or to data stored, processed or transmitted through such systems, the crown counsel [or the examining judge] shall employ all the appropriate technical means **to render such data inaccessible**" (emphasis added).

Thus, if the data at issue present the characteristic of constituting the **object of the offence** (for example, content disclosing a terrorist offence) or have been generated by the offence (for example, a computerised forgery) and being **contrary to public order or morality** (for example, offences concerning content), **the crown counsel or the examining judge is required to render them inaccessible** by all appropriate technical means. According to the preparatory papers for the law of 28 November 2000 on computer crime, this particular provision is distinct from the others made by Article 39bis CIC in enabling the crown counsel or the examining judge to **eliminate the computerised data concerned**.

Concerning all these measures to make data inaccessible, the law gives no further details on what should be understood by "**appropriate technical means**" to achieve this end. The prevailing legal theory is that the authorities in charge of the investigation or inquiry consult the police offices specialising in data processing, the FCCU or the CCUs. According to the preparatory papers for the law, measures to "prevent access" to computerised data, referred to in Article 39bis §3 1st indent and §4 CIC, only concern **measures blocking access to the website** and so concern only the Internet access providers; conversely, measures to "render inaccessible" the said data, prescribed in Article 39bis §3 indent 2 CIC, concern **both blocking measures and measures to remove the data** at issue

---

4 Article 39bis, para. 3 indent 1 CIC. See also Article 39bis, para. 4 CIC. The CIC may be freely consulted under: http://www.ejustice.just.fgov.be/loi/loi.htm (15.08.2015).

and are directed both at Internet access providers and at hosts.[5] Thus, in a judgment of 22 October 2013, the Court of Cassation recalled that Internet access providers could be compelled under Article 39bis §4 CIC to block access to the infringing data in the computer system.[6] In practice, as regards removal of data under Article 39bis §3 indent 2 CIC, removal of the said data will be carried out if the host is in Belgium, and the data will be blocked through the agency of the Internet access providers where the hosts are located abroad.
Because they occur in the context of a criminal justice inquiry, little publicity is given to cases of application of such blocking and/or removal measures. It nevertheless appears from the press that the website of the "Sharia4Belgium" cell was rendered inaccessible in June 2012 in the context of a criminal justice inquiry for incitement to rioting in Brussels in 2012, in retaliation for the arrest of a woman who refused to take off her *niqab* the wearing of which in public is prohibited in Belgium.[7] Such measures were to all appearances adopted in pursuance of Articles 39bis and/or 89 CIC.

The measures taken in pursuance of Article 39bis, para. 3 indent 2 CIC have come under criticism in that measures to block and/or remove illicit content adopted in accordance with this provision are firstly meant to be temporary for the purposes of the inquiry and non-permanent, whereas in practice the decisions taken under this provision are permanent. Secondly, it has been argued that these blocking and/or removal measures should actually be intended to establish the true facts and to preserve evidence, not to render an illegal content inaccessible. Even so, in The Pirate Bay case, the Court of Cassation confirmed in its judgment of 22 October 2013 that "an order issued by the examining judge on the basis of Article 39bis of the Code of Criminal Procedure can be issued for finding out the truth, for confiscation or restoration, for ending actions which seem to constitute an offence, or for safeguarding civil interests". The Court of Cassation also held that such measures did not constitute a general monitoring obligation, which is prohibited pursuant to Article 15 of Directive 2000/31/EC.[8]

These measures must be combined with certain special rules on the exemption of Internet **hosting service providers** from responsibility. Under directive 2000/31/EC, Article XII.19 Code of Economic Law (CDE) stipulates that the service provider hosting information is not held responsible for the information stored on condition (a) "of having no genuine knowledge of the illegal activity or information or, as regards a civil action for redress, being unaware of facts or circumstances which disclose the unlawful character of the activity or information"; or (b) "of acting promptly as soon as made aware to remove the information or render access to it impossible, and of acting in accordance with the procedure [described below]". Indeed, the law further provides that "where [the provider of hosting] is genuinely aware of unlawful activity or information, he shall communicate these forthwith to the crown counsel" and that "as long as the crown counsel has taken no decision about copying, inaccessibility and removal of documents stored in a computer system, the [provider of hosting] can only take measures aimed at preventing access to the information".

