



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 641-664

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.

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.

SPAIN

Spain is one of those countries which have developed special legislative measures for blocking and removing illegal Internet content.

1. Legal Sources

The legislation regulating the blocking, filtering and removal of Internet content in Spain is found mainly in two laws, one on information society services and the other on intellectual property. Also relevant is criminal law, under which the blocking and interruption of services may be ordered, either preventively or definitively. Other legal instruments exist which also provide for measures of this type. The Personal Data Protection Act and the Gaming Act are two examples. In view of the existence of special legislation on the blocking and removal of illegal Internet content, the measures taken in the specific field of games of chance are not covered in this national report.

1.1. The Information Society Services and Electronic Commerce Act (Ley de servicios de la sociedad de la información y de comercio electrónico - LSSI)¹

The law regulating the blocking, filtering and removal of Internet content is the LSSI, which transposes Directive 2000/31/EC and applies to remote electronic services provided for a fee by information society service providers at the individual request of the recipient (even if the service to the consumer is free).²

In parallel with the general principle of the **free provision of services** which exists in the information society, Article 8 LSSI provides for a series of restrictions. Article 8 LSSI is derived from Article 3.4 of Directive 2000/31/EC, under which Member States may take measures to restrict the freedom to provide information society services. The restrictive measures may be taken in respect of content detrimental to **public policy**, the protection of **public health** and the protection of **consumers and users**, respect for **human dignity, non-discrimination**, the protection of **young people and children** and **intellectual property** rights (cf. sections 2.1 and 2.2). On this subject the legal authorities emphasise that the adoption of measures restricting freedom in the information society under the LSSI is subject to the legal provisions regulating other areas, such as unfair competition, intellectual property, the protection of private life, etc.³ The penultimate paragraph of Article 8.1 LSSI⁴ provides as follows:

“When the restrictive measures mentioned in this paragraph are adopted and implemented, the guarantees, norms and procedures provided for by law in order to **protect the right to private, personal and family life, personal data, freedom of expression and freedom of information**, where these may be affected, must be respected in all circumstances” (our emphasis).

¹ Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, available at http://noticias.juridicas.com/base_datos/Admin/l34-2002.html (27.02.15).

² Excluding services provided by voice telephone, fax, telex, simple exchanges of information by e-mail, television and radio broadcasting and teletext.

³ P. Asensio, *Derecho Privado de Internet*, 5^è. ed., Pamplona 2015, p. 150.

⁴ Art. 8.1 LSSI, penultimate paragraph: « En la adopción y cumplimiento de las medidas de restricción a que alude este apartado se respetarán, en todo caso, las garantías, normas y procedimientos previstos en el ordenamiento jurídico para proteger los derechos a la intimidad personal y familiar, a la protección de los datos personales, a la libertad de expresión o a la libertad de información, cuando estos pudieran resultar afectados ».

One author notes that from the point of view of legislative methods such reference to sources external to the LSSI creates a “certain confusion”.⁵

In addition to Article 8 LSSI five more articles regulate the obligations and responsibilities of the different information society actors:

- **Intermediary service providers.** Under Article 11 LSSI these are required to cooperate with the competent judicial or administrative bodies (cf. sections 2.1 and 3)⁶ and, where necessary, **remove** content deemed unfit. The measures provided for in this article must be “objectively proportional and non-discriminatory” (cf. section 5) and may be adopted preventively or to enforce decisions (Article 11.4 LSSI).
- **Network operators and Internet access providers.** Article 14 LSSI provides that these operators are not responsible for the content provided by the users of their services, unless they actually modify or choose that content. Purely technical changes to content do not count.
- **Service providers who make temporary copies of data.** Under Article 15 LSSI these are not responsible for the content, provided that they do not modify the information, that they give access only to those users who meet the conditions laid down by law, that they respect the standards generally applicable and accepted in the sector in updating the information and that they do not interfere with the lawful use of technologies generally accepted and used for data acquisition in the sector. Article 15 e) LSSI⁷ specifically mentions the obligation to **remove** or **block** information when the operators are **effectively aware**:
 - a) that Internet content has been removed from the website where it was initially posted,
 - b) that access to said content has been rendered impossible, or
 - c) that a competent court or administrative body has ordered the removal of the content or the blocking of access to it.

⁵ P. Asensio, op. cit., p. 150.

⁶ The annex to the LSSI defines a “competent body” as “any judicial or administrative authority, at the State, Autonomous Community or local level, or public body dependent thereon, acting within the sphere of competence assigned to it by law”: « todo órgano jurisdiccional o administrativo, ya sea de la Administración General del Estado, de las Administraciones Autonómicas, de las Entidades locales o de sus respectivos organismos o entes públicos dependientes, que actúe en el ejercicio de competencias legalmente atribuidas ».

⁷ Art. 15 LSSI : « Los prestadores de un servicio de intermediación que transmitan por una red de telecomunicaciones datos facilitados por un destinatario del servicio y, con la única finalidad de hacer más eficaz su transmisión ulterior a otros destinatarios que los soliciten, los almacenen en sus sistemas de forma automática, provisional y temporal, no serán responsables por el contenido de esos datos ni por la reproducción temporal de los mismos, si:

- a) No modifican la información.
- b) Permiten el acceso a ella sólo a los destinatarios que cumplan las condiciones impuestas a tal fin, por el destinatario cuya información se solicita.
- c) Respetan las normas generalmente aceptadas y aplicadas por el sector para la actualización de la información.
- d) No interfieren en la utilización lícita de tecnología generalmente aceptada y empleada por el sector, con el fin de obtener datos sobre la utilización de la información, y
- e) Retiran la información que hayan almacenado o hacen imposible el acceso a ella, en cuanto tengan conocimiento efectivo de:
 - 1.º Que ha sido retirada del lugar de la red en que se encontraba inicialmente.
 - 2.º Que se ha imposibilitado el acceso a ella, o
 - 3.º Que un tribunal u órgano administrativo competente ha ordenado retirarla o impedir que se acceda a ella».

In such cases the operators will not be held responsible for **having removed** the information in question or rendered access to it impossible. They will, on the other hand, be held responsible for not having removed it if they were effectively aware of the aforementioned facts.

- **Hosting and storage service providers.** Article 16 LSSI contains provisions on the removal by these providers of content which is illegal or detrimental to property or rights of a third party which qualify for compensation (cf. section 2.2).
- **Service providers who offer links to search tools or content.** Article 17 LSSI mentions the obligation for these providers, under certain conditions, to **delete** or **block** links to content which is illegal or detrimental to property or rights of a third party which qualify for compensation (cf. section 2.2.).

1.2. The Intellectual Property Act (*Ley de Propiedad Intelectual - LPI*)⁸

Provisions concerning the **removal** and **suspension** of content are also found in the LPI. Article 158 ter LPI contains a series of provisions on such matters and in particular on the appointment of the Second Section of the Intellectual Property Commission as the body responsible for protecting intellectual property rights from violation by information society service providers (cf. sections 2.1 and 2.2). Article 158 ter LSSI lays down the powers of this body which, where appropriate, can propose the removal, blocking or interruption of an Internet service. The procedure before the Second Section of the Intellectual Property Commission is explained in Articles 13-24 of Royal Decree 1889/2011 of 30 December 2011⁹ (see section 3).

Lastly, the **enforcement** of decisions of the Second Section of the Intellectual Property Commission requires **judicial authorisation** under Article 122 bis of the Administrative Procedure Act (LPCA) (cf. sections 2.1 and 3).¹⁰ This is considered a guarantee of lawfulness.

⁸ Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia, available at http://noticias.juridicas.com/base_datos/Admin/rdleg1-1996.html (27.02.15).

⁹ Real Decreto 1889/2011, de 30 de diciembre, por el que se regula el funcionamiento de la Comisión de Propiedad Intelectual, available at http://noticias.juridicas.com/base_datos/Admin/rd1889-2011.html (03.03.15).

¹⁰ Law 29/1998, of 13 July, *Reguladora de la Jurisdicción Contencioso-administrativa*, available at: http://noticias.juridicas.com/base_datos/Admin/l29-1998.t5.html#a122b (02.03.15). One important field in Spain is online gambling. Article 47 of the Gaming Act (LJ - Law 13/2011 of 27 May 2011) provides for measures in respect of intermediary service providers. The National Gaming Commission is responsible for “avoiding” the exercise of illegal gambling activities by information society service providers (Article 47 LJ). The Gaming Commission can adopt interim or final measures to stop illegal gambling activities on the Internet or have unauthorised gambling content removed. Under paragraph 3 of Article 47 LJ the Commission can order intermediary service providers to suspend the service or take it down in keeping with Article 8 LSSI. The measures taken must be proportionate and non-discriminatory. The Gaming Act (*Ley 13/2011, de regulación del juego*), is available at: http://noticias.juridicas.com/base_datos/Admin/l13-2011.t6.html#a42 (03.03.15).

1.3. The Personal Data Protection Act (*Ley Orgánica de Protección de Datos de Carácter Personal - LOPD*)¹¹

The LOPD contains two articles relating, among other things, to the deletion of personal data. They are articles 16 and 18 LOPD, which enshrine the right of persons concerned by certain stored data to request the deletion thereof (cf. section 2.1.2.).

1.4. The Spanish Criminal Code (*Código Penal Español - CPE*)¹²

The Internet lends itself to the commission of various types of crime (drug trafficking, terrorism, paedophilia, illegal gambling, violation of intellectual property rights, etc.). Article 33.7 CPE provides, in respect of legal entities, for the **suspension of their activities** and the **closing** of the establishment concerned for a period of up to 5 years, as well as a ban – temporary or final – on engaging in the future in any activities that facilitated, served as a cover for or served to commit the crime. Article 129.1 CPE extends the application of these measures to companies, organisations, groups of people and “any other entity that has no legal status”.

