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 539-553

This document is part of the Comparative Study on blocking, filtering and take-down of illegal Internet content in the 47 member States of the Council of Europe, which was prepared by the Swiss Institute of Comparative Law upon an invitation by the Secretary General. The opinions expressed in this document do not engage the responsibility of the Council of Europe. They should not be regarded as placing upon the legal instruments mentioned in it any official interpretation capable of binding the governments of Council of Europe member States, the Council of Europe's statutory organs or the European Court of Human Rights.

Avis 14-067

Lausanne, 20 December 2015
National reports current at the date indicated at the end of each report.

Dorigny – CH – 1015 Lausanne - Tel : +41 (0)21 692 49 11 - Fax : +41 (0)21 692 4949 –
www.isdc.ch – info@isdc.ch

I. INTRODUCTION

On 24th November 2014, the Council of Europe formally mandated the Swiss Institute of Comparative Law ("SICL") to provide a comparative study on the laws and practice in respect of filtering, blocking and takedown of illegal content on the internet in the 47 Council of Europe member States.

As agreed between the SICL and the Council of Europe, the study presents the laws and, in so far as information is easily available, the practices concerning the filtering, blocking and takedown of illegal content on the internet in several contexts. It considers the possibility of such action in cases where public order or internal security concerns are at stake as well as in cases of violation of personality rights and intellectual property rights. In each case, the study will examine the legal framework underpinning decisions to filter, block and takedown illegal content on the internet, the competent authority to take such decisions and the conditions of their enforcement. The scope of the study also includes consideration of the potential for existing extra-judicial scrutiny of online content as well as a brief description of relevant and important case law.

The study consists, essentially, of two main parts. The first part represents a compilation of country reports for each of the Council of Europe Member States. It presents a more detailed analysis of the laws and practices in respect of filtering, blocking and takedown of illegal content on the internet in each Member State. For ease of reading and comparison, each country report follows a similar structure (see below, questions). The second part contains comparative considerations on the laws and practices in the member States in respect of filtering, blocking and takedown of illegal online content. The purpose is to identify and to attempt to explain possible convergences and divergences between the Member States' approaches to the issues included in the scope of the study.

II. METHODOLOGY AND QUESTIONS

1. Methodology

The present study was developed in three main stages. In the first, preliminary phase, the SICL formulated a detailed questionnaire, in cooperation with the Council of Europe. After approval by the Council of Europe, this questionnaire (see below, 2.) represented the basis for the country reports.

The second phase consisted of the production of country reports for each Member State of the Council of Europe. Country reports were drafted by staff members of SICL, or external correspondents for those member States that could not be covered internally. The principal sources underpinning the country reports are the relevant legislation as well as, where available, academic writing on the relevant issues. In addition, in some cases, depending on the situation, interviews were conducted with stakeholders in order to get a clearer picture of the situation. However, the reports are not based on empirical and statistical data, as their main aim consists of an analysis of the legal framework in place.

In a subsequent phase, the SICL and the Council of Europe reviewed all country reports and provided feedback to the different authors of the country reports. In conjunction with this, SICL drafted the comparative reflections on the basis of the different country reports as well as on the basis of academic writing and other available material, especially within the Council of Europe. This phase was finalized in December 2015.

The Council of Europe subsequently sent the finalised national reports to the representatives of the respective Member States for comment. Comments on some of the national reports were received back from some Member States and submitted to the respective national reporters. The national reports were amended as a result only where the national reporters deemed it appropriate to make amendments. Furthermore, no attempt was made to generally incorporate new developments occurring after the effective date of the study.

All through the process, SICL coordinated its activities closely with the Council of Europe. However, the contents of the study are the exclusive responsibility of the authors and SICL. SICL can however not assume responsibility for the completeness, correctness and exhaustiveness of the information submitted in all country reports.

2. Questions

In agreement with the Council of Europe, all country reports are as far as possible structured around the following lines:

1. What are the legal sources for measures of blocking, filtering and take-down of illegal internet content?

Indicative list of what this section should address:

- Is the area regulated?
- Have international standards, notably conventions related to illegal internet content (such as child protection, cybercrime and fight against terrorism) been transposed into the domestic regulatory framework?

- Is such regulation fragmented over various areas of law, or, rather, governed by specific legislation on the internet?
- Provide a short overview of the legal sources in which the activities of blocking, filtering and take-down of illegal internet content are regulated (more detailed analysis will be included under question 2).

2. What is the legal framework regulating:

2.1. Blocking and/or filtering of illegal internet content?

Indicative list of what this section should address:

- On which grounds is internet content blocked or filtered? This part should cover all the following grounds, wherever applicable:
  - the protection of national security, territorial integrity or public safety (e.g. terrorism),
  - the prevention of disorder or crime (e.g. child pornography),
  - the protection of health or morals,
  - the protection of the reputation or rights of others (e.g. defamation, invasion of privacy, intellectual property rights),
  - preventing the disclosure of information received in confidence.
- What requirements and safeguards does the legal framework set for such blocking or filtering?
- What is the role of Internet **Access** Providers to implement these blocking and filtering measures?
- Are there soft law instruments (best practices, codes of conduct, guidelines, etc.) in this field?
- A brief description of relevant case-law.

2.2. Take-down/removal of illegal internet content?

Indicative list of what this section should address:

- On which grounds is internet content taken-down/ removed? This part should cover all the following grounds, wherever applicable:
  - the protection of national security, territorial integrity or public safety (e.g. terrorism),
  - the prevention of disorder or crime (e.g. child pornography),
  - the protection of health or morals,
  - the protection of the reputation or rights of others (e.g. defamation, invasion of privacy, intellectual property rights),
  - preventing the disclosure of information received in confidence.
- What is the role of Internet Host Providers and Social Media and other Platforms (social networks, search engines, forums, blogs, etc.) to implement these content take down/removal measures?
- What requirements and safeguards does the legal framework set for such removal?
- Are there soft law instruments (best practices, code of conduct, guidelines, etc.) in this field?
- A brief description of relevant case-law.

3. Procedural Aspects: What bodies are competent to decide to block, filter and take down internet content? How is the implementation of such decisions organized? Are there possibilities for review?

Indicative list of what this section should address:

- What are the competent bodies for deciding on blocking, filtering and take-down of illegal internet content (judiciary or administrative)?
- How is such decision implemented? Describe the procedural steps up to the actual blocking, filtering or take-down of internet content.
- What are the notification requirements of the decision to concerned individuals or parties?
- Which possibilities do the concerned parties have to request and obtain a review of such a decision by an independent body?

4. General monitoring of internet: Does your country have an entity in charge of monitoring internet content? If yes, on what basis is this monitoring activity exercised?

Indicative list of what this section should address:

- The entities referred to are entities in charge of reviewing internet content and assessing the compliance with legal requirements, including human rights – they can be specific entities in charge of such review as well as Internet Service Providers. Do such entities exist?
- What are the criteria of their assessment of internet content?
- What are their competencies to tackle illegal internet content?