Useful particulars of this apparatus are given by the preparatory papers for the law which initially transposed directive 2000/31 in this respect. The explanatory memorandum thus provides that:

---

5 See in particular: B. Losdyck, Les saisies and les perquisitions de matériel informatique: les "garde-fous" entourant leur mise en œuvre, RDTI, 2013/52, p. 36.

6 Cass., 22 October 2013, R.G. no. P.13.0550.N, Tijdschrift voor Strafrecht , note by: SCHOEFS, Raf; Noot 'Strijd tegen The Pirate Bay over andere boeg gegooid: databeslag toegestaan' 2014, nr. 2, p. 126-142.

7 See in particular: http://www.lesoir.be/7764/article/actualite/belgique/2012-06-07/porte-parole-sharia4belgium-arr%C3%AAt%C3%A9 (15.08.2015).

8 Cass. 22 October 2013, no. P.13.0550.N, available under: http://jure.juridat.just.fgov.be/JuridatSearchCombined/?lang=fr&jur=1 (15.08.2015).

"The provider of hosting should only be held responsible on the threefold condition of having been **aware of the presence of contentious matter on its server**, of the **manifest illegality** of such matter[…] and having shown **inaction**."[9]

Article XII.19 CDE makes reference to the principle "***notice and take down***", in pursuance whereof hosting providers are required to remove illicit content from the very moment when they have genuine knowledge of it. However, the legislator specified the mechanism as follows: as soon as **aware** of illicit content, **the host is required to take the measures to render it inaccessible**, and to inform the crown counsel of them. **For as long as the crown counsel or the examining judge have not taken the blocking or removal measures** referred to in Article 39bis CIC or 89 CIC, **the provider of hosting nevertheless may only block access to the site concerned (to the exclusion of removal measures).** Once these measures are ordered as part of a criminal justice inquiry, the host is of course obliged to carry them out. According to the *ratio legis* of the law, the host will nevertheless be held responsible only if he, cumulatively, was aware of the illegal content and of its ***manifest* illegality**, and did not take the measures to render it inaccessible. By "manifest illegality", the legislator means contents of a revisionist, paedophile or indisputably offensive kind.[10] More precise information is not available.

2.2. Offence against public health and morality

The situation is similar in every respect when the content is illegal in that it contains **child pornography images**. As child pornography is punishable under criminal law,[11] the investigation or inquiry will make it possible to take such **blocking or removal measures as the crown counsel or the examining judge may deem expedient**, in pursuance of Articles 39bis CIC or 89 CIC (see section 2.1 above).

It is noted that since the closure of the platform for reporting illicit contents (www.ecops.be), users can report child pornography offences to the Foundation for Missing and Sexually Exploited Children, a Belgian foundation in the public interest known under the designation "**Child focus**". This foundation's responsibility is then to transmit the information to the police offices specialising in Internet affairs.

Child pornography sites are also subject to measures of blocking directly by a host with genuine knowledge of the site's illegal content, in accordance with Article XII.19 CDE (see section 2.1 above). A measure of this kind may give rise to litigation before the civil court. Thus, in a case where a person had developed and operated a website through which, under his responsibility and with his knowledge, a collection of hyperlinks was offered to sites plainly having a child pornography content, the Court of Cassation upheld the Court of Appeal decision that the person could not benefit from the conditional exemption from responsibility favouring those who engage in a hosting activity.[12]

Where **combating of on-line games of chance** is concerned, the Games of Chance Board has drawn up a **black list of the on-line games of chance which have not obtained the necessary licence** for their operation. This list is freely accessible on the Board's Internet site.[13] These sites for on-line games of chance are blocked following an agreement concluded by the Board with various Internet

---

9 Travaux Parlementaires, 2002-2003, Doc. 50/2100/01, p. 48.

10 Ibidem.

11 See in particular: Article 383bis Penal Code.

12 Cass. 03.02.2004, P.03.1427.N, available under: http://jure.juridat.just.fgov.be/JuridatSearchCombined/?lang=fr&jur=1 (15.08.2015).

