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 147-162

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.

CYPRUS

1. Legal Sources

The blocking, filtering and take down of illegal internet content in Cyprus is **not governed by legislation specific to the Internet**. Nevertheless, it is possible to undertake such measures on the basis of **general civil and criminal law provisions** and also on the grounds of **certain specific laws**. International standards, being conventions relating to illegal Internet content, have generally been transposed into the domestic regulatory framework and enable blocking, filtering and take down of particular types of illegal content.

Specifically, Internet content can be illegal under the **Cypriot Copyright Law no. 59/1976**[1] as well as the **Cyprus Betting Law no. 106(I)-2012**[2] and the **Law on combating sexual abuse and sexual exploitation of children, and child pornography no. 91(I)/2014.**[3]

Cyprus ratified the **Cybercrime Convention of the Council of Europe**[4] with the Law no. 22(III)/2004[5] and the **Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote, 25.X.2007**) with the Law no. 21(III) of 2014.[6]

Furthermore, Cyprus signed and ratified the **Additional Protocol concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems**.[7]

The **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data** was ratified by Cyprus with the Law no. 28(III) 2001 and the **Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows**[8] was ratified by Cyprus with the Law no. 30(III) 2003. The provisions of the EU's Data Protection Directive 95/46/EC were transposed into the law of Cyprus by the Law no. 138(I) 2001.

The dissemination of terrorist publications and the incitement of terrorism via the publishing of statements which are likely to be understood as a direct or indirect encouragement of acts of

---

1 «Οι περί του Δικαιώματος Πνευματικής Ιδιοκτησίας Νόμοι του 1976 μέχρι 1993 (59/1976)». For the full text of the Law in Greek, see: http://www.cylaw.org/nomoi/enop/non-ind/1976_1_59/index.html.

2 «Ο περί Στοιχημάτων Νόμος του 2012 (N. 106(I)/2012)». For the full text of the law in English see: http://www.nba.com.cy/eas/eas.nsf/page01_gr/page01_gr?OpenDocument.

3 The law implemented in Cyprus the Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating sexual abuse and sexual exploitation of children, and child pornography, replacing the Council Framework- Decision 2004/68/JHA.

4 The Budapest Convention on Cybercrime, CETS no. 185.

5 Law of 2004 ratifying the Cybercrime Convention (N. 22(III)/2004).

6 "Ο περί της Σύμβασης του Συμβουλίου της Ευρώπης για την Προστασία του Παιδιού από τη Σεξουαλική Εκμετάλλευση και τη Σεξουαλική Κακοποίηση (Κυρωτικός) Νόμος του 2014 εκδίδεται με δημοσίευση στην Επίσημη Εφημερίδα της Κυπριακής Δημοκρατίας σύμφωνα με το Άρθρο 52 του Συντάγματος".

7 Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems, CETS no. 189. See: Implementation of the Protocol to the Convention on Cybercrime on Xenophobia and Racism: Results of ECRI monitoring, 9 June 2015, Project Cybercrime @Octopus, available at: https://rm.coe.int/CoERMPublicCommon SearchServices/DisplayDCTMContent?documentId=0900001680304ffa.

8 CETS No.181.

terrorism are not regulated by the Law no. 110(I)/2010 (Cypriot Terrorist Act of 2010).[9] Nevertheless, Cyprus ratified the **Council of Europe Convention on the Prevention of Terrorism**[10] with the Law no. 22 (III) of 2010.[11] Furthermore, Cyprus implemented the Council Framework Decision 2008/913.23 with the Law no. 134(I)/2011 on combating certain forms and expressions of racism and xenophobia by means of criminal law. Cyprus has also ratified the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems with the Law no. 26(III)/2004.

Section 99 of the **Law no. (70(I)/2001) about medicinal products for use by humans**[12] prohibits the distance selling via the use of information society services of medicinal products which have not been authorized by the Council of medicinal products or the EU. Nonetheless, there is no specific provision about the blocking/filtering of such sites.

Section **17 of Cap 148 (the law on torts**) establishes the tort of defamation.[13] Additionally, section **149 (6) of the law on electronic communications and post services Law no. 112(I)/2004**)[14] states that the sending of grossly offensive and/or indecent or obscene or menacing character messages is a criminal offence.[15]

Cyprus has implemented the Personal Data Protection Directive 95/46 with the Law no. 138 (I) 2011.[16] The provisions of the Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector and the EU Regulation Nº 611/2013 of 24 June about measures applicable to the notification of personal data breaches for the European telecommunications industry were implemented in the Law no. 156 (I) 2004 on electronic communications.[17]

---

9 «Ο περί Καταπολέμησης της Τρομοκρατίας Νόμος του 2010 (N. 110(I)/2010). For the full text of the law in Greek, see: http://www.cylaw.org/nomoi/enop/non-ind/2010_1_110/index.html.

10 Council of Europe Convention on the Prevention of Terrorism, Warsaw, 16.V.2005. For the full text of the Convention see: http://conventions.coe.int/Treaty/EN/Treaties/Html/196.htm.

11 Article 5 of the Convention, whose title is "Public provocation to commit a terrorist offence", provides as following: "*For the purposes of this Convention, "public provocation to commit a terrorist offence" means the distribution, or otherwise making available, of a message to the public, with the intent to incite the commission of a terrorist offence, where such conduct, whether or not directly advocating terrorist offences, causes a danger that one or more such offences may be committed. 2 Each Party shall adopt such measures as may be necessary to establish public provocation to commit a terrorist offence, as defined in paragraph 1, when committed unlawfully and intentionally, as a criminal offence under its domestic law*".

