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 285-301

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.

GREECE

1. Legal Sources

1.1. Constitution

The right to participate in the Information Society and the right of access to information is protected by the Greek Constitution (art. 5A par. 1 & 2[1]). This provision is interpreted as the right of all people to participate in the Information Society and it follows that **the state has a responsibility to assist in the advancement of this goal**, or, in other words, **not to hinder the enjoyment of such right**. Following that guideline, under Greek law, **there is no specific *in toto* law for measures of blocking, filtering and taking down illegal Internet content**.

Furthermore, censorship and any other preventive measures are prohibited (Art. 14 par. 2[2] of the Greek Constitution), while the seizure of newspapers and other publications before or after circulation is prohibited (art 14 par. 3[3]).

1.2. International Instruments

1.2.1. Convention on Data Protection

In 1992, Greece ratified[4] the Convention of the Council of Europe on Data Protection.[5]

1.2.2 Conventions on Cybercrime and on the Prevention of terrorism

Greece has signed the **Convention on Cybercrime**,[6] but has not yet implemented it in domestic law. In order for the ratification of the aforementioned Convention as well as the transposition of the Directive 2013/40/EU on attacks against information systems, the Hellenic Ministry of Justice, Transparency and Human Rights launched a public consultation regarding the draft bill, beginning on

---

1 **Art. 5A** of the Greek Constitution (last revision of 2008) reads: "**1.** All persons have the right to information, as specified by law. Restrictions to this right may be imposed by law only insofar as they are absolutely necessary and justified for reasons of national security, of combating crime or of protecting rights and interests of third parties. **2.** All persons have the right to participate in the Information Society. Facilitation of access to electronically transmitted information, as well as of the production, exchange and diffusion thereof, constitutes an obligation of the State, always in observance of the guarantees of articles 9, 9A and 19."

2 **Art. 14 par. 2:** "The press is free. Censorship and all other preventive measures are prohibited".

3 **Art. 14 par. 3:** "The seizure of newspapers and other publications before or after circulation is prohibited. Seizure by order of the public prosecutor shall be allowed exceptionally after circulation and in case of: **a)** an offence against the Christian or any other known religion. **b)** an insult against the person of the President of the Republic. **c)** a publication which discloses information on the composition, equipment and set-up of the armed forces or the fortifications of the country, or which aims at the violent overthrow of the regime or is directed against the territorial integrity of the State. **d)** an obscene publication which is obviously offensive to public decency, in the cases stipulated by law.

4 Greek Law 2068/1992.

5 Convention for the Protection of individuals with regard to Automatic Processing of Personal Data, known as **Convention No.108**. Opened for signature in Strasbourg on 28 January 1981.

6 Council of Europe Convention on Cybercrime, CETS No. 185, Budapest, dated 23.11.2001.

18th March 2016 and expiring on 1st April 2016.[7] The draft bill also includes the Additional Protocol to the Convention, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems Greece has signed, but has not yet ratified the **Convention on the Prevention of Terrorism,**[8] and the **Council Framework Decision on Combating Terrorism.**[9]

1.2.3. Conventions on Child Pornography

In 2007, Greece ratified and implemented the UN Optional Protocol on the sale of children, child prostitution and child pornography,[10] adopting the specific references to the Internet and emerging technologies.

In addition, in 2008 Greece ratified and implemented the **Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse**[11] (known as the **Lanzarote Convention**).

1.3. EU Instruments

1.3.1. Electronic Commerce Directive

In 2003 the Greek legislator implemented the Directive "for Electronic Commerce" (hereinafter ECD) without adopting any specific regulations for blocking, filtering and taking down of illegal Internet content. Taking as a guideline the immunity provided for by ECD, **filtering and taking down content** by **access** and **host** providers has been applied, mainly for violations of copyright,[12] through case-law granting either injunction relief or imposing criminal sanctions. However, the legal framework for copyright protection is not able to cover other aspects of illegal content.

---

7 Earlier, an attempt was made to ratify the Convention in 2008, including an additional section for the regulation of blogs and bloggers, without success.

8 Council of Europe Convention on the Prevention of Terrorism CETS No. 196, Warsaw, 16.5.2005.

9 Initially Decision 2002/475/JHA of 13 June 2002 amended by Decision 2008/919/JHA of 28 November 2008.

10 UN Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography Adopted and opened for signature, ratification and accession by UN General Assembly resolution A/RES/54/263 of 25 May 2000, entered into force on 18 January 2002 (ratified by Greek Law 3625/2007).

11 Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse CETS No. 201, Lanzarote 25.10.2007 (ratified by Greek Law 3727/2008).

12 Having as a legal basis, apart from the ECD immunity considerations: 1) Directive 2001/29/EC, of 22.5.2001 on the harmonisation of certain aspects of copyright and related aspects in the information society (Copyright Directive) and 2) Directive 2004/48/EC of 29.4.2004 on the enforcement of intellectual property rights, as these have been transposed into domestic law by arts. 28B, 64 and 64A of Law 2121/1993 (the Greek Copyright Law).

1.3.2. Data Protection

In 1997, Greece implemented the **Data Protection Directive,**[13] while a constitutional amendment in 2001 has awarded constitutional[14] status to the protection of personal data. Similarly, in 2002, Greece harmonized the **e-Privacy Directive 2002/58**[15] and, in 2006, the **Data Retention Directive 2006/24**.[16]

1.3.3. Council Framework Decision combating racist and xenophobic content

Law 4285/2014 has recently harmonised Greek legislation with the Council Framework Decision on combating racist and xenophobic content.[17] Greek Law criminalises racist content, xenophobia, hate speech, denial, gross minimisation, approval or justification of genocide or crimes against humanity as these have been recognised by international courts or the Greek Parliament. Article 3 of the Law provides that when such actions are committed through the Internet or other means of communication, then the place of committing the crime (*locus delicti*) is considered to be the entire Greek territory, as long as access to the particular media is completed in Greece and irrespective of the place of establishment of the media i.e. if the "access" machinery is in Greece, regardless of the main server/source of information being established elsewhere. Therefore, if the illegal content is accessed in Greece then the perpetrator could be subject to the sanctions, no matter if the illegal content is hosted in hardware outside Greece. A Court decision may include, *inter alia*, sanctions such as the blocking/take down of the relevant Internet content.

1.3.4. Child Pornography Directive

In 2002, art. 348A was introduced into the Greek Penal Code in order to combat **child pornography**. The particular article has been recently amended in order to harmonise with the **Child Pornography Directive**[18] (see infra par.2.1.2).