Following a reform of the Spanish Criminal Code by the Organic Law of 30 March 2015¹³ (Act No. 1/2015, amending the Criminal Code), which entered into force on 1 July 2015, a new provision allows the courts to order the **removal** or **blocking** of Internet sites for, *inter alia*, posting content **inciting hatred** (cf. section 2.1.2). Article 510 CPE – which bans the promotion and dissemination of hate speech of a racist, anti-Semitic, religious, ideological, etc. nature – is one of the provisions amended by Act No. 1/2015. The new version of Article 510 CPE provides, in paragraph 6,¹⁴ for the courts to order the destruction, deletion or removal of books, archives, documents, articles and “any type of support by which the offence was committed”. When the offence was committed using **information technology** and means of communication, the **withdrawal of the content** will be ordered. Where content “of a predominantly hate-inciting nature” is disseminated via an Internet access portal or a service of the information society, the court will order the service to be **blocked or interrupted**.

In the fields of **child pornography and the protection of people with disabilities**, Act No. 1/2015¹⁵ provides for measures to block or remove harmful Internet content (cf. section 2.2.). The same applies to violations of intellectual property rights (cf. section 2.2).

¹¹ Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, available at http://noticias.juridicas.com/base_datos/Admin/lo15-1999.html (04.023.15).

¹² Ley Orgánica 10/1995, de 23 de noviembre, de modificación del Código Penal, available at http://noticias.juridicas.com/base_datos/Penal/lo10-1995.html (09.03.15).

¹³ Ley Orgánica 10/1995, de 23 de noviembre del Código Penal, modificado por art. Único.235 de Ley Orgánica núm. 1/2015, de 30 de marzo. RCL\2015\439 (private database).

¹⁴ Art. 510.6) CPE: « El juez o tribunal acordará la destrucción, borrado o inutilización de los libros, archivos, documentos, artículos y cualquier clase de soporte objeto del delito a que se refieren los apartados anteriores o por medio de los cuales se hubiera cometido. Cuando el delito se hubiera cometido a través de tecnologías de la información y la comunicación, se acordará la retirada de los contenidos. En los casos en los que, a través de un portal de acceso a internet o servicio de la sociedad de la información, se difundan exclusiva o preponderantemente los contenidos a que se refiere el apartado anterior, se ordenará el bloqueo del acceso o la interrupción de la prestación del mismo ».

¹⁵ Ley Orgánica núm. 1/2015, op. cit., Art. 189.8: « Los jueces y tribunales ordenarán la adopción de las medidas necesarias para la retirada de las páginas web o aplicaciones de internet que contengan o difundan pornografía infantil o en cuya elaboración se hubieran utilizado personas con discapacidad necesitadas de especial protección o, en su caso, para bloquear el acceso a las mismas a los usuarios de Internet que se encuentren en territorio español ».

Article 13 of the Criminal Procedure Act¹⁶ also provides for the adoption of **preventive measures** when an offence has been committed. In ordering these measures the court must respect the principles of objectivity, proportionality and non-discrimination.¹⁷ The parties concerned must be notified immediately of the **court decision**. All this can also be applied to information society service operators who commit or participate in the commission of an offence.¹⁸

1.5. International sources

As regards international instruments, Spain has ratified the following Council of Europe Conventions: the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse,¹⁹ the Convention on Cybercrime,²⁰ the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems,²¹ the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data²² and the Convention on the Prevention of Terrorism.²³ Once published in the Official Gazette, these conventions become part of the Spanish legal system.²⁴

¹⁶ Real Decreto de 14 de septiembre de 1882, aprobatorio de la Ley de Enjuiciamiento Criminal, available at http://noticias.juridicas.com/base_datos/Penal/lecr.l1t2.html#a13 (08.03.15).

¹⁷ E. Núñez, *Delitos cometidos a través de Internet. Cuestiones procesales*, Madrid 2010, p. 287 ss. Voir aussi *Buenas prácticas para la persecución de los delitos contra la propiedad intelectual actuación de las fuerzas y cuerpos de seguridad*, Publication of the Ministry of Education, Culture and Sport, p. 28, available at http://www.mecd.gob.es/cultura-mecd/dms/mecd/cultura-mecd/areas-cultura/propiedad-intelectual/mc/mbp/capitulos/Actuacion_Cuerpos_Seguridad.pdf (03.03.15).

¹⁸ E. Núñez, *op. cit.*, p. 293 ff.

¹⁹ Instrumento de Ratificación del Convenio del Consejo de Europa para la protección de los niños contra la explotación y el abuso sexual, hecho en Lanzarote el 25 de octubre de 2007, ratificado por Instrumento de 22 de julio de 2010, available at https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-17392 (03.08.15).

²⁰ Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001, Publicado en «BOE» núm. 226, de 17 de septiembre de 2010, páginas 78847 a 78896 (50 págs.) available at http://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-14221 (27.02.15).

²¹ Instrumento de Ratificación del Protocolo adicional al Convenio sobre la Ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos (RCL 2010\2474), hecho en Estrasburgo el 28-1-2003, available at http://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-793&lang=eu (03.09.15).

²² Instrumento de Ratificación del Protocolo Adicional al Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, a las Autoridades de control y a los flujos transfronterizos de datos, hecho en Estrasburgo el 8 de noviembre de 2001, Jefatura del Estado BOE 20 septiembre 2010, núm. 228, [pág. 79619] available at <https://www.boe.es/buscar/doc.php?id=BOE-A-2010-14380> (03.09.15).

²³ Instrumento de Ratificación del Convenio del Consejo de Europa para la prevención del terrorismo (Convenio nº 196 del Consejo de Europa), hecho en Varsovia el 16 de mayo de 2005, available at <http://www.boe.es/boe/dias/2009/10/16/pdfs/BOE-A-2009-16476.pdf> (27.02.14).

²⁴ Under Article 96.1 of the Spanish Constitution, validly concluded international treaties, once officially published in Spain, shall form part of the internal legal order. A. Aronovitz, *Espagne, en Conséquences institutionnelles de l'appartenance aux Communautés européennes* (Bertil Cottier, ed.), Publications de l'Institut suisse de droit comparé, Vol. 18, Schulthess, Zurich, 1991, Chap. 1.2.

2. Legal Framework

The conditions applicable to the blocking or filtering of illegal Internet content being similar to those governing its removal, this section covers all these measures. We shall highlight certain specific aspects of removal measures in section 2.2.

2.1. Blocking and/or filtering of illegal Internet content

As stated above, the judicial authorities and certain administrative authorities may, in their respective fields of competence, take steps to block and/or of remove illegal content.

Article 8.1 LSSI lists the cases in which the content of an Internet page may be **interrupted (blocked)** or the data **removed**, namely:

- a. To protect **public order, criminal investigations, public safety and national defence**.
- b. To protect **public health** or people or legal entities in their capacity as consumers or users, even when they are acting as investors.
- c. To protect **human dignity** and the **principle of non-discrimination** on grounds of sex, race, religion, opinion, nationality, disability or “any other personal or social circumstance”.
- d. To protect **young people and children**.
- e. To protect **intellectual property rights**.

As will be explained in section 3, the authority responsible for taking measures to “restore law and order” (Article 158 LPI) in the field of intellectual property is the Second Section of the Intellectual Property Commission.²⁵ As regards personal data, the Spanish Data Protection Agency orders the removal of content at variance with the guarantees imposed by the LOPD (see section 1.3 above), that is to say where no consent has been given, the information is inaccurate or the aim pursued is no longer applicable. In this context data may be removed even where the tenor is racist or xenophobic - for example, if an online publication disparages people with disabilities or foreigners. According to information communicated by a correspondent in Spain, there is no administrative authority in charge of blocking or removing content in other areas and judicial channels must be used.²⁶

²⁵ Tribunal Supremo (Sala de lo Contencioso-Administrativo, Sección 4ª) Sentencia de 31 mayo 2013 RJ\2013\4561 (private database) : « Téngase en cuenta que la Sección Segunda de la Comisión ejerce, ex artículo 158.4 de tanta cita, las funciones previstas en los artículos 8 y concordantes de la Ley 34/002 , de 11 de julio (RCL 2002, 1744, 1987), de servicios de la sociedad de la información y del comercio electrónico, que ya preveía que se adoptarían las "medidas necesarias para que se interrumpa su prestación o para retirar los datos que los vulneran ", relacionando a continuación los principios contra los que puede atentar un determinado servicio de la sociedad de la información. Entre estos se cita la salvaguarda del orden público, la investigación penal, la seguridad pública y la defensa nacional (apartado a); la protección de la salud pública (apartado b); el respeto a la dignidad de la persona y al principio de no discriminación (apartado c); la protección de la juventud y de la infancia (apartado d); y, como hace al caso, la salvaguarda de los derechos de propiedad intelectual (apartado c) ».

²⁶ Under Article 11.3 of Law 56/2007, amending the LSSI, where the removal or blocking of Internet pages affects freedom of expression or information it may only be implemented by order of the judicial authorities. . Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información, available at <https://www.boe.es/buscar/doc.php?id=BOE-A-2007-22440> (17.09.15). According to one view, each of these bodies may, within the general framework of its powers, intervene to remove Internet content deemed outrageous as child pornography, fake drugs , or dangerous games, in the same way that they can act in non-virtual areas: David Cierco, Director General para el Desarrollo de la Sociedad de Información, in Luz Fernández, “Nunca se ha censurado

The enforcement of decisions of the Second Section of the Intellectual Property Commission **requires judicial authorisation**. This guarantees the lawfulness of the measure taken, bearing in mind that blocking an Internet site may violate fundamental rights, particularly **freedom of expression**.