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

Indicative list of what this section should address:

- Does the law (or laws) to block, filter and take down content of the internet meet the requirements of quality (foreseeability, accessibility, clarity and precision) as developed by the European Court of Human Rights? Are there any safeguards for the protection of human rights (notably freedom of expression)?
- Does the law provide for the necessary safeguards to prevent abuse of power and arbitrariness in line with the principles established in the case-law of the European Court of Human Rights (for example in respect of ensuring that a blocking or filtering decision is as targeted as possible and is not used as a means of wholesale blocking)?
- Are the legal requirements implemented in practice, notably with regard to the assessment of necessity and proportionality of the interference with Freedom of Expression?
- In the case of the existence of self-regulatory frameworks in the field, are there any safeguards for the protection of freedom of expression in place?
- Is the relevant case-law in line with the pertinent case-law of the European Court of Human Rights?

For some country reports, this section mainly reflects national or international academic writing on these issues in a given State. In other reports, authors carry out a more independent assessment.

PORTUGAL

1. Legal Sources

Portugal falls into the category of jurisdictions which have **specific legislation** on the activities of information society players. Among other things, this legislation deals with measures such as interruption of Internet access by information society service providers (blocking) and take-down/removal of certain types of Internet content.

The main pieces of legislation in this area are Decree-Law No. 7/2004 of 7 January 2004, the law on data protection and the law on intellectual property.

1.1. Decree-Law 7/2004 of 7 January 2004 (DL)[1]

The DL transposes Directive 2000/31/EC of 8 June 2000 on the information society and in particular electronic commerce. According to Article 3.1 DL, "information society service" means any service provided at a distance by electronic means, for remuneration (or at least in the context of an economic activity) at the request of the recipient. Legal commentators have pointed out that this definition is sufficiently broad to also include Internet users who occasionally provide Internet services in a non-professional capacity and in some cases even for free.[2]

The DL provides for **freedom of communication and browsing on the Internet.** The freedom to provide services in the context of the information society is not absolute, however, as Article 7 DL contains a number of restrictions. These apply to content which poses a threat to **public policy** and **public security**, the protection of **public health** and consumer and user protection, respect for **human dignity**, **non-discrimination**, **youth and child welfare** and **intellectual property** rights (cf. sections 2.1 and 2.2).

In addition to the freedom to provide information society services, there is also the so-called **"non-liability" rule** whereby **information society service providers** are, in principle, not liable for the content that they transmit or host. This rule applies to providers of transmission, temporary and server-based storage, hyperlink and search engine services, provided they comply with certain (general) supervisory obligations[3] (cf. sections 2 and 3).

Art. 13 DL[4] contains a series of obligations requiring information society service providers to, *inter alia*:

---

1 Ministério da Justiça, Decreto-Lei n. 7/2004 de 7 de Janeiro, available at http://www.anacom.pt/render.jsp?contentId=952094#.VaYEGWc1-os (23.03.15).

2 V. Marques Dias, Universidade de Lisboa, Faculdade de direito, a responsabilidade dos prestadores de serviços em rede - as inovações do decreto-lei 7/2004 - relatório de direito da sociedade da informação, notes 22 and 23, available at http://www.verbojuridico.com/doutrina/2011/veradias_responsabilidadeprestadoresservicosrede.pdf (23.04.15).

3 A. Dias Pereira, Princípios do comércio electrónico (breve apontamento ao dl 7/2004, 7.1), available at https://estudogeral.sib.uc.pt/bitstream/10316/28782/1/PRINC%C3%8DPIOS%20DO%20COM%C3%89RCIO%20ELECTR%C3%93NICO.pdf (25.05.15).

4 Art. 13 DL : « Deveres comuns dos prestadores intermediários dos serviços. Cabe aos prestadores intermediários de serviços a obrigação para com as entidades competentes:
a) De informar de imediato quando tiverem conhecimento de actividades ilícitas que se desenvolvam por via dos serviços que prestam;

a) immediately notify the competent authorities on becoming aware of any illegal activities undertaken via the services rendered by them,
b) meet requests to identify the recipients of their services with whom they have storage agreements,
c) comply promptly with any instructions to terminate an infringement, including removing or disabling access to content,
d) supply lists of owners of storage sites, whenever so requested.

We will return in sections 2 and 3 to the subject of take-down/removal and blocking of Internet content.

Portugal recognises four types of information society players, depending on the kind of service provided: those which act as a "mere conduit", those which provide temporary storage, those which provide hosting services and those which engage in activities involving content aggregation services (search engines, providers of hyperlinks, etc.). Under the terms of the DL, the first three types of activity are covered by the conditional exemption from liability, in line with Directive 2000/31/EC of 8 June 2000. Portugal has extended these exemption rules to include providers of content aggregation services.

Accordingly, the system of liability applicable to hosting providers generally also applies to providers of **content aggregation services** who offer search engines that allow access to potentially illegal content[5]. Content aggregation, however, is not deemed to be irregular merely on the grounds that the destination website contains illegal information. The link is legal if it is performed "with objectivity and caution" (*objetividade e distanciamento*), in the context of the exercise of the right to information. The assessment as to whether it is legal or illegal will depend on the individual circumstances, namely:

- possible confusion between the contents of the source site and the destination sites;
- the automatic or intentional character of the link;
- the area of the destination website to which the link is made[6].

---

b) De satisfazer os pedidos de identificar os destinatários dos serviços com quem tenham acordos de armazenagem;
c) De cumprir prontamente as determinações destinadas a prevenir ou pôr termo a uma infracção, nomeadamente no sentido de remover ou impossibilitar o acesso a uma informação;
d) De fornecer listas de titulares de sítios que alberguem, quando lhes for pedido ».

5 Art. 17 DL : « Responsabilidade dos prestadores intermediários de serviços de associação de conteúdos.
Os prestadores intermediários de serviços de associação de conteúdos em rede, por meio de instrumentos de busca, hiperconexões ou processos análogos que permitam o acesso a conteúdos ilícitos estão sujeitos a regime de responsabilidade correspondente ao estabelecido no artigo anterior".

6 Art. 19 DL : « Relação com o direito à informação. 1 — A associação de conteúdos não é considerada irregular unicamente por haver conteúdos ilícitos no sítio de destino, ainda que o prestador tenha consciência do facto.
2 — A remissão é lícita se for realizada com objectividade e distanciamento, representando o exercício do direito à informação, sendo, pelo contrário, ilícita se representar uma maneira de tomar como próprio o conteúdo ilícito para que se remete.
3 — A avaliação é realizada perante as circunstâncias do caso, nomeadamente: a) A confusão eventual dos conteúdos do sítio de origem com os de destino; b) O carácter automatizado ou intencional da remissão; c) A área do sítio de destino para onde a remissão é efectuada".

1.2. Law on personal data protection (LPD)[7]

The LPD incorporates into Portuguese law Directive 95/46/EC on the protection of individuals with regard to the processing of personal data. Article 4.1 LPD provides that the LPD applies to personal data processing, whether performed entirely or partially by automatic means.
Article 22.3.b) LPD confers on the National Commission for Data Protection (CNPD) the power to order the **blocking, erasure or destruction of unlawfully processed data** and also to **prohibit, temporarily or permanently, the processing of such data** (see sections 2.1 and 2.2).