---

13 Directive 95/46/EC of The European Parliament and of The Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (transposed into domestic law by Greek Law 2472/1997).

14 **Art. 9A of the Greek Constitution** reads: "*All persons have the right to be protected from the collection, processing and use, especially by electronic means, of their personal data, as specified by law. The protection of personal data is ensured by an independent authority, which is constituted and operates as specified by law*".

15 Directive 2002/58/EC of 12.7.2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications, transposed by Greek Law 3471/2006).

16 Directive 2006/24/EC of 15.3.2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (Greek Law 3917/2011). Note, however that said Directive has been cancelled by ECJ Decisions C-293/12 *Digital Rights Ireland Ltd v Minister for Communications*, *Marine and Natural Resources* and C-594/12 *Kärntner Landesregierung*.

17 Council Framework Decision 2008/913/JHA of 28.11.2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law.

18 Directive 2011/92/EU of 13.12.2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (The Greek Penal code has been amended by art. 8 of Law 4267/2014).

2. Legal Framework

Countless "intermediaries" function as go-betweens for the transmission of Internet information: Classical access and host providers (ISPs), search engines (Google, Yahoo), social networks (Facebook, Myspace), electronic encyclopaedias (Wikipedia), websites for video uploading (YouTube), blogs, internet games platforms (Second Life, World of Warcraft), platforms for short messages (Twitter) etc. Why is it important[19] to address these for blocking / filtering / take-down measures? First, their technical contribution is indisputable, without access and host providers there is no Internet. They are the only entities that can be easily traced in order to seek compensation and sometime act as scapegoats, although they are only the messengers.[20] Secondly, at the current stage of things, it seems that Internet intermediaries are the only entities able to enforce such blocking / filtering / take down methods for Internet content either by a) intervening during an allegedly illegal or harmful action or b) by taking preventive / dissuasive measures. It has been observed that such methods may be extremely effective for certain types of illegal behaviour. Therefore, the liability of Internet Intermediaries has not only to do with the *stricto sensu* responsibility, but with their ability to fully control information flows over the Internet, to prohibit or allow, to define unilaterally the terms of access, to block or facilitate users, to impose commercial, political or cultural rules of manipulation, to guarantee data security and integrity.

Under the civil law structure of Greek law in order to establish such indirect liability of the Intermediaries, and hence to **block / filter / take-down information** one has to examine the existence of a "causal link", which is allegedly being offered by the Internet Intermediary to third parties for the commitment of infringements / unlawful acts. Such construction has mainly been influenced by the relevant common law theory for secondary liability for infringements in the area of **intellectual property** and **defamation**. However, under Greek legal doctrine the messenger may not be held liable for the message. In theory, it seems easy to target Internet intermediaries in order to implement blocking / filtering / take-down actions, but practice shows that intermediaries do not commit illegal acts themselves, so it would be necessary to prove that they provide a "causal link" (i.e. the means) for such acts by third parties.

One possible basis for establishing such secondary liability would be to follow the theory of "adequate cause"[21] and prove that the intervention of the intermediary constitutes the indispensable link in the chain of events that has led to the illegal result. It is obvious that such argumentation could provide adequate grounds for establishing liability in cases of copyright infringement, but seems rather weak in cases of defamation or similar harmful content. It is precisely that particular difficulty[22] to connect the behaviour of Intermediaries to the damage caused, that has led to the adoption of systems of immunity ("safe harbours" under US terminology) for Intermediaries, like the system set out in the ECD.

Based on the immunity provided for by ECD, the Greek system introduces a horizontal approach for all types of liability. In the particular area of the Liability of Intermediaries, commentators agree that Internet liability concerns all types of responsibility both under civil, administrative or criminal law,

---

19 G. N. Yannopoulos, The Liability of Internet Intermediaries [in Greek], Athens 2013, p. 9.

20 Compare verse 277 of Sophocles' Antigone : «…*That no man loves the messenger of ill*… » (transl. R. Jebb).

21 It should be mentioned, however, that under art. 65 par. 3 of Greek law 2121/1993 (the Greek Copyright Law, harmonising art. 13 of Enforcement Directive 2004/48) the establishment of an adequate cause is not required in the case of compensation claims for copyright infringements.

22 G. Yannopoulos, op. cit. pp. 55-56.

which leads to a general legal liability. Following theory developed in the EU,[23] it has been proposed to introduce a "special type of liability" reflecting the liability defined in Section No. 4 of ECD referred to as: *Liability* (*responsabilité*, *Verantwortlichkeit*). In view of the consolidation of the internal market, such horizontal regulation, no matter if sanctions are being characterised as civil, administrative or criminal, simply means that **the safe harbour is offered to Internet Intermediaries without discrimination and without examining the grounds of liability**.[24] Under that system, Greek legal theory has also developed the view[25] that the notion of liability does not only concern civil-type compensation but, in a broader sense, comprises all instances that intermediaries may be held liable for "illegal" or "harmful" content, which must be blocked / filtered / taken-down. The ECD system is completed with the known **prohibition of a general obligation of the Intermediaries to permanently monitor content** (art. 15 ECD, art 14 Greek PD)**.**

2.1. Blocking and/or filtering of illegal Internet content

In the majority of cases, blocking and / or filtering of illegal content targets access providers. However, given the multitude of Intermediaries it cannot be ruled out that a Court may order a host provider to block or filter content either in a preventive (e.g. by not allowing the posting of particular content to a blog) or a restrictive manner (e.g. by not allowing access to content), which would lead to quasi removal of content (see par. 2.2).

Still, the critical element in order to establish liability is that of "knowledge": Internet intermediaries are responsible for their own content, but **for third party content they must have knowledge of the infringement / harmful / unlawful material** in order to be held liable and, hence, to proceed with further action such as blocking / filtering / removal of content. The Greek Presidential Decree harmonising the ECD follows a similar wording and, while access providers stay immune, caching and hosting intermediaries must act "expeditiously" upon obtaining such knowledge in order to remove or to disable access to the information.

2.1.1. Injunction by civil courts

An identical paragraph in the three articles[26] of the Greek Presidential Decree 131/2003 concerning the liability of intermediaries, allows for **a Court or an Authority** to order the termination or prevention of an illegal activity or infringement and the cease of any offense thereafter. **Such type of measure may comprise the order to disable access to illegal information on Internet**. The Greek law does not define which is the competent Authority, however competence should be traced between the Hellenic Data Protection Authority (HDPA), the Hellenic Authority for Communication Security and Privacy (HACSP) or the National Telecommunications and Post Commission (NTPC). In terms of

---

23 See for example F. Ufer, Die Haftung der Internet Provider nach dem Telemediengesetz, Recht der Neuen Medien, Hamburg 2007, p. 38 and A. Schmoll, Die deliktische haftung der Internet-Service-Provider, Peter Lang, Frankfurt am Main 2001, p. 38.