In a case judged in 2013,²⁷ the Supreme Administrative Court analysed the appellant's argument that making the Second Section of the Intellectual Property Commission the body in charge of applying restrictive measures to Internet activities in order to "restore law and order" violated the principle of effective judicial supervision, because the Section **is not a judicial body**. The court rejected the appeal. It held that the appellant was basing himself on what he thought should be the ideal system for safeguarding protected rights, i.e. that the question of "restoring law and order" should be brought directly before a judicial body, not an administrative one. It pointed out that such a proposal was "as legitimate an option as any other", but that the model adopted by Spanish law, while different from that proposed by the appellant, was not illegal. In the present case, the court added, the role played by the Second Section of the Intellectual Property Commission was not of the "*ius puniendi*" type. According to the court the Second Section of the Intellectual Property Commission only had the power to "restore law and order", which did not include imposing sanctions.²⁸ That power remained with the judiciary. That is why the powers of the Second Section of the Intellectual Property Commission as the body in charge of applying restrictive measures to activities on the Internet in order to "restore law and order" were not deemed to be illegal.

That said, the actual blocking or removal of Web content can only be done by the judicial authorities. We will return to this point in section 3. Our research did not produce any further information concerning the conditions of application of such measures by the judicial authorities.

In other areas the judicial authorities have the power to have illegal content blocked or removed.

un contenido en Internet en España", El País 9.2.07, available at http://tecnologia.elpais.com/tecnologia/2007/02/09/actualidad/1171013278_850215.html : « Realmente pueden retirar un contenido de Internet? Los principales cambios que estamos introduciendo están en el artículo 8 y 11, pero el texto ya estaba en la Ley anterior, sólo hemos eliminado unos supuestos y, por otro lado, hemos hecho una transposición de la directiva europea. Pero en ningún caso se da la base jurídica para que nadie pueda intervenir ningún tipo de contenido en Internet. Sólo se establece un procedimiento por el cual si un órgano competente, por ejemplo una Comunidad Autónoma, puede actuar en situaciones que a nadie le parecen escandalosas, como puede ser la retirada de determinados juegos peligrosos, fármacos falsos o pornografía infantil. Todos estos supuestos están contemplados en el mundo analógico, el físico, por lo que es lógico que estos órganos competentes también puedan actuar en el mundo digital porque así lo contempla nuestro marco jurídico. Si hay una ley que está diciendo que una Comunidad Autónoma tiene competencias para retirar un juguete peligroso, también tiene competencia para hacerlo en Internet".

²⁷ Tribunal Supremo (Sala de lo Contencioso-Administrativo, Sección 4ª) Sentencia de 31 mayo 2013, op. cit.

²⁸ Tribunal Supremo (Sala de lo Contencioso-Administrativo, Sección 4ª) Sentencia de 31 mayo 2013, op. cit.: "No estamos, por otro lado, ante una regulación propia del derecho sancionador, sino únicamente ante el restablecimiento de la legalidad en internet frente a los embates contra la propiedad intelectual. No se trata, por tanto, del ejercicio del " ius puniendi " del Estado, sino de reponer las cosas a su situación legal, cuando dicha legalidad ha sido conculcada por los responsables de los servicios de la sociedad de la información".

2.1.1. Protection of intellectual property rights

Article 3 j) of the Telecommunications Act²⁹ protects the interests of users, and in particular the constitutional rights of **non-discrimination**, the **protection of one's reputation and private life**, the **protection of children and young people**, the **protection of personal data** and the **confidentiality** of communications.

Article 158 ter LPI, paragraph 4, states that the Second Section of the Intellectual Property Commission may order information society service providers to stop a service which infringes intellectual property rights. The Second Section may also order the **removal of content** likely to damage property. These measures may include recourse to technical means and the obligation of due diligence to put a stop to the violation and make sure it does not happen again.

The Spanish legal system recognises the **obligation to respect fundamental rights and guarantees when applying restrictive measures** in the information society. Accordingly, when the above-mentioned measures are applied, the guarantees, rules and procedures laid down by Spanish law must be respected in order to protect **the right to private, personal and family life, personal data, freedom of expression and freedom of information**, when there is a risk of them being affected. The LSSI expressly states, in Article 11.3, that in the adoption and execution of measures to interrupt a service or remove content, the guarantees, norms and procedures provided for in the law to protect the right to private and family life, personal data, and freedom of expression and information, when there is a risk of them being affected, must always be respected. Paragraph 3 of Article 11 LSSI further states that in all cases where the Constitution or the laws regulating the rights and freedoms concerned assign exclusive power to the judicial authorities, they alone may take steps to block and remove content (cf. section 3). Article 11.3 LSSI further establishes that decisions to authorise the "seizure" of Internet pages or impose other **restrictions affecting freedom of expression and information may only be taken by the competent judicial bodies**.

Only **the competent judicial authority**, therefore – as the guardian of **freedom of expression**, of the right to literary, artistic, scientific and technical creation and production, and of **freedom to impart and receive information** – may authorise the execution of measures ordered by the Second Section of the Intellectual Property Commission³⁰ (the procedural aspects are covered in section 3). Naturally, a victim of a violation of his or her intellectual property rights may apply directly, as part of the judicial action taken, for the blocking of an illegal site (see the "Adidas" case, below).

2.1.2. Criminal law

Article 510 CPE was amended by Organic Law No. 1/2015 of 30 March 2015,³¹ which entered into force on 1 July 2015. Article 510 CPE,³² as amended, prohibits the following violations of public order:

²⁹ Ley 9/2014, de 9 de mayo de telecomunicaciones, available at http://www.boe.es/diario_boe/txt.php?id=BOE-A-2014-4950 (3.3.15).

³⁰ A. Losana, Ley 56/2007, de 28 de diciembre, de medidas de impulso de la Sociedad de Información, Pamplona 2008, cf. 6.1, available at BIB 2008\539 (private database): « En particular, la autoridad judicial se configura como garante del derecho a la libertad de expresión, derecho de producción y creación literaria, artística, científica y técnica (art. 8.1 LSSI in fine) ».

³¹ Ley Orgánica 10/1995, de 23 de noviembre del Código Penal, modificado por art. Único.235 de Ley Orgánica núm. 1/2015, de 30 de marzo. RCL\2015\439 (private database), en vigor desde 1.7.15.

³² Artículo 510. [Provocación a la discriminación, odio o violencia contra grupos]. « 1. Serán castigados con una pena de prisión de uno a cuatro años y multa de seis a doce meses: a) Quienes públicamente fomenten, promuevan o inciten directa o indirectamente al odio, hostilidad, discriminación o violencia contra un grupo, una parte del mismo o contra una persona determinada por razón de su pertenencia

1. The public encouragement and promotion **incitement to hatred, discrimination or violence** against a group, part of a group or a person in particular for being a member of that group, on grounds of racism, anti-Semitism or other motives linked to ideology, religion or beliefs, family circumstances, membership of an ethnic group, race or nation, national origin, gender, sexual orientation or identity, health or disability;
2. The production, conception, possession for dissemination, provision of access to, distribution, dissemination or sale of, writings or **any other material the content of which might directly or indirectly encourage, promote or incite hatred, hostility, discrimination or violence** against a group, part of a group or a person in particular for being a member of that group, on grounds of racism, anti-Semitism or other motives linked to ideology, religion or beliefs, family circumstances, membership of an ethnic group, race or nation, national origin, gender, sexual orientation or identity, health or disability;
3. The public **denial**, banalisation or exaltation of **genocide, crimes against humanity** or against protected persons in armed conflicts, or the **exaltation of the authors** of acts against a group, part of a group or a person in particular for being a member of that group, on grounds of racism, anti-Semitism or other motives linked to ideology, religion or beliefs, family circumstances, membership of an ethnic group, race or nation, national origin, gender, sexual orientation or identity, health or disability and who foster or encourage violence, hostility, hatred or discrimination against them;
4. Violation, by humiliation, scorn or discredit, of the **dignity** of any member of the groups mentioned above;
5. **The exaltation or justification**, by any means of public expression or dissemination, of **crimes** committed against a group, part of a group or a person in particular for being a member of that group, on grounds of racism, anti-Semitism or other motives linked to ideology, religion or beliefs, family circumstances, membership of an ethnic group, race or nation, national origin, gender, sexual orientation or identity, health or disability, or those who perpetrate them.

a aquél, por motivos racistas, antisemitas u otros referentes a la ideología, religión o creencias, situación familiar, la pertenencia de sus miembros a una etnia, raza o nación, su origen nacional, su sexo, orientación o identidad sexual, por razones de género, enfermedad o discapacidad.

b) Quienes produzcan, elaboren, posean con la finalidad de distribuir, faciliten a terceras personas el acceso, distribuyan, difundan o vendan escritos o cualquier otra clase de material o soportes que por su contenido sean idóneos para fomentar, promover, o incitar directa o indirectamente al odio, hostilidad, discriminación o violencia contra un grupo, una parte del mismo, o contra una persona determinada por razón de su pertenencia a aquél, por motivos racistas, antisemitas u otros referentes a la ideología, religión o creencias, situación familiar, la pertenencia de sus miembros a una etnia, raza o nación, su origen nacional, su sexo, orientación o identidad sexual, por razones de género, enfermedad o discapacidad.

c) Públicamente nieguen, trivialicen gravemente o enaltezcan los delitos de genocidio, de lesa humanidad o contra las personas y bienes protegidos en caso de conflicto armado, o enaltezcan a sus autores, cuando se hubieran cometido contra un grupo o una parte del mismo, o contra una persona determinada por razón de su pertenencia al mismo, por motivos racistas, antisemitas u otros referentes a la ideología, religión o creencias, la situación familiar o la pertenencia de sus miembros a una etnia, raza o nación, su origen nacional, su sexo, orientación o identidad sexual, por razones de género, enfermedad o discapacidad, cuando de este modo se promueva o favorezca un clima de violencia, hostilidad, odio o discriminación contra los mismos.

