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 236-255

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.

FRANCE

1. Sources

France is party to all the Council of Europe conventions in the field of Internet governance. It has signed and ratified the Cybercrime Convention drawn up in Budapest on 23 November 2001. This was published in the Official Gazette of the French Republic by means of Decree No. 2006-580 of 23 May 2006 promulgating the Convention on Cybercrime.[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 also published in the Official Gazette by means of Decree No. 2006-597 of 23 May 2006.[2]

The Convention on the Prevention of Terrorism, adopted on 16 May 2008 in Warsaw, signed by France on 22 May 2006, was published in the Official Gazette by means of Decree No. 2008-1099 of 28 October 2008.[3]

The Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, signed in Lanzarote on 25 October 2007, was published in the Official Gazette by means of Decree No. 2011-1385 of 27 October 2011.[4]

Lastly, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, adopted in Strasbourg on 28 January 1981 was published in the Official Gazette by means of Law No. 82-890 of 19 October 1982.[5] The Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows, adopted in Strasbourg on 8 November 2001, was published in the Official Gazette by means of Law No. 2007-301 of 5 March 2007.[6]

Matters relating to the blocking and filtering of websites and the removal/take-down of unlawful content on websites are governed in France by various **laws and regulations** which vary in accordance with the reasons underlying these restriction measures.

Law No. 2004-575 of 21 June 2004 on ensuring confidence in the digital economy (hereinafter the "LCEN") is the main legislative text relating to the blocking of and removal of unlawful content from

---

1 Decree No. 2006-580 of 23 May 2006 promulgating the Convention on Cybercrime, drawn up in Budapest on 23 November 2001, Official Gazette of the French Republic (JORF), 24 May 2006.

2 Decree No. 2006-597 of 23 May 2006 promulgating the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, drawn up in Strasbourg on 28 January 2003, JORF, 27 May 2006.

3 Decree No. 2008-1099 of 28 October 2008 promulgating the Council of Europe Convention on the Prevention of Terrorism (together with the appendix), adopted in Warsaw on 16 May 2005, signed by France on 22 May 2006, JORF, 30 October 2008.

4 Decree No. 2011-1385 of 27 October 2011 promulgating the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (together with a declaration and a reservation), signed in Lanzarote on 25 October 2007, JORF, 29 October 2011.

5 Law No. 82-890 of 19 October 1982 promulgating the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, adopted in Strasbourg on 28 January 1981, JORF, 20 October 1982, 3163.

6 Law No. 2007-301 of 5 March 2007 authorising the approval of the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows, adopted in Strasbourg on 8 November 2001, JORF, 7 March 2007.

websites. It provides that both the judicial and administrative authorities may order the blocking or filtering of certain sites subject to certain criteria, and the removal of content from those sites. The relevant provisions of this law for this study were first amended by Law No. 2011-267 of 14 March 2011 on domestic security guidance and planning, known as LOPPSI 2. More recently, the LCEN was supplemented by Law No. 2014-1353 of 13 November 2014 on scaling up counter-terrorism provisions.

In the field of intellectual property rights, the Intellectual Property Code also contains provisions enabling the courts to order the removal of content from websites which breach intellectual property rights.

With regard to the protection of privacy, the Civil Code provides that the civil courts may order any measure to prevent or halt the violation at issue.

There are certain other areas in which there is an administrative or semi-administrative blocking mechanism. For example, in the field of personal data protection, the French Data Protection Agency (CNIL) has the authority to ensure the cessation of the processing of personal data carried out on the Internet in the circumstances set out in Law No. 78-17 of 6 January 1978 on Information Technology, Data Files and Individual Liberties. Similarly, the Online Gaming Regulatory Authority is able to ask the president of the Regional Court to ensure that website hosts and Internet access providers block access to an online gaming service which is in violation of the legal conditions in force.

2. Applicable regulations

2.1. Blocking and/or filtering of illegal website content

2.1.1. The protection of national security and morality

In application of Article 12.3 of Directive 2000/31/EC on e-commerce, the LCEN provides that Internet service providers (hereinafter ISPs) can be obliged, **by the courts**, to terminate or prevent an infringement caused by the content of a website. The LCEN stipulates that:

> "the judicial authority may require, upon summary or ex parte application, that [the hosting service] or, by default, [the online public communications access provider] take any appropriate measures to prevent or halt harm or damage resulting from the content of an online public communication service."[7]

In practice, these measures ordered by the civil courts consist of making specific online content inaccessible. Such action by the court may result in provisional measures or a final decision. First of all, the measures are directed towards a hosting service (see Section 2.2); it is only if the latter fail to act that measures are then directed towards the various ISPs; in this case, the operation has to be repeated with each technical intermediary. Given the general nature of this provision, it must be regarded as being applicable **irrespective of the ground for the unlawfulness** of the content found by the court. As explained below, certain areas are subject to special regulations regarding blocking, filtering and unlawful content removal on the Internet.

The issue of the extent of the judge's powers vis-à-vis ISPs under Article 6.I.8 LCEN was raised before the French courts in a case in which the Ministry of the Interior sought to take action against a number of websites alleging police violations and in so doing, disseminating insulting and defamatory

[7] Article 6.I.8 LCEN.

remarks about the public authorities (in particular the police) along with personal data collected without the knowledge of the persons concerned. Further reference to this case will be made in Section 2.1.3. below, on blocking and filtering measures taken in order to protect privacy and personal data.

In a decision of 10 February 2012 relating to this case, the Paris Regional Court ordered one of the sites concerned to be blocked by the various ISPs for six months. In so doing, the court held that it had been impossible to identify the hosting services or the content editors of the site in question despite the steps taken by the Ministry of the Interior to this effect. With regard to other websites to which the court case also referred, the court decided that blocking was not appropriate as the Ministry of the Interior had not indicated whether or not it had attempted to identify the hosting services and editors.

Moreover, in order to step up the fight against terrorism in particular and to restructure the action taken against child pornography, the French legislature recently[8] introduced new provisions into the LCEN and the Criminal Procedural Code.

Indeed, the French legislature introduced new provisions in the LCEN by virtue of which websites disseminating images constituting a criminal offence under the legislation relating to **child pornography**[9] or **inciting or condoning acts of terrorism**,[10] may be **removed** from the Internet or **blocked**. These measures take place further to a decision by the competent administrative authority, and consequently without any court intervention.

---

8 Law No. 2014-1353 of 13 November 2014 on scaling up counter-terrorism provisions, available (in French only) on www.legifrance.gouv.fr.

9 Article 227-23 of the Criminal Code provides: "Taking, recording or transmitting a picture or representation of a minor with a view to circulating it, where that image or representation has a pornographic character, shall be punishable by five years' imprisonment and a fine of €75,000. The above acts shall also be punishable where the image or representation concerns a child under the age of 15 even if they were not committed with a view to circulating the said image or representation.
The same penalties shall apply to offering, making available or distributing such an image or representation by whatever means, and to importing or exporting it or enabling it to be imported or exported.
The penalties shall be increased to seven years' imprisonment and a fine of €100,000 where an electronic communication network has been used to circulate the image or representation of the minor to an unrestricted public.
Habitually consulting or paying a fee to an online public communication service making available such an image or representation, acquiring or storing such an image or representation by whatever means, shall be punishable by two years' imprisonment and a fine of €30,000.
The offences set out in this Article shall be punishable by ten years' imprisonment and a fine of €500,000 where they are committed by an organised gang.
Attempting to commit the offences set out in this Article shall be subject to the same penalties.
The provisions of this Article shall also apply to pornographic images of a person whose physical appearance is that of a minor unless it is proven that the person in question was 18 years of age on the date the image was taken or recorded."