12 For the full text of the law in Greek see: "Ο Περί Φαρμάκων Ανθρώπινης Χρήσης (Έλεγχος Ποιότητας, Προμήθειας και Τιμών) Νόμος του 2001 (70(I)/2001)", http://www.cylaw.org/nomoi/enop/non-ind/2001_1_70/index.html.

13 "Ο περί Αστικών Αδικημάτων Νόμος (ΚΕΦ.148)".

14 "Ο Περί Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομικών Υπηρεσιών Νόμος του 2004 (112(I)/2004)".

15 More precisely, according to this provision, "*Any person who-(A) sends by the use of a public communications network, a message, or whatever content, which is grossly offensive and of an indecent or obscene or menacing character, or (B) sends by the use of a public communication network a message, or whatever content, which can cause annoyance, harassment and / or needless anxiety to another person, which the sender knows to be false is guilty of an offense and is liable on conviction to a fine not exceeding one thousand seven hundred euros (€ 1.700)".*

16 «Ο Περί Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου) Νόμος του 2001 (138(I)/2001)».

17 "Ο περί Ορισμένων Πτυχών των Υπηρεσιών της Κοινωνίας της Πληροφορίας και ειδικά του Ηλεκτρονικού Εμπορίου καθώς και για Συναφή Θέματα Νόμος του 2004 (N. 156(I)/2004)".

Furthermore, in the absence of specific legislation on the topic, a general power of the Court in civil proceedings to issue interim orders (injunctions) on the grounds of article **32 of the Courts of Justice Law no. 14/60 (**which confers power to the Court to grant injunctions in all cases in which it appears to the Court just and convenient to do so) could possibly be used for blocking and the take down of Internet content, including for example, defamatory content, confidential information, trade secrets or IP infringing content.[18]

Finally, section **27 of the Code of Criminal Procedure** which enables the competent judicial authorities to issue a "search warrant" could be used for the seizure of personal computers used or intended to be used for the commission of Internet related crimes.

2. Legal Framework

The **legislation of Cyprus permits site blocking, filtering and taking down of illegal content in specific cases** for particular types of illegal or harmful content. Generally, blocking, filtering and take down of illegal content is supplemented by legislation in limited areas and court orders in the form of injunctions, but in practice such measures have not yet been ordered by Cypriot courts. So, while it is possible to order or apply such measures, there is **no relevant case law** as yet.

Preliminary remarks on Internet intermediaries' safe harbour regime
When implementing the E-Commerce's Directive intermediaries' asylum, Cyprus followed closely the relevant provisions of the Directive. Articles 12, 13, 14 and 15 of the Directive were transposed verbatim in sections 15, 16, 17 and 18 of Law no. 156 (I) 2004 on electronic communications.[19] Cypriot legislation has established a safe harbour regime for mere conduit, hosting and caching activities. It has not extended this regime to other activities, such as the activities of search engines, the provision of hyperlinks or of online market places. **The law has not established a specific mechanism of notice and take down procedures**. There is no case law that further interprets those provisions.

The relevant provision implementing article 12 of the E-Commerce Directive is section 15 of the law 156 (I) 2004. According to this provision, where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network (mere conduit), the service provider is not liable for the information transmitted, on condition that the provider: (a) does not initiate the transmission; (b) does not select the receiver of the transmission; and (c) does not select or modify the information contained in the transmission. The acts of transmission and of provision of access referred to in paragraph 1 include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission. This provision does not affect the possibility for a court or administrative body to impose on the service provider appropriate measures to terminate or prevent the infringement. There is no relevant Cypriot case law on the application of section 15.

According to section 16 of law 156 (I) 2004, which implements section 13 of the E-Commerce Directive, where an information society service is provided that consists of the transmission in a

---

18 Demades Overseas Ltd v Studio Mast Ltd (Civil appeal no. 9636 και 9637), 18/07/96 ·Parico Aluminium Designs Ltd v Muskita Aluminium Co. Ltd (2002) 1 AAD 2015.

19 "Ο περί Ορισμένων Πτυχών των Υπηρεσιών της Κοινωνίας της Πληροφορίας και ειδικά του Ηλεκτρονικού Εμπορίου καθώς και για Συναφή Θέματα Νόμος του 2004 (Ν. 156(Ι)/2004)".

communication network of information provided by a recipient of the service, the service provider is not liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request (caching), on condition that: (a) the provider does not modify the information; (b) the provider complies with conditions on access to the information; (c) the provider complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry; (d) the provider does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and (e) the provider acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement. This provision does not affect the possibility for a court or administrative authority to require a service provider to terminate or prevent an infringement.

Section 17 of the law 156 (I) 2004 implements the section 14 of the E-commerce directive. More specifically, according to this provision, where an information society service is provided that consists of the storage of information provided by a recipient of the service (hosting), the service provider is not liable for the information stored at the request of a recipient of the service, on condition that: (a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or (b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information. This provision does not apply when the recipient of the service is acting under the authority or the control of the provider. There is no relevant Cypriot case law on the application of section 17.

Section 18 of the law 156 (I) 2004 implemented section 15 of the E-commerce directive. According to this provision, intermediaries are not subject to a general obligation to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity. Nonetheless, information society service providers must promptly to inform the competent Public authority (being the Ministry of Industry and Tourism) of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements.

2.1. Blocking and/or filtering of illegal Internet content

The possibility of Internet Service Providers (“ISPs”) blocking and/or filtering illegal content contained in websites is a measure that is principally directed to websites which contain child abuse material and child pornography, illegal betting and copyright infringing content, however there is not yet any case law invoking these laws. Furthermore, it is a priori theoretically possible to order such measures on the grounds of section 32 of the Courts of the Justice Law no. 14/1960 about interim orders, but this possibility has also not yet been confirmed by case law.