13 See: https://www.gamingcommission.be/opencms/opencms/jhksweb_fr/establishments/Online/blacklist/index.html (15.08.2015).

access providers present on the Belgian market.[14] These blocking sanctions are accompanied by freezing of capital transfers from and to these sites. The sanctions are all of a contractual nature but can also operate in the context of criminal proceedings under Article 39bis and 89 CIC.

Regarding the media audiovisual services, in Belgium the communities have an exclusive competency to regulate them. The Flemish Act on Radio and Television Broadcasting of 27 March 2009[15], that stablisehes the Flemish legal framework in this filed, allows in its Article 44 the Flemish Media Regulator (the regulatory authority for media in Flanders) to force a service provider or network operator to temporarily suspend the transmission of linear television programs by a television broadcaster based on violations of art. 38 and 42 of the same Decree, i.e. programs which are forbidden by reason of incitation to hatred and protection of minors against content that is detrimental to their physical, mental or moral development. Hence, if such linear television programs were to be transmitted by internet, the Regulator could force the network operator or service provider to block the transmission. This regulation is based on article 3 of the Audiovisual Media Services Directive 2010/13/EU of 10 March 2010. For the French Community of Belgium, the relevant articles are 9 and 159 of the Audiovisual Media Services Decree of 26 March 2009.

2.3. Infringement of the rights of others

Anti-discrimination is the object of several statutes both at the federal level and at the Community and regional levels.[16] At the federal level, the law of 10 May 2007 to combat certain forms of discrimination and the law of 30 July 1981 to punish certain acts inspired by racism and xenophobia assign an important role to the **Interfederal Centre for Equal Opportunities**, an independent government agency competent in that field (hereinafter "Centre").

The Centre is first of all the preferential contact point for victims who can turn to it for initial advice on situations of discrimination encountered but also for conflict management. Accordingly, the Centre can act in various ways on a report coming within its remit: firstly, negotiation and conciliation of the parties to the dispute will have pride of place; next, the Centre can issue a warning and a reminder of the law to the person or institution complained of; it can also refer the matter to the implicated person's managerial or disciplinary authority; the Centre is also competent to give opinions in judicial proceedings without being a party to the litigation; finally, the Centre can bring or be joined to an action at law, whether criminal or civil. When taking action at law, the Centre always acts in its own name and on its own behalf, not the victim's.

Where civil action is concerned, the aforementioned laws both afford the possibility for the **civil judge** to determine the existence of an act constituting a violation of the aforementioned statutory provisions and to order its cessation, even if the act is also punishable under criminal law. The **action for an injunction** to that effect is brought and examined under the summary application procedure by the presiding judge of the court of first instance, or, depending on the nature of the act, by the presiding judge of the labour court or commercial court.[17] On the Internet, the injunction comprises the possible obligation of the host or of other players to **remove the illegal content from the**

---

14 Ibidem.

15 See: http://www.vlaamseregulatormedia.be/sites/default/files/act_on_radio_and_television_broadcasting.pdf

16 For an overview of the legislation applicable over Belgian territory on prevention of discrimination, see: http://www.diversite.be/photographie-des-legislations-antidiscrimination (15.08.2015).

17 See: Article 20 Law of 10 May 2007 to prevent certain forms of discrimination (M.B., 30.05.2007) and article 18, Law of 30 July 1981 to punish certain acts inspired by racism and xenophobia, amended by the law of 10 May 2007 (MB 30.05.07) and the law of 17 August 2013 (M.B. 05.03.2014).

Internet or to make it otherwise inaccessible. These laws further provide that where the acts concerned by the injunction proceedings are also brought before a criminal court, the latter may only rule on the criminal proceedings after a decision which has acquired res judicata force has been delivered in respect of the injunction proceedings.[18] Injunction proceedings are brought by the user who is the victim but may also be brought by the Centre, by one of the interest groupings, by the state prosecution department or, depending on the nature of the act, by the prosecution service before the labour court.

If there is matter for the charging of a criminal offence, the Centre or the injured user may lodge a **complaint** with the prosecution or the police which, if considered justified, will take the same blocking and/or removal measures as those set out in section 2.1.

The procedure and the **measures for blocking and/or removal** described in section 2.1 are also applicable where the acts interfering with the rights of others on the Internet constitute **offences of defamation or slander**, punishable under criminal law.