2. Serán castigados con la pena de prisión de seis meses a dos años y multa de seis a doce meses [...]:

b) Quienes enaltezcan o justifiquen por cualquier medio de expresión pública o de difusión los delitos que hubieran sido cometidos contra un grupo, una parte del mismo, o contra una persona determinada por razón de su pertenencia a aquél por motivos racistas, antisemitas u otros referentes a la ideología, religión o creencias, situación familiar, la pertenencia de sus miembros a una etnia, raza o nación, su origen nacional, su sexo, orientación o identidad sexual, por razones de género, enfermedad o discapacidad, o a quienes hayan participado en su ejecución [...]».

Paragraph 3 of the amended version³³ provides for penalties in the upper half of the scale to be imposed where the violations are committed via the social media, **by Internet** or using information technologies to make the content available to large numbers of people. As regards the removal or blocking of content, paragraph 6 of Article 510³⁴ now provides for **the courts to order the destruction, deletion or rendering unusable** of the books, archives, documents, articles and **“any type of support constituting the object of the offence”**. When the offence was committed using computer and communication technology, **the removal of the content** will be ordered. The last paragraph of Article 510.6 CPE provides that should an Internet access portal or an information society service be found to be “preponderantly” disseminating incitement to hatred, the court will **order the blocking or interruption of the service**. It is worth noting that the expression “preponderantly” in Article 510.6 CPE,³⁵ concerning the offence of incitement to hatred, also appears in Article 270.3 CPE in respect of violations of intellectual property rights. Indeed, under Article 270.3 CPE, when an Internet site or an information society service exclusively or preponderantly disseminates content protected by an intellectual property right the court will order the **interruption of the service** and any other provisional measure needed to protect intellectual property rights.

In the specific field of **child pornography and the abuse of people with disabilities** who need protection, Article 189.8 of the CPE, as amended by Organic Law No. 1/2015, requires the courts to order the adoption of any **measures necessary to secure the removal of Web pages or Internet programmes** containing or disseminating child pornography or featuring people with disabilities in need of special protection. These measures may include **the blocking of access** to the pages concerned for users on Spanish soil. In a Circular of 19 June 2015,³⁶ the Principal State Counsel issued the following instructions to public prosecutors who have to implement such measures:

“As it is impossible to determine in advance whether the removal or simply the blocking [of the illegal content] is necessary, prosecutors shall, where applicable, request its removal as an interim (*cautelar*) measure and, in the alternative and as an interim measure, the blocking of the pages or applications concerned. If the interim measure is refused, prosecutors shall seek the permanent removal or blocking of the content.”³⁷

³³ Art. 510.3 CPE « Las penas previstas en los apartados anteriores se impondrán en su mitad superior cuando los hechos se hubieran llevado a cabo a través de un medio de comunicación social, por medio de internet o mediante el uso de tecnologías de la información, de modo que, aquel se hiciera accesible a un elevado número de personas».

³⁴ Art. 510.6) CPE : « El juez o tribunal acordará la destrucción, borrado o inutilización de los libros, archivos, documentos, artículos y cualquier clase de soporte objeto del delito a que se refieren los apartados anteriores o por medio de los cuales se hubiera cometido. Cuando el delito se hubiera cometido a través de tecnologías de la información y la comunicación, se acordará la retirada de los contenidos ».

³⁵ Art. 510.6 *in fine* CPE : « En los casos en los que, a través de un portal de acceso a internet o servicio de la sociedad de la información, se difundan exclusiva o preponderantemente los contenidos a que se refiere el apartado anterior, se ordenará el bloqueo del acceso o la interrupción de la prestación del mismo ».

³⁶ Fiscalía General del Estado, Circular 2/2015, sobre los delitos de pornografía infantil tras la reforma operada por LO 1/2015, available at https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Circular_2_15_pornografia_infantil.pdf?idFile=24b87ad2-9488-488a-ab0a-15d88e3048ed (30.06.15).

³⁷ Fiscalía General del Estado, Circular 2/2015, op. cit., p. 50: “Como quiera que en los primeros momentos podrá no ser conocido si cabe la retirada o únicamente el bloqueo, los Sres. Fiscales, cuando sea necesario, instarán la medida cautelar de retirada y, alternativamente la medida cautelar de bloqueo de tales páginas o aplicaciones. De no haberse acordado esta medida con carácter cautelar, los Sres. Fiscales interesarán que se adopte en sentencia”.

Where public safety is concerned, there are some new provisions in the relevant Organic Law (the LOPC), which entered into force on 1 July 2015.³⁸ The law does not directly concern the blocking and removal of Internet content, but it could apply to the Internet with a little flexibility in the interpretation of certain articles. Generally speaking the purpose of the LOPC is to “regulate a wide and varied set of actions of various kinds” to protect the public, property and individuals and maintain law and order (Article 1.2 and Article 3 LOPC³⁹).

- Article 4 LOPC⁴⁰ requires the authorities to respect the principles of lawfulness, equality of treatment, non-discrimination, proportionality, efficacy and responsibility and guarantee the full and effective enjoyment of people’s fundamental rights and freedoms, including freedom of assembly and demonstration and **freedom of expression and information**. However, the wording of some of the provisions of the LOPC is not sufficiently clear at this stage as to how rights such as freedom of expression and information are affected. For example, Article 39.2.b) LOPC⁴¹ provides for sanctions such as the confiscation of the “property, means or instruments used to prepare or commit the offence”, which could apply, in certain cases, to information society service providers (cf. section 5).

Lastly, in the field of **intellectual property**, Article 270.2 CPE as amended by Organic Law No. 1/2015⁴² makes it an offence for any person, in the context of the information society and with a

³⁸ Ley Orgánica de protección de la seguridad ciudadana N° 4/2015, de 30 marzo, entered into force on 1/7/2015, RCL 2015\442 (private database).

³⁹ Art. 3 LOPC : « Artículo 3. Fines. Constituyen los fines de esta Ley y de la acción de los poderes públicos en su ámbito de aplicación: a) La protección del libre ejercicio de los derechos fundamentales y las libertades públicas y los demás derechos reconocidos y amparados por el ordenamiento jurídico.
b) La garantía del normal funcionamiento de las instituciones.
c) La preservación de la seguridad y la convivencia ciudadanas.
d) El respeto a las Leyes, a la paz y a la seguridad ciudadana en el ejercicio de los derechos y libertades.
e) La protección de las personas y bienes, con especial atención a los menores y a las personas con discapacidad necesitadas de especial protección.
f) La pacífica utilización de vías y demás bienes demaniales y, en general, espacios destinados al uso y disfrute público.
g) La garantía de las condiciones de normalidad en la prestación de los servicios básicos para la comunidad.
h) La prevención de la comisión de delitos e infracciones administrativas directamente relacionadas con los fines indicados en los párrafos anteriores y la sanción de las de esta naturaleza tipificadas en esta Ley.
i) La transparencia en la actuación de los poderes públicos en materia de seguridad ciudadana ».

⁴⁰ Artículo 4 LOPC : « Principios rectores de la acción de los poderes públicos en relación con la seguridad ciudadana. 1. El ejercicio de las potestades y facultades reconocidas por esta Ley a las administraciones públicas y, específicamente, a las autoridades y demás órganos competentes en materia de seguridad ciudadana y a los miembros de las Fuerzas y Cuerpos de Seguridad se regirá por los principios de legalidad, igualdad de trato y no discriminación, oportunidad, proporcionalidad, eficacia, eficiencia y responsabilidad, y se someterá al control administrativo y jurisdiccional. En particular, las disposiciones de los capítulos III y V deberán interpretarse y aplicarse del modo más favorable a la plena efectividad de los derechos fundamentales y libertades públicas, singularmente de los derechos de reunión y manifestación, las libertades de expresión e información, la libertad sindical y el derecho de huelga ».

⁴¹ Art. 39.2.b) LOPC : « b) El comiso de los bienes, medios o instrumentos con los que se haya preparado o ejecutado la infracción y, en su caso, de los efectos procedentes de ésta, salvo que unos u otros pertenezcan a un tercero de buena fe no responsable de dicha infracción que los haya adquirido legalmente ».

⁴² Art. 270.2. CPE: « La misma pena se impondrá a quien, en la prestación de servicios de la sociedad de la información, con ánimo de obtener un beneficio económico directo o indirecto, y en perjuicio de

view to direct or indirect financial gain to the detriment of the victim, actively (that is to say, not in a “purely technical” manner) to facilitate access on the Internet to protected works or services without the authorisation of the rights holders. This includes targeted advertising and links towards the works even if the links were initially supplied by the recipients of their services. Paragraph 3 of Article 270 CPE⁴³ as amended provides for the courts, in such cases, to order the removal of the works or services concerned. It also provides, where an Internet site or an information society service exclusively or preponderantly disseminates material protected by an intellectual property right, for the court to order the **interruption (blocking) of the service** and any provisional measure necessary to protect the intellectual property rights in issue.

The Attorney General approved a “circular” on December 21, 2015⁴⁴ to instruct the Attorneys on how to implement the LPI in order to effectively tackle infringements of intellectual property rights. In particular, the new Circular provides criteria as regards the public character of linking activities, the notion of indirect economic benefit, the multiplying effect of online infringement and subsequent penalties, or the non-exhaustive character of the list of infringements conducts reflected in the law, among other.

2.1.3. Codes of conduct and other practices

The blocking or removal of illegal Internet content are measures which are also found in **Internet codes of conduct**. Article 18 LSSI provides for the public authorities to encourage the development and application of voluntary codes of conduct in firms, associations and commercial, professional and consumer organisations, in the fields covered by the LSSI. The codes of conduct may concern procedures for the detection and removal of illegal content, the protection of recipients of unwanted messages or even the extrajudicial settlement of disputes. Consumer and user associations and organisations representing people with disabilities are automatically involved in the development of these codes of conduct when their respective interests could be affected. The codes of conduct must have special regard to the protection of minors and of human dignity: special codes may be developed in these fields. The codes must be accessible by electronic means and their translation into the official languages in Spain and the EU is encouraged. Article 10 g) LSSI requires information society service providers to put in place “permanent, easy-to-use, direct and free” electronic means of accessing the codes of conduct to which they may have subscribed.⁴⁵

tercero, facilite de modo activo y no neutral y sin limitarse a un tratamiento meramente técnico, el acceso o la localización en internet de obras o prestaciones objeto de propiedad intelectual sin la autorización de los titulares de los correspondientes derechos o de sus cesionarios, en particular ofreciendo listados ordenados y clasificados de enlaces a las obras y contenidos referidos anteriormente, aunque dichos enlaces hubieran sido facilitados inicialmente por los destinatarios de sus servicios».