2.1.1. Blocking and/or filtering of Internet content on the grounds of section 32 of the Courts of Justice Law

It is not certain whether the general provisions of section 32 of the Courts of Justice Law no. 14/1960 about **interim orders could be applied for obliging ISPs to block and/or filter sites containing illegal content**. Indeed, since there is not yet any relevant case law, **only doctrinal assessments can be made**.

On the one hand, it could be argued that blocking orders fall within the authority and discretion of the civil courts to grant injunctions, relying on, among others, UK case law, which can be used as a persuasive non-binding precedent. Indeed, Mr. Justice Arnold in the case Cartier International and Others v. BSkyB and others,[20] had to consider whether a power to order ISPs to block trademark infringing sites could be found in the general jurisdiction to grant injunctions found in section 37(1) of the Senior Courts Act 1981,[21] which is the counterpart of section 32 of the Courts of the Justice Law no. 14/1960. In the UK, like in Cyprus, there is a special provision in the UK Copyright, Designs and Patents Act 1988[22] enabling the Court to order such measures, but there is no equivalent statutory provision in relation to trade mark infringement. Mr. Justice Arnold accepted that the power of the Court to grant injunctions is "unlimited" and can be exercised in new ways.

On the other hand, it could be argued that site blocking by ISPs requires special legislation, and that, as a result, it could be ordered only in the specific cases clearly provided by law. This was the stand of the District Court of Tel Aviv on July, 1st 2015 in the *ZIRA* case,[23] where it was held that there is no authority for the courts to order ISPs to take any actions in disputes between plaintiffs and third party defendants.

So, while it is probable that the courts in Cyprus can use section 32 of Courts of the Justice Law no. 14/1960 about interim orders as a possible legal ground for obliging ISPs to block and/or filter sites, this possibility has not yet been confirmed by case law.

2.1.2. Child abuse and child pornography

Article 11 of Law 91(I)/2014 implemented article 25 of the Directive 2011/92/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography. More specifically, Article 11 (1) provides that **the Court** in any stage of the procedure **can order the prompt removal of web pages containing or disseminating child pornography**. Article 11 (2) enables the Court to order the blocking of access to web pages containing or disseminating child pornography towards Internet users resident in Cyprus.

ISPs offering services or access to the Internet within the territory of the Republic of Cyprus, **are obliged**, **as from the moment they gain knowledge or are informed by the competent authority** of the existence of child pornographic content on any site, **to immediately take appropriate measures for the interruption of access by Internet users.**[24]

2.1.3. Copyright infringing content

Article 13 (5) of Law 59/1976 concerning the protection of copyright implements article 8.3 of the Information Society Directive[25] and provides that right holders are in a position to apply for an **injunction against intermediaries whose services are used by a third party to infringe a copyright or related right.** No specific freedom of expression safeguards are established by the law, but in general

---

20 [2014] EWHC 3354 (Ch).

21 According to this provision, "The High Court may by order (whether interlocutory or final) grant an injunction or appoint a receiver in all cases in which it appears to the court to be just and convenient to do so".

22 Section 97A of the Copyright, Designs and Patents Act 1988.

23 Civil file (Tel Aviv) 37039-05-15 ZIRA v' John Doe et al (July 1, 2015).

24 The definition of "competent authority" will be explained in section 3 (Procedural aspects).

25 Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, Official Journal L 167, 22/06/2001 P. 0010 – 001.

the relevant CJEU's case law must be followed**.** This provision does not presuppose or prerequisite the intermediaries' liability. Generally, all appropriate remedies will be considered by courts. The provision has not been applied yet by Cypriot courts, but it could be used in order to stop or prevent copyright infringements by various means, such as by blocking access to an infringing website.
Moreover, articles 15, 16 and 17 of Law 156 (I) 2004[26] provide that the intermediaries' immunity regime that was established by the E-Commerce Directive does not affect the **possibility for a court or administrative authority to impose appropriate measures on a service provider to terminate or prevent an infringement**.

2.1.4. Online Betting

According to section 65 of the law 106/2012 about online betting, Internet providers have the obligation to block websites which do not have the relevant permission to provide services of online betting. Indeed, betting services in Cyprus via electronic means are offered legally only if the betting operator is authorized by the National Betting Authority. **The National Betting Authority provides a list of websites that must be blocked by ISPs**. Access to sites that offer electronic betting services which are licensed by Member States of the European Union has not been barred by reason of the transitional provision of Article 91 (3) of the Law 106 (I) 2012.

According to this provision, legal persons that, at the time of the entry into force of this Law, are licensed to conduct online betting on the basis of a license issued by a Member State of the European Union may continue to provide such services only for the type of betting services which are authorized by this law and until they are granted a license from the National Betting Authority, provided that they have submitted an application for a license pursuant to the provisions of this Law. However, it has recently been ruled that such a blockage when used against a legal person that is established in another EU member State violates primary European law (sections 43 and 49 EC). More precisely, the order to block the website concerned was found to be illegal, since the Republic of Cyprus has not yet issued the appropriate regulations and has not officially opened a procedure that enables companies that are established in other member states to ask for a permission from the National Betting Authority to operate in Cyprus.[27]

2.1.5. Terrorist statements

The Cypriot Terrorist Act of 2010[28] does not contain specific provisions prohibiting the dissemination of terrorist publications and the incitement of terrorism via the publishing of statements which are likely to be understood as a direct or indirect encouragement of acts of terrorism. Nonetheless, Cyprus ratified the **Council of Europe Convention on the Prevention of Terrorism[29]** with the Law no. 22 (III) of 2010.[30] Furthermore, it could theoretically be possible to sentence certain such activities on

---

[26] "Ο περί Ορισμένων Πτυχών των Υπηρεσιών της Κοινωνίας της Πληροφορίας και ειδικά του Ηλεκτρονικού Εμπορίου καθώς και για Συναφή Θέματα Νόμος του 2004 (Ν. 156(Ι)/2004)". Available on line in Greek at: http://www.cylaw.org/nomoi/indexes/2012_1_106.html.