1.3. Law on intellectual property (LPI)[8]

Freedom in the information society is limited by the fact that it is prohibited to commit illegal acts, including infringements of intellectual property rights through the illegal use of protected material such as texts, musical compositions, films, computer programs, databases, trademarks and distinctive signs.[9]

Besides the usual protective procedures provided for in Articles 362 et seq. of the Portuguese Code of Civil Procedure,[10] the LPI allows the **judicial authorities** to take various measures involving **blocking** access to certain websites and **removing** Internet content (see sections 2.1 and 2.2).

1.4. International sources

At international level, Portugal has ratified the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse,[11] the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[12] and the Convention on the Prevention of Terrorism.[13] Once they have been officially published, these conventions form part of the Portuguese legal system.[14]

---

7 Lei da protecção de dados pessoais, Lei n.º 67/98 de 26 de Outubro, available at : http://www.cnpd.pt/bin/legis/nacional/lei_6798.htm (23.04.15).

8 Lei n.º 16/2008, de 1 de Abril, Transpõe para a ordem jurídica interna a Directiva n.º 2004/48/CE, do Parlamento Europeu e do Conselho, de 29 de Abril, relativa ao respeito dos direitos de propriedade intelectual, procedendo à terceira alteração ao Código da Propriedade Industrial, à sétima alteração ao Código do Direito de Autor e dos Direitos Conexos e à segunda alteração ao Decreto-Lei n.º 332/97, de 27 de Novembro, available at https://dre.pt/application/dir/pdf1sdip/2008/04/06400/0189401983.pdf (04.06.15).

9 A. Dias Pereira, op. cit., ch. 4.4.

10 Lei n.º 41/2013, de 26 de junho, Aprova o Código de Processo Civil, available at https://dre.pt/application/dir/pdf1sdip/2013/06/12100/0351803665.pdf (04.06.15).

11 Convenção do Conselho da Europa para a Proteção das Crianças contra a Exploração Sexual e os Abusos Sexuais. Aprovada pela Resolução da Assembleia da República n.º 75/2012, ratificada pelo Decreto do Presidente da República n.º 90/2012, Diário da República I, n.º 103, de 28/05/2012; Lei n.º 113/2009 de 17 de Setembro Estabelece medidas de protecção de menores, em cumprimento do artigo 5.º da Convenção do Conselho da Europa contra a Exploração Sexual e o Abuso Sexual de Crianças, available at http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1139&tabela=leis (23.04.15).

12 Convenção para a Protecção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal. Adoptada e aberta à assinatura em Estrasburgo, a 28 de Janeiro de 1981.

13 Convenção do Conselho da Europa relativa ao branqueamento, detecção, apreensão e perda dos produtos do crime e ao financiamento do terrorismo, Diário da República, de 4 de Junho, o Aviso n.º 77/2010, a República Portuguesa depositou junto do Secretário-Geral do Conselho da Europa, o instrumento de ratificação da Convenção do Conselho da Europa relativa ao branqueamento, detecção, apreensão e perda dos produtos do crime e ao financiamento do terrorismo, adoptada em Varsóvia a 16 de Maio de 2005. Portugal a ratifié cette convention par le Decreto do Presidente da

2. Legal Framework

As already stated, under Article 11 DL,[15] Portugal applies the "assimilation" (*equiparação*) principle, which requires that all information society service providers be treated in the same way. This means that information society players are governed by **common rules on liability**, with slight differences *mutatis mutandis.*[16] In according providers of content aggregation services (such as search engines and hyperlinks) the same status as hosting providers, Portugal has gone beyond what is required under Directive 2000/31/EC.[17]

The general rule is that **there is no blanket due diligence requirement** regarding the information that is transmitted or stored. Nor does the law require information society players to investigate possible illegal acts.[18] Legal commentators refer here to the "non-liability regime" for service providers.[19]

2.1. Blocking and/or filtering of illegal Internet content

2.1.1. Restrictive measures under the DL

Art. 7 DL[20] provides that restrictions may be placed on the movement of an information society service if it features **illegal content,** meaning content which poses a threat to **human dignity, public policy** (including the protection of minors and the fight against incitement to hatred on grounds of race, sex, religion or nationality), **public health**, **national security and defence**, **consumer and investor r**ights.

República n.º 78/2009, de 27 de Agosto, tendo depositado o seu instrumento de ratificação em 22 de Abril de 2010).

14 Under Article 8.2 of the Portuguese Constitution, the rules set out in international agreements duly ratified or approved by Portugal enter into force in Portuguese internal law once they have been officially published. « 2. As normas constantes de convenções internacionais regularmente ratificadas ou aprovadas vigoram na ordem interna após a sua publicação oficial e enquanto vincularem internacionalmente o Estado Português » ; A. Aronovitz, Portugal, 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.

15 Art. 11 DL : « Princípio da equiparação. A responsabilidade dos prestadores de serviços em rede está sujeita ao regime comum, nomeadamente em caso de associação de conteúdos, com as especificações constantes dos artigos seguintes ».

16 A. Dias Pereira, op. cit. Ch. 4.

17 A. Dias Pereira, op. cit. Ch. 4 ; V. Marques Dias, op. cit.

18 A. Dias Pereira, op. cit. Ch. 4.

19 V. Marques Dias, A responsabilidade dos prestadores de serviços em rede - as inovações do decreto-lei 7/2004 - Relatório de direito da sociedade da informação, available at http://www.verbojuridico.com/doutrina/2011/veradias_responsabilidadeprestadoresservicosrede.pdf (09.06.15).

20 Artigo 7 DL : « Medidas restritivas. 1. Podem ser adotadas medidas, incluindo providências concretas contra um prestador de serviços, restritivas à circulação de um determinado serviço da sociedade da informação proveniente de outro Estado membro da União Europeia na medida em que possa lesar ou ameaçar gravemente:
a) A dignidade humana ou a ordem pública, incluindo a protecção de menores e a repressão do incitamento ao ódio fundado na raça, no sexo, na religião ou na nacionalidade, nomeadamente por razões de prevenção ou repressão de crimes ou de ilícitos de mera ordenação social;
b) A saúde pública;
c) A segurança pública, nomeadamente na vertente da segurança e defesa nacionais;
d) Os consumidores, incluindo os investidores ».

The DL refers to the possibility of blocking access to Internet content[21] in several provisions. Art. 13 DL, under the heading "Common duties of intermediary service providers", contains a requirement to comply promptly with any decisions taken by the authorities (ANACOM or the courts), the purpose of which is to terminate an infringement, by disabling **access** (*impossibilitar o acesso*) to information. In addition, Art. 15.3 DL provides that intermediary service providers may be liable if they do not act expeditiously to block Internet access in cases where they are aware that information has been removed from the initial source, or that access to such information has been disabled, or that a court or administrative authority has ordered such removal or disablement.