⁴³ Art. 270.3. CPE: « En estos casos, el juez o tribunal ordenará la retirada de las obras o prestaciones objeto de la infracción. Cuando a través de un portal de acceso a internet o servicio de la sociedad de la información, se difundan exclusiva o preponderantemente los contenidos objeto de la propiedad intelectual a que se refieren los apartados anteriores, se ordenará la interrupción de la prestación del mismo, y el juez podrá acordar cualquier medida cautelar que tenga por objeto la protección de los derechos de propiedad intelectual. Excepcionalmente, cuando exista reiteración de las conductas y cuando resulte una medida proporcionada, eficiente y eficaz, se podrá ordenar el bloqueo del acceso correspondiente ».

⁴⁴ Circular 8/2015 de la Fiscalía General del Estado., available at https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/CIRCULAR_8-2015.pdf?idFile=d7b418c1-6aa4-406a-bceb-19b2a9495c52 (12.04.16)

⁴⁵ In another area, that of the armed forces, the Ministry of Education, Culture and Sport provides a good practice handbook for the prosecution of offences against intellectual property. Buenas prácticas para la persecución de los delitos contra la propiedad intelectual actuación de las fuerzas y cuerpos de

Article 158 ter LPI, paragraph 4, also creates the possibility of developing voluntary codes of conduct with regard to measures of collaboration with intermediary, electronic payment or advertising services to make effective the fight against the offer of online content that infringes intellectual property rights.⁴⁶

In practice, there are many codes of conduct covering the different aspects of the Internet. The case-law mainly concerns **electronic commerce**, Directive 2000/31CE stressing the need to develop codes of conduct.⁴⁷ Examples include the OPTIMAWEB code of conduct of the National Association of Internet Enterprises,⁴⁸ the “confidence online” code of conduct,⁴⁹ or the Code of the Spanish Electronic Commerce Association.⁵⁰ This last code has a chapter on the protection of minors under 18, in particular in respect of personal data processing and advertising. The Ministry of Culture has proposed a code of conduct for teaching establishments which covers intellectual property rights among other things.⁵¹ There is also a code of conduct for mobile telephone network operators, designed to encourage sensible use by minors.⁵² This code contains a chapter on illegal content. Under the code, the operators cooperate with the police and security forces in the performance of their duties in respect of content prohibited by criminal law, particularly content likely to have harmful effects on children and young people. The mobile operators undertake to remove certain content they host and to limit access to content declared illegal by the judicial authorities. Illegal content is removed, or access to it blocked, within the time-frame set out in the courts’ decisions. The code also provides for operators to set up filters to restrict access to the pages concerned when the authorities publish lists of Web sites hosting content they consider illegal.

Lastly, the code provides for operators to cooperate with public authorities and private organisations known to be involved in fighting illegal content, particularly child pornography, on the Internet in tracking down and blocking access to such material. And in the field of self-regulation, Spain has “seals of quality” (*Sellos de Calidad* or *Sellos de Garantía*) for Internet sites. Article 18 of the Code of the Spanish Electronic Commerce Association states that the aim of the “seal” is to identify those firms which have accepted the ethical standards set out in the Code. Compliance with the Codes is normally monitored by a body before which complaints may be brought. In the case of the Code of the Spanish Electronic Commerce Association (Article 22 ff), a committee analyses consumers’

seguridad, op. cit. available at <http://www.mecd.gob.es/cultura-mecd/areas-cultura/propiedad-intelectual/mc/mbp/capitulos.html> (03.03.15).

⁴⁶ “Podrán desarrollarse códigos de conducta voluntarios en lo referido a las medidas de colaboración de los servicios de intermediación, los servicios de pagos electrónicos o de publicidad previstas en este artículo”.

⁴⁷ M. Nuñez, Artículo 18 : Códigos de Conducta, in *La Nueva Ley de Internet* (Javier Cremades coord.), La Ley, Madrid, 2003, p. 299 ; J. Prenafeta, *Autorregulación, Códigos de Conducta y Sellos de Confianza en Internet*, Noticias Jurídicas 2.2003, available at <http://noticias.juridicas.com/articulos/20-Derecho-Informatico/200302-1355131211033420.html>

⁴⁸ Available at <http://www.a-nei.org/codigo-de-conducta/codigo-de-conducta-optimaweb.html> (03.03.15).

⁴⁹ Available at http://www.autocontrol.es/pdfs/cod_confianzaonline.pdf (03.03.15).

⁵⁰ Available at http://ciberconta.unizar.es/leccion/proteccion/descargas/cod_aece.pdf (03.03.15).

⁵¹ Ministerio de Cultura, Código de Conducta Sobre el Uso de Material protegido, available at http://www.mecd.gob.es/cultura-mecd/dms/mecd/cultura-mecd/areas-cultura/propiedad-intelectual/lucha-contra-la-pirateria/Guia_Universidades_2007.pdf(03.03.15).

⁵² Code Of Conduct For Mobile Operators Designed to Encourage Responsible Use By Underage Persons Of Electronic Content Services Supplied Via Mobile Telephone Networks In Spain, available at <http://www.gsma.com/gsmEurope/wp-content/uploads/2012/04/spaincoc0308.pdf> (03.08.15).

complaints. The sanctions provided for are a warning, a reprimand, temporary or permanent loss of the quality seal or expulsion from the Association.

Case-law

1. The “Adidas” case.⁵³ The Barcelona Commercial Court ordered an interim ban on any attempt to exploit Adidas products, and in particular those products advertised on four Web pages. The defendants were the owners of the domain names “camisetasfutbolchina.es”, “camiseta-realmadrid.es”, “camisetafutbolbarata.es” and “camisetasclub.es”. The Web pages “www.camisetasfutbolchina.es” and “www.camisetafutbolbarata.es” automatically redirected users to sites on which the defendants sold, *inter alia*, copies of sports gear under the ADIDAS brand name, in violation of the intellectual property rights of the ADIDAS brand. The court then ordered the provisional blocking of access to the Web pages “www.camisetasfutbolchina.es”, “www.camisetafutbolbarata.es”, “www.camiseta-realmadrid.es” and “www.camisetasclub.es”, owned by the defendants, by having Red.es, the public authority in charge of domain names, cancel the domain names “www.camisetasfutbolchina.es”, “www.camisetafutbolbarata.es”, “www.camiseta-realmadrid.es” and “www.camisetasclub.es”. Lastly, in the alternative, “were the previous measure to prove ineffective”, the court ordered the partial blocking of the Web pages “www.camisetasfutbolchina.es”, “www.camisetafutbolbarata.es”, “www.camiseta-realmadrid.es” and “www.camisetasclub.es”, by sending the order to the different Internet access providers operating in Spain “to prevent access” to these pages from Spain. The court also ordered the temporary blocking of four Web pages belonging to the defendants. The pages offered products identical to those of the claimant as “replicas” of the original products. The court issued this order as an “alternative measure” to enable Internet access providers operating in Spain to “prevent access” to these pages in Spain. As it was a temporary measure, it was open to appeal within 20 days.
2. The “Uploaded.to” case.⁵⁴ In this case, on which the Second Section of the Intellectual Property Commission ruled on 27 July 2012, the AGEDI (the body which handles intellectual property rights for phonographic producers) lodged a complaint against the site “uploaded.to”, owned by a Swiss data storage company, for allowing users to download various protected works. Mention was also made in the complaint of an information society service provider (“bajui.com”), which provided links to the “uploaded.to” site. The ruling of the Second Section of the Intellectual Property Commission demanded the removal of the disputed content within 48 hours or, in the alternative, the presentation of proof that there had been no violation. The order was also sent to the link provider “bajui.com”, for having proposed links to the services of “uploaded.to”. By the end of the 48-hour time-limit the content had been removed from the “uploaded.to” site, which the authorities took as an acknowledgment of the violation of the intellectual property rights in issue. “Bajui.com” was told to remove the disputed links, failing which, as an information society intermediary it could be fined between 150.001 and 600.000 euros (Articles 38.2 and 39.2 LSSI).
3. The “Uber” case.⁵⁵ In a decision of 9 December 2014 the Madrid Commercial Court took interim action against “Uber” for unfair competition. In the operative part of the decision the court ordered the cessation and prohibition in Spain of the “Uberpop” transport and similar services, as well as the **removal of the content of, access to and the services proposed by the company on, the Web page “www.uber.com”** or any other page the company might use for similar purposes.

⁵³ Juzgado de lo Mercantil de Barcelona Auto de 30 abril num. 195/2012, AC\2012\387 (private database).

⁵⁴ Sección Segunda de la Comisión de Propiedad Intelectual, Código de expediente: E/2012/00012, Número de registro: T002012N0000000585, Solicitante: Asociación de Gestión de Derechos Intelectuales (AGEDI), 27.7.2012, available at <http://comunicacion21.com/wp-content/PDF/Curso/ResolBajui.pdf> (05.03.15).

⁵⁵ Juzgado de lo Mercantil de Madrid Auto de 9 diciembre 2014, JUR\2014\286106 (private database).

Lastly, the court prohibited the use of any application (app) and any medium or technological or computer system to provide this type of transport service in Spain.