[27] Supreme Court, Betfair International Plc's v. Republic of Cyprus, case 492/2013, 30/4/2013.

[28] «Ο περί Καταπολέμησης της Τρομοκρατίας Νόμος του 2010 (Ν. 110(Ι)/2010". For the full text of the law in Greek, see: http://www.cylaw.org/nomoi/enop/non-ind/2010_1_110/index.html.

[29] Council of Europe Convention on the Prevention of Terrorism, Warsaw, 16.V.2005. For the full text of the Convention see: http://conventions.coe.int/Treaty/EN/Treaties/Html/196.htm.

[30] Article 5 of the Convention, whose title is "Public provocation to commit a terrorist offence", provides as following: "*For the purposes of this Convention, "public provocation to commit a terrorist offence" means the distribution, or otherwise making available, of a message to the public, with the intent to incite the commission of a terrorist offence, where such conduct, whether or not directly advocating terrorist offences, causes a danger that one or more such offences may be committed. 2 Each Party shall adopt such measures as may be necessary to establish public provocation to commit a terrorist*

the legal grounds of section 57 of the Cyprus Penal Code, Cap 154, according to which advocating and encouraging "unlawful association" via written statements is a criminal offence. Nevertheless, there is **not a specific provision in the Cyprus Penal Code or the Cyprus Code of Criminal Procedure about the taking down of such content or the blocking/filtering of such sites**.

2.1.6. Hate and xenophobic speech

Cyprus implemented the Council Framework Decision 2008/913.23 with the Law no. 134(I)/2011 on combating certain forms and expressions of racism and xenophobia by means of criminal law. Cyprus also ratified the Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems with the Law no. 26(III)/2004.

The Cypriot Criminal Code Cap. 154 has been recently amended in order to criminalize the deliberate public, and in a threatening fashion, incitement to hatred or violence, and the incitement to hatred or violence, verbally or through the press, textually or pictorially or by any other means, against any group of persons, or a member of a group based on their sexual orientation or gender identity (article 99A). Nonetheless, the criminal complaint can be initiated only on the authorization of the Attorney General.
In both cases, **no special procedures for the blocking or filtering of hate and xenophobic speech are established by the law**.

2.1.7. Private regulation of ISPs

The legal framework governing the blocking and/or filtering of illegal Internet content is not governed by ISPs' self-regulation. There are **no voluntary codes or best practices** that are concluded or followed by all or certain service providers on this issue. However, in the terms of use of the services of each of the ISPs, there are generally particular clauses that permit the service providers to terminate the provision of services or disclose data to third parties in case of violation of the law.[31]

2.2. Take-down/removal of illegal Internet content

2.2.1. General framework

Taking down/removal of illegal Internet content could theoretically be achieved on the grounds of **general provisions permitting the Court to order an injunction** on the basis of article 32 of the Courts of Justice Law 14/60, whose justification lies in the law of equity.

To date, the conditions of application of section 32 have been defined by Cyprus case law mainly in the context of cases not related to Internet.[32] In general, courts order such measures rather

---

offence, as defined in paragraph 1, when committed unlawfully and intentionally, as a criminal offence under its domestic law".

31 For example, article 8. 3 of the general terms of use of "Primetel" services stipulates that "the Company and the Subscriber are bound against each other to treat in strict confidence and secrecy any information or data provided by the Company to the Subscriber and vice versa, for the purposes of or pursuant to the Agreement, unless the specific information is already in the public domain or their disclosure is necessary in accordance with a court judgment or order or with the applicable legislation for the time being." See: http://www.primetel.com.cy/en/terms.

32 Odysseos v. Pieris Estated Ltd and Others (1982) 1 CLR · Constantinides v. Makriyiorghou (1978) 1 CLR 585· Karydas Taxi Co Ltd v. Andreas Komodikis (1975) 1 C.L.R. 321 ·A. Kytala v. Άnna Chrysanthou and others (1996) 1 A.A.Δ. 253· T.A. Micrologic Computer Consultants Ltd v. Microsoft Corporation (2002) 1(Γ) A.A.Δ. 1802,

cautiously.[33] Section 32 of the Courts of Justice Law confers power on the Court to grant an injunction **in all cases in which it appears to the Court just or convenient to so do**. However, the justice and convenience of the case is not the sole consideration to which the Court shall pay attention and certain supplementary conditions have to be met: a) a **serious question arises to be tried at the hearing** b) there appears to be a **"probability" that plaintiff is entitled to relief and** c) **unless it shall be difficult or impossible to do complete justice at a later stage without granting an interlocutory injunction.**[34]

The injunction mainly concerns measures to stop the use, disclosure, exploitation of illegal or harmful content by the defendant in the context of a civil action**, while the adjudication of the main civil action is still pending**. The purpose of the interim order is to prevent the defendant from doing something, or alternatively to order the defendant to act in a specific way until the end of the adjudication of the main civil action. **If the plaintiff succeeds in the main civil action, the order becomes permanent**.