24 See in that vein the Introductory Report on German Law for Electronic Commerce (BT-Drs 14/6098 of 17-5-2001, Elektronischer Geschäftsverkehrgesetz - EGG), for the harmonisation of the ECD stating that immunity concerns also criminal law («…*die Beschränkungen der Vernatwortlichkeit gelten auch für den Bereich des Strafrechts*…»).

25 See Yannopoulos, The Liability of Internet Intermediaries, op.cit., references in footnote 241, p.57.

26 See the same text in arts. 11 par. 3 (for access providers), 12 par. 2 (for cache providers) and 13 par 3 (for host providers) reading "*This Article shall not affect the possibility to impose to the service provider, by means of a judicial or administrative decision, [the obligation] to terminate or prevent an infringement*". This wording corresponds to arts. 12 par. 3, 13 par. 2 and 14 par. 3 of the ECD. Note, however that the Greek Presidential Decree does not follow the exact wording of art 14 par. 3 ECD, which allows to "*establish procedures governing the removal or disabling of access to information*".

Court procedure, the Greek Law[27] is clearer and allows for such remedy to be taken by an **Injunction Procedure** in front of the First Instance Civil Court according to the rules of the Greek Civil Procedure.[28] The necessary prerequisite of obtaining such an injunction is that "information society rights must seem under threat of infringement". The Court may also issue a Provisional Order until the Injunction Decision.[29]

For **copyright infringements** a similar type of injunction[30] is also provided for in articles 64 and 64A of the Greek Copyright Law 2121/1993, harmonising respectively article 8 paragraph 3 of the Copyright Directive 2001/29[31] and article 11 of the Enforcement Directive 2004/48.[32] Particularly under article 64 of the Greek Law, the civil court may take **any measure in order to prevent future infringement/violation of intellectual property rights or may prohibit the continuation/repetition of the infringement/violation**, while under article 64A such injunction **may be enforced against intermediaries** (including Internet intermediaries). In one case this has been interpreted by the Courts as the ability to order access providers to block content (see *infra* paragraph, Case 4658/2012).

The Greek **Trademark** Law takes a similar approach:[33] the right holder may seek an injunction ordering the confiscation of products bearing the violated sign, or the provisional blocking of distribution. Such an injunction may also comprise actions **against the means for committing an infringement**. In that sense, it **may include blocking of access that can be enforced against intermediaries**.

In addition, the Greek Unfair Competition Law[34] has a similar provision for injunctive relief against **unfair commercial practices**, in order to remove the infringement and block future violations.

2.1.2. Child Pornography

As explained in par. 1.4, Greece has harmonised the existing article 348A of the Greek Penal Code with the Child Pornography Directive.[35] Nevertheless, article 25 of the Directive (measures against websites) has been harmonised separately by article 18 of Law 4267/2014, stating that the competent Public Prosecutor (of the first and appeal degree) is able to **order the "elimination" (which is understood as meaning "taking down") of a website hosted in Greece**, that contains or transmits child pornography material. Furthermore, in the event that the website cannot be traced in Greece or elsewhere, the Prosecutor may order the temporary (for two months) **deactivation of any Domain Name assigned in Greece**, hosting or leading to such a website. Finally, where the website is neither hosted in Greece, nor belonging to a domain name assigned in Greece, the Prosecutor may order the **blocking of access to such websites**. The Order must be able to be fully justified in the particular circumstances and is addressed to the owner of the website and the National

---

27 art. 17 of Presidential Decree 131/2003 (= art. 18 ECD).

28 Arts 682 et. seq. of the Greek Code of Civil Procedure. Please note that as of 1.1.2016 an extended amendment of the Code will come into force.

29 Arts 691 par. 2 of the Greek Code of Civil Procedure. Normally an Injunction is Greece will be decided within 1-6 months following petition, while a Provisional Order may be issued within 1-2 days.

30 See G. Yannopoulos op. cit. p. 242.

31 Directive 2001/29/EC, of 22.5.2001 on the harmonisation of certain aspects of copyright and related rights in the information society.

32 Directive 2004/48, of 29.4.2004 on the enforcement of intellectual property rights.

33 Arts. 153, 154 of Greek Law 4072/2012.

34 Art. 20 of Law 146/1914.

35 Directive 2011/92/EU of 13.12.2011 on combating the sexual abuse and sexual exploitation of children and child pornography (supra par. 1.3.4).

Telecommunications and Post Commission (NTPC). NTPC must, in turn, notify all **access providers** registered in Greece as per Greek Telecommunications Law (Law 4070/2012). Apart from seeking compliance, NTPC may demand that the provider takes steps to increase awareness amongst users. The option of Prosecutor's Orders has been introduced very recently and has not yet been tested.

There is no special provision in order to block access in the event of other types of criminal behaviour (e.g. incitement of terrorism) and the only recourse is the general provisions of articles 185 (praising of a crime) and 186 (challenge and offer to perform a felony or misdemeanour) of the Greek Penal Code.[36]

2.1.3. Anti-discrimination law

In order to activate Law 4285/2014 (see supra 1.3.3) to block content that is xenophobic, racist or constitutes hate speech, a **criminal prosecution** must be instigated either by an individual complaint to the authorities (police, prosecutor's office) or by an ex officio indictment of the prosecutor. The law is very recent so it is not yet clear how **courts** will proceed with blocking / filtering of websites following conviction of the owner for a criminal offense for illegal content.