These requirements are in line with the list of obligations which the DL places on each service provider, in particular to promptly notify the authorities (administrative decisions are taken by ANACOM and the **courts then authorise their enforcement**, see 2.2) if they become aware of any illegal activities conducted via the services rendered by them, to comply with requests to identify the recipients of their services with whom they have storage agreements, and to **promptly comply with any decisions on the part of the authorities, the purpose of which is to prevent or stop an infringement**, namely to **remove or disable access** to information and to provide lists of owners of hosted websites.[22]

2.1.2. Restrictive measures under the LPD

As was pointed out in section 1.2, Art. 22.3.b) LPD assigns the CNPD the **power to order the blocking, erasure** or destruction of **unlawfully processed data,** and also to **prohibit, temporarily or permanently, the processing of such data**. To this end, Art. 24 LPD **requires public and private entities to co-operate** with the CNPD, meaning that they must, for example, provide the CNPD with any information it may request and allow the commission to have access to computer systems and files in which personal data are stored, and to any relevant documentation.

Under Article 23.3 LPD, in the performance of its functions, the CNPD may issue binding decisions. These decisions are **subject to judicial review by the Central Administrative Court** (cf. section 3).

2.1.3. Protection of intellectual property rights

Art. 225 LPI[23] provides that, in relation to the offences provided for in the LPI, ancillary penalties may be imposed, such as confiscation of the objects used to commit the offence and the disabling (or, where appropriate, destruction) of instruments, devices, goods and services whose sole purpose is to facilitate the elimination or unauthorised neutralisation of any technical measures taken.

---

21 "Filtering" is not specifically mentioned but "disabling access" could be deemed to include such measures.

22 P. Venâncio, Prestação de serviços em rede, JusNet 12/2008.

23 Art. 225.1 LPI: "Relativamente aos crimes previstos nos artigos anteriores, podem ser aplicadas as seguintes penas acessórias:
a) A perda dos instrumentos usados na prática dos crimes, incluindo o lucro ilícito obtido;
b) A inutilização e, caso necessário, a destruição dos instrumentos, dispositivos, produtos e serviços cujo único uso sirva para facilitar a supressão ou neutralização, não autorizadas, das medidas eficazes de carácter tecnológico, ou que permita a supressão ou modificação, não autorizadas, da informação para a gestão electrónica de direitos".

Article 227 LPI[24] deals with injunctions (*procedimentos cautelares*) and states that rights-holders may – where a violation has occurred or is about to occur – request **that measures be taken (blocking, removal) to protect their rights.** Such action may be taken against intermediaries, in particular in the context of Internet, whose services are used by a third party to infringe a copyright or related right, without prejudice to the right of the rights-holders to inform the intermediaries, in advance and directly, of any illegal acts, for the purposes of preventing or terminating them.

2.2. Take-down/removal of illegal Internet content

The DL refers to the possibility of **removing** (retirar) Internet content in the following articles:
Art. 13 DL, under the heading "common duties of intermediary service providers" contains a requirement to comply promptly with any decisions the purpose of which is to **terminate an infringement**, namely to remove (remover) the data.

Article 15.3 DL provides that intermediary service providers may be liable if they do not act expeditiously to remove information in cases where they are aware that the information has been removed from the initial source, or that access to such information has been disabled, or that a court or administrative authority has ordered such removal or disablement.

In addition, Art. 16 DL provides that hosting providers and/or providers of content aggregation services are liable for the information stored where the information is "**obviously illegal**" and they fail to **remove** (*retirar*) such information or the corresponding link. In addition, with regard to providers of content aggregation services (search engines, hyperlinks, etc.), Art. 17 DL provides that such providers will be liable **if they allow access** to content that is obviously illegal.

With regard to the case provided for in Articles 16 and 17 DL, Article 18 DL[25] states that if the illegal nature of the information is not "obvious", the service provider **is not obliged to remove the content or to disable access** to it merely because an interested party alleges that there has been a violation of the law.
In such cases, the interested party who wishes the illegal content to be removed, or access to it to be disabled, can ask the regulator (ANACOM) to adopt a "provisional settlement" within 48 hours (see section 3). With regard to duration, Article 18.5 DL[26] states that the regulator may alter the terms of such settlement "at any time".

---

[24] Art. 227 LC : « 1 - Os titulares de direitos podem, em caso de violação dos mesmos ou quando existam fundadas razões de que esta se vai produzir de modo iminente, requerer ao tribunal o decretamento das medidas cautelares previstas na lei geral, e que, segundo as circunstâncias, se mostrem necessárias para garantir a protecção urgente do direito.
2 - O disposto no número anterior aplica-se no caso em que os intermediários, a que recorra um terceiro para infringir um direito de autor ou direitos conexos, possam ser destinatários das medidas cautelares previstas na lei geral, sem prejuízo da faculdade de os titulares de direitos notificarem, prévia e directamente, os intermediários dos factos ilícitos, em ordem à sua não produção ou cessação de efeitos ».

[25] Art. 18 DL : « 1. Nos casos contemplados nos artigos 16.º e 17.º, o prestador intermediário de serviços, se a ilicitude não for manifesta, não é obrigado a remover o conteúdo contestado ou a impossibilitar o acesso à informação só pelo facto de um interessado arguir uma violação.
2. Nos casos previstos no número anterior, qualquer interessado pode recorrer à entidade de supervisão respectiva, que deve dar uma solução provisória em quarenta e oito horas e logo a comunica electronicamente aos intervenientes.
3. Quem tiver interesse jurídico na manutenção daquele conteúdo em linha pode nos mesmos termos recorrer à entidade de supervisão contra uma decisão do prestador de remover ou impossibilitar o acesso a esse conteúdo, para obter a solução provisória do litígio".

[26] Art. 18.5 DL: "5 - A entidade de supervisão pode a qualquer tempo alterar a composição provisória do litígio estabelecida".

Whoever has an interest in maintaining the content online, however, can appeal to the regulator against a decision by the service provider to remove or disable access to that content (see section 3).

Accordingly, under the rules in place in Portugal, except in cases where the illegality is obvious, the interested parties can ask the regulator (ANACOM) to adopt such provisional measures as it deems appropriate in the circumstances. Any action which the regulator may take is purely **temporary,** however, and any permanent measures that may be required must be imposed by the courts. It will further be noted that ANACOM is an independent authority[27] that acts very swiftly (within 48 hours), at the request of an interested party, and that if a party objects to the removal measures, it has the right to appeal. Under Article 51 of the Decree-Law No. 39/2015 of 16 March 2015,[28] ANACOM's activities are subject to judicial review by the administrative courts.

It should also be pointed out that Article 37.2 DL[29] provides for fines ranging from €5,000 to €100,000 for information society players who, *inter alia*:

- fail to comply with a decision by the regulator or the courts, ordering them to "**terminate**" an infringement pursuant to Art. 13 c) DL;
- fail to inform the authorities of any illegal activities of which they may be aware and which are undertaken via the services rendered by them pursuant to Art. 13 a);
- **fail to remove** content which is obviously illegal, as provided for in Articles 16 and 17 DL;
- **fail to remove or to disable access** to information hosted by them, where they are aware that the information in question has been **removed from its initial source** or that **access** to the source has been disabled or that a court or administrative authority has ordered **such removal or access disablement** with immediate enforcement pursuant to Art. 15.3) DL.