In this context, an interim order was awarded in order to restrain the defendant from using and disclosing confidential information of her former employer, including trade secrets and personal data of the employer's clients.[35] Injunctions have also been awarded for the protection of a business name[36] or a trademark.[37]

Recently, a demand for an injunction on the grounds of section 32 of Law no.14/60 was filed **against Facebook** asking the District Court of Paphos to order the company to remove a number of offensive comments posted on a local business profile aimed at a local man and to take steps to ensure that any future related comments were taken down immediately. The Court accepted in principle the granting of the order, but before issuing definitely the order gave guidelines that the claim must be officially notified to Facebook and the issue is thus still pending while that occurs.[38]

Additionally, section 27 of the Code of Criminal Procedure enables the competent judicial authorities to issue a **"search warrant" if there is reasonable ground for believing that** there is in any location (a) **anything upon or in respect of which any offence has been or is suspected to have been committed**; or (b) **anything which there is reasonable ground for believing will afford evidence as to the commission of any offence** or (c) **anything on which there is reasonable ground for believing is intended to be used for the purpose of committing any offence**. The "search warrant" can authorize the person therein named to (a) **search such location** for any such thing and to seize and carry such thing before the Court out of which the search warrant is issued or some other Court to be dealt with according to law; and (b) **to apprehend and bring before a Judge the occupier of the house** or location where the thing is found or any person in or about such house or location being in

---

33 For a denial of award of an injunction, see: District Court of Limassol, METAQUOTES SOFTWARE LTD v QASSEM HAMADEH, 07.01.2014, Claim no: 3349/2013 (trade secrets and confidential information) District Court of Limassol, Attorney General of the Republic v Philippos A. Trikomitis and Son Limited, 26.11.2014, Claim No: 305/14 (trademark protection).

34 See: Odysseos v. Pieris Estated Ltd and Others (1982) 1 CLR.

35 District Court of Limassol, LQD MARKETS LTD v NIKOLETT PALINKAS, 13.5.2014.

36 Supreme Court, Demades Overseas Ltd v Studio MAST LTD (1996) 1 CLR 799· Supreme Court, CTO PUBLIC COMPANY LIMITED, EXPOSAL LIMITED v 1. BAT (CYPRUS) LIMITED, 2. ROTHMANS OF PALL MALL LIMITED, (2012) 1 A.A.Δ. 178.

37 Supreme Court, Evans & Sons Limited v Spyros Ioannou and others, 20/12/2001, (2001) 1 A.A.Δ. 2092.

38 District Court of Paphos, Neophytos Georgiou v Facebook Inc., and others, no. of the action 569/2015, 23/4/2015, available on line at: http://www.cylaw.org/cgi-bin/open.pl?file=apofaseised/pol/2015/4120150130.htm&qstring=facebook (Please note that the Court's order is elliptic and that it was not possible to find more information as to this case).

possession of such thing, if the Judge thinks fit so to direct in the warrant. This provision has been used by the police for the seizure of personal computers which are suspected to have been used for the commission of offences or for which there is reasonable ground for believing that they are intended to be used for the purpose of committing an offence. The seizure of the computer has as an indirect result that the offender cannot practically use the computer (including all the passwords and other information contained in it) for the commission of the offence, since he is deprived of the necessary means to commit it.

Nonetheless, **it is doubtful whether this "seizure process" can also be applied for the seizure of intangible goods**, such as a domain names. Indeed, **the ratio of this procedure is mainly the preservation of evidence** for the commission of an offence[39] and not to obtain a preliminary injunction against the website in an ex parte proceeding. Furthermore, depending on the circumstances of each case, the **proportionality of this measure could be questioned**. Once again, there is no relevant case law.

2.2.2. Take down of copyright infringing content

The taking down/removal of illegal content can also be ordered on the grounds of the Law no. 59/1976 on the protection of copyright. Section 13 (5) of Law no. 59/1976 provides that right holders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right. In this context, right holders could ask the Court to take down copyright infringing content from a website hosting such content provided by a third party. Moreover, section 13 (5) of law 59/1976 also enables copyright holders to ask the Court to order an injunction against copyright infringers. According to this provision, infringements of copyright shall be actionable at the suit of the owner of the copyright. Besides, an action for such an infringement may result in any of such reliefs, whether damages, injunction, accounts or others, as is available in any corresponding proceedings in respect of infringement of other rights including the right of delivery up to the owner of copyright, who is deemed to be their owner, of all the copies which appear to the Court to be infringing copies of the copyright in the work.

2.2.3. Take down of content which is a breach of personal data

Cyprus has implemented the Personal Data Protection Directive 95/46 with the Law no. 138 (I) 2011.[40] There are no specific regulation, recommendations or guidelines about the taking down, removal, blocking/filtering of sites or platforms which illegally process personal data.

In general, the **Commissioner for Personal Data Protection** has the competence to report to law enforcement authorities the complaints for breach of personal data. The Commissioner can also impose as an administrative penalty on the data controller the destruction of the archive where the

---

39 Concrete Mix Ltd v Police (1991) 2 ΑΑΔ 360, where it was held that "*The provisions relating to the seizure and detention of items (for investigative and evidentiary purposes) are arranged in chronological order which reflects the three separate stages are defined and regulated by law. Article 27 governs the power to confiscate objects. These may be seized during the execution of a warrant investigation, provided that the examination is necessary for the purposes of police investigation. Object confiscation under Article 27 provides only a limited right to detention until the launch, as soon as possible before the Court, as provided in Article 32 (1) of the Act. The Court of justice will finally decide the necessity of further detention of the object for the purposes of investigations and future criminal proceedings. The provisions of section 32 (1) provide discretion to the Court to order the detention and custody object seized by the police authorities until the completion of criminal proceedings whatsoever arising from police investigations.*"

40 «Ο Περί Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου) Νόμος του 2001 (138(I)/2001)».

illegal processing of personal data has taken place and the interruption of the illegal processing. Consequently, the **removal/take down of illegally processed personal data could be ordered by the Commissioner as a form of interruption of the illegal processing**. In that case, the Commissioner cannot proceed on the removal or taking down, but only an administrative decision ordering the interruption of illegal processing will be imposed on the infringer. Unfortunately for our purposes, there is no relevant case law and no relevant decisions of the Commissioner for Personal Data Protection.