4. The Desiderio case.⁵⁶ In this case a *rap* singer posted songs on the net with lyrics justifying and exalting the actions of terrorist groups and encouraging them to continue. The singer was found guilty at first instance under Article 578 of the Spanish Criminal Code,⁵⁷ which prohibits the glorification (*enaltecimiento*) or the justification “by any public means of expression or dissemination” of the acts of people who have taken part in the execution of acts or terrorism or who harm, humiliate or belittle the victims of such acts. In his appeal to the Supreme Court, the appellant relied on the right to freedom of expression and artistic creation. The court rejected that argument and upheld the prison sentence delivered by the lower court. As to whether access to the illegal content was blocked, or the content removed, as far as we know neither the first-instance court nor the court of appeal addressed the issue, and the illegal content is still accessible on the net.

2.2. Take-down/removal of illegal Internet content

The basis on which content can be removed from the Internet was analysed in section 2.1. In this section, we shall look at certain specific aspects of the measures used to remove content.

Article 16 LSSI contains rules relating specifically to the responsibility of Internet hosting or content storage service providers. They are not responsible for the content if:

- a. they were not “effectively aware” that the information provided was illegal or detrimental to property or rights of a third party which qualify for compensation, and
- b. they act with diligence to remove the data or block access to it were they to become “effectively aware” of the situation.

Under Article 16.1 *in fine* LSSI, an information society service provider is **effectively aware** of illegal content when a competent authority has declared it illegal, ordered its withdrawal or the blocking of access to it, or declared it harmful and the Internet service provider has been informed of that decision. The article specifies that this does not detract from any content detection and withdrawal procedures the service providers may apply based on voluntary agreements.

In the special case of the of intermediary service providers,⁵⁸ Article 17.1 LSSI⁵⁹ states that they are not responsible of the information contained in the services they offer provided that they are not

⁵⁶ Tribunal Supremo, (Sala de lo Penal, Sección 1ª) Sentencia num. 106/2015 de 19 febrero 2015, RJ\2015\1064 (private database).

⁵⁷ Código penal, Art 578 : « El enaltecimiento o la justificación por cualquier medio de expresión pública o difusión de los delitos comprendidos en los artículos 571 a 577 de este Código o de quienes hayan participado en su ejecución, o la realización de actos que entrañen descrédito, menosprecio o humillación de las víctimas de los delitos terroristas o de sus familiares se castigará con la pena de prisión de uno a dos años. El Juez también podrá acordar en la sentencia, durante el período de tiempo que el mismo señale, alguna o algunas de las prohibiciones previstas en el artículo 57 de este Código », available at http://noticias.juridicas.com/base_datos/Penal/lo10-1995.l2t22.html#a578 (06.06.15).

⁵⁸ See the “CEDRO” case in the part of this section on case-law.

⁵⁹ Art. 17 LSSI : « Responsabilidad de los prestadores de servicios que faciliten enlaces a contenidos o instrumentos de búsqueda. 1. Los prestadores de servicios de la sociedad de la información que faciliten enlaces a otros contenidos o incluyan en los suyos directorios o instrumentos de búsqueda de contenidos no serán responsables por la información a la que dirijan a los destinatarios de sus servicios, siempre que:

effectively aware that the information is illegal or detrimental to property or rights of a third party which qualify for compensation, and, **should they become aware of it, that they act with diligence to remove or block the link concerned**. Paragraph 2 of Article 17 LSSI specifies that the service provider will be considered to be **effectively aware** when:

- a. a competent authority has declared the content illegal and ordered its withdrawal or the blocking of access to it, and
- b. the service provider has been informed of a decision declaring the content harmful (cf. section 2.2.).

In a case judged in 2012 in the Province of Álava, the court ruled that in the absence of a decision the service provider is not effectively aware and cannot be held responsible for the information accessed via the link provided.⁶⁰

Under criminal law service providers who provide links to Internet sites are generally exempt from liability. The reason is that they do not themselves reproduce the public communication of the content of the sites towards which they provide links.⁶¹

In respect of the **protection of personal data**, Article 16.2 LOPD provides for the **removal** of data that cannot be processed in keeping with the requirements of the LOPD, “especially when they are inexact or incomplete”. Where applicable, the Spanish Data Protection Agency can take such a decision within 6 months of the complaint being lodged (Article 18.3 LOPD). Article 44 LOPD makes it a “very serious” offence **not to stop** the illegal processing of personal data in breach of a decision of the Data Protection Agency (cf. the “Google” case below). The data deleted remain at the disposal of the courts and the authorities until the end of the limitation period for the offence concerned, in order that the relevant responsibilities connected with the data processing may be established (Article 16.3 LOPD). Lastly, the case-law has also acknowledged “the right to be forgotten”, that is to say the right not to be found by Internet search engines⁶² (cf. the “Google Spain S.L.” case, below).

Article 18.1 LSSI addresses the **codes of conduct** of information society service providers (cf. section 2.1.), stating that they may, in particular, cover procedures for detecting and removing illegal content. Under paragraph 2 of Article 18 LSSI consumer and user associations and organisations representing people with disabilities should be involved in the development of these codes of conduct when their respective interests might be affected. In particular, codes of conduct must make

a) No tengan conocimiento efectivo de que la actividad o la información a la que remiten o recomiendan es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización, o

b) Si lo tienen, actúen con diligencia para suprimir o inutilizar el enlace correspondiente.

Se entenderá que el prestador de servicios tiene el conocimiento efectivo a que se refiere el párrafo a) cuando un órgano competente haya declarado la ilicitud de los datos, ordenado su retirada o que se imposibilite el acceso a los mismos, o se hubiera declarado la existencia de la lesión, y el prestador conociera la correspondiente resolución, sin perjuicio de los procedimientos de detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios y de otros medios de conocimiento efectivo que pudieran establecerse.

2. La exención de responsabilidad establecida en el apartado 1 no operará en el supuesto de que el proveedor de contenidos al que se enlace o cuya localización se facilite actúe bajo la dirección, autoridad o control del prestador que facilite la localización de esos contenidos ».

⁶⁰ Audiencia Provincial de Álava (Sección 2ª), Caso Cinetube. Auto núm. 52/2012 de 3 febrero. ARP 2012\219 (private database).

⁶¹ I. Fernández-Díez, La responsabilidad de los intermediarios en internet en materia de propiedad intelectual, Madrid, 2014 p. 25.

⁶² P. Castellano, El reconocimiento del derecho al olvido digital en España y en la UE, Barcelona 2015, p. 217 et 221.

special provision for the protection of minors and of human dignity. One example is the “confidence online” code of conduct,⁶³ which concerns the storage of personal data, Article 33 of which provides that entities which adhere to the code and are responsible for or in charge of data files must adopt appropriate security measures to protect the integrity and confidentiality of the content stored, and make every effort to keep abreast of advances in this field. The members must adopt a security document listing the in-house technical and organisational measures they are required to take, depending on the type of data stored and how sensitive the content is. The consumer must be informed in clear and simple terms of the level of protection applied. Another example, this time outside the ambit of data protection legislation, is the code of conduct for mobile telephone network operators (see section 2.1.3 above), which includes provisions on the removal of illegal content or the blocking of access to it.

Case-law

1. The SGAE case.⁶⁴ The appellant in this case had hosted pages containing insults against the Spanish Society of Authors and Publishers (*Sociedad General de Autores y Editores, SGAE*). In its final decision the Supreme Court emphasised the due diligence obligation of Internet hosting services and the test of “effective awareness” of content (Article 16 LSSI). The Supreme Court upheld the decision of the lower court finding that the host was effectively aware of the offending content and should have shown due diligence, *inter alia* because the domains attributed to those who had sent the illegal content had a telling name.⁶⁵
2. The www.diariodecadiz.es case.⁶⁶ Here the web page of an electronic newspaper had published (then taken down) offensive comments following the detention of a local police chief. In its judgment the court referred to the rules of the LSSI on the responsibility of Internet hosting services (Article 16 LSSI), declaring that the intention of the law was not to restrict freedom of expression by establishing prior censorship on the Internet. The law did, however, impose an obligation of due diligence and cooperation with the authorities in identifying the authors of illegal content and reminding them of their responsibilities. While web hosts were generally exempt from responsibility, they were nevertheless subject to certain obligations. This meant that once the service provider effectively became aware of illegal content, it was expected to act with due diligence to put a stop to the offence. In the case in point the host had taken down the offending comments and the court found that it had acted with due diligence. The host was therefore not liable.
3. The “Google Spain S.L.” case.⁶⁷ In this case, judged on appeal on 30 December 2014, a person brought a complaint against Google Spain S.L. before the Data Protection Agency, alleging that when they did a search for their name on that search engine the result showed an announcement mentioning the person’s name in connection with the sale by auction of a real-estate property seized in order to recover a debt owed to social security. The Director of the Data Protection Agency decided in favour of the complainant and ordered the adoption of the necessary measures to avoid the indexing of the applicant’s personal data in order to prevent the person’s

⁶³ Código Ético de Confianza Online (auquel renvoi le Ministère de l’industrie, l’énergie et le tourisme dans sa page <http://www.lssi.gob.es/empresas/Paginas/empresas.aspx> (10.03.15), available at http://www.autocontrol.es/pdfs/cod_confianzaonline.pdf (10.03.15).

⁶⁴ Tribunal Supremo, (Sala de lo Civil, Sección 1ª) Sentencia num. 773/2009 de 9 diciembre, available at RJ\2010\131 (private database).

⁶⁵ The name was “www.putasgae.org”

⁶⁶ Audiencia Provincial de Cádiz (Sección 2ª) Sentencia num. 326/2010 de 4 noviembre, available at AC\2011\652 (private database).