A specific regulation on **protection of privacy** is also noted. Under the law of 8 December 1992 on protection of privacy in respect of personal data processing,[19] the **Internet service provider may be required**, in accordance with a decision delivered by the **presiding judge of the court of first instance**, **to delete personal data** not processed under certain conditions prescribed by law.[20]

Moreover, the aforementioned law defines certain **criminal offences** with regard to protection of privacy.[21] When these offences are held proven, **the criminal court can order the deletion of the personal data** concerned.[22]

Such orders regarding the protection of privacy may be directed as appropriate at an Internet service provider described as a “data manager”[23] or “third party”[24] performing “personal data processing”[25] on behalf of the data manager.

---

18 Ibid.

19 Law of 8 December 1992 on the protection of privacy in respect of personal data processing, M.B., 18 March 1993.

20 See articles 12 and 14, Law of 8 December 1992.

21 See in particular: article 39, Law of 8 December 1992.

22 Article 41, Law of 8 December 1992.

23 “Data manager” is understood as the natural or legal person, the de facto association or the public administration which, singly or in conjunction with others, determines the ends and means of personal data processing (article 1, para. 4, indent 1, Law of 8 December 1992).

24 “Third party” is understood as the natural person, the legal person, the de facto association or the public administration, other than the person concerned, the data manager, the sub-contractor and the persons who, placed under the direct authority of the data manager or the sub-contractor, are authorised to process the data (article 1, para. 6, Law of 8 December 1992).

25 “Processing” is understood as any operation or set of operations whether or not performed with the aid of automated processes and applied to personal data, such as collection, recording, organisation, storage, adaptation or alteration, recovery, consultation, use, communication by transmission, distribution or any other form of provision, approximation or interconnection, as well as blocking, deletion or destruction of personal data (article 1, para. 2, Law of 8 December 1992); “personal data” is understood as any information concerning an identified or identifiable natural person, hereinafter referred to as “person concerned”; a person who can be identified directly or indirectly, particularly with reference to an identification number or to one or more specific elements peculiar to his/her physical, physiological, mental, economic, cultural or social identity, is deemed identifiable (article 1, para. 1, Law of 8 December 1992).

The Privacy Commission set up by the law of 8 December 1992 can report certain acts constituting **criminal offences** within its purview to the state prosecution service – possibly resulting in **measures to block and/or remove** illegal content on the Internet (see section 2.1 above).

Finally, it is appropriate to observe that in all areas the law of judicial process recognises summary procedure making it possible to petition the presiding judge of the commercial court or court of first instance to take provisional measures pending the settlement of the substantive dispute where this is justified by the urgency of the situation. Under this procedure, the presiding judge may "order **all measures necessary for protecting the rights of persons unable to take the necessary steps**".[26] In case of absolute need, the matter may even be referred to the presiding judge at the simple request of the interested party.

2.4. Infringement of rights of intellectual property

Rights of intellectual property also enjoy effective protection before the civil court, whether the presiding judge of the court of first instance or of the commercial court (depending on the nature of the facts of the case).[27] In the context of an **action for an injunction to desist**, the presiding judge may in fact **direct, having found an infringement of the rights of intellectual property, that the agents desist from the services which they make available and which are used by third parties to violate the rights of intellectual property.**[28]

Article XI. 334 CDE makes such provision as regards infringement of a patent, a complementary certificate of protection, a breeder's right, a copyright, a neighbouring right, the right of a producer of databases or a right in respect of a topography of a semiconducting product. For other types of intellectual property rights, including **protection of trademarks**, Article XVII.14 par. 1 and 4 CDE provides that the owners of intellectual property rights, including trademark owners, may bring an action for an injunction against the party responsible for the infringement and that the competent court may also deliver an injunction to desist against the agents whose services are used by a third party to infringe a right.

Action for an injunction in matters of protecting intellectual property rights has been applied on several occasions by the courts.