2.1.4. Gambling Law

Gambling Law imposes a regulatory regime[37] for the blocking of websites. The **Greek Gaming Commission** (GGC), which is an independent Authority, is entitled to publicise from time to time a **"blacklist" of prohibited gambling sites**. Blacklisted websites are generally those that are not licensed[38] by the GGC and, hence, not taxed by the Greek State. According to the wording of the law, all Internet Service Providers ("ISPs") – generally understood as meaning all "access providers" - operating in Greece and registered with the Telecommunications Commission (see NTPC *supra*), as per telecommunications legislation, must disable access to those "blacklisted" sites. The wording of the Law states, generally, that "domain names" and "IP addresses" should be included in the "blacklist". It is not clear, in the particular provision, which blocking method should be followed: that of blocking the DNS names or the IP addresses? It is also not obvious if any other hardware or software identification or labelling of the blacklisted website is required. It is affirmed however, in article 3.4 of the Internet Gambling Regulation,[39] that blocking must take place when access is attempted for "an IP address residing within the Greek territory", without any other indication as to how to identify such "residence" of an IP address. Additionally, ISPs must not allow "any action of commercial communication" of illegal gambling providers. Again, it is not evident whether ISPs must block any type of advertisement including, for example, frames and nested hyperlinks. It is also interesting to note that the simple posting of the "blacklist" in GGC's website is considered to constitute "adequate knowledge" and proof of evidence against ISPs. Furthermore, according to the law, the GGC is also entitled to send to the ISPs a list of "key-words" that indicate a connection to

---

36 For the particular case of terrorism definitions may be found in art 187A of the Greek Penal Code. As explained Greece has not ratified CoE Convention on the Prevention of Terrorism, CETS No. 196 (see supra footnote 8), however, certain guidelines of the Convention have been implemented in articles 187, 187A and 187B of the Greek Penal Code.

37 Arts 45-48 of Law 4002/2011 as amended.

38 As prescribed by art, 48 par. 8 of Law 4002/2011 and backed by GGC Regulation for the Conduct and Control of Internet Gambling (Decision No. 23/3/23.10.2012, Official Gazette B-2952/5.11.2012, as amended by GGC Decision No. 51/3/26.4.2013, Official Gazette B-1147/13.5.2013).

39 GGC Regulation for the Conduct and Control of Internet Gambling (Decision No. 23/3/23.10.2012, Official Gazette B-2952/5.11.2012, as amended by GGC Decision No. 51/3/26.4.2013, Official Gazette B-1147/13.5.2013).

Internet gambling. Where ISPs are requested to provide a domain name that includes any such "key-word", they have 15 days within which to notify GGC accordingly.

2.1.5. Domain abuse

The National Telecommunications and Post Commission (NTPC), the independent authority in charge of the regulation of telecommunications in Greece, is also responsible for supervising the ".gr" domain.[40] NTPC is, according to the Domain Name Regulation, entitled to delete domain names that: infringe existing intellectual property rights including trademarks, that have been registered in bad faith and that clash with moral perceptions or Greek public policy. [41] The concept of "public policy"[42] is closer to that of "public order"/"safety" so as to cover the limitations of article 10 ECHR. However, the application of "moral perceptions" in order to delete a domain name is facing certain difficulties[43] in view of the international nature of the Internet. The procedure may be instigated either by an individual complaint or *ex officio*. While a procedure for deletion is underway, the chairman of NTPC may issue a decision[44] for the provisional suspension of a domain name in the event that there are only indications of reasons for deletion, or if a court Provisional Order imposes such a suspension.

2.1.6. Case-law

Following the above analysis, **case-law** for blocking / filtering is limited to copyright cases and has dealt with the issue of imposing injunctions to intermediaries in order to filter access to illegal sites (mainly by blocking DNS names). The most important decisions are as follows:[45]

2.1.6.1. Decision 4658/2012 of the First Instance Court of Athens

In an injunction case, following a petition by collecting societies, the Court ordered major access providers in Greece to cut off the access to particular DNS addresses that infringed copyright. Apart from the copyright rules, the Court mentioned articles 12 and 15 ECD, as well as the *Scarlet* and *Sabam* decisions[46] of the ECJ. The Court accepted that a general blocking of access in order to protect IP rights would be disproportionate and incompatible with article 5A paragraph 2 of the Greek Constitution (Right to participate to Information Society, *supra* paragraph 1.1). The Court denied the direct applicability of Directive 2009/140 (which was at that stage not yet harmonised in Greece, see *infra*), but accepted that proportionate and necessary measures may be imposed in order to protect another right. Therefore, **blocking of a particular webpage infringing copyright was permitted** and the Court granted the injunction ordering the blocking of specific URL and IP addresses. Interestingly, the blocked sites contained only hyperlinks towards copies of protected works hosted in international file sharing websites. Controversially, the Court tried (see *infra*, case-law on hyper-linking) to associate hyperlinking with the hosting of copies of the works.

---

40 By virtue of art. 12 par. 24 of Law 4070/2012 (The Greek Telecommunications Law).

41 See art. 10 par. 2 of NTPC Regulation No.750/2/Official Gazette B-412/24-3-2015 (The Domain Name Regulation).

42 The notions of "moral perceptions" and "public policy" coincide with the terms of the general clause of art. 33 of the Greek Civil Code regarding the applicability of foreign law (compare arts 17 and 27 of the Swiss Federal Act on Private International Law of 18/12/1987).

43 For example in 2005 NTPC, by applying the notion of "moral perceptions", has denied the name "www.bourdela.gr" (a site about brothels in Greece). Ever since, however, the site operates under the name "www.bourdela.com".

44 Art 11 of the Domain Name Regulation.

45 See also D. Maniotis et.al., Greece, in Jos Dumortier et. al (Eds.), International Encyclopaedia of Laws for Cyberlaw, Kluwer Law International BV, Netherlands, 2013, p. 105 et. seq.

46 C-70/10 *Scarlet v Sabam* and C-369/10 *Sabam v Netlog.*

It is worth noting that such an injunction has been considered as a technological method in the area of copyright, having an educational effect to both providers and users, without charging them directly with liability. In the case of Internet intermediaries, this has resulted in some sort of a more "rigid" duty of care against users, somewhat additional to the standard duty of care requirements under contract or tort law.

2.1.6.2. Decision 13478/2014 of the First Instance Court of Athens

In this case, contrary to the one set out above, the injunction was not granted. Five collective organisations had filed a petition, asking several access and host providers to block access to **sites dispensing illegal copies of intellectual works** (mainly music and movies) protected under the Greek IP legislation. The Court's decision initially clarified the legal position of Internet intermediaries and their liability, stating that by a combination of the Greek IP law (Law 2121/1993) and the Presidential Decree 131/2003 harmonising ECD and Greek legislation concerning the secrecy of communications (L. 3471/2006, PD 47/2007 and L. 2225/1994), it is not possible for access providers to reveal personal data of users connecting to the Internet.