⁶⁷ Audiencia Nacional (Sala de lo Contencioso-Administrativo, Sección 1ª), Sentencia num. 45/2014 de 30 diciembre 2014, available at JUR\2015\57265 (private database).

name from being associated with the offending information in the future. Google Spain S.L. appealed that decision. The Court of Appeal found that personal data obtained via a search engine – which was an information society intermediary for the purposes of the LSSI – could affect the data subject’s dignity. Accordingly, the Director of the Data Protection Agency, a body competent to oversee the application of the Data Protection Act in Spain, had the power to require the people responsible for processing the data to take the necessary steps to avoid violations of the LOPD. This power was attributed to the Agency by the LOPD in order to achieve the results prescribed in Articles 8 and 17 LSSI, namely the blocking or removal of the offending content. The court then analysed the consequences of this in the instant case. It found that the Google platform carried out “data processing” within the meaning of the LOPD. The logical consequence of that was that anyone wishing to exercise their right of opposition against the data base must show that when they did a search of their own name in the data base the results included links to illegal information. As this was what had happened in the instant case, the court rejected Google Spain’s appeal. It should be noted that the decision of the Director of the Data Protection Agency had not explicitly ordered the removal of the offending information but had used an unfortunate turn of phrase, requiring Google Spain S.L to adopt “the necessary measures to avoid indexation and make sure they do not appear in search results on the Web pages” (“*que adopte las medidas necesarias para que se evite la indexación y no aparezcan en su búsqueda respecto de las páginas Web*”). The court pointed out that this confusing wording shed doubt on what exactly was required of Google Spain S.L. Lastly, the court clarified the situation, explaining that Google Spain S.L. was to adopt the necessary measures to **remove** or **delete** from the list of results obtained by a search using the complainant’s name any links to the Web pages complained of.

4. The “CEDRO” case.⁶⁸ In this case, judged on appeal on 22 July 2014, an Internet site was reported to the Second Section of the Intellectual Property Commission for violation of intellectual property rights, in particular by giving access to literary works. The complaint also concerned an intermediary service provider, which listed the corresponding links. The Court of Appeal explained that under Article 18 of Royal Decree 1889/2011 intermediary information society service providers could be notified, as “interested parties”, of the existence of proceedings against a site to which their service provided links, for example to inform them of the possibility of future requests to identify those responsible for the illegal acts, so that decisions against them could be enforced. However, the court concluded, proceedings could not be brought against an intermediary alone when there was no identifiable information society protagonist responsible for the dissemination of the illegal content.

3. Procedural Aspects

The administrative authority competent in the first instance to order the blocking, suspension and removal of Internet content that violates intellectual property rights is the **Second Section of the Intellectual Property Commission** (cf. section 2.1.1). Under Article 8.2 LSSI, in order to adopt the measures mentioned in Article 8.1 LSSI (namely the removal of content and the suspension of access), the competent authority may ask the intermediary service provider to communicate any data that could help identify those responsible for the information society services used to carry on the activities presumed to be illegal.⁶⁹

⁶⁸ Audiencia Nacional, (Sala de lo Contencioso-Administrativo, Sección 1ª) Sentencia de 22 julio 2014, available at JUR\2014\205860 (private database).

⁶⁹ See the “CEDRO” case in section 2.2. The procedure before the Commission is laid down in Royal Decree 1889/2011, available here: <http://www.boe.es/boe/dias/2011/12/31/pdfs/BOE-A-2011-20652.pdf> (1.07.15).

Spanish law guarantees **respect for fundamental rights** when restrictive measures are applied to information society participants (cf. section 2.1). In conformity with Articles 18.1 and 18.3 of the Spanish Constitution⁷⁰ (enshrining the right to protection of one's honour, private life and image, including where computer technology is used), when decisions on measures to put a stop to the violation of the rights protected by Article 8 LSSI are enforced, **judicial authorisation** must be obtained under Article 122 of the Administrative Proceedings Act (LPCA). Decisions of the Second Section of the Intellectual Property Commission must not affect the rights protected by the Constitution. These include the protection of **law and order** and **criminal investigations**, of **public security** and **national defence**, of **public health** and private individuals, of **consumers' or users' rights**, even when they are acting as investors, of a person's **dignity, non-discrimination**, and the **protection of children and young people** and of **intellectual property** rights. Under Article 122 bis 2) LPCA, measures adopted by the Second Section of the Intellectual Property Commission to suspend or block information society services or remove content that violates intellectual property rights in accordance with the LSSI (cf. section 1) cannot be executed without a **judicial decision**.

This also applies to the rights protected by Article 20 of the Constitution,⁷¹ including freedom of expression, communication, opinion, thought, etc., and paragraph 5 of the same Article, which establishes that publications, recordings and other means of information cannot be seized without a **judicial decision**.

Paragraph 1 of Article 122 bis 2) LPCA⁷² thus establishes that the execution of measures adopted by the Second Section of the Intellectual Property Commission to "suspend or block information society services or remove content that violates intellectual property rights [...] requires a prior judicial decision".⁷³ The second paragraph of Article 122 bis 2) provides for the judge, within two days of

⁷⁰ Spanish Constitution Art. 18 : « 1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.

2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.

3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.

4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

⁷¹ Art. 20 Cst. : « 1. Se reconocen y protegen los derechos: a) A expresar y difundir libremente los pensamientos, ideas y opiniones mediante la palabra, el escrito o cualquier otro medio de reproducción.

b) A la producción y creación literaria, artística, científica y técnica.

c) A la libertad de cátedra.

d) A comunicar o recibir libremente información veraz por cualquier medio de difusión. La ley regulará el derecho a la cláusula de conciencia y al secreto profesional en el ejercicio de estas libertades.

2. El ejercicio de estos derechos no puede restringirse mediante ningún tipo de censura previa.

3. La ley regulará la organización y el control parlamentario de los medios de comunicación social dependientes del Estado o de cualquier ente público y garantizará el acceso a dichos medios de los grupos sociales y políticos significativos, respetando el pluralismo de la sociedad y de las diversas lenguas de España.

4. Estas libertades tienen su límite en el respeto a los derechos reconocidos en este Título, en los preceptos de las leyes que lo desarrollen y, especialmente, en el derecho al honor, a la intimidad, a la propia imagen y a la protección de la juventud y de la infancia.

⁷² Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, available at http://noticias.juridicas.com/base_datos/Admin/l29-1998.t5.html#a122 (29.06.15).

⁷³ Ley 29/1998, art. 122 bis 2) first paragraph : « La ejecución de las medidas para que se interrumpa la prestación de servicios de la sociedad de la información o para que se retiren contenidos que vulneren la propiedad intelectual, adoptadas por la Sección Segunda de la Comisión de Propiedad Intelectual en

receiving notification of the Commission's decision, to summon to an adversarial hearing the legal representatives of the administrative authorities, the public prosecutor's office (*Ministerio fiscal*⁷⁴), and the holders of the rights and freedoms affected or their representatives.

Within two days following that hearing the judge issues a formal decision (*auto*) allowing or rejecting the measure.⁷⁵ Under article 80.1.b) of the LPCA an appeal against that decision may be lodged to the court.⁷⁶

In the specific field of **cyber security**, under additional provision 9 of the LSSI,⁷⁷ in conformity with their codes of conduct, information society service providers must identify the users affected by cyber security incidents of which they are informed by the supervisory authority and tell the users concerned what steps to take to resolve the incidents. If the users fail to eliminate the causes of the incident within the deadline fixed by the authority, the service providers must then, at the request of the supervisory authority, **isolate (*aislar*) the equipment or the service** concerned by the security incident in order to avoid adverse effects on third parties, until the security threat has been eliminated. This applies to any service located in Spain, all services with a domain name ending in ".es" and any services registered in Spain. When blocking or removal measures are ordered by the judicial authorities, the procedure to follow is that laid down in the law covering civil or criminal procedure, depending on the area in respect of which the measures are taken. Similarly, the

aplicación de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la información y de Comercio Electrónico, requerirá de autorización judicial previa de conformidad con lo establecido en los párrafos siguientes ».

⁷⁴ There is a Public Prosecutor in Spain who specialises in Computer Crime (*Fiscal de Sala de Criminalidad Informática*) and whose duties include intervening in criminal proceedings involving computer crime: https://www.fiscal.es/fiscal/publico/ciudadano/fiscal_especialista/criminalidad_informatica/funciones/!ut/p/a1/04_Sj9CPykssy0xPLMnMz0vMAfGjzOI9HT0cDT2DDbzcFzSzcDBzdPYOdTD08jL19TIEKInErsAgywas_wAyg3wAHcDTAp9_E2Qy_SAFRNmPRwEB_4frR-FT4u9nhl8BOIjACvCFAaFQKMgNDQ2NMMj0TdUBABgarhU/dI5/d5/L2dBISEvZ0FBIS9nQSEh/ (05.07.15); Instrucción 2/2011 sobre el fiscal de sala de criminalidad informática y las secciones de criminalidad informática de las fiscalías, available at https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/memoria2012_vol1_instru_02.pdf?idFile=6311c525-d23a-45d7-9e50-458f6f8c3406 (30.06.15).

⁷⁵ Ley 29/1998, art. 122 bis last paragraph : « En el plazo improrrogable de dos días siguientes a la recepción de la notificación de la resolución de la Comisión y poniendo de manifiesto el expediente, el Juzgado convocará al representante legal de la Administración, al Ministerio Fiscal y a los titulares de los derechos y libertades afectados o a la persona que éstos designen como representante a una audiencia, en la que, de manera contradictoria, el Juzgado oír a todos los personados y resolverá en el plazo improrrogable de dos días mediante auto. La decisión que se adopte únicamente podrá autorizar o denegar la ejecución de la medida ».

⁷⁶ "El recurso contra el Auto será el de apelación en un solo efecto, es decir, ante el mismo Juzgado"

⁷⁷ Disp. Ad. 9, LSSI: « 4. Conforme a los códigos de conducta que se definan en particular, los prestadores de servicios de la sociedad de la información deberán identificar a los usuarios afectados por los incidentes de ciberseguridad que les sean notificados por el CERT competente, e indicarles las acciones que deben llevar a cabo y que están bajo su responsabilidad, así como los tiempos de actuación. En todo caso, se les proporcionará información sobre los perjuicios que podrían sufrir u ocasionar a terceros si no colaboran en la resolución de los incidentes de ciberseguridad a que se refiere esta disposición.