10 Article 421-2-5 of the Criminal Code provides: "Directly inciting acts or terrorism or publicly condoning such acts shall be punishable by five years' imprisonment and a fine of €75,000 where these acts are committed using an online public communication service.
Where the acts are committed in the press, the audio-visual media or by means of online public communication tools, the specific provisions of the laws governing such matters shall apply with regard to identifying the persons responsible."

In pursuance of the Decree of 5 February 2015[11] implementing the provisions recently introduced into the LCEN by the law of 13 November 2014 on scaling up counter-terrorism provisions, the administrative authority responsible for the blocking and/or removal of websites is the Directorate General of the **National Police**, the Central Office for Combating ITC-related Crime (hereinafter the "OCLCTIC"). Within this administrative authority, only certain individually designated officers are authorised by the Head of the Office to implement the blocking procedure.

In application of Article 6-1.1 LCEN, the OCLCTIC orders the Internet hosting services of the sites in question to remove the Internet content. Where the content has not been removed within 24 hours, the OCLCTIC may **notify the ISPs of the list of electronic addresses** of the online public communication services which are in violation of the said criminal-law provisions. Within 24 hours of this notification, the ISPs must, by any appropriate means, prevent access to the services provided by the electronic addresses included on the list and links redirecting to those services. However, the LCEN provides that where there is no public information on the editor of the site – such publication being required by Article 6, III LCEN – the OCLCTIC may notify the ISPs of the addresses of the websites to be blocked in application of its decision, without previously requesting removal of the data.

Legal entities which fail to comply with the obligations laid down in the LCEN with regard to child pornography-related content or content inciting or condoning terrorism, as indicated above, shall be punished by a **fine** of €375,000 and a **prohibition**, either permanent or for a maximum of 5 years, from carrying out directly or indirectly one or more professional or social activities. In addition, the decision in question will be displayed or disseminated either in the press or by any other electronic public communication means.

Furthermore, in application of the new Article 706-23 of the Criminal Procedural Code, introduced by the law of 13 November 2014 on scaling up counter-terrorism provisions, the criminal courts may, in summary proceedings, order, at the request of the public prosecutor or any natural or legal person having a legitimate interest to act, the termination of an online public communication service on the grounds of facts constituting a criminal offence of inciting or condoning terrorism, where such facts constitute a manifestly unlawful infringement[12].

Lastly, in the **online gaming** field, it is the **Online Gaming Regulatory Authority** (hereinafter the "ARJEL") which has responsibility for monitoring online gaming sites, where necessary under the supervision of the courts. The public prosecution service or any natural or legal person having a legitimate interest to act may also refer a matter to the ARJEL.

The ARJEL sends **a formal notice**, by any means whereby receipt thereof can be established, to unauthorised online gaming or betting operators (i.e. operators which have not been granted an exclusive right or a licence as specified in the law) and to any individual offering online gambling or games of chance in contravention of the legal and regulatory provisions, with a reminder of the provisions relating to the penalties laid down and the blocking and/or removal of websites, requiring those operators to comply with this prohibition and requesting their observations within eight days.

---

11 Decree 2015-125 of 5 February 2015 on the blocking of sites inciting or condoning terrorism and sites circulating pornographic images and representations of minors, JORF, 6 February 2015. This decree entered into force on 7 February 2015.

12 A similar Article is contained in the Law of 29 July 1881 on Freedom of the Press, concerning some of the offences it contains, in particular offences of inciting discrimination, hate and violence, offences of condoning crimes and contesting crimes against humanity (Art. 50-1 of the Law of 29 July 1881).

Once this deadline has passed, if the operator in question has failed to terminate the betting, gambling or games of chance activity, the president of the ARJEL may **refer the matter to the president of the Paris Regional Court** for the latter to issue an injunction ordering the **website hosting services and ISPs to terminate access to this service.**

The president of the ARJEL may also refer the matter to the president of the Paris Regional Court for the latter to issue an injunction ordering any measure to be taken to **ensure that the site of the operator in question can no longer be indexed** by a search engine or directory.

2.1.2. Protection of intellectual property rights

The Intellectual Property Code (hereinafter the "IPC") contains provisions specifically relating to the field of intellectual property rights and which provide for the blocking of websites whose activities violate intellectual property rights.

For example, Article L.336-2 IPC provides that where there is an infringement of copyright or a neighbouring right caused by the content of an online public communication service, the regional court, ruling if need be in summary proceedings, may order, at the request of holders of copyright over protected works or property or of the beneficiaries of the said holders, or of companies responsible for the collection and apportionment of copyright fees or professional defence organisations, **all measures to prevent or put an end to such infringement of copyright or a neighbouring right by any person able to help resolve the issue**.[13] These measures may include blocking and filtering measures, and removal from the Internet of the infringing items.

It was on the basis of Article L.336-2 IPC that the Paris Regional Court delivered a judgment on 4 December 2014 ordering the ISPs to block access in France to websites of the Pirate Bay network, which were entirely or virtually entirely dedicated to making available audio recordings without the consent of the authors, which constitutes a violation of copyright, as provided for in Article L.336-2 IPC.[14] The operative provisions of the judgment, in an interlocutory injunction, stipulated that the blocking measure had to be implemented by the ISPs at the latest fifteen days following notification of the judgment and for a period of 12 months following implementation of the measure. It was also on this legal basis that the Paris Regional Court, in an interlocutory judgment, ordered the T411 website to be blocked by the various ISPs on the ground that its activity was entirely or virtually entirely dedicated to making available audio recordings without the consent of the authors, which constituted a violation of copyright.[15]

In the field of **trademark infringement** too, measures may be taken to prevent or put an end to an infringement. On the Internet, the courts may order intermediaries, such as online trading site operators, to ensure that offers of counterfeit products are no longer accessible.

In urgent proceedings, Article L.716-6 IPC provides that the civil court may:

---

13 Similarly, Article 336-1 IPC provides that "where a software application is mainly used to unlawfully make available works or property protected by a literary and artistic property right, the president of the Regional Court may, ruling in summary proceedings, order, subject to a penalty, any measures in keeping with the state of the art that are necessary for the protection of this right.
The measures thereby imposed must not be such as to radically alter the fundamental features or initial purpose of the software."

14 Paris Regional Court, 3rd Division, urgent applications section, 4 December 2014, No. 14/03236, available (in French only) on www.legalis.net (accessed on 30 April 2015).

15 Paris Regional Court, 3rd Division, 1st Section, 2 April 2015, No. 14/08177, available (in French only) on www.legalis.net (accessed on 8 April 2015).

> "order, if need be subject to a penalty, the alleged counterfeiter or the intermediaries whose services he or she uses, to take measures to prevent an imminent violation of the rights conferred by the title or to prevent continuation of the allegedly infringing acts."[16]

In addition, where the circumstances demand that such measures be taken without the presence of both parties, in particular where any delay would cause irreparable damage to the petitioner, the court may also "order any urgent measures, upon ex parte application".[17]

Accordingly, the court may prohibit the continuation of the allegedly infringing acts or order the seizure or handing over to a third party of the products suspected of infringing the rights conferred by the title, to prevent their being introduced into commercial circulation.[18] The civil courts may also order the ISPs to block a website offering infringing products for sale, or the hosting service or editor to remove the products from the site in question.