---

27 ANACOM is an independent administrative authority: "A natureza da redenominada Autoridade Nacional de Comunicações (ANACOM), enquanto entidade administrativa independente com funções de regulação do setor das comunicações, está há muito consolidada […]", premable of Décret-loi n.º 39/2015, of 16 march 2015, available at http://www.anacom.pt/render.jsp?contentId=1349601#.VaXw0mc1-os (15.07.2015).

28 Decree-law n.º 39/2015, op. cit, art. 51: " Controlo judicial. 1 - A atividade de natureza administrativa dos órgãos e agentes da ANACOM fica sujeita à jurisdição administrativa, nos termos da respetiva legislação.
2 - As sanções por infrações contraordenacionais são passíveis de recurso para o Tribunal de Concorrência, Regulação e Supervisão.
3 - Das decisões proferidas no âmbito da resolução de litígios cabe recurso para os tribunais, nos termos previstos na lei". Decree-Law 67/2012, of 20 March 2012 and Law 46/2011, of 24 June 2011 established the court for intellectual property and the court for competition, regulation and supervision http://www.anacom.pt/render.jsp?categoryId=345250 (14.07.15).

29 Art. 37.2 DL: "Constitui contra-ordenação sancionável com coima de E 5000 a E 100 000 a prática dos seguintes actos pelos prestadores de serviços: a) A desobediência a determinação da entidade de supervisão ou de outra entidade competente de identificar os destinatários dos serviços com quem tenham acordos de transmissão ou de armazenagem, tal como previsto na alínea b) do artigo 13.o; a) […] b) O não cumprimento de determinação do tribunal ou da autoridade competente de prevenir ou pôr termo a uma infracção nos termos da alínea c) do artigo 13.o; c) A omissão de informação à autoridade competente sobre actividades ilícitas de que tenham conhecimento, praticadas por via dos serviços que prestam, tal como previsto na alínea a) do artigo 13.o; d) A não remoção ou impedimento do acesso a informação que armazenem e cuja ilicitude manifesta seja do seu conhecimento, tal como previsto nos artigos 16.o e 17.o; e) A não remoção ou impedimento do acesso a informação que armazenem, se, nos termos do artigo 15.o, n.o 3, tiverem conhecimento que foi retirada da fonte, ou o acesso tornado impossível, ou ainda que um tribunal ou autoridade administrativa da origem ordenou essa remoção ou impossibilidade de acesso para ter exequibilidade imediata; f) A prática com reincidência das infracções previstas no n.o 1".

Under Article 38.3 DL,[30] additional penalties may be imposed on information society players. These include the "confiscation in favour of the state" of property used to commit the infringement, a ban on pursuing an activity for a maximum of six years in the case of natural persons and disqualification from managerial positions in companies which provide services. Bans or disqualification for periods of more than two years may be imposed only by the courts, at the request of the administrative authority.

The possibility of adopting measures of this kind under the LPI and the LPD was dealt with in section 2.1.

It should further be noted that, when it comes to protecting intellectual property rights, the General Inspectorate for Cultural Activities ("Inspeção-General das Atividades Culturais") is responsible, *inter alia*, for supervision, taxation and monitoring in the field of copyright and related rights.[31] In this context, the Inspectorate carries out inspections at national level for the purpose of detecting breaches of copyright, institutes proceedings and has the power to **order seizures.** In 2014, for example, the Inspectorate seized, *inter alia*, 306,807 files containing musical works, 280 files containing scientific and literary works, 2 sets of IT equipment, USB sticks and PCs.[32] It appears from a recent decision in 2015, examined below, that the Inspectorate has had occasion to order website hosts and intermediary providers of data aggregation services to disable access to a website which violated copyright and neighbouring rights.

Case law

Case law relating to the take-down/removal of websites is rare, if it exists at all. We did manage, however, to identify a few relevant cases.

On 28 April 2015,[33] Lisbon Central Court, at the request of the National Association representing Portuguese taxi drivers, ordered the head office of UBER in the United States to shut down (*encerrar*) the website www.uber.com in Portugal. The court likewise ordered the closure and prohibition of content, access and provision of transport services in Portugal via the website www.uber.com and

30 Art. 38 DL: "Sanções acessórias. 1 — Às contra-ordenações acima previstas pode ser aplicada a sanção acessória de perda a favor do Estado dos bens usados para a prática das infracções.
2 — Em função da gravidade da infracção, da culpa do agente ou da prática reincidente das infracções, pode ser aplicada, simultaneamente com as coimas previstas no n.o 2 do artigo anterior, a sanção acessória de interdição do exercício da actividade pelo período máximo de seis anos e, tratando-se de pessoas singulares, da inibição do exercício de cargos sociais em empresas prestadoras de serviços da sociedade da informação durante o mesmo período.
3 — A aplicação de medidas acessórias de interdição do exercício da actividade e, tratando-se de pessoas singulares, da inibição do exercício de cargos sociais em empresas prestadoras de serviços da sociedade da informação por prazo superior a dois anos será obrigatoriamente decidida judicialmente por iniciativa oficiosa da própria entidade de supervisão.
4 — Pode dar-se adequada publicidade à punição por contra-ordenação, bem como às sanções acessórias aplicadas nos termos do presente diploma".

31 Decreto Regulamentar n.º 43/2012 de 25 de maio, Diário da República, 1.ª série — N.º 102 — 25 de maio de 2012, 2777 et Ministério da Cultura, Decreto-Lei n.o 80/97 de 8 de Abril, Diário da República N.o 82 —8-4-1997 I série-A 1583.

32 Inspeção-Geral das Atividades Culturais, Boletim estatístico, 2014, p. 62, available at http://www.igac.pt/paginaJanelaExterna.aspx?codigono=6592AAAAAAAAAAAAAAAAAAA&cpp=1 (20.07.15).

33 Lisbon Central Court, decision of 28 April 2015. Extracts from this decision are available on the website of the *Associação nacional dos transportadores rodoviários em automóveis ligeiros*: http://antral.pt/pt/noticias/tribunal-de-lisboa-proibe-a-uber-de-operar-em-portugal-multa-de--10-000-00-por-cada-dia-de-infra/ (29.6.15).

any other websites used for the same purpose. To ensure compliance with these measures, **the court ordered that all telecommunications operators registered in Portugal**, in particular those involved in providing the service in question, **be notified of the obligation to suspend the transmission and hosting of data, access to telecommunications networks** and the supply of any other equivalent services connected with the Uber website. The court also ordered the Portuguese regulator ANACOM to act within the scope of its mandate to enforce the court's decision.

Legal literature on the subject mentions two other administrative decisions. The first, adopted by ANACOM pursuant to Article 18.2 DL, does not provide any further information on the case in question while the second has not been published.[34]

The first of these decisions, dated 18 May 2004, related to the case of Nokia Portugal v. Verza Facility Management, Google and others[35] and was issued against a hosting provider and providers of content aggregation services. The hosting provider was ordered to remove the offending website while the intermediary service providers were ordered to prevent aggregation of the content in question.

The second decision, dating from 2005, is, according to the relevant literature,[36] very short, and requires website hosts and intermediary providers of data aggregation services to disable access to websites which violate copyright and neighbouring rights. This decision was adopted by the General Inspectorate for Cultural Activities "Inspeção-General das Atividades Culturais".