En el caso de que los usuarios no ejerciesen en el plazo recomendado su responsabilidad en cuanto a la desinfección o eliminación de los elementos causantes del incidente de ciberseguridad, los prestadores de servicios deberán, bajo requerimiento del CERT competente, aislar dicho equipo o servicio de la red, evitando así efectos negativos a terceros hasta el cese de la actividad maliciosa.

El párrafo anterior será de aplicación a cualquier equipo o servicio geolocalizado en España o que esté operativo bajo un nombre de dominio «.es» u otros cuyo Registro esté establecido en España».

possibilities of appeal are those generally open to the interested parties in civil or criminal proceedings.

Lastly, concerning the protection of personal data, when removal measures are ordered by the Data Protection Agency there are two possible means by which interested parties can challenge those measures, namely a “*recurso de reposición*” lodged with the Director of the Agency (Article 116 of Law 30/1992⁷⁸), and an administrative appeal under Article 25 of Law 19/1998.⁷⁹ When a “*recurso de reposición*” is lodged with the Director of the Data Protection Agency that procedure has to run its course before an appeal can be lodged with the administrative court.

4. General Monitoring of Internet

In Spain there are numerous public and private bodies whose task it is to monitor the Web in various ways, according to their competences and the subject matter concerned.

In the first instance, Article 35.1 LSSI places responsibility for the supervision and monitoring of the Internet with the **Ministry of Industry, Energy and Tourism**. Article 35.1 *in fine* LSSI remains vague, stating that the competent authorities mentioned in the LSSI include the administrative and judicial authorities, each in their own field. Article 35.2 LSSI establishes that the authorities mentioned in Article 35.1 LSSI have the power to “carry out any inspection activities necessary for them to perform their supervisory role”. However, in the face of the threat of cyber attacks, in 2013 the Spanish Government set a strategy in place, spearheaded by a body called the **National Cyber Security Council** (*Consejo de Ciberseguridad Nacional*).⁸⁰ The Council organises cooperation between bodies with responsibilities in the cyber security field in Spain, such as the ministries and the CSIRTs (*Computer Security Incident Response Teams*).⁸¹

⁷⁸ Act 30/1992, Art.116: «1. Los actos administrativos que pongan fin a la vía administrativa podrán ser recurridos potestativamente en reposición ante el mismo órgano que los hubiera dictado o ser impugnados directamente ante el orden jurisdiccional contencioso-administrativo.

2. No se podrá interponer recurso contencioso-administrativo hasta que sea resuelto expresamente o se haya producido la desestimación presunta del recurso de reposición interpuesto », available at http://www.fomento.gob.es/NR/rdonlyres/FD4B6CA1-58FA-4686-B024-2C3590AE2E30/130739/Ley_30_1992_consolidado.pdf (15.07.15).

⁷⁹ Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, Art. 25 : « 1. El recurso contencioso-administrativo es admisible en relación con las disposiciones de carácter general y con los actos expresos y presuntos de la Administración pública que pongan fin a la vía administrativa, ya sean definitivos o de trámite, si estos últimos deciden directa o indirectamente el fondo del asunto, determinan la imposibilidad de continuar el procedimiento, producen indefensión o perjuicio irreparable a derechos o intereses legítimos. 2. También es admisible el recurso contra

la inactividad de la Administración y contra sus actuaciones materiales que constituyan vía de hecho, en los términos establecidos en esta Ley », available at http://noticias.juridicas.com/base_datos/Admin/l29-1998.t3.html#a25 (15.07.15). Legal doctrine : E. Deiros, Recursos contra una resolución de la Agencia Española de Protección de Datos, 2012, available at <http://evamunoz.es/recursos-contra-una-resolucion-de-la-agencia-espanola-de-proteccion-de-datos/> (15.07.15).

⁸⁰ Estrategia De Ciberseguridad Nacional 2013 Presidencia Del Gobierno, 2013, available at (06.03.15).

⁸¹ There are several national CSIRTs, one of which is the National Cryptology Centre, responsible for assisting and cooperating with the public administration on cyber security matters: <https://www.ccn-cert.cni.es/>, other is the CERT-SI, assisting the cyber protection of Critical Infrastructures https://www.incibe.es/CERT/Infraestructuras_Criticas/ and supporting the services provided to citizens and families via the Internaut Security Office, whose Internet site is at: <https://www.osi.es/>. There are also a number of Spanish public and private CERTs from regional governments, financial or

The detection and surveillance of pornographic content involving minors and of Internet fraud, cyber attacks and piracy, is carried out in the field by the police “**Technological Investigation Brigade**” (*Brigada de Investigación Tecnológica*).⁸² The Brigade belongs to the Directorate General of Police and Guardia Civil⁸³ and its tasks include collecting evidence, bringing offenders to justice and placing the material collected in the hands of the courts.

There is also the Guardia Civil’s “**Telematic Crime Group**” (*Grupo Delitos Telemáticos*),⁸⁴ whose job is to investigate crime on computer systems and networks.

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

Measures such as the blocking, filtering and suspension of Web pages are in principle an **obstruction of the freedom of expression** enshrined in Article 10 of the European Convention on Human Rights. The obstruction may also affect third parties unrelated to the dispute in the context of which such measures are taken.⁸⁵

Accordingly, as explained in section 2.1 above, under the LSSI, when measures are adopted and implemented to block or remove content, **the guarantees, norms and procedures provided for by law in order to protect the right to private, personal and family life, personal data, freedom of expression and freedom of information** where these may be affected, must be respected in all circumstances. Furthermore, where the Constitution or the law attribute exclusive powers to the courts, only the judicial authorities can implement measures to block and remove content.

In keeping with the precepts of the European Court of Human Rights,⁸⁶ Article 11.4 LSSI requires that the measures referred to in Article 11 LSSI be **objective, proportionate** – that is to say not general in scope but as targeted as possible – and **non-discriminatory**.

For example, the case-law in Spain has rejected the possibility of “prior censorship” of Internet content. In the *www.diariodecadiz.es* case (see section 2.2.), the Cadiz Provincial Court held:

“In short [...] Spanish law has opted not to impose the obligation on service providers to monitor content in a general manner and a priori, that is to say before the content is posted, so as not to interfere with freedom of expression and other values. However, under Article 11 LSSI [service providers] do have an obligation of due diligence, in addition to that provided for in Article 16 LSSI, imposing a series of obligations in respect of content and of cooperation with the authorities in order to identify offenders and make them accountable for their illegal activities or the illegal content they disseminate on the Internet, or to stop the further dissemination of the content.”⁸⁷

insurance institutions or telecom and security companies that participate in the activities of First (<https://www.first.org/>).

⁸² Brigada de Investigación Tecnológica, site Internet available at http://www.policia.es/org_central/judicial/udef/bit_quienes_somos.html (03.03.15).

⁸³ The place the brigade occupies in the organisation chart can be seen here: http://www.policia.es/org_central/judicial/udef/bit_quienes_somos.html (03.03.15).

⁸⁴ Grupo de delitos telemáticos, site Internet: https://www.gdt.guardiacivil.es/webgdt/la_unidad.php (03.03.15).

⁸⁵ P. Asensio, op. cit., p. 155.

⁸⁶ CEDH, case no 3111/10, Ahmet Yildirim v. Turkey, 18 December 2012.

⁸⁷ Case *www.diariodecadiz.es*, op. cit. Dans le même sens : Audiencia Provincial de Barcelona (Sección 19ª). Sentencia núm. 98/2010 de 3 marzo. AC 2010\941 (private database): “If we carried out *a priori*

As to jurisdiction, **only the competent judicial authority** (the guardian of freedom of expression, the right to literary, artistic, scientific and technical creation and production, and freedom to impart and receive information) can authorise the implementation of the measures ordered by the Second Section of the Intellectual Property Commission (the procedural aspects are dealt with in section 3 above). The intervention of the courts thus appears to afford a guarantee against the execution of arbitrary administrative decisions.

In the light of the above, it would appear that Spanish law meets the foreseeability requirement laid down by the European Court of Human Rights: on the one hand it exhaustively lists the grounds on which action can be taken to block a service or remove illegal content, setting the corresponding limits and, on the other, it provides for a system of judicial guarantees before such measures can be taken. A proviso to this may be raised by the recent developments introduced in the LOPC, mentioned in section 2.1.2. As already explained, the provisions do not directly concern the blocking and filtering of information on the Internet, but could apply to the Internet if certain articles were interpreted with a degree of flexibility. The wording of certain provisions of the LOPC is not sufficiently clear, making it difficult to say at this stage how rights like freedom of expression and information will be affected by it. Nor is the way the provisions will be applied to information society service providers clearly defined. For example, Article 39.2.b) LOPC⁸⁸ provides for sanctions such as the confiscation of the “property, means or instruments which served to prepare or commit the offence, except if they belong to a *bona fide* third party who is not responsible for the offence”. In certain cases this could apply to information society service providers, except where they can be considered as innocent “*bona fide* third parties”. However, bearing in mind the requirement of “effective awareness” of the unlawfulness of the Internet content under Article 16 of the LSSI, it is safe to say that a third party will not be considered to have acted in good faith if they were effectively aware of the illegal content.

Dr. Alberto Aronovitz
October 2015

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

88 controls it would generate situations where freedom of expression was undermined, as censorship would be carried out pre-emptively to avoid disputes.”
Art. 39.2.b) LOPC : « b) El comiso de los bienes, medios o instrumentos con los que se haya preparado o ejecutado la infracción y, en su caso, de los efectos procedentes de ésta, salvo que unos u otros pertenezcan a un tercero de buena fe no responsable de dicha infracción que los haya adquirido legalmente ».