In these summary proceedings on trademark counterfeiting, the petitioner has to adduce evidence of the likely nature of the interference with his or her rights or of the fact that such interference is imminent. In this connection, in a case in which the Swiss Life Health Insurance company brought an action against one of its brokers for trademark infringement in application of Article L.716-6 IPC, the urgent applications judge refused to order the cessation of the counterfeiting in question – by means of removal of the trademarks from the websites concerned – holding that the petitioner had not adduced evidence of the likely nature of trademark infringement, particularly as it had been impossible to identify the editor of the website on which the infringement had been detected.

With regard to the substance of trademark infringement litigation, under Articles L.716-13 and L.716-15 IPC the courts may order the removal, destruction or confiscation of infringing products together with the equipment and instruments relating to these infringements. On the Internet, however, these measures relate to the hosting services and editors of the websites in question (see Section 2.2.2, below); they are ordered by both the civil and criminal courts.

Concerning the protection of **domain names**, where the infringing item is a domain name, the owner of the infringed trademark may apply for cancellation of registration of the domain name or even for the domain name at issue to be transferred to his or her ownership,[19] which entails a blocking of the website corresponding to the domain name in question.

Lastly, on 11 March 2015, the Minister for Culture and Communication presented to the Council of Ministers a paper on the fight against piracy on the Internet. One of the aims of this Action Plan is to extend the use of the urgent procedure, the immediate emergency procedure, individual applications and joint applications among the available judicial remedies in order to monitor over time the effectiveness of blocking measures issued against technical intermediaries. The plan also suggests establishing regional centralisation of judicial action in this field.[20] However, at the time of writing of this report, these measures are just in the planning stage.

2.1.3. Protection of privacy and personal data

---

16 Article L.716-6 IPC.

17 Ibid.

18 Ibid.

19 Article L.45-2, 2 and L.45-6 of the Post and Electronic Communications Code. See also: Comm. 9 June 2009, Prop. Ind. 2009, Comm. 61 (available only in French).

20 Ministry of Culture and Communication, Anti-Piracy Action Plan, 11 March 2015, available (in French only) on www.culturecommunication.gouv.fr *(accessed on 30 April 2015).*

Measures to end violations of privacy on the Internet, violations of the right to one's image and of an individual's personal data focus above all, quite naturally, on removing the unlawful content from the Internet. This will be looked at in greater detail in Section 2.2.3.

However, in application of Article 9 of the Civil Code, the civil courts may order, including in summary proceedings, any measures to prevent or put an end to an infringement of the right to privacy. Nonetheless, other legal bases for action are more appropriate to digital material. For example, as stated in Section 2.1.1, in application of the LCEN, ISPs (as well as other players for that matter) may be obliged, **by the courts**, to put an end to or prevent the prejudice caused by the content of a website.

The issue of the extent of the judge's powers vis-à-vis ISPs under Article 6.I.8 LCEN was raised before the French courts in a case in which the Ministry of the Interior sought to take action against a series of websites alleging police violations and in so doing, disseminating insulting and defamatory remarks about the public authorities (in particular the police) along with personal data collected without the knowledge of the persons concerned. In a decision of 10 February 2012, the Paris Regional Court ordered one of the sites concerned to be blocked by the different ISPs for six months. In so doing, in accordance with the provisions of Article 6.I.8 LCEN, the court held that it had been impossible to identify the hosting services or the content editors of the site in question despite the steps taken by the Ministry of the Interior to this effect. With regard to other websites to which the court case also referred, the court decided that blocking was not appropriate as the Ministry of the Interior had not indicated whether or not it had attempted to identify the hosting services and editors.

2.1. Removal of unlawful Internet content

2.1.1. Protection of national security and morality

As stated above (see Section 2.1.1), French law provides for the possibility for the civil courts, upon summary or ex parte application, to order hosting services or ISPs to take any appropriate measures to prevent or halt harm or damage resulting from the content of an online public communication service. As stipulated in Article 6.I.8 LCEN, the courts will first of all order the hosting services to take these measures and only if the latter are unknown will they turn to the ISPs.

In addition, the LCEN lays down a system for the removal, by hosting services, of unlawful content on the Internet. This system, to be found in several jurisdictions, is known by the term "notice and take-down". In this connection, the LCEN provides that the civil liability of hosting services cannot be incurred "on account of the activity or information stored at the request of a recipient of the service if they do not have actual knowledge of their unlawful nature or are unaware of facts or circumstances from which the unlawful nature is apparent, or if, upon obtaining such knowledge or awareness, they have acted promptly to remove or disable access to that information".[21]

Accordingly, there can be no removal of Internet content if the hosting service has no **actual knowledge of the unlawful nature** of the content. To facilitate proof of actual knowledge of the unlawful nature of the content, the law lays down a **rebuttable presumption of knowledge** of the facts at issue by the hosting service when the latter receives notification of the various items listed by the LCEN, such as the date, description and location of the facts, the reasons why the content must be removed together with a reference to the legal provisions and the factual justifications, a copy of the correspondence sent to the author or editor of the information demanding the suspension, removal or modification of the content, or supporting evidence that it has been

[21] Article 6, I, 2 LCEN.

impossible to contact the author or editor. This optional notification procedure is a means of demonstrating the hosting service's awareness of the unlawful content hosted and obliging the host to take prompt action. However, in accordance with the text of the law, while notification may lead to a presumption of actual knowledge, such awareness can also be proved by other means.

It is not enough to notify the existence of unlawful content for the hosting service to be recognised as liable for not having promptly removed the said Internet content. The hosting service has a **margin of appreciation**: the service is free to remove the content notified as unlawful but is only obliged to do so in particular circumstances. In application of an interpretative reservation by the Constitutional Council:

> "These provisions [relating to the liability of hosting services] should not have the effect of incurring the liability of a hosting service that has not removed information notified as being unlawful by a third party if such information is not manifestly unlawful or if its removal has not been ordered by a court".[22]

Therefore, where there is no court order, a hosting service is not obliged to disable access to unlawful content on the Internet unless such content is of a **manifestly unlawful nature**.[23] The hosting service will accordingly not be punished for having failed to remove content which was not obviously unlawful. Initially, the concept of manifestly unlawful content was intended to relate solely to child pornography, incitement to racial hatred or condoning crimes against humanity. However, several court decisions have had the effect of extending the concept of manifestly unlawful content to other categories, such as in the field of copyright infringement or defamation (see Sections 2.2.2 and 2.2.3). One author maintains that the manifestly unlawful nature of disputed information is the consequence of a deliberate violation of an explicit and unambiguous positive law provision.[24] Moreover, in view of the recent legislative amendments to strengthen the fight against terrorism, it is reasonable to consider that any hosted images or statements which constitute criminal offences of inciting or condoning terrorism are manifestly unlawful content, obliging hosting services to disable access to such content even without any court intervention, failing which they could be held civilly and criminally liable.

With regard to these offences of child pornography or acts inciting or condoning terrorism, the LCEN also provides for blocking via a mere administrative decision of the OCLCTIC. Indeed, in application of Article 6-1.1 LCEN, the OCLCTIC can ask the hosting services of the websites in question or editors to remove these contents from the Internet. In so doing, the administrative authority has to simultaneously inform the ISPs. If there is no removal of these contents within 24 hours, the OCLCTIC can notify the ISPs of the list of the websites concerned, who must then block access to these addresses immediately.