In a case concerning infringements of copyright made possible by use of the "**thepiratebay.org**" Internet site in Belgium, the Antwerp Court of Appeal, in the civil proceedings and on the application for an injunction to desist referred to in Article XI.334 CDE, ordered two Internet access providers to block access to The Pirate Bay site for their subscribers by setting up DNS blocking, at the request of the *Belgian anti-piracy federation* (B.A.F.). The judgment overturned the decision of the Antwerp commercial court which had refused to impose such a blocking measure on the Internet access providers, deeming it disproportionate to the offence and challenging the appropriateness and effectiveness of the measure sought.[29] Further to the Court of Appeal judgment, the B.A.F. sent a letter to other Internet access providers, threatening them with legal action if they did not also block access to the site concerned. This move has been strongly criticised for forcing Internet access providers to apply blocking measures by extrajudicial means and without consultation of civil society

---

26 Article 584, Judicial Code

27 Article XVII.14 CDE.

28 Article XI.334 para. 1 indent 2 CDE and Article XVII.14 para. 4 CDE.

29 Antwerp (1st chamber) no. 2010/AR/2541, 26 September 2011, AM 2012, liv. 2-3, 216; Computerr. (Pays-Bas) 2013, liv. 4, 217, note TSHIANANGA, B., SOMERS, G.; ICIP 2011, liv. 5-6, 731; RABG 2011, liv. 18, 1269, note VAN EECKE, P., FIERENS, A.

or of the end users.[30] The facts of the case indicate that the measure blocking the Internet site was circumvented afterwards. The B.A.F. then decided to bring a complaint in criminal law for offences of infringement of copyright committed via the aforesaid Internet site (see below).

In another case, the Lancôme perfumes and cosmetics company sued the company eBay, selling on-line goods and services, over imitations of products with the Lancôme brand put on line on the eBay on-line sales site. Lancôme's application to the courts sought to have eBay ordered to prevent the posting on line of such products and to pay Lancôme damages. The eBay company relied on its status as host and on the conditional non-liability deriving from it. In its judgment, the commercial court firstly defined the type of activity pursued by eBay in relation to posting of sales offered by its customers, and inferred, as far as the relevant activity by eBay was concerned, that it was a **hosting activity**, enjoying an exemption from responsibility subject to the conditions prescribed by Belgian law (cf. section 2.1. above). The court moreover found that **eBay had always taken care to answer Lancôme's demands to remove from the Internet certain contents** recognised as illegal, but that it was permissible to consider that **eBay should be able to verify the validity of Lancôme's claims** regarding each content at issue and that eBay could not be ordered to take **measures to prevent such illegality from recurring**, as that would **constitute a general monitoring obligation prohibited** by directive 2000/31/EC.[31]

Attention is also drawn to the case of the Société belge des auteurs, compositeurs et éditeurs (**SABAM**) v. Scarlet (formerly Tiscali), an Internet access provider, in a dispute in which SABAM sought, by applying for the injunction to desist referred to in Article XI.334 CDE (formerly article 87 of the law of 30 June 1994 on copyright and neighbouring rights), to have Scarlet compelled by court order to take steps to put a stop to the infringements of copyright committed by its customers. The Brussels Court of Appeal, in its judgment of 28 January 2010, decided to ask the Court of Justice of the European Union (CJEU) two preliminary questions. The CJEU answered these two questions after rephrasing them in its judgment of 24 November 2011.[32] It held that while general monitoring obligations were prohibited, **a court could order** a provider of Internet access, or any other **technical intermediary**, to take **measures to end infringements of intellectual property rights, or to prevent further infringements**. In the opinion of the CJEU, such measures can be taken against an Internet access provider **in so far as they comply with the limitations prescribed in directives** 2001/29, 2004/48 and 2000/31. The measures taken must be **effective and dissuasive**, **not consist in a general monitoring obligation** and ensure a **proper balance between rights and freedoms**. The **measure desired by SABAM**, which would compel the Internet access provider to carry out active monitoring of all the electronic communications of all customers in order to single out the unlawful ones among them, **would correspond to generalised monitoring**, incompatible with Article 15 of directive 2000/31 and with Article 3 of directive 2004/48. According to the CJEU, the installation of a filtering system for an unlimited time, at the sole expense of the Internet access provider, in order to have current infringements stopped and prevent future infringements, and involving systematic analysis of all contents exchanged with collection of the IP addresses of the provider's customers, **does not safeguard the balance which the court should seek between protection of the rights of copyright holders and other fundamental rights including freedom of expression**. Thus, where that freedom is concerned, the measure at issue is deemed contrary to Community law in **not adequately distinguishing between unlawful and lawful content**, and therefore its **application would be liable to cause the blocking of communications with lawful content**.