2.2.4. Private regulation of ISPs

The legal framework governing the blocking and/or filtering of illegal Internet content is not governed by ISPs' self-regulation. There are no voluntary codes or best practices that are concluded or followed by all or certain service providers on this issue.

2.2.5. Constitutional safeguards against arbitrary take down of internet content

There are **no special requirements** that have been established for the take down/removal of Internet content **except for the provisions of the Constitution** of the Republic of Cyprus **safeguarding freedom of expression** (article 19 of the Constitution), **privacy** (article 15 of the Constitution) **and the secrecy of communications** (article 17 of the Constitution).

Article 19 of the Constitution of Cyprus provides as following "*(1) Every person has the right to **freedom of speech and expression in any form**. (2).This right includes freedom to hold opinions and receive and impart information and ideas without interference by any public authority and regardless of frontiers. (3). The exercise of the rights provided in paragraphs 1 and 2 of this Article may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary only in the interests of the security of the Republic or the constitutional order or the public safety or the public order or the public health or the public morals or for the protection of the reputation or rights of others or for preventing the disclosure of information received in confidence or for maintaining the authority and impartiality of the judiciary*". The Supreme Court of Cyprus has constantly affirmed a status of reinforced protection for the right of freedom of expression, which is characterized as a blessing and a feature of every civilized society.[41] The right to access the Internet is interwoven with the right to information and communication, which is protected by article 19 of the Constitution.[42]

Nonetheless, **freedom of expression is not an absolute right, but it is subject to restrictions** in accordance with article 19 par. 3 of the Constitution. More precisely, "*the following main principles govern freedom of expression: (a) freedom is the rule and restriction is the exception; (b) restriction should be provided by law;(c) restriction should be necessary for a constitutionally prescribed legitimate aim; and (d) restriction should be proportional to the legitimate aim pursued within a democratic society*".[43]

In this context, the balancing of the freedom of expression with other rights is made with caution and with reference to the principles set by the European Court of Human Rights in the Sunday Times[44]

---

41 Supreme Court, Georgios Chatzinicolaou v Police (1976) 2 C.L.R. 63.

42 OSCE Comparative Study on Freedom of Speech and Internet Available at: http://www.osce.org/fom/80723?download=true (30.07.2015).

43 C. Stratilatis, A. Emilianides, Media Law, Cyprus, Kluwer Law International, International Encyclopaedia of Laws series., 2015, p. 44.

44 Sunday Times v UK [1979] 2 EHRR 245.

and the Handyside[45] cases.[46] In general, it is well established in case law that the restrictions to fundamental rights should not affect the core of the guaranteed rights and they should be directly related to the constitutional goal that makes them acceptable.[47] In this context, in a case concerning the balancing of freedom of press with the protection of the authority of the judiciary via the criminal offence of contempt of court, the Supreme Court opted for an interpretation of article 19 of the Constitution favoring the freedom of press when declaring that "*In the light of the modern trend in interpreting and applying provisions relating to human rights, such as Article 19 of our Constitution and the corresponding article 10 of the European Convention on Human Rights, which forms part of our own Law as well, and in the light of the European Court of Human Rights judgment of "The Sunday Times case", some of which we have quoted in the present judgment, section 122 (b) of Cap. 154, which is a restriction of the right of expression, must be applied in each particular case in a manner as favourable as possible for the freedom of press*".[48] A certain preeminence of the freedom of speech has also been highlighted by the Supreme Court in the case Police v. Ekdotiki Eteria (1982) 2 C.L.R. 63,[49] where it was stressed that «*Article 19.1 proclaims the right to freedom of speech and expression in every form. This is the basic norm, establishing the paramount nature of the right signifying the commitment of the State to the fullness of the right. Limitations are the exception and authority for their introduction must be sought in the Constitution itself and from no other source*". [50]

Furthermore, it is important to note that Cypriot case law has so far been very cautious on issues of **protection of privacy and of the secrecy of communications**. On the legal grounds of articles 15 and 17 of the Constitution (protection of privacy and of the secrecy/confidentiality of communications), the Supreme Court has found illegitimate and contrary to the Constitution the use of IP address of the accused as a means of proof of an illegal activity (violation of privacy, defamation etc.).[51] While the obligation to issue a warrant in order to oblige the ISP to reveal the identity of his user is well established by the Cypriot case law, a lot of uncertainty prevails regarding the collection of the IP address itself. In a case where someone had modified a Facebook account in a defamatory way, the plaintiff had by himself collected the perpetrator's IP address through the Facebook advanced options and given it to the police. The Cypriot judge in first instance decided that the entire procedure was illegal: since the IP address is a personal datum, judicial supervision of the collection process should have occurred. This decision sought to force the police to ask for not only a warrant against the ISP for the identification of the IP's address owner (which seems logical), but also a second and earlier warrant, for the collection of the IP address itself. However, this case provoked so much confusion that the Cypriot judges in the same case on appeal recently ruled to the contrary, deciding that the IP address by itself – that is without connection to the ISP log – is not a personal datum.[52]