2.3. Codes of conduct

Article 42 DL[37] provides that the body responsible for supervising the information society is to encourage the creation of codes of conduct and to disseminate them by electronic means. To this end, it will encourage the involvement of associations and organisations representing consumers, in particular in the drafting and implementation of codes of conduct. Where account needs to be taken of their specific needs, associations representing people with disabilities must be consulted. On contacting ANACOM, we were informed that they have no such codes in their possession.

3. Procedural Aspects

Orders to remove Internet content or to disable access to information on the Internet may be issued by the administrative authority or the courts, depending on the circumstances (Article 15.3 DL[38]).

---

34 Study on liability of internet intermediaries – BC. General trends in the EU, 12.11.2007, available at http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/final_report_en.pdf (06.06.15).

35 A. Van Der Perre, Study on the Liability of Internet Intermediaries, Country Report – Portugal, November 2007, available at http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/portugal_12 nov2007_en.pdf (14.07.15).

36 Ibidem.

37 Art. 42 DL: "Códigos de conduta. 1 — As entidades de supervisão estimularão a criação de códigos de conduta pelos interessados e sua difusão por estes por via electrónica.
2 — Será incentivada a participação das associações e organismos que têm a seu cargo os interesses dos consumidores na formulação e aplicação de códigos de conduta, sempre que estiverem em causa os intereses destes. Quando houver que considerar necesidades específicas de associações representativas de deficientes visuais ou outros, estas deverão ser consultadas".

38 Art. 15.3 DL: "As regras comuns passam também a ser aplicáveis se chegar ao conhecimento do prestador que a informação foi retirada da fonte originária ou o acesso tornado impossível ou ainda

The **administrative** authority (see sections 2.2. and 5) can adopt provisional measures concerning any content which is illegal. According to Article 18 DL, service providers are not bound to remove content or to disable access to a website if the illegality is not obvious (see sections 2.1 and 2.2). Article 18.2 DL, however, goes on to state that any interested party may apply to the **regulator (ANACOM)**, which must then find a **provisional solution** within 48 hours and communicate it to the parties by electronic means. The purpose of the measures thus imposed is to **order that the Internet content in question be removed.** In this context, the administrative authority may adopt interim measures ordering the removal of or disabling of access to problematic data via hyperlinks. Whoever has an interest in maintaining access to problematic content can appeal to the regulator against any such decision.[39]

At the request of the interested party, the **courts** will resolve the dispute **permanently**. Article 18.8 DL states that recourse to administrative procedures, as prescribed in paragraphs 2 and 3 of Article 18 DL, does not prevent the interested persons from also taking legal action, including even at the same time.[40] The decision of the competent judicial authority is subject to **ordinary means of appeal**.

In the context of **personal data protection**, the CNPD has the power to issue binding decisions. Judicial review is provided under Article 23.3 LPD, according to which the CNPD's decisions are subject to **judicial review** by the Central Administrative Court.

Lastly, the **courts** have the power to order Internet service providers to block Internet access pursuant to Article 7 DL and also for the purpose of protecting intellectual property rights. Such decisions, whether handed down in ordinary criminal or civil proceedings, can be challenged by ordinary means of appeal.

As regards safeguards for freedom of expression in cases where ANACOM or the courts adopt measures involving blocking or the removal of content, on 12 June 2015 the Council of Ministers adopted Resolution No. 36/2015, approving the "National Cyberspace Security Strategy".[41] Among the principles enshrined in this strategy, which is aimed at combating cybercrime, are **proportionality** of the measures to be adopted by ANACOM and the protection of fundamental rights, in particular **freedom of expression**, the right to privacy and data protection. Any action by ANACOM is subject to the cross-sectoral requirement which applies to all administrative authorities, namely the requirement to act in such a way that the measures adopted are proportionate to the objectives pursued (Art. 7.2 DL). This helps to avoid any measures that might result in "overblocking".

---

que um tribunal ou entidade administrativa com competência sobre o prestador que está na origem da informação ordenou essa remoção ou impossibilidade de acesso com exequibilidade imediata e o prestador não a retirar ou impossibilitar imediatamente o acesso".

39 Art. 18.2 et 18.3 DL: "2. Nos casos previstos no número anterior, qualquer interessado pode recorrer à entidade de supervisão respectiva, que deve dar uma solução provisória em quarenta e oito horas e logo a comunica electronicamente aos intervenientes.
3. Quem tiver interesse jurídico na manutenção daquele conteúdo em linha pode nos mesmos termos recorrer à entidade de supervisão contra uma decisão do prestador de remover ou imposibilitar o acesso a esse conteúdo, para obter a solução provisória do litígio".

40 Art. 18.7 et 18.8 DL: "7. A solução definitiva do litígio é realizada nos termos e pelas vias comuns.
8. O recurso a estes meios não prejudica a utilização pelos interessados, mesmo simultânea, dos meios judiciais comuns".

41 Resolução do Conselho de Ministros n.º 36/2015, de 12 de junho, Aprova a estratégia nacional de segurança do ciberespaço. Resolução do Conselho de Ministros n.º 36/2015, de 12 de junho, available at http://www.anacom.pt/render.jsp?contentId=1359087#.Ve0sr2cVios (04.08.15).

4. General Monitoring of Internet

Portugal does not have an entity in charge of monitoring Internet content with a view to removing certain content or blocking access to it. Article 35 DL[42] provides for the creation of a "central supervisory body" called ANACOM (*Autoridade Nacional de Comunicações*).

ANACOM's tasks include checking to ensure that websites comply with the provisions on e-commerce, instituting proceedings in cases involving violations of the DL and imposing sanctions (Art. 36 DL[43]).

Mention should also be made of two bodies responsible for monitoring illegal activity on the Internet. The first is a hotline called "Linha Alerta",[44] whose purpose is to provide the authorities with information gleaned from reports received from the public and to work with Internet service providers to ensure that problematic content is swiftly removed. The public can provide information anonymously by electronic means. The reports are assessed by the hotline operators and, where appropriate, passed on to the authorities. According to the Linha Alerta website, the kind of content with which the hotline is concerned is **child pornography** and content that is **racist** or **condones violence**.[45]

- Child pornography means any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or representation of the sexual parts of a child for primarily sexual purposes and also the exploitation of children in order to create such images.

---

42 Art. 35 DL : « 1 — É instituída uma entidade de supervisão central com atribuições em todos os domínios regulados pelo presente diploma, salvo nas matérias em que lei especial atribua competência sectorial a outra entidade. 2 — As funções de entidade de supervisão central serão exercidas pela ICP — Autoridade Nacional de Comunicações (ICP-ANACOM) ».