---

30 See in particular: https://www.eff.org/fr/deeplinks/2011/12/belgian-isps-vs-the Internet-freedom (15.08.2015).

31 Comm. Bruxelles (7è Ch.), 31 July 2008, RDTI, 2008, no. 33, p. 521 ff.

32 CJEU, 24 November 2011, Scarlet Extended SA v. Sabam, case C-70/10.

Under the provisions of book XI and book XV of the Code of Economic Law, certain infringements of intellectual property rights constitute **criminal offences.**[33] In such a case, the blocking measures are decided by the crown prosecutor or the examining judge under the provisions of the Code of Criminal Procedure on **seizure of computerised data** (see section 2.1 above). In instances where the facts of the case disclose the existence of a criminal offence, the prosecution or the examining judge can decide to render the computerised data inaccessible, pursuant to Articles 39bis CIC or 89 CIC. On this subject, reference is made to the details given above (section 2.1). It should be noted, however, that a breach of public order or morality will be harder to prove where a violation of intellectual property rights is concerned. The prosecution acts either of its own motion or upon a user's complaint, which may be brought through the agency of the Federal Public Service for the Economy.

In connection with the aforementioned action for an injunction to desist in *The Pirate Bay* case, and following the circumvention of the measure blocking the Internet site which was ordered in the civil proceedings, blocking measures were actuated at the level of the criminal prosecution during the criminal investigation of the breaches of copyright arising from the use of "**thepiratebay.org**" site on the Internet from Belgium. In this case, the examining judge had delivered an order requiring all operators and Internet access providers to render "thepiratebay.org" site inaccessible. More specifically, the order stated that the content hosted by the server coupled with the domain name "thepiratebay.org" must be rendered inaccessible. Furthermore, the operators were required to employ all possible technical means to block access to the domain names associated with this server. **The order** specified the technical means that could be employed to determine the domain names concerned. In this way the examining judge sought to prevent measures circumventing the blocking order. The order delivered in fact remained "open-ended" and **allowed blocking of certain domain names not explicitly mentioned in the order but sufficiently identified**. Several operators appealed this decision. The Court of Cassation nevertheless refused to censure the court chamber which had confirmed this order, holding that measures adopted in pursuance of Articles 39bis and 89 CIC could be validly adopted in order to help ascertain the truth, effect confiscation or restitution, terminate actions apparently constituting a crime, or protect civil interests. It also stated that such an order did not infringe the prohibition of obliging Internet service providers to carry out general monitoring of the Internet.[34]

2.5. Codes of conduct

The association of Internet service providers has concluded among its members a code of conduct providing that Internet service providers should add to the general conditions of provision of their services to users or customers a "good conduct" section containing a reference to proper behaviour on the Internet. In general, this reference is formulated in very vague terms, without further precision, enabling the Internet service providers – from the contractual standpoint – to take any appropriate measure, notably blocking measures, vis-à-vis their customer.[35] The terms of the "proper conduct on the Internet "and the practical consequences of its absence are specified in the general terms of the internet service providers and therefore depend on each provider.

---

33 The CDE accordingly makes provision, in particular, for the offence of infringement of copyright and neighbouring rights (Article XI.293 CDE and Article XV.104 CDE), the offence of infringement of copyright in respect of a computer programme (Article XI.304 CDE and Article XV.105 CDE) or again the offence in respect of trademarks (Article XV.103 et seq. CDE).

34 Cass. 22 October 2013, no. P.13.0550.N, available under: http://jure.juridat.just.fgov.be/JuridatSearchCombined/?lang=fr&jur=1 (15.08.2015).

35 ISPA, code of conduct, available under: www.ispa.be

3. Procedural questions

While Belgium earlier set up a centralised platform for reports concerning the Internet, accessible on the site www.ecops.be, it was closed recently because of the too-large number of reports and the unfeasibility of dealing with all of them in a reasonable time. The agencies concerned by these reports, the Federal Public Service for the Economy as well as the police and the organisations active in the field, are conferring in order to develop a new mechanism for reporting and processing complaints concerning the Internet. Meanwhile, as already mentioned in section 2, users are requested to report illicit contents which they encounter directly to the competent authorities according to the type of content: Federal Public Service for the Economy, police, Child Focus and prosecution service.