The Court then affirmed that access providers do not play an active role and they neither initiate nor select the receiver of the transmission (in line with article 12 of the e-Commerce Directive) and, that there was no deliberate collaboration with one of the recipients of the service in order to undertake illegal acts as provided in preamble No. 44 of ECD. Therefore, the defendants benefit from the **immunity of access providers** under article 11 of PD 131/2003 (i.e. article 12 of ECD). In the same vein, the Court concluded that the defendants fall under the immunity of article 13 of PD 131/2003 (article 14 of ECD) because **as host providers they do not have actual knowledge of illegal activity or information**. As a result, the Court dismissed the argument of the Plaintiffs according to which they had informed the Defendants of the illegal activity and required a particular degree of certainty in the "knowledge" obtained, which should be equivalent to the notion of "Direct Intent" of article 27 par. 2[47] of the Greek Penal Code. In that sense, **the claimed "notification"** of the Plaintiffs to the Defendants, concerning the illegal activity, has been assessed as not meeting the above criteria and, in particular, **has not found that the Defendants had the required profound "knowledge" of the illegality of their actions**. The Court emphasised that such notification only referred to part of the stored (hosted) information, which was otherwise legal.

Further in the text of the decision, the Court referred to preamble No. 45 of the ECD, which stipulates that an injunction "*can in particular consist of orders by courts or administrative authorities requiring the termination or prevention of any infringement, including the removal of illegal information or the disabling of access to it*". However, the Court concluded that the petitioned injunction contradicts article 14 of PD 131/2003 (= article 12 ECD), since the Defendants did not themselves host the allegedly infringing works. The Court accepted that these works were being transmitted either through a forum, or via hyperlinks, or via p2p networks, and, therefore **the requested blocking of information could not be limited to the allegedly illegal content, but would be extended to any kind of information connected or similar to the initial "illegal" content**. In that sense the Defendants, as intermediaries, would end up with **the burden of a general obligation to monitor** any kind of transmitted information, since no other method of control exists. Furthermore, since the **proposed technical means of blocking** operate automatically and **cannot distinguish between "legal" and "illegal" uses of the protected works**, it is certain that the application of such an automated "filtering" system would also block legal content.

---

[47] Art. 27 par. 2 sec. 1 GPC: *"If a statute requires knowledge of a certain particular as an element, conditional intent shall not suffice*".

The Court affirmed, that **such method, apart from the ECD considerations, contradicts the principle of proportionality, the freedom of information** (article 5A paragraph 1 Greek Constitution), **the right of participation in the Information Society** (article 5A paragraph 2 Greek Constitution), the right to protect personal data (article 9A) and the right of secrecy of communications (article 19). It was evident to the Court that by limiting access, legal actions of the users would be affected, together with "illegal" actions. Such unauthorised intervention, according to the Court, does not meet the terms of necessity and proportionality, which are required for an injunction. The argument of the Court was enhanced by the fact that several of the "illegal" sites had, in the meantime, changed their IP addresses. The Court admitted, finally, that such "filtering" infringes the right of the providers to conduct business (article 16 of the EU Charter of Fundamental Rights), but also contradicts the basic principle of net neutrality, while the cost imposed to providers is disproportionate to the envisaged gain. Interestingly the Greek decision, issued in 2014, does not seem to take into account decision C-314/12 *UPC Telekabel Wien v Constantin Film* of the ECJ, which had followed the same argumentation.

In December 2015 the Court of First Instance issued its Decision No 10452/2015 by which it reaffirmed the above Decision No 13487/2014 (of the same court). In fact it ruled that the first Decision created a precedent which could not be overruled by an injunction.

2.1.7. The particular problem of secrecy of communications

In Greece, the protection of both personal data and of secrecy of communications is backed by Constitutional provisions (articles 9A and 19, respectively). Two independent authorities supervise each field: The Hellenic Data Protection Authority (HDPA) and the Hellenic Authority for Communication Security and Privacy (HACSP). In particular, **for communication data to be revealed, a criminal investigation must be instigated for a particular list of serious crimes**, contained in a list proscribed by law (Law 2225/1994). Under current legislation, common **Internet crimes resulting in harmful or illegal content, such as copyright infringement or defamation, are not included in the list of serious crimes**.

As a result, a major issue has arisen in Greece concerning the revelation of personal data, and in particular the revelation of external communication data, including the IP address, by the relevant Internet intermediaries, to the authorities. In an initial Guideline,[48] the Public Prosecutor of the Supreme Court (*Areios Pagos*) adopted the view that whether a Prosecutor's Order or a Judicial Decision exists or not, police and investigation authorities are entitled to ask Internet intermediaries to reveal external communication data and that HACSP has no jurisdiction over the matter. Subsequently, and in view of Directive 2006/24 (Greek Law 3917/2011), two newer Guidelines[49] have introduced a milder view, limiting the **reveal of data only for cases of malicious or threatening telephone calls** (not Internet content) **and only if a Preliminary Examination or a Preliminary Criminal Investigation or a Criminal Investigation has been ordered by a Public Prosecutor**.

Still, the problem of Internet intermediaries (to reveal or not to reveal the data) has not been resolved,[50] while ECJ case law, such as *Promusica* and *Tele2*[51] has led to ambiguous interpretations. In

---

48 Guideline 9/2009 of Prosecutor G. Sanidas.

49 Guideline 12/2009 of Prosecutor I. Tentes and Guideline 9/2011 of Prosecutor Ath.Katsirodis. Furthermore Decision 91/2012 of the Appeal Court of Thrace has clarified that the Guidelines may only be applied to criminal procedures and not to civil litigation.

50 There are different approaches regarding the interpretation and the legal validity of above mentioned Guidelines, as regards their implementation on internet content.

51 C-275/06 *Productores de Música de España v Telefónica de España SAU* and C-557/07 *LSG - Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH v Tele2 Telecommunication GmbH*

particular cases, providers of mobile services in Greece have been asked by authorities (police, public prosecutor) to reveal customers' data as per the above Guidelines. In most cases they have refused to submit the data on the basis that the crimes under investigation are not included in the list of serious crimes (Law 2225/1994) and the secrecy of communications therefore cannot be lifted. In some instances, the Boards of Directors have been charged with disobedience and harbouring a criminal, but later have been acquitted at the Court. There is currently an on-going investigation against providers in relation to illegal online gambling.

2.2. Take-down/removal of illegal Internet content

2.2.1. Notice- and-take-down

Greek PD 131/3003 has not included at all the wording of article 14 paragraph 3 of the ECD, which provides for "notice and take-down" procedures. Therefore, any such procedure in Greece requires either a change in legislation, or may be introduced by contract or by voluntary codes of practice.