In addition, in application of the LCEN, the OCLCTIC may notify the operators of search engines or directories of the electronic addresses of the sites involved in these two types of criminal offence, who are then required to take all appropriate steps to **stop the indexing** of the sites in question.

Supplementing the Decree of 5 February 2015, Decree No 2015-253 of 4 March 2015 specifies the procedures for delisting sites in breach of the provisions of Articles 227-23 and 421-2-5 of the Criminal Code. By virtue of this decree, the OCLCTIC is authorised to notify search engine or directory operators of the electronic addresses of these unlawful sites for the purposes of delisting. Delisting

---

22 Constitutional Council, 10 June 2004, No. 2004-496 DC, available (in French only) on www.conseil-constitutionnel.fr (accessed on 30 April 2015).

23 See Paris Court of Appeal, 4 April 2013, Pole 1, available (in French only) on www.legalis.net (accessed on 30 April 2015).

24 Castets-Renard C., *Droit de l'internet: droit français et européen*, Paris, 2012, p. 295, No. 789.

may also be requested even for sites subject to an existing administrative blocking request. Like the ISPs, the search engine or directory operators, who cannot amend the list of addresses and must preserve the confidentiality of the data entrusted to them, have 48 hours to take any appropriate measures to stop the indexing of the websites concerned. The OCLCTIC must in addition, verify at least once every three months that these addresses continue to link to unlawful content.

2.1.2. Protection of intellectual rights

Some of the measures for removing website content on the ground that it is in violation of intellectual rights are based on the same provisions as the blocking measures looked at above (see Section 2.1.2), for example court orders to halt or prevent the prejudice caused by a website, in application of Article 6, I, 8 LCEN (see Section 2.1.2 above).

Nonetheless, the field of protection of intellectual rights contains legal provisions which have the same effect but which are specific to this area. For example, Article 336-2 IPC provides that where there is an infringement of copyright or a neighbouring right caused by the content of an online public communication service, the regional court, ruling if need be in a summary procedure, may order, at the request of holders of copyright over protected works or property or of the beneficiaries of the said holders, or of companies responsible for the collection and apportionment of copyright fees or professional defence organisations, **all measures to prevent or halt to such infringement of copyright or a neighbouring right by any person able to help resolve the issue**

In addition, as the "notice and take-down" procedure referred to above (see Section 2.2.1) is of general application, it can also be applied with regard to websites in breach of intellectual rights. A user may inform the web host of the existence of unlawful content; once notified, the host must remove the manifestly unlawful content, but has discretion when it comes to removing content which is not *manifestly* unlawful. In the field of intellectual rights, it will often be difficult to establish the *manifestly* unlawful nature of the content of a site. Assessing the infringing nature of the use of a trademark or work more often than not necessitates evaluating the circumstances surrounding the dissemination at issue, in which on principle the host, as technical intermediary, has no direct involvement. Accordingly, the Paris Regional Court ruled on the infringement of a trademark in a case brought by companies belonging to the H&M group against Google and YouTube regarding the hosting by the latter of videos linking the H&M brand to images of blood and words such as "Hate and Death" and "Harassment and Death". Ruling in summary proceedings, the court held that the use of the trademark on the website in question "sought neither to designate nor promote a product for sale, but merely to inform website visitors of the possible conduct of the company owning the trademark. Consequently, its aim was not to inform consumers about the nature or origin of a product and was not used in the course of trade"; for this reason it was held that the infringement of the trademark was not apparent and the host had not been at fault for not removing the content at issue, which was not manifestly unlawful. However, by way of a compromise, the court ordered that the content, the manifestly unlawful nature of which had not been established, be either removed or made inaccessible on the ground that maintaining its accessibility would cause the petitioner damage which it would be preferable to avoid.[25]

Other provisions in the IPC authorise the courts to order specific measures such as the **confiscation or destruction** of counterfeit products or products which infringe copyright, and the **withdrawal of such products from commercial circulation**. For example, Article L.331-1-4 IPC provides that:

> "in the event of a civil conviction for infringement of a copyright or neighbouring right or the rights of a database producer, the court may order, at the request of the injured party, that

[25] Paris Regional Court, summary proceedings, 4 April 2013, RLDI 2013/94 No. 3129.

> the items made or manufactured in breach of these rights, the media used to collect the data unlawfully extracted from a database and the equipment or instruments predominantly used for their production or manufacture be withdrawn or permanently removed from commercial circulation, destroyed or confiscated for the benefit of the injured party."

The same applies in the field of trademarks. Article L.716-13 IPC provides that:

> "Natural persons guilty of [certain trademark infringement offences, in particular the import, export or production of goods under an infringing trademark for the purposes of selling, supplying, offering for sale or hiring of the said goods, or the holding without legitimate reason of goods under an infringing trademark, reproducing, imitating, using a trademark or knowingly delivering a product or service other than that which has been requested under the registered trademark][26] may be ordered to remove, at their expense, from commercial circulation, the items deemed to be infringing and any item which has been used or was designed to commit the offence.
>
> The court may order the destruction, at the expense of the convicted party, or the return to the injured party of the objects and items withdrawn from commercial circulation or confiscated."

Accordingly, insofar as they can oblige the hosting service or editor of the site to remove the items concerned form the online sales website, these equate to measures for the removal of unlawful Internet content. However, even where there is no specific provision making it possible to prohibit, by order, the putting online of infringing items, the case law indicates that measures prohibiting continuation of an activity deemed to be in violation of the provisions on the protection of intellectual rights is one means to ensure full compensation for the damage, the relevance of which

---

[26] Article L.716-9 IPC: "Any person who, for the purpose of selling, supplying, offering for sale or hiring goods under an infringing trademark:
a) imports, exports, re-exports or trans-ships goods under an infringing trademark;
b) reproduces on an industrial scale goods presented under an infringing trademark;
c) gives instructions or orders to commit the acts set out in a) and b) above,
shall be liable to four years' imprisonment and a fine of €400,000.
Where the offences provided for under this Article have been committed by an organised criminal group or on an online public communication network or where the facts relate to goods posing a danger to the health or safety of human beings or animals, the penalties shall be increased to five years' imprisonment and a fine of €500,000."
Article L.716-10 IPC: "The penalty of three years' imprisonment and a fine of €300,000 shall be handed down to any person who:
a) holds without legitimate reason, imports or exports goods under an infringing trademark;
b) offers for sale or sells goods presented under an infringing trademark;
c) reproduces, imitates, uses, affixes, removes or modifies a trademark, a collective trademark or a collective mark of certification in violation of the rights conferred by the registration thereof and the prohibitions deriving therefrom. The offence, laid down in this present paragraph c) shall not be considered to have been constituted where prescription assistance software makes it possible, should the prescriber so wish, to prescribe using an international non-proprietary name, in accordance with the rules of good practice provided for in Article L. 161-38 of the Social Security Code;
d) knowingly delivers a product or provides a service other than that which has been requested under a registered trademark.
The offence, under the conditions provided for in d) shall not be considered to have been constituted if the pharmacist exercises the capacity of substitution provided for under Article L. 5125-23 of the Public health Code.
Where the offences provided for in a) to d) have been committed by an organised criminal group or on an online public communication network or where the facts relate to goods posing a danger to the health or safety of human beings or animals, the penalties shall be increased to five years' imprisonment and a fine of €500,000."