43 Art 36 D L : « 1— As entidades de supervisão funcionam como organismos de referência para os contactos que se estabeleçam no seu domínio, fornecendo, quando requeridas, informações aos destinatários, aos prestadores de serviços e ao público em geral.
2 — Cabe às entidades de supervisão, além das atribuições gerais já assinaladas e das que lhes forem especificamente atribuídas: a) Adoptar as providências restritivas previstas nos artigos 7.o e 8.o;
b) Elaborar regulamentos e dar instruções sobre práticas a ser seguidas para cumprimento do disposto no presente diploma;
c) Fiscalizar o cumprimento do preceituado sobre o comércio electrónico;
d) Instaurar e instruir processos contra-ordenacionais e, bem assim, aplicar as sanções previstas;
e) Determinar a suspensão da actividade dos prestadores de serviços em face de graves irregularidades e por razões de urgência.
3 — A entidade de supervisão central tem competência em todas as matérias que a lei atribua a um órgão administrativo sem mais especificação e nas que lhe forem particularmente cometidas.
4 — Cabe designadamente à entidade de supervisão central, além das atribuições gerais já assinaladas,
quando não couberem a outro órgão: a) Publicitar em rede os códigos de conduta mais significativos de que tenha conhecimento;
b) Publicitar outras informações, nomeadamente decisões judiciais neste domínio;
c) Promover as comunicações à Comissão Europeia e ao Estado membro de origem previstas
no artigo 9.o;
d) Em geral, desempenhar a função de entidade permanente de contacto com os outros Estados membros e com a Comissão Europeia, sem prejuízo das competências que forem atribuídas as entidades sectoriais de supervisão ».

44 See the website: https://linhaalerta.internetsegura.pt/ (04.08.15).

45 Missão, available at: https://linhaalerta.internetsegura.pt/index.php?option=com_content&view=article&id=16&Itemid=31&lang=pt (04.08.15).

- Condoning violence refers to any content which encourages the commission of an offence, either through direct incitement or by expressing approval of or condoning an offence which has already been committed. This includes content relating to terrorist propaganda.
- "Racism" is understood in the wide sense to include incitement to hatred, violence or racial or religious discrimination through racist, revisionist or neo-Nazi discourse.

The second body worth mentioning is the "Centro Internet Segura".[46] Run by the Foundation for Science and Technology under the wing of the Ministry of Education and Science, the centre aims to tackle "malicious or illegal" content. It also seeks to "minimise the impact of illegal on-line content that is harmful to the public; to promote safe Internet use and public awareness of the risks of using the Internet".

The centre has two instruments for raising awareness about problematic content. The first (Seguranet) targets schoolchildren while the second (Internet Segura) is aimed at the public at large. The Centre also has two hotlines, one for reporting illegal content and another for providing support and clarification on issues relating to the safe use of information and communication technologies.

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

In Portugal, the administrative authority can block access or order the removal of Internet content only as a provisional measure. The power to adopt final measures lies exclusively with the courts. As pointed out in section 2.2., under the rules applicable in Portugal, except in cases of manifest illegality, the interested parties can ask ANACOM to take such measures as it deems appropriate to deal with illegal content. Any action ANACOM may take will be temporary, as only the courts are empowered to resolve disputes permanently. The fact that this power is vested in the courts helps to ensure respect for the law, including notably the principle of freedom of expression.

The system would thus seem to provide the necessary safeguards to prevent arbitrary administrative decisions, since the courts are bound to observe the rights enshrined in the Portuguese Constitution.[47] These include the principle of equality (Article 13 of the Constitution), access to law and effective judicial protection (Article 20), a person's right to his or her personal identity, good name and reputation, image, the right to speak out, and the right to the protection of the intimacy of his or her private and family life (Article 26), inviolability of home and correspondence (Article 34) and the right of access to one's personal data (Article 35) as well as freedom of expression, media and press freedom.

---

46 Centro Internet Segura, website available at: https://www.fct.pt/dsi/internetsegura/ (04.08.15); Internet Segura: Linha Alerta https://www.fccn.pt/pt/servicos/seguranca/internet-segura-linha-alerta/denuncia-de-conteudos-ilegais/ (04.08.15).

47 Portuguese Constitution, available at: http://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx (25.05.15). In Portugal, the courts can refuse to apply provisions that violate the Constitution. Any ruling they may give on such matters may be contested before the Constitutional Court. Art. 204 Cst : « Apreciação da inconstitucionalidade. Nos feitos submetidos a julgamento não podem os tribunais aplicar normas que infrinjam o disposto na Constituição ou os princípios nela consignados ».

Freedom of expression and information is enshrined in Art. 37 Cst.[48] Everyone possesses the right to express and make known his or her thoughts freely by words, images or any other means, and also the right to inform, obtain information and be informed without hindrance or discrimination. The exercise of these rights must not be prevented or restricted by any type or form of censorship.[49] Offences committed in the exercise of these rights are punishable under the general principles of criminal law or the law governing administrative offences. The right of reply and rectification and the right to compensation for losses suffered are equally and effectively secured to all natural persons and legal entities. Illegal acts which undermine freedom of expression and information are to be judged by the courts or an independent administrative authority respectively, in the manner provided for by law.

In addition, Article 38 Cst.[50] guarantees freedom of the press and the media. Article 38 Cst. provides *inter alia* for freedom of expression and creativeness, the right to access sources of information, the

---

48 Art. 37 Cst : « Liberdade de expressão e informação. 1. Todos têm o direito de exprimir e divulgar livremente o seu pensamento pela palavra, pela imagem ou por qualquer outro meio, bem como o direito de informar, de se informar e de ser informados, sem impedimentos nem discriminações.
2. O exercício destes direitos não pode ser impedido ou limitado por qualquer tipo ou forma de censura.
3. As infracções cometidas no exercício destes direitos ficam submetidas aos princípios gerais de direito criminal ou do ilícito de mera ordenação social, sendo a sua apreciação respectivamente da competência dos tribunais judiciais ou de entidade administrativa independente, nos termos da lei.
4. A todas as pessoas, singulares ou colectivas, é assegurado, em condições de igualdade e eficácia, o direito de resposta e de rectificação, bem como o direito a indemnização pelos danos sofridos ».

49 In 2012, the Supreme Court held[49] that the Constitution recognises that there are limits to the right to inform and to freely express one's thoughts, in particular in the field of criminal law and illegal activities. Freedom of expression and information cannot prevail over a person's right to his or her **good name** and **reputation**, to **moral integrity** and the **right to privacy**. Paragraph 2 of Article 335 of the Portuguese Civil Code states that where rights which are not of the same type conflict, whichever right is considered superior must prevail. In a conflict between freedom of expression and a person's right to his or her good name and reputation, therefore, notwithstanding the fact that both rights are deserving of respect, "it is clear that the first right, by reason of the restrictions and limitations to which it is subject, may not harm the good name and reputation of others, save where there is a higher relevant public interest".
Supremo Tribunal de Justiça, Secção Cível, Acórdão de 28 Jun. 2012, Processo 3728/07.0TVLSB.L1.S1 Relator: Manuel Fernando Granja Rodrigues da Fonseca. Jurisdição: Cível JusNet 4684/2012 (base privée); Código civil, available at http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?ficha=301&artigo_id=&nid=775&pagina=4&tabela=leis&nversao=&so_miolo= (06.06.15), art. 335 « (Colisão de direitos). 1. Havendo colisão de direitos iguais ou da mesma espécie, devem os titulares ceder na medida do necessário para que todos produzam igualmente o seu efeito, sem maior detrimento para qualquer das partes.
2. Se os direitos forem desiguais ou de espécie diferente, prevalece o que deva considerar-se superior ».
At the level of the lower courts, Lisbon Court held that the exercise of freedom of expression may be subject to certain conditions, restrictions and sanctions which are necessary in a democratic society, notably in order to safeguard **national security, territorial integrity, public safety, crime prevention, internal order, protection of health and morals, protection of the right of others to their good name,** to **prevent the disclosure of confidential information** and to ensure the authority and impartiality of the judiciary. This approach echoes that taken by the European Convention on Human Rights, Tribunal da Relação de Lisboa, Acórdão de 26 Fev. 2010, Processo 734/05.3, Jurisdição: Cível, JusNet 1279/2010 (private database).