When the blocking and/or removal measures are ordered in the context of a criminal inquiry or investigation in accordance with the provisions on seizure of computerised data made in Articles 39bis and 89 CIC, these provisions stipulate that the crown counsel or the examining judge informs the computer system manager of the search conducted in the computer system and communicates a summary of the data copied, made inaccessible or removed.[36] This communication requirement is not subject to a time limit, nor prescribed in such terms that its non-fulfilment would invalidate the measures, and this may prompt the crown counsel or the examining judge to await an opportune moment in the criminal inquiry to pass the relevant information to the manager of the computer system. Besides, this manager is not always easy to identify, especially when he takes steps to prevent identification.

Furthermore, the persons affected by the measure of seizure can request the withdrawal of these measures in certain circumstances. Articles 28sexies and 61quater CIC provide that any person prejudiced by an investigative act relating to his property can ask the crown counsel or the examining judge to withdraw it. They make their pronouncement within the 15 days following the lodging of the request. The crown counsel or the examining judge can dismiss the request “if they consider that the needs of the investigation so require, where withdrawal of the act interferes with protection of the rights of the parties or others, where withdrawal of the act poses a danger to persons or possessions, or in cases where the law prescribes restitution or confiscation of such possessions”. They can also grant complete, partial or conditional withdrawal. An appeal against the decision by the crown counsel or the examining judge can be made to the indictments chamber in the court of first instance. It rules on the case within 15 days. Thereafter, there still remains an appeal on points of law against the indictments chamber’s decision, in so far as a legal defect can be pleaded.

On the other hand, where the blocking and/or removal measures are ordered by the judge in civil litigation, the ordinary remedies apply. Thus the decision by the presiding judge of the court of first instance or the commercial court may be reviewed by the Court of Appeal; an appeal on points of law against the Court of Appeal decision is also available in so far as a legal defect can be pleaded.

4. General Internet monitoring

In accordance with directive 200/31/EC and Article XII.20 CDE, Internet service providers are under no general obligation to monitor the information which they transmit or store, or any general obligation to be active in detecting facts or circumstances which point to unlawful activities. This does not prevent the competent judicial authorities from laying down a temporary monitoring

[36] Article 39bis para. 5 CIC and Article 89 CIC.

obligation in a specific case where this possibility is provided by a law.[37] In addition, Internet service providers are obliged to inform the competent judicial or administrative authorities promptly of the alleged unlawful activities engaged in by the recipients of their services, or of the alleged illegal information supplied by the latter. They are also required to disclose to the competent judicial or administrative authorities, at their request, all information in their possession useful for the detection and ascertainment of the offences committed through their agency.[38]

As already explained, the agencies concerned by reporting of illegal contents on the Internet, the Federal Public Service for the Economy, the police and the organisations active in the field, have been conferring since the closure of the www.ecops.be platform in order to develop a new mechanism for reporting and processing complaints about the Internet. In that connection the writer has been informed that the possibilities for Internet monitoring by the specialised police offices in the future were not to be ruled out at the present stage.

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

The conditions under which blocking or removal of information on the Internet can be carried out are generally **prescribed by law**. In criminal law, they come within the ambit of a specific procedure for **seizure of computerised data** under the authority of the examining judge or the crown counsel. This legal framework has been criticised, however.

The principal criticism is that the blocking and/or removal measures ordered under the CIC are intended to be **temporary measures ordered in the context of a criminal investigation**, and therefore **not a legal measure allowing Internet sites to be indefinitely blocked**. By leaving the question of blocking and/or removal of information concerned by the investigation entirely in the hands of the examining judge or the crown counsel, **this question is removed from judicial oversight**.