---

45 Handyside v UK [1979] 1 EHRR 737.

46 See: Supreme Court, Georgios Chatzinicolaou v Police (1976) 2 C.L.R. 63·

47 See inter alia: Yiorgalla v. X "Christodoulou (2000) 1 AAD 2060· Karatzia n. Papakyriacou (2001) 1 AAD 2113).

48 Cosmos Press Ltd and Another v The Police (1985) 2 CLR 73.

49 Police v. Ekdotiki Eteria (1982) 2 C.L.R. 63.

50 Alitheia Ekdotiki Etairia Ltd and others v Andrea Aloneyti, Civil appeal. No. 10703, 29 November 2002.

51 See for example: Supreme Court, Criminal appeal no. 135/2008 (http://www.cylaw.org/cgi-bin/open.pl?file=apofaseis/aad/meros_2/2011/2-201107-135-08.htm&qstring=IP) and Supreme Court, civil appeal 134/2011 (http://www.cylaw.org/cgi-bin/open.pl?file=apofaseis/aad/meros_1/2012/1-201209-134-11.htm&qstring=IP).

52 Supreme Court, Isaia, 17 July 2014, appeal number 402/2012.

3. Procedural Aspects

As a general principle, blocking, filtering and taking down of illegal Internet content shall only be ordered **by a Court**.

One **exception** to this rule is the case of the **blocking of sites offering online betting**. Indeed, according to section 65 of the Cyprus Betting Law No. 106/2012, Internet providers have an obligation to block websites that do not have the permission to provide services of online betting. The **National Betting Authority**, which is an **independent administrative body**, **provides a list with illegal websites that must be blocked by ISPs**. The Authority is obliged to notify ISPs, by electronic means, of every Uniform Resource Locator (URL) address through which betting services are offered and that are not covered by Class B licensed bookmaker or services. The Authority may impose a fine up to thirty thousand euro (€30,000) to an ISP in the case of a breach of these provisions. ISPs are not liable in respect of transmitted services of betting providers or in the case of automatic or intermediary or temporary storage of information of betting providers.[53] **The decision of the National Betting Authority** establishing the list of the websites to be blocked is **of an administrative nature** and **can be reviewed by the Supreme Court**.

In respect of the other two explicit cases where site blocking and filtering is permitted –copyright infringement and child abuse and child pornography – the decision to block/filter is normally taken **by the competent Court**.

More specifically, article 13 (5) of Law no. 59/1976 about **copyright protection** provides that right holders are in a position to apply for a **court injunction against intermediaries whose services are used by a third party to infringe a copyright or related right**.

As to child pornography and child abuse, Section 11 of Law no. 91(I)/2014 provides that the **Court in any stage of the procedure can order the prompt removal of web pages containing or disseminating child pornography**. Section 11 (2) enables the Court to order the blocking of access to web pages containing or disseminating child pornography towards Internet users who reside in Cyprus. Nonetheless, according to section 11 (3) of the Law, **ISPs offering** services or access to the Internet within the territory of the Republic of Cyprus, **are obliged, as from the moment they gain knowledge or are informed by the "competent authority" of the existence of child pornographic content** on any site, **to immediately take appropriate measures for the interruption of access** by Internet users. The law gives a **broad definition of the term "competent authority"**. Article 2 of the law states that competent department "*means the Law Office of the Republic, the Ministry of Labour, Welfare and Social Security, the Social Welfare Services and Social Security of the Ministry of Labour, Welfare and Social Security, the Ministry of Health, Mental Health Services of the Ministry of Health, Ministry of Education and Culture, the Ministry of Justice and Public Order, the Police, the Ministry of Interior, the Civil Registry and Migration and Asylum Service of the Interior Ministry, the Ministry of Foreign Affairs and consular authorities of the Republic abroad*". So, it appears that the notification to the ISPs can be made by any competent authority and **not necessarily by the judiciary**. If ISPs do not comply with this obligation, they are criminally liable and subject to a criminal offense which is punishable by imprisonment not exceeding three years or a fine not exceeding €170,000 or with both penalties. It is noteworthy that **the law does not specifically define whether ISPs can contest the notification addressed to them by the "competent authority" and the relevant procedure**. But since the non-compliance of the ISPs with the notification is a criminal offence, **ISPs can normally exercise**

[53] For the full text of the Law in English, see: http://www.nba.com.cy/eas/eas.nsf/page01_gr/page01_gr?OpenDocument.

an appeal against the court decision which condemns them on the grounds of the general provisions of criminal procedure law.

4. General Monitoring of Internet

There is no special legislation in Cyprus on general monitoring of the content of the Internet and, as a result, there is no specific entity charged with reviewing general Internet content.
Cyprus implemented Directive 2006/24/EC 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/E with the law no. 183 (I) 2007. As a result, Cypriot service providers were obliged to store information concerning the telecommunication traffic of the end users and to deliver, upon a court order or a letter of the Attorney General, such information to the police investigator in the frame of the investigation and prosecution of criminal activities. Nonetheless, the annulation of the Directive 2006/24/EC by the Court of Justice of the European Union[54] removed the legal basis of Law no. 183 (I) 2007, which is no longer applicable. This was clearly stated by the Supreme Court of Cyprus in the case *Attorney General v Isaia*[55] where it was held that it followed from the annulation of the Directive that the whole existing system of gaining access to electronic communications data by the police in order to investigate serious criminal offenses must collapse, since the latter now lacks its legal foundation.

The National Betting Authority, which creates the **list of Internet sites illegally offering betting services without a license**, has a restricted scope of intervention limited to the field of on line betting. To this end and within the limits of its mission, the **National Betting Authority may operate monitoring activities of the Internet in search for illegal content**. In any case, the blocking of sites offering betting services without a license is implemented by ISPs to which the list of the sites to be blocked is notified by the National Betting Authority.