It has been proposed[52] that the introduction of a formal "notice and take-down" procedure, based on the similar procedure of the US Digital Millennium Copyright Act, may solve a number of problems, as has occurred in several EU countries. Such procedure may, to a certain degree, be extended to also cover other aspects of illegal or harmful content, such as defamation or libel cases.[53]

A Greek draft bill implementing the EU directive on collective management[54] includes, among other, a provision introducing a Notice and Take Down procedure for copyright infringements on the Internet. A special Committee will be established at the Hellenic Copyright Organisation (OPI) and will be entitled to decide on alleged copyright infringements on the Internet, among other by instructing providers to remove or block access to illegal content. The draft law also includes an amendment to the law on the secrecy of communications. Accordingly, it will be possible to reveal the identity of those committing serious copyright infringements e.g it would be possible to reveal the holder of an IP address used for copyright infringements on a commercial scale.[55]

2.2.2. Injunction by civil courts

The legal basis for injunctive relief is paragraph 3 of article 13 of Greek Presidential Decree 131/2003 (i.e. 14 paragraph 3 ECD). The wording of the Greek law allows for the remedy to be extended in the hypothetical event of some sort of non-regulated "secondary" liability. In such a case the Court may order any suitable measure against the intermediary. In that sense, case-law is more fascinating in the non-regulated areas of hyperlinks and search engines, which are not covered under the wording of the Greek PD 131/2003 (compare: article 21 paragraph 2 ECD). In several cases,[56] the Greek courts have tried to establish liability by expanding the term "Information Society Services" or "intermediary".

Nevertheless, the critical element in order to establish liability is that of "knowledge": Internet intermediaries are responsible for their own content, but **for third party content they must have**

52 See G. Yannopoulos op. cit. p. 298.

53 See the recent New Zealand's Harmful Digital Communications Bill, Government Bill, 168-3.

54 Directive 2014/26/EU of the European Parliament and of The Council of 26.2.2014 on collective management of copyright and related rights and multi-territorial licensing of rights in musical works for online use in the internal market.

55 The draft bill is currently in the Parliament (19/4/2016).

56 See G. Yannopoulos op.cit., references in footnote 725, p.178.

knowledge of the infringement / harmful / unlawful material in order to be held liable and, hence, to proceed with further action such as blocking / filtering / removal of content. The Greek Presidential Decree harmonising the ECD follows a similar wording and, while access providers stay immune, caching and **hosting intermediaries must act "expeditiously" upon obtaining such knowledge** in order to remove or to disable access to the information.

In a recent case, the Multimember First Instance Court of Athens[57] ("FIC") decided that "deep linking" leading to "downloading" or "streaming" of videos and movies, does not constitute infringement of IP rights. The Court considered it critical that the rightholder did not introduce (i.e. via the hosting intermediary) any measures to control access e.g. some payment method, or by creating an account or even by requesting the simple registration of users. The Court referred to the ECJ Case *Svensson*[58] and the ECJ Order *Bestwater*,[59] supporting the view that the intermediary who has posted the hyperlinks does not host copies of the freely accessible works in his/her own servers and, therefore, he/she has not committed presentation or transmission of the audiovisual works to a "new" audience as per copyright law. Earlier, in a criminal case known as the "Greek-movies" case[60] the Court decided that the inclusion of hyperlinks pointing to already published works in other websites did not fall under the notion of reproduction or public performance of Greek copyright law and, therefore, did not constitute infringement. In order to grant immunity, the Court requested that the copyright holder had not introduced any technological measures or other licensing limitations. On the contrary, in another case, the same FIC of Athens[61] decided that the owner of a radio station website, which linked to another site, infringed copyright, because copyrighted music was made available to the public without license; as a result, the FIC ordered the removal of the hyperlinks.

Finally, in an injunction case,[62] the chairing Judge of the Court of First Instance of Athens initially issued a Provisional Order and then the Court issued an Injunction Decision, ordering Google to cease the **auto-complete** function, which had been producing insulting and defamatory results when typing the name of a known journalist. The Court also ordered a known blog to stop reproducing the insulting information. The Court diagnosed a substantive danger of insult to the personality, as per article 57 of the Greek Civil Code, recognising also the ability of the search engine to organise preventive measures. As long as the search engine controls the specific algorithm of the auto-complete function then it is able to delete the insulting comments. The Court considered itself competent to order an injunction to be applied in the territory of Greece, dismissing the objection of Google that its legal seat is placed in California. The Court referred to a term of Google's Standard Terms of Service and to the fact that Google keeps a local branch in Greece.

It should be noted, however, that the problem of the General Terms and Conditions of **search engines** and **social networks**, directing to the laws of US (mostly California), has not yet been addressed. Such clauses have been characterised as illegal by the Greek Courts in cases of consumer protection, but the Courts have not yet produced any domestic judgements and case law for the

---

57 Decision No. 5249/2014.

58 C-466/12 of 13.2.2014 *Nils Svensson and Others v Retriever Sverige AB*.

59 Order C-348/13 of 21.10.2014 *BestWater International GmbH v Michael Mebes and Stefan Potsch*.

60 See Decision of Magistrate's Court of Kilkis 965/2010. Commented by D. Kalavrouzioti, Journal for Media Law (DIMEE), 2, 2011, 194, who emphasises that the Court has not examined the particular details of the case i.e. who has uploaded the illegal content, if there was any financial profit in relation to advertisement etc.

61 Court of First Instance of Athens Decision No. 4042/2010, commented by D. Kalavrouzioti, Journal for Media Law (DIMEE), 2, 2011, 195.

62 Decision 11339/2012 of the First Instance Court of Athens, commented by G. Yannopoulos, The liability of search engines for suggest and autocomplete services, Journal for Media Law (DIMEE), 2, 2013, 168 [in Greek].

jurisdictional problems of removal of content. For the case of tort, Courts have to be guided by the existing case law of the ECJ, such as the cases *eDate Advertising GmbH*[63] and *Cornelius de Visser.*[64]

2.2.3 Data protection for content removal

Another method that could lead to removal of content would be to activate the data protection legislation. The legal basis for an individual would be to exercise the right of objection to the processing of his/her data, under the Greek Data Protection Law.[65] Only individuals may apply under this provision, and only for data falling under the categorisation of the law.[66]. In most cases examined here, the Internet intermediary would fall under the capacity of the data controller to whom the application must be addressed, in writing. It must include a request for a specific action, such as the correction, temporary non-use, locking, non-transfer or deletion of data. If the controller does not respond within 15 days, then the individual may refer the matter to the Data Protection Authority, who may impose a provisional suspension of the processing (of data) until reaching its final decision.[67]

2.2.4 Soft Law – Codes of Practice

As far as it regards Codes of Conduct, the Greek PD 131/2003 has maintained in article 15 the quasi "wishful thinking" of article 16 of the ECD for the introduction of "soft law". Such codes must, under the Greek PD, be ratified by the Minister of Development. However, self-regulation in Greece has a limited scope of application. Additionally, article 17 paragraph 1 PD 131/2003 provides for alternative dispute resolution by referral to the domestic rules for consumer protection.