50 Art. 38 Cst : « Liberdade de imprensa e meios de comunicação social. 1. É garantida a liberdade de imprensa. 2. A liberdade de imprensa implica:

right to found publications and independence of the media from the political authorities. Under Article 39 Cst.,[51] an independent administrative authority is responsible for regulating the activities of the media in such a way as to ensure the right to information and freedom of the press, independence from the political and economic powers, respect for fundamental personal rights, freedoms and guarantees, and the possibility of expression and confrontation of the different lines of opinion.

Article 266 Cst.[52] requires the administrative authorities to respect such civil rights and interests as are protected by law. In the performance of their functions, administrative bodies are accordingly required to respect the principles of equality and prohibition of discrimination, proportionality, justice, impartiality and good faith. Similarly, Article 18.2 Cst.[53] lays down the principle of proportionality as a general limitation on the authorities, in the exercise of their functions. In the words of the Portuguese Constitutional Court:

---

a) A liberdade de expressão e criação dos jornalistas e colaboradores, bem como a intervenção dos primeiros na orientação editorial dos respectivos órgãos de comunicação social, salvo quando tiverem natureza doutrinária ou confessional;
b) O direito dos jornalistas, nos termos da lei, ao acesso às fontes de informação e à protecção da independência e do sigilo profissionais, bem como o direito de elegerem conselhos de redacção;
c) O direito de fundação de jornais e de quaisquer outras publicações, independentemente de autorização administrativa, caução ou habilitação prévias.
3. A lei assegura, com carácter genérico, a divulgação da titularidade e dos meios de financiamento dos órgãos de comunicação social.
4. O Estado assegura a liberdade e a independência dos órgãos de comunicação social perante o poder político e o poder económico, impondo o princípio da especialidade das empresas titulares de órgãos de informação geral, tratando-as e apoiando-as de forma não discriminatória e impedindo a sua concentração, designadamente através de participações múltiplas ou cruzadas.
5. O Estado assegura a existência e o funcionamento de um serviço público de rádio e de televisão.
6. A estrutura e o funcionamento dos meios de comunicação social do sector público devem salvaguardar a sua independência perante o Governo, a Administração e os demais poderes públicos, bem como assegurar a possibilidade de expressão e confronto das diversas correntes de opinião.
7. As estações emissoras de radiodifusão e de radiotelevisão só podem funcionar mediante licença, a conferir por concurso público, nos termos da lei".

51 Art. 39 Cst : « Regulação da comunicação social. 1. Cabe a uma entidade administrativa independente assegurar nos meios de comunicação social:
a) O direito à informação e a liberdade de imprensa;
b) A não concentração da titularidade dos meios de comunicação social;
c) A independência perante o poder político e o poder económico;
d) O respeito pelos direitos, liberdades e garantias pessoais;
e) O respeito pelas normas reguladoras das actividades de comunicação social;
f) A possibilidade de expressão e confronto das diversas correntes de opinião;
g) O exercício dos direitos de antena, de resposta e de réplica política.
2. A lei define a composição, as competências, a organização e o funcionamento da entidade referida no número anterior, bem como o estatuto dos respectivos membros, designados pela Assembleia da República e por cooptação destes".

52 Art. 266 Cst: "Princípios fundamentais. 1. A Administração Pública visa a prossecução do interesse público, no respeito pelos direitos e interesses legalmente protegidos dos cidadãos.
2. Os órgãos e agentes administrativos estão subordinados à Constituição e à lei e devem actuar, no exercício das suas funções, com respeito pelos princípios da igualdade, da proporcionalidade, da justiça, da imparcialidade e da boa-fé ».

53 Art. 18.2 Cst: "A lei só pode restringir os direitos, liberdades e garantias nos casos expressamente previstos na Constituição, devendo as restrições limitar-se ao necessário para salvaguardar outros direitos ou interesses constitucionalmente protegidos".

"[…] the requirement for proportionality is expressly referred to in Article 18.2 Cst, but, in generic terms, as a general limitation on the exercise of public authority, it may be said to follow ineluctably from the very principle of the rule of law, as enshrined in Article 2 of the Constitution".[54]

The lack of case law prevents us from assessing how the existing provisions are implemented in practice, but our research has shown that the legislation specifying the blocking and take-down/removal measures that can be adopted by the competent administrative authority (ANACOM) and the courts seems to **meet the requirements laid down by the European Court of Human Rights.**[55] For one thing, the measures in question are set out in a decree-law which is freely **accessible.** The restrictions contained therein also offer a degree of **foreseeability**, to the extent that they apply only to certain types of content which pose a threat to **public policy**, **public safety**, protection of **public health** and consumer and user protection, respect for **human dignity**, **non-discrimination**, **child and youth welfare** and **intellectual property** rights. Added to this is the aforementioned requirement for **proportionality** when adopting restrictive measures. In addition, ANACOM, as an independent administrative authority governed by Portuguese law, is required under the Constitution to observe the **principles of proportionality**, prohibition of discrimination, **impartiality** and good faith. ANACOM, moreover, acts only at the request of an interested party and any measures it may take are merely **provisional** in character, **the courts having sole jurisdiction to resolve matters permanently** (under Articles 7.2.b) and 8 DL, however, where illegal content derives from an EU state, ANACOM can act ex officio if an interested state so requests and also in emergencies). Lastly, as well as **judicial remedies**, the DL provides for the possibility of appeal to the administrative authority itself.

It is nevertheless regrettable firstly that ANACOM's decisions are not systematically published, in the interests of greater transparency, and, secondly, that the DL is not more specific about the types of Internet content that would justify ANACOM deciding to block or remove content. The concept of a threat to public policy, for example, is a rather elastic one, which allows the regulator considerable leeway.

Dr. Alberto Aronovitz

October 2015

---

54 Tribunal Constitucional, Acórdão 88/2004 de 10 Fev. 2004, Processo 411/03: "Nesta matéria, a exigência de proporcionalidade está expressamente mencionada no n.º 2 do artigo 18º da Constituição, mas, em termos genéricos, como limitação geral ao exercício do poder público, pode considerar-se que tal resulta iniludivelmente do próprio princípio do Estado de Direito, consagrado no artigo 2º da mesma Constituição.

55 CEDH, Case no 3111/10, Ahmet Yildirim v. Turkey, 18 December 2012.