the civil courts have the authority to assess, even where there is no text providing for such. The Paris Regional Court made such an assessment in a case in which the French railway company complained of the infringement of its trademarks, by the editor of a website, for purposes prejudicial to the company.[27]

Lastly, with regard to the hosting service and the indexing service preventing previously removed unlawful Internet content from being once again put online, in particular using a different URL, the Court of Cassation held, in three judgments, that neither the hosting service nor the indexing service could be held liable for not having prevented previously removed unlawful content from being put back online, if they were not notified that unlawful content, which had already been removed in accordance with the "notice and take-down" procedure, had been put back online. In its ruling, the Court of Cassation held that obliging Internet stakeholders to prevent any reposting would mean subjecting them to a general obligation to monitor the images they stored and to seek out unlawful reproductions, and ordering them to set up, in a way that was disproportionate to the aim pursued, of a blocking mechanism with no limitation in time.[28]

2.1.3. The protection of privacy-related rights

With regard to violations of privacy, Article 9 of the French Civil Code provides that the civil courts may "without prejudice to the right to compensation for any injury suffered, order any measures (…) to prevent or put an end to a violation of privacy." In urgent cases, these measures may be ordered in summary proceedings. In this connection, the Court of Cassation has stated that the mere finding of a violation is sufficient to warrant urgent proceedings.

Nonetheless, other legal bases for action are more appropriate to digital material. For example, in civil matters the courts may require, upon summary or ex parte application, the hosting services or ISPs to take any measures necessary to prevent or halt harm or damage resulting from the content of an online public communication service (see above, Section 2.1.3). As stipulated in Article 6.I.8 LCEN, the courts will first of all order the hosting services to take these measures and only if the latter are unknown will they turn to the ISPs.

In addition, as the "notice and take-down" procedure referred to above (see Section 2.2.1) is of general application, it can also be applied with regard to websites in breach of the privacy of third parties. A user may inform the web host of the existence of unlawful content; once notified, the host must remove the manifestly unlawful content, but has discretion when it comes to removing content which is not *manifestly* unlawful. In the field of protection of the right to privacy, defamation, etc., it will often be difficult to establish the *manifestly* unlawful nature of the content of a site.

One author maintains that the manifestly unlawful nature of disputed information is the consequence of a deliberate violation of an explicit and unambiguous positive law provision, and gives as an example revisionist and anti-Semitic statements. Case law would appear to adopt a restrictive approach to what is to be regarded as manifestly unlawful content. In the field of defamation, in a case brought by the H&M group against several website hosts, the Regional Court held, in summary proceedings, that an assessment of the potentially defamatory nature of the content of these websites required an analysis of the circumstances prevailing at the time of their

---

27 Paris Regional Court, 3rd Division, 2nd Section, 11 June 2010, available (in French only) on www.legalis.net (accessed on 30 April 2015).

28 Court of Cassation, Civil Division 12 July 2012, Nos. 11-15.165, 11-13.669 and 11-13.666, available (in French only) on www.legalis.net; Casanova A., *La Cour de Cassation préfère le "notice and take down" au "notice and stay down", au risque de voir les ayants droit "knocked down"*, Hebdo édition affaires No. 307, 6 September 2012, Lexbase, No. N3328BTG.

dissemination, in which on principle an operator, as merely a technical intermediary, had no direct involvement. The Court concluded that the hosting services were not at fault, holding that the statements in question, potentially defamatory, were not manifestly unlawful.[29] Similarly, the Paris Court of Appeal held that the dissemination on a website of an article reproducing the petitioner's statements in strongly critical terms was not manifestly unlawful content justifying a removal measure.[30]

Finally, it should be noted that the delisting measures are have recently been recognized French case law[31]. This was inspired by case law of the Court of Justice of the European Union[32] which determined that it is the right of every European national to the removal of content linked to his private life. This means erasing the links to Internet pages on which his or her name or information about him or her appear, without erasing the information from the source site.

2.1.4. Protection of personal data

In the field of personal data protection, the French Data Protection Agency (CNIL) has exceptional powers to halt any processing of personal data which fails to comply with the conditions laid down in Law No. 78-17 of 6 January 1978 on Information Technology, Data Files and Individual Liberties.[33] Concerning the conditions for the processing of personal data, the aforementioned law lays down, depending on the type of processing in question, a system of notification or prior authorisation by the CNIL, or a prohibition of certain data of a personal nature. Accordingly, the CNIL's Restricted Committee can order the data controller to cease the processing at issue where the said processing is subject to the notification requirement, or withdraw authorisation already given by the CNIL prior to the processing. This decision is made following a hearing of all parties and in cases where the data controller has failed to comply with the notice served to him or her by the CNIL.[34] In addition, if the processing of personal data leads to the violation of freedoms, such as human identity, human rights, privacy or individual or public freedoms, the CNIL may initiate an urgent procedure, following which it may decide to interrupt the processing for a maximum period of three months, lock the data in

---

29 Paris Regional Court, summary proceedings, 4 April 2013, available (in French only) on www.legalis.net (accessed on 30 April 2015). For further information on this case, see Section 2.2.2 above.

30 Paris Court of Appeal, Pole 1, 2nd Division, 4 April 2013, available (in French only) on www.legalis.net (accessed on 30 April 2015).

31 Paris Regional Court, summary proceedings, 19 December 2014, Marie France M. v. Google France and Google Inc., available (in French only) on www.legalis.net.

32 CJEU, Grand Chamber judgment C-131/12, 13 May 2014, Reference for a preliminary ruling, Google Spain SL and Google Inc. v. AEPD and Mario Costeja González, available on www.curia.europa.eu.

33 Law No. 78-17 of 6 January 1978 on Information Technology, Data Files and Individual Liberties, available on www.legifrance.gouv.fr (accessed on 30 April 2015). Article 2 sets out the scope of the law. It applies to "the automatic processing of personal data as well as to the non-automatic processing of personal data that are or may be contained in a personal data filing system, with the exception of processing carried out for the exercise of exclusively private activities, where the data controller meets the conditions [of the territorial scope provided for in in Article 5].
Personal data means any information relating to a natural person who is or can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to them. In order to determine whether a person is identifiable, all the means that the data controller or any other person uses or may have access to should be taken into consideration.
Processing of personal data means any operation or set of operations in relation to such data, whatever the mechanism used, especially the obtaining, recording, organisation, retention, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, deletion or destruction."

34 Article 45 I of Law No. 78-17 of 6 January 1978 on Information Technology, Data Files and Individual Liberties, available on www.legifrance.gouv.fr (accessed on 30 April 2015).

question for the same maximum period, or, where the processing in question is carried out by the state, inform the Prime Minister so that the necessary measures can be taken to end the violation identified. Lastly, in the event of serious and immediate violation of the above rights and freedoms, the Chair of the CNIL may request, by means of an urgent application, the competent court to order, if necessary applying a daily penalty, any security measures necessary for the protection of these rights and freedoms.[35]

3. Procedural matters

3.1. Administrative blocking and removal

The procedure leading to the administrative blocking of websites disseminating images constituting a criminal offence under the child pornography legislation or the legislation relating to incitement to or condoning of acts of terrorism, as provided for in the LCEN, is described in the Decree of 5 February 2015 on the **blocking of sites inciting or condoning terrorism and sites circulating pornographic images and representations of minors.**

Under this Decree of 5 February 2015, the administrative authority responsible for the blocking and/or removal of websites is the Directorate General of the **National Police**, the **Central Office for Combating ITC-related Crime** (the "OCLCTIC"). Within this administrative authority, only **certain individually designated officers** are authorised by the Head of the Office to implement the blocking procedure.[36]

In application of Article 6-1 LCEN, the OCLCTIC must first of all request removal of the unlawful content from the hosting service and/or content editor. In so doing, it must, in pursuance of Article 6-1.1 LCEN, **simultaneously inform the ISPs**. The hosting service and/or editor must remove the unlawful content within 24 hours.