E-Business Forum, a public consultation initiative of the Ministry of Development has drafted a Code of Practice and Ethics of ISPs in co-operation with **Safenet**, a non-profit organisation. The Code provides for the introduction of a hotline (**www.safeline.gr**) that accepts complaints about illegal or harmful content, especially child pornography, racist and xenophobic materials etc. Similarly, the Ministry for Education has introduced "blacklists" for sites not to be visited by pupils and students. There is no official acceptance of such soft-law and the Courts have not yet produced any decisions. The Gaming Commission's "blacklist" is prescribed by law and does not fall within the "soft law" category.

In March 2013 a memorandum of cooperation was signed between a large number of Greek collecting societies and two major national internet service providers, endeavouring, among other to raise awareness regarding the impact of digital piracy and to emphasise the legal requirement to respect copyright and related rights.[68]

3. Procedural Aspects

As set out above, **in Greece there is no general law on blocking, filtering or taking down illegal Internet content**. The independent Greek Gaming Commission (GGC) is responsible only for the

---

63 Joint cases C-509/09 *eDate Advertising GmbH v X* and C-161/10 *Olivier Martinez, Robert Martinez v MGN Limited*.

64 C-292/10 *G v Cornelius de Visser.*

65 Art. 13, of Law 2472/1997 (art 14 of Data Protection Directive 95/46)

66 Art. 2 par (a) of Law 2472/1997 (art. 2 par (a) of Data Protection Directive 95/46).

67 Art. 13, par.2 of Law 2472/1997.

68 Available (in Greek) at http://opi.gr/

limited scope of "blacklisted" gambling sites (supra 2.1.4). GGC may not block content directly, but may impose fines to those Internet intermediaries that do not block access to the "blacklist", while the law entails heavy criminal and administrative sanctions. In view of these sanctions, most ISPs operating in Greece have abided by the law to date.

The Orders of the Prosecutor for Child Pornography (supra 2.1.2) have not yet been tested, but they would be limited to the respective subject matter. In any event, the Prosecutor must notify[69] the host provider and the Order is executed immediately. It is questionable how such notifications will be made to providers residing outside Greece or even outside the EU.

Finally, the Data Protection Authority (supra 2.2.3) may only handle complaints of individuals regarding personal data and not generic information. The ability to immediately block data processing is limited to case that the objection right of the data subject is not satisfied.[70] Furthermore, if a decision of the DPA is pending, the Chairman or the DPA, following petition of the data subject, may issue[71] a Provisional Order for the suspension of the data processing until a final decision is reached. Another option for the data subject is to seek a court injunction for the suspension or interruption of any automated processing of personal data that concerns the valuation of his/her personality, work abilities, financial solvency, trustworthiness and behaviour in general.[72] Any appeal against such a decision must take the normal route through the administrative courts.
Therefore, the main procedural way to order a) an access provider to block/filter or b) a host provider to take-down/remove illegal content is to **obtain a court decision on injunctive relief**.[73] The chairing Judge has the right, ex officio, to issue a "Provisional Order"[74] prescribing the exact measures to be taken until the Injunction Decision. Normally, petitioners seek to obtain such an "Order" because it may be issued within 1-2 days. The parties have the right to ask the Court to recall or modify the measure[75] if the factual circumstances have changed.

As explained, article 17 of Presidential Decree 131/2003 (implementing article 18 ECD) provides the legal basis for such a procedure and, in particular, allows measures of blocking or take down if information society rights seem under threat of infringement. The Court may order **any "adequate measure"** and may **even issue a Provisional Order for immediate action against an Intermediary**. The Greek legislator, having in mind copyright and trademark infringements, has inserted a section introducing the ability "*to seize / confiscate the means for the illegal or harmful activity*". In that case, it is obligatory for the Court to issue a Provisional Order and the case may proceed *in absentia* of the defendants. Nonetheless, such power of confiscation seems ineffective in the digital world. In the event that the Internet intermediaries do not comply with the court decision or provisional order, they face severe criminal sanctions.[76]

---

69 Art. 18 par. 1 of Law 4267/2014 (implementing art. 25 of Child Pornography Directive Directive 2011/92/EU.

70 Art. 13 par. 2 of Law 2472/1997.

71 Art. 19 par. 7(a) of Law 2472/1997.

72 Art. 14 Law 2472/1997.

73 Arts 682 et seq. of the Greek Code of Civil Procedure (please note that substantial changes of GCCP, to be inaugurated on 1.1.2016, have taken place in July 2015 by Law 4335/2015). New art. 686 of GCCP provides notification of the party concerned via electronic means.

74 Currently art 691 and as of 1.1.2016 new art. 691A of Greek Code of Civil Procedure as inserted by Law 4335/2015.

75 Arts 696 par. 3 of the Greek Code of Civil Procedure (not affected by the changes).

76 Greek Penal Code art. 232A.

As far as it concerns Domain Name abuse, the **National Telecommunications and Post Commission** may examine[77] complaints for "abusive" or unlawful use of domain names and may decide as a first instance quasi tribunal. In case they disagree with the NTPC's decision, **the parties may appeal to the administrative courts**.

In practice, injunction measures for blocking access have been imposed via the exposed case law (supra paragraphs 2.1.6 and 2.2.2). However, given the fact that domain names and IP addresses may easily be modified, the end result had only minor practical consequences. The significance of such measures lies mainly with the educational effect to the public, as experience from copyright infringement cases shows.

4. General Monitoring of Internet

The **Greek Police Division for Electronic Crime**, being the competent Authority for the prosecution of lCT or internet-related crimes as stipulated in Article 31 of Presidential Decree 178/2014, monitors Internet content in the sense of detecting criminal offenses such as fraud, child pornography, hacking, software piracy, credit card fraud, chat rooms crimes etc., but also with an aspiration of preventing harmful actions. The Division offers vital help in emergency cases of illegal content (e.g. cases of blackmail, suicide attempts etc.). This, of course, has nothing to do with blocking of content and is specifically directed at crime prevention. Police do not have the right to violate constitutional rights like freedom of expression or secrecy of communications or to unlawfully obtain the personal data of citizens, unless there is an ongoing investigation subject to the guarantees of the judicial authorities, who may order temporary monitoring and even then only in specific cases.