Other criticisms contend that it is not appropriate to place these measures in the context of seizure of computerised data, since they have nothing to do with establishing the true facts. Nonetheless, the Court of Cassation did not see fit to censure the ruling of the indictments chamber, holding in its judgment of 22 October 2013 that "an order issued by the examining judge on the basis of Article 39bis of the Code of Criminal Procedure can be issued for finding out the truth, for confiscation or restitution, for ending acts which seem to constitute an offence, or for the protection of civil interests".[39] Thus measures to block and remove illegal content on the Internet can be ordered with the aim both of ascertaining the truth and of eliminating illegal content.

Lastly, concerning the obligations to inform the persons affected by seizure, by not prescribing a time limit to inform the manager of the computer system targeted by the blocking and/or removal measure, and not stipulating that failure to inform would invalidate the measure, the legislator has given the examining judge or the crown counsel some latitude according to the needs of the inquiry. From the standpoint of fundamental rights, this could be problematic. That said, it should be observed that having regard to the preliminary title of the CIC, undue flexibility in enforcing this

---

37 The Code of Criminal Investigation notably provides for measures on tracing and location of telecommunications and recording of private communications and telecommunications (Articles 87 ff. CIC).

38 Article XII.20 CDE.

39 Cass. 22 October 2013, no. P.13.0550.N, available under: http://jure.juridat.just.fgov.be/JuridatSearchCombined/?lang=fr&jur=1 (15.08.2015).

obligation to inform may lead to problems of admissibility of evidence in criminal proceedings, particularly if "**the irregularity committed has vitiated the reliability of the evidence"** or "**if it is contrary to the right to a fair trial to make use of the evidence**" (Article 32, preliminary title of the CIC).

In civil proceedings, the conditions under which the judge can order the intermediaries to stop the services enabling third parties to commit infringements of, in particular, intellectual property rights, are clearly defined by law. Thus they evidently show sufficient predictability. In particular, a reading of the preparatory papers allows modulation of the legal rules of responsibility in the matter which constrain hosts. According to these papers, if genuinely aware of the illegality of a hosted content, the host' responsibility is only likely to be involved if the content in question is "**manifestly illegal**" and he has not taken measures to render it inaccessible. Thus, where content not *manifestly* illegal is concerned, the *ratio legis* of Article XII.19 CDE indicates that the host is required to block it only in compliance with an obligation imposed by order in the context of a criminal court inquiry. If not so required, he may nevertheless decide voluntarily to apply a measure blocking that content but in that event is open to possible legal action by the person whom the unjustified blocking measure prejudiced. The mechanism thereby established has the appearance of ensuring sufficient predictability of the system for the benefit of hosts. It appears to uphold freedom of expression in not encouraging hosts to block Internet sites with probable illegal content too readily, out of fear that their responsibility would be involved for not doing so.
Where blocking measures are concerned, a certain practice reported is for the party requesting the measure to give the Internet access providers or hosts notice to block the site or sites in question or face legal action. This kind of approach was adopted by the *Belgian anti-piracy Federation* (B.A.F.) in *The Pirate Bay* case: after obtaining a court order for a measure whereby certain Internet access providers would block that site, the BAF issued a notice to several other Internet access providers to comply with the court decision, although they were not parties to it, informing them that otherwise the BAF would bring court proceedings against them. This course of action was strongly criticised for coercing Internet access providers to take blocking measures of their own accord, that is without a judicial intervention meant to ensure balance between the impact of the blocking measures on freedom of expression and the infringements of intellectual property rights.[40]

Finally, it is noted that there was a proposal to make it possible for racist and more generally discriminatory content to be subject to purely administrative blocking and/or removal measures by the Interfederal Centre for Equal Opportunities, without any prior judicial intervention. Its author felt that such an arrangement would have the advantage of allowing speedier settlement than the intervention of the slow, retributive judicial machinery, and would allow hosts to be relieved of a task – distinguishing what is and what is not illegal – which, in this field, can prove awkward and would be better fulfilled if it were the outcome of action by an independent authority specialising in the question, which the centre is.[41]

Stéphanie De Dycker, LL.M.
Legal Adviser, Swiss Institute of Comparative Law
15.08.2015

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

[40] See in particular: https://www.eff.org/fr/deeplinks/2011/12/belgian-isps-vs-the Internet-freedom (15.08.2015).

[41] Y. Poullet, La lutte contre le racisme et la xénophobie sur l'internet, J.T., 2006/23, no. 6229, p. 401-412.