In cases where the OCLCTIC is unable to contact the editor or hosting service in order to request removal of the unlawful content – despite the fact that the details of these individuals must by law be publicly available – the OCLCTIC can contact the ISPs directly and demand that the website be blocked, without first of all asking the host or editor to remove the content. The OCLCTIC also asks the ISPs to block access to the site if the content has not been removed by the host or editor within the 24-hour deadline.

The **electronic addresses** to be blocked **are forwarded** to the ISPs **through secure channels** ensuring the integrity and confidentiality of the information. In addition, the electronic addresses in question comprise either a domain name or the name of the host in the form of a domain name preceded by the name of the server. The **ISPs cannot modify the list of electronic addresses to be blocked**, either by adding, deleting or altering addresses and are obliged to maintain the confidentiality of the data entrusted to them.

Users of the online public communication services to which access has been blocked are directed to a **Ministry of the Interior information page**, specifying – for both grounds for blocking (child pornography sites or sites inciting or condoning terrorism) – the reasons for the protection measures and the available remedies. Certain individuals retain access to the electronic addresses of the online public communication services to which access has been blocked. These are the OCLCTIC officers

35 Article 45 II and III of Law No. 78-17 of 6 January 1978 on Information Technology, Data Files and Individual Liberties, available on www.legifrance.gouv.fr (accessed on 30 April 2015).

36 For more information, see Section 2.1.1 above.

individually designated and duly authorised by their senior managers, and a qualified specialist designated by the CNIL, whose role is to ensure compliance with the regulations of the removal and blocking orders and the conditions under which the list of electronic addresses in question is drawn up, updated, notified and used. This CNIL specialist may at any time recommend that the blocking and/or removal measure be terminated if he or she identifies any irregularity. If the OCLCTIC fails to act upon this recommendation, he or she may refer the matter to the competent administrative court, by means of a summary or ex parte application

An administrative or judicial appeal may be lodged against the measure to block the website in question. An administrative appeal (either an internal administrative appeal (*recours gracieux)* or an appeal to a higher body (*recours hiérarchique))* may be lodged against the administrative decision to block a website, following which the administrative authority will be asked to review the file. The *recours gracieux* is brought before the same authority, the OCLCTIC, while the *recours hiérarchique* is brought before the OCLCTIC's higher authority, in this case the Minister of the Interior. If this appeal does not result in a change to the situation, the person who submitted the appeal may file an appeal before the competent administrative court, and then the Administrative Court of Appeal; as a final resort, it is also possible to lodge an appeal on points of law to the Conseil d'Etat.

The OCLCTIC **verifies every three months** that the content of the offending communication service is still unlawful. Where this service is no longer operating or the content is no longer unlawful, the OCLCTIC removes the corresponding electronic addresses from the list and immediately informs the CNIL specialist and the ISPs. The latter must, within 24 hours and by all appropriate means, restore access to the services provided by the electronic addresses removed from the list and the links redirecting to those services.

Decree 2015-125 also provides that **any additional costs** resulting from the obligations placed on ISPs in respect of the administrative blocking of websites will be eligible for **financial compensation paid for by the state**. "Additional costs" refers to the additional investment and specific intervention costs incurred as a result of those obligations.

To obtain compensation, ISPs must forward to the OCLCTIC a document detailing the number and type of the necessary interventions and the cost of any investment carried out. The General Council for the Economy, Industry, Energy and Technology analyses the document submitted, looking at particular at the customary estimated costs in the sector concerned. Upon production of an invoice, the state pays compensation equivalent to the additional cost approved by the aforementioned General Council.

Decree No. 2015-253 of 4 March 2015, in application of the new provisions of the LCEN introduced by the law of 13 November on scaling up counter-terrorism provisions, **specifies the procedure for delisting sites inciting or condoning terrorism and sites circulating pornographic images and representations of minors. By virtue of this decree, the OCLCTIC notifies search engine or directory operators** of the electronic addresses **for which indexing must be blocked in application of Article** 6-1 LCEN. These addresses are forwarded through secure channels, guaranteeing the confidentiality and integrity of the information. Within 48 hours of receiving the notification, the search engine or directory operators must take every appropriate measure to stop the indexing of those addresses. They must not modify the list of electronic addresses, either by adding, deleting or altering addresses and are obliged to maintain the confidentiality of the data entrusted to them. The specialist designated by the CNIL monitors compliance with the regulations of the de-indexing procedures in the same way as in respect of the administrative blocking of websites. The available remedies are also the same as in the case of the administrative blocking of websites.

3.2. Court-ordered blocking and removal

The other content removal or website blocking measures, described above, are ordered by the courts: essentially, the courts can order, upon summary or ex parte application, all measures to prevent or halt the harm caused by the content of a website (Article 6, I, 8 LCEN),[37] this is also possible in respect of copyright and neighbouring rights (Article 336-2 IPC)[38] and violations of privacy (Article 9 Civil Code).[39]

Like any judgment, these court injunctions are notified to the defendants, i.e. the ISPs, the hosting services, content editors, search engine operators etc. If the parties concerned do not comply voluntarily, the court injunctions can, in principle, be enforced. The losing parties may, if necessary, lodge an ordinary-law appeal against judgments delivered at first instance with the Court of Appeal, and then an appeal on points of law with the Court of Cassation.

4. General Internet monitoring

Under the LCEN, **hosting services and ISPs are not subject to a general duty to monitor** the information they transmit or stock, nor to actively seek out facts or circumstances indicating unlawful activities. The fact that there is no obligation was recently confirmed by the Court of Cassation, when it held that obliging Internet stakeholders to prevent any reposting of unlawful content which they have removed following due notification by users would be tantamount to subjecting them to a general duty to monitor the images they stock and to look for unlawful reproductions. This could not be accepted.[40]

The LCEN provides that Internet stakeholders may be required by the courts to engage in **targeted and temporary monitoring**. For example, the Paris Commercial Court, in summary proceedings, ordered the removal of advertisements for perfumes outside the accredited selective distribution network and the introduction, for a six-month period, of a filtering system to identify and remove advertisements for products of the brands concerned.[41]

Internet intermediaries are also required to establish a procedure whereby anyone is able to **bring to their attention** any relevant information for combating crimes against humanity, inciting or condoning acts of terrorism, incitement to racial hatred, hatred of persons on the grounds of their gender, sexual orientation or identity, disability, child pornography, incitement to violence, especially incitement to violence against women and abuse of human dignity.[42] They are also **obliged to inform the competent public authorities** of any unlawful activities notified to them that may be conducted by the recipients of their services.[43]

---

37 See Sections 2.1.1 and 2.1.2.

38 See Sections 2.1.2 and 2.2.2.

39 See Sections 2.1.3 and 2.2.3.

40 Court of Cassation, Civil Division, 12 July 2012, Nos. 11-15.165, 11-13.669 and 11-13.666, available (in French only) on www.legalis.net; Casanova A., *La Cour de Cassation préfère le "notice and take down" au "notice and stay down", au risque de voir les ayants droit "knocked down"*, Hebdo édition affaires No. 307, 6 September 2012, Lexbase, No. N3328BTG.