Furthermore, from a technical point of view, it is not possible to monitor Internet content efficiently. The traditional system of civil liability in Greece has offered more arguments in favour of the system of immunity of ECD and support for **the prohibition of a general obligation to monitor content** (article 15 ECD, article 14 Greek PD).

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

Following the European Parliament compromise of 5th November 2009, the Greek Law 4070/2012 harmonising the Telecommunications Directive 2009/140[78] has repeated[79] in article 3 the ambitious wording, referring to article 10[80] of ECHR, and stating that "…*Measures taken by Member States… shall respect the fundamental rights and freedoms of natural persons, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and general principles of Community law. Any of these measures … liable to restrict those fundamental rights or freedoms may only be imposed if they are appropriate, proportionate and necessary within a democratic society,*

---

77 Art. 10 par. 12 of NTPC Domain Name Regulation No.750/2/Official Gazette B-412/24-3-2014

78 Directive 2009/140/EC, of 25.11.2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services.

79 With several ambiguities in relation to the original text of the Directive, see Yannopoulos op.cit. pp. 189-190

80 See a similar reference to art. 10 ECHR in Internet Recommendation CM/Rec (2008) 6, 26.3.2008 *on measures to promote the respect for freedom of expression and information with regard to Internet filters*, according to which users may object the use of filters. See also CoE document: *Human rights guidelines for Internet Service Providers*, H/Inf (2008) 9, available at www.coe.int.

and their implementation shall be subject to adequate procedural safeguards in conformity with the European Convention for the Protection of Human Rights and Fundamental Freedoms and with general principles of Community law, including effective judicial protection and due process". The obscure wording of the law, however, does not directly answer the critical question of whether **private entities, such as Internet intermediaries are allowed to restrict fundamental rights such as the right to access a network?** Although the ECHR case-law is clear in several of the above matters, the particular legislation has not yet been tested in full scale by the Greek courts. Only in passim, decision FIC Athens 4658/2012 (see supra par. 2.1.6), accepts, before harmonisation, that article 3 of Directive 2009/140 is not directly applicable[81] while adjudicating a dispute between private entities.

In the case of the general injunction measures, as per ECD, regarding copyright infringement, trademark violations, defamation and other harmful content the **legitimate goal** of the restriction may be founded in article 10 part 2 of ECHR regarding "reputation or rights of others". Although the legal framework does not appear to be sufficiently precise, the intervening court is able to interpret the rules in a specific manner and **to apply the principle of proportionality** ensuring that the restrictive measure has the narrowest effect in a democratic society. The fact that the restriction is decided by a Court, even in an injunction, means that **the Court in each individual case will make an *ad hoc* assessment of the two conflicting rights, in order to decide whether the freedom of expression of the intermediary precedes the right of the claimant or vice versa**. The Courts in Greece have mainly used that principle, which has been helpful in order to establish, for example, whether personal data of customers of access providers must be revealed in case of copyright infringements and whether blogs and bloggers fall under the rigid liability legislation for traditional editors.

The recent law for Prosecutor's Order in the case of **Child Pornography** provides that an "**individually and fully justified Order**" **must be notified to the owner of the website** so as to have the illegal content removed.[82] In that sense the Greek Law is trying to comply with article 10 of ECHR, establishing that the **restriction to the freedom of expression** is pursuing a **legitimate goal** and is **necessary in a democratic society**. Further down in article 18 paragraph 2 of the same Law, the owner of a **deactivated domain name** is entitled to a petition (quasi appeal) to the Prosecutor for the domain to be reactivated. Again, both the initial Order and the "appeal" decision must be "**individually and fully justified**" and **notified to the domain owner**. The same applies to the blocking of a website with child pornography content (article 18 paragraph 3). It is evident that the Greek legislator is trying, *inter alia*, to cover certain aspects of article 6 of ECHR (fair trial) and article 10 ECHR (freedom of expression). Given the limited scope of child pornography, the rules are precise and specific and they confer a limited range of discretion to the authorities.

A question could be raised regarding the blocking of blacklisted "illegal" gambling sites (see above section 2.1.4). In the eyes of the Greek legislator, these sites are illegal, but they have a legitimate licence elsewhere in the EU. Such prohibition may, therefore, contradict the principles of **necessity** and **proportionality** in connection with the enjoyment of property (ECHR, Protocol 1) or the economic freedom and transfer of services within the EU (see also article 16 of the EU Charter of Fundamental Rights). However, the restriction has been imposed by a law enacted by Greek Parliament, so we must wait either for a Greek court to declare the law unconstitutional or contradictory to the ECHR, or for the case to reach the European Court of Human Rights or the ECJ.

So far as it concerns **predictability** for restrictions to freedom of expression, it is obvious that host intermediaries have a duty of care, which can be reasonably expected as per each individual case. It

---

81 The Greek Decision supports its argument by referring to ECJ case law C-397/01 to C-403/01, *Pfeiffer*, C- 91/92, *Faccini Dori*, etc.

82 See art. 18 par. 1 of Law 4267/2014 harmonising art. 25 of Child Pornography Directive 2011/92/EU.

is characteristic that in the case law already exposed (see above sections 2.1.6 and 2.2.2) the Greek Courts have tried to establish **a higher standard for the duty of care of service providers**, in the sense that they are **effectively the "gatekeepers" of the modern era**.

It is true that for law enforcement over the new medium, the **judiciary is best equipped to solve the problem of proportionate balance between conflicting interests** and to impose restricting measures. **Otherwise, Internet intermediaries would be charged with judicial duties**: they would be obliged to decide the legality of content being transferred or hosted in their systems and to take action by blocking, filtering or taking down such content. Such a role is **not appropriate** for them and would **create insecurity and uncertainty** as to what is legal or not.

The legal framework and case law in Greece, like in the EU, shows that the role of intermediaries is changing from simple "conduits" to broader **"gatekeepers" of the modern Information Society**. In a digital world, users must be convinced that they do not endanger something more than in a similar transaction in the analogue universe. To achieve that goal, Greek Courts, while imposing restrictive measures, have tried to balance the demand for freedom to enjoy Information Society rights with the demand for privacy, data protection and security. When the suppressive enforcement of the rule of law over the Internet was condemned to fail, judges tried to generate an educational effect through their decisions. They have attempted, in line with the EU dynamics, to develop a sense of responsibility to those who hold the keys of electronic transactions and who decide about impacts on citizen's fundamental rights. Creating a responsible Internet intermediary is not only a matter of statute or case-law, but rather **a matter of attitude of the Internet key-players** who must seek, in the first place, to create confidence on behalf of the users.

Dr. Giorgios Yannopoulos
03.10.2015

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