41 Paris Commercial Court, summary proceedings, 26 July 2007 and 31 October 2007, available (in French only) on www.legalis.net (accessed on 30 April 2015).

42 Art. 6, I, 7, sub-paragraphs 3 and 4 LCEN.

43 Art. 6, I, 7, sub-paragraph 4 LCEN.

In addition, the competent police department in this field, the **OCLCTIC**, monitors the Internet to identify any criminal offences. This monitoring is carried out with a view not only to the prosecution of the perpetrators of criminal offences[44] but also to undertake the department's powers of blocking and/or removal of unlawful content for certain of these offences. As stated above with regard to the administrative removal and blocking measures carried out by the OCLCTIC, this concerns content constituting offences in the field of child pornography and inciting and condoning acts of terrorism.[45] This monitoring is carried out on the OCLCTIC's own initiative and via **a notification mechanism**, available on the Internet, enabling any user to notify any unlawful conduct on the Internet.[46] A platform for receiving, processing and referring these notifications (PHAROS) has also been established, enabling the OCLCTIC officers assigned to this platform to process the notifications in order, where applicable, to prosecute the perpetrators of the criminal offences identified and/or block and/or remove unlawful Internet content.[47]

In addition, the Homeland Security Code (CSI) provides for intelligence gathering with the help of Internet operators in order to protect national security, safeguard the essential elements of the scientific and economic potential of France, prevent terrorism and organised crime and prevent the reorganisation or continued operation of groups dissolved in application of the law. Article L. 851-1 of the CSI authorises for the purposes of the above, **the collecting, with the assistance of ISPs and hosting services, information or documents processed or served on their networks** or electronic communication services, including the technical data relating to the identification of subscription or connection numbers to electronic communication services, the identification of all subscription or connection numbers associated with a given individual, the location of the terminal equipment used and the communications of a subscriber relating to the list of outgoing and incoming calls, the duration and date of the communications.[48]

Moreover, an **Intelligence Bill** was promulgated on 24 July 2015.[49] The aim of this Bill is to provide a general legal framework for the intelligence services, which has been lacking hitherto. In application of this Bill, the Prime Minister may, acting upon an opinion given by a new administrative authority, the National Commission for the Monitoring of Intelligence Techniques, oblige ISPs and hosting services in particular to implement a means of identifying a terrorist threat from the information they process and exclusively on the basis of the automatic processing of anonymous data. This system will be used solely for the purposes of preventing terrorism. The Bill provides that if such a threat were to be identified, the Prime Minister may decide to waive anonymity.[50]

---

44 The police's monitoring resources were increased by the law of 13 November 2014 on scaling up counter-terrorism provisions. Article 706-87-1 of the Code of Criminal Procedure provides that the duly designated officers of the competent police departments are immune from punishment for certain acts carried out in order to identify offences committed on the Internet, such as contact, using a pseudonym, with persons likely to be involved in the commission of crimes.

45 See Sections 2.1.1 and 2.2.1 above.

46 See https://www.internet-signalement.gouv.fr/PortailWeb/planets/Accueil!input.action (accessed on 30 April 2015).

47 Decree of 16 June 2009 establishing the PHAROS notification harmonisation, analysis, cross-reference and orientation platform, available (in French only) on www.legifrance.gouv.fr **(accessed on 30 April 2015).**

48 See also Articles L.246-2 to 5 CSI for further information on the procedure for administrative access to connection data.

49 Law 2015-912 of 24 July 2015 on Intelligence, available on: www.legifrance.gouv.fr (accessed on 17 November 2015).

50 Art. L. 851-3 CSI.

Lastly, after the terrorist attacks on the French newspaper Charlie Hebdo, the Government announced a national plan against racism and anti-Semitism, one aspect of which is the fight against propagation of racism and anti-Semitism on the Internet. In particular, the Government announced its intention to establish a national unit against hatred on the Internet[51]. This Action Plan provides for the setting up of "cyberpatrols" in charge of searching the Internet for the most common racist or anti-Semite content and to initiate the enquiry in view of criminal prosecution of the authors. Our research so far has not enable to identify concrete legislative or regulatory measures in view of setting up such surveillance mechanism.

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

The principle of Freedom of Expression is laid down in the Declaration of the Rights of Man and the Citizen of 1789 to which the Preamble of the Constitution of the French Republic makes explicit reference. Article 11 of the 1789 Declaration is worded as follows:

> "The free communication of ideas and opinions is one of the most precious rights of man. Any citizen may therefore speak, write, and publish freely, except what is tantamount to the abuse of this liberty in the cases determined by law."[52]

Article 1 of the LCEN reasserts the commitment to the freedom of public electronic communication, stating that:

> "The exercise of this freedom may be limited only to the extent required, firstly, by respect for other people's humanity, liberty and property, for the pluralist nature of the expression of thoughts and opinions, and secondly, by the need to safeguard public order, by the requirements of national defence, by the demands of public service, by the technical constraints inherent in the means of communication, and by the need, in the case of audio-visual media, to develop audio-visual production."[53]

The provisions of this law relating to the administrative blocking and removal of unlawful content have nonetheless given rise to lively debate. Decree of 5 February 2015 implementing provisions recently introduced in the LCEN by the Law of 13 November 2014 on scaling up counter-terrorism and the Decree of 4 March 2015 concerning the delisting of websites targeted by this law, are challenged before the administrative supreme court, the Conseil d'Etat.[54]

The system of administrative blocking of **child pornography sites**, first introduced in 2011 by the Law on domestic security guidance and planning ("LOPPSI 2") was, prior to its promulgation, submitted for review by the Constitutional Council, by a number of members of the National Assembly and the Senate. In its decision of 10 March 2011, the Constitutional Council nevertheless approved the system, stating that:

> "the contested provisions only grant the administrative authority the power to limit access to public online communications services in order to protect Internet users if and insofar as they distribute child pornography; that the decision of the administrative authority may be

---

51 Plan national de lutte contre le racisme et l'antisémitisme, 17 April 2015, available (in French only) at : http://www.gouvernement.fr/sites/default/files/liseuse/4040/master/index.htm.

52 Declaration of the Rights of Man and the Citizen of 1789, available on: www.legifrance.gouv.fr (accessed on 30 April 2015).

53 Article 1 IV LCEN.

54 Conseil d'Etat, (Association French Data Network and others), available (in French only) at: www.arianeinternet.conseil-etat.fr.

> challenged at any time and by any interested party before the competent courts, if appropriate in summary proceedings; that, under these conditions, these provisions ensure that the objective of constitutional standing of safeguarding public order is reconciled with the freedom of communication guaranteed under Article 11 of the 1789 Declaration of the Rights of Man and the Citizen in a manner that is not disproportionate."[55]

Accordingly, in the view of the Constitutional Council, the blocking by simply an administrative decision of websites which "distribute child pornography" is a restriction of freedoms, in particular the freedom of expression, which is proportionate to the legitimate aim pursued, namely the safeguarding of public order. In addition, it offers adequate protection against arbitrary decisions and abuse of rights insofar as the administrative decision is circumscribed by law and, in particular, it may at any time be challenged before the courts.

On the strength of this precedent, the government tabled before parliament the Bill on scaling up counter-terrorism provisions, which led to the Law of 13 November 2014 referred to above, and in application of which the OCLCTIC is empowered to block or remove not only child pornography sites but also sites whose content incites or condones terrorism. The advocates of this administrative blocking system that has been introduced maintain that the restriction on freedoms, in particular the freedom of expression, could be justified on national security grounds:

> "We have, in the past, suspended democratic freedoms. The latter cannot be substantively the same in peace and in war. The point is that war has now been declared on us."[56]

In addition, the defenders of this system held that the restriction on the freedom of expression was subject, on the one hand, to review by the qualified specialist in an independent administrative authority (CNIL) and, on the other, to ex post judicial review, which the Constitutional Council ruled was sufficient guarantee, at least with regard to the administrative blocking of sites which "distribute child pornography".[57]

Notwithstanding the above, two institutions delivered a negative opinion on the Bill which eventually became the Law of 13 November 2014. The National Digital Council underlined the disproportionate nature of the measure which, in its view, was not justified by conditions such as an imminent emergency or the absence of any other possible solution. It also stated that:

> "[u]nlike the child pornography provisions, (…) determining the notions of acts of terrorism and defence of terrorism is open to subjective interpretation and bears a real risk of ending up as a mere offence for holding certain views."[58]

For its part, the National Consultative Human Rights Commission took the view that

> "the intervention of the courts is necessary to order and monitor the blocking of a website given that such a measure constitutes serious interference with the freedom of expression

---

55 Constitutional Council, 2011-625, 10 March 2011, paragraph 8, available on www.conseil-constitutionnel.fr (accessed on 30 April 2015).

56 A. Tourret, National Assembly, Debates, 15 September 2014, available (in French only) on www.assemblée-nationale.fr (accessed on 30 April 2015).

57 Constitutional Council, 2011-625, 10 March 2011, paragraph 8, available on www.conseil-constitutionnel.fr (accessed on 30 April 2015). For arguments in favour of the Law of 13 November 2014, see: Mayaud Y., *Terrorisme, Répertoire de droit pénal et procédure pénale*, Dalloz, 2015, No. 481; Ségur P., *La terrorisme et les libertés sur l'internet*, AJDA 2015, p. 160.

58 National Digital Council, Opinion No. 2014-3 on Article 9 of the Bill on scaling up counter-terrorism provisions, 15 July 2014, p. 5., available on www.cnnumerique.fr (accessed on 30 April 2015).

> and communication. Any ex ante restriction on expression on the Internet entails a serious presumption of non-compliance with Article 10 of the ECHR."[59]

In this connection, it recommended that the government assign the authority to block Internet access to a judge for civil liberties, ruling within a very short time-frame, upon referral from the competent prosecution department, in particular further to a notification via PHAROS. This recommendation was not acted upon.

The Commission further held that court intervention for such a restriction was required by the fact that the measure was one for the police (i.e. the organ responsible for criminal investigations) and not the administrative authorities. It emphasised that:

> "the administrative blocking of access to websites inciting or condoning terrorist acts would blur the traditional distinction between the police and the administrative authorities. The new text empowers the administrative authorities to take a blocking decision, even though one or more offences have already been committed. It cannot therefore be considered that this is a purely administrative procedure designed to prevent incitement to or condoning of terrorism. The new provisions undoubtedly fall within the remit of the police, subject to the directives and supervision of the judicial authority, the only body with jurisdiction to prosecute and punish offences. This is therefore a violation of the principle of the separation of powers."[60]

Lastly, it should be noted that in an older decision, the Constitutional Council had criticised a legal provision authorising an independent administrative authority to suspend a subscriber's subscription to the Internet on account of the unlawful use made of this access, on the ground that such a restriction on freedom of expression required the intervention of the courts.[61] This measure was proposed as a means of protecting copyright and neighbouring rights, to penalise the behaviour of Internet users violating this protection. The change in the Constitutional Council's position in its 2011 decision with regard to child pornography sites can be explained by the seriousness of the violations penalised or the importance of the protected rights. The greater the interests and values to be protected by a restrictive measure, the more acceptable the restriction of the freedom of expression would appear to be. This appears all the more relevant that France has already for some time now declared that it was **at war against terrorism**, and, that it has declared the **state of emergency** ("l'état d'urgence") after the terrorists attacks of 13 November 2015[62].

In conclusion, in expectation of the decision of the Conseil d'Etat concerning the decree of 5 February 2015 and the decree of 4 March 2015, **it is not certain that the administrative blocking of websites inciting or condoning acts of terrorism is compatible with the emerging case law of the European Court of Human Rights in this field**. The concepts of incitement to and condoning of terrorism are interpreted on the basis of rules of law and under the dual supervision of the qualified

---

59 National Consultative Human Rights Commission, Opinion on the Bill on scaling up counter-terrorism provisions, 25 September 2014, JORF No. 0231 of 5 October 2014, paragraphs 19-20, available (in French only) on www.legifrance.gouv.fr (accessed on 30 April 2015); see also: Kleitz C., *Internet, sécurité et liberté d'expression: bis repetita placent*, Gaz. Palais, 25 September 2014, No. 268, p. 3; Tréguer F., *La LCEN, le juge et l'urgence d'une réforme*, 27 April 2013, available (in French only) on www.wethenet.eu (Accessed on 30 April 2015); Champeau G., *10 problèmes posés par la censure d'Islamic-News.info*, 16 March 2015, available (in French only) on www.numerama.com (accessed on 30 April 2015).

60 Ibidem. See also : E. Dreyer, *Le blocage de l'accès aux sites terroristes ou pédopornographiques*, Semaine Juridique, Ed. Générale, 6 April 2015, nr. 14, doctr. 423.

61 Constitutional Council, 2009-580 DC, 10 June 2009, paragraph 16 et seq., available on www.conseil-constitutionnel.fr (accessed on 30 April 2015).

62 Decrees nr. 2015-1475, 1476 and 1478 of 14 November 2015 applying the modified Law nr. 55-385 of 3 April 1955 for establishing a state of emergency, J.O. 14-15.11.2015.

specialist within the CNIL first of all, and subsequently by the courts in the event of a judicial appeal against the administrative blocking or removal decision. Such review possibilities seem to ensure sufficient safeguards from the perspective of freedom of expression. However, while the Constitutional Council appears to accept that freedom of expression can be restricted without the intervention of a judicial authority in the case of websites distributing child pornography, this administrative blocking measure nonetheless applies to an objective condition, i.e. the presence of pornographic images involving children. Determining the concepts of incitement to and condoning of acts of terrorism may, however, prove more difficult insofar as it is a more subjective issue.

Lastly, with respect to the fight against hatred speech on the Internet, one should also mention the Opinion of the National Consultative Commission for human rights that was issued on 12 February 2015. In this Opinion, the CNCDH makes several recommendations, among which the amendment of the LCEN in view of distinguishing among the Internet intermediaries those that have an "active role" and impose upon such intermediaries an obligation to proactively detect hatred speech content as well as an obligation to inform the competent authorities of such content; it also recommends the creation of a specific independent administrative authority in charge of assisting host providers and Internet access providers in their task of identifying hatred speech on the Internet[63].

Stéphanie De Dycker, LL.M.
Legal Adviser, Swiss Institute of Comparative Law
30.04.2015

Revised on 30.10.2015 taking into consideration comments from France on this report

[63] Commission nationale consultative des droits de l'homme, Opinion on the fight against online hate speech, 12 February 2015, available at: http://www.cncdh.fr/sites/default/files/15.02.12_avis_lutte_discours_de_haine_internet_en.pdf (15.11.2015).