In respect of **child pornography**, the blocking/filtering of the site is only implemented by the ISPs and not decided by them. So, in both cases, ISPs are obliged to apply such measures and they do not have any competence to themselves assess the illegality of the Internet content that is blocked or removed. Indeed, it is the competent authorities of article 11(3) Law 91(i)/2014 who may order ISPs to immediately take appropriate measures for the interruption of access by Internet users to sites containing child pornography. The law does not consider whether the competent authorities are authorized to operate monitoring activities to identify such content and if so, under what terms and safeguards. The Cypriot special police cybercrime department usually identifies such sites after notification by other national authorities or by Europol or Interpol in the frame of international cooperation. The Cypriot special police cybercrime unit[56] has a broad competence for crimes related to the Internet as described in the Cybercrime Convention which has been ratified by Cyprus with the Law no. 22(III)/2004, but also generally for any illegal Internet content. There is also a hotline that has been set for reporting illegal material on the Internet.[57]

Article 13 (5) of Law 59/1976 on the **protection of copyright** implements article 8.3 of the Information Society Directive and provides that right holders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or

---

54 CJUE, Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and others, C-293/12 και C-594/12, 8.4.2014.

55 Supreme Court, Attorney General v Isaia and others, (Civil appeal no. 402/2012), 7 July 2014.

56 See: http://www.police.gov.cy/police/police.nsf/All/ACD1089AAF7A228FC22579170025CB0B?OpenDocument (in Greek).

57 More information available at : http://www.saferinternet.org/cyprus.

related right. This provision does not presuppose or prerequisite the intermediaries' liability. The provision has not yet been applied by Cypriot courts, but it could be used in order to stop or prevent copyright infringements by various means. Normally, all appropriate remedies will be considered by courts, including information disclosure, or DNS and IP address blocking. In light of the Scarlet[58] and Netlog[59] CJEU's decisions, deep packet inspection or URL blocking should be excluded, since it is extremely intrusive to the right of privacy, data protection and secrecy of communications. It is noteworthy that in Cyprus, even if there is no specific privacy tort such as in the UK, Cypriot case law has recognized that violation of privacy is a tort on the legal grounds of article 15 of the Constitution of Cyprus.[60] Cypriot Constitution also guarantees the secrecy of communications (article 17 of the Constitution), while personal data protection is established by the law that has implemented the relevant EU Directives. So, every preventive blocking method which requires a general monitoring of the content of packets will normally be deemed to be contrary to the Constitution.

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

Since there is **no specific legal framework**, ISPs self-regulating framework and Cypriot case law on issues of blocking, filtering and take-down of Internet content, it is **not possible to assess whether the safeguards as to freedom of expression on these issues are respected in practice**.

In general, in respect of other cases of illegal online content (such as, for example, breach of personal data, defamation and incitement to terrorism) no special procedures or guidelines for the removal/take down, blocking, filtering or contestation of those acts by the presumed infringer have been established. Furthermore, there are no ISP codes of conduct regulating these situations. Although the general criminal and civil procedure law provisions apply, the **lack of specific mechanisms and procedures for dealing with those restrictive measures can be a source of uncertainty**.

In the two explicit cases where the law clearly provides for the blocking/filtering of sites containing illegal Internet content— namely sites offering **online betting services** without a license and sites containing child abuse material and **child pornography**— **the requirements of foreseeability and accessibility of the law appear to be met**.

Since ISPs do not have any competence of evaluation of the illegality of the Internet content or of the illegal character of the site, **the only possible concern could theoretically be about how the competent authorities evaluate the illegality of the content**/site that has to be blocked/take down since, in particular, no official data nor clear criteria can be found in this respect. Also, this may pose the question of legal remedies available to persons concerned by the restrictive measure.

---

58 CJEU, Scarlet Extended SA v Societe Belge des Auteurs, Compositeurs et Editeurs SCRL (SABAM), Case C-70/10, Judgment of 24 November 2011, par. 50 : "Moreover, the effects of that injunction would not be limited to the ISP concerned, as the contested filtering system may also infringe the fundamental rights of that ISP's customers, namely their right to protection of their personal data and their freedom to receive or impart information, which are rights safeguarded by Articles 8 and 11 of the Charter respectively".

59 CJEU, Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV, Case C-360/10, Judgment of 16 February 2012.

60 Article 15 provides as following: "*1.Every person has the right to respect for his private and family life. 2. There shall be no interference with the exercise of this right except such as is in accordance with the law and is necessary only in the interests of the security of the Republic or the constitutional order or the public safety or the public order or the public health or the public morals or for the protection of the rights and liberties guaranteed by this Constitution to any person*".

In the case of online betting websites, it is clear that the **sites are blocked upon an administrative decision of the National Betting Authority** only if they have not been granted a license to operate in Cyprus by that authority. It is worth noting that the competent authority in this respect, the National Betting Authority, is an independent administrative authority and that its competence is restricted to identifying online betting websites which do not have a proper license to operate in Cyprus. Moreover, as already noted, legal remedies are available to the person concerned with the restrictive measure.

The situation is less clear in the case of blocking of websites containing **child pornographic content**: while the law 91(I)/2014 (section 11 (2) (a) and (b)) sets as a prerequisite that the blocking/filtering decision is taken by a court—which shall normally respect the principles and safeguards of the European Convention on Human Rights—, Section 11 (3) enables "any competent authority" (and not necessarily a judicial authority) to ask ISPs to block access to web sites containing child pornography or child abuse material. So, **it is possible that such a demand is addressed to ISPs without a prior judicial evaluation**, **while the law does not provide any special procedure or means for the ISPs or the persons concerned by the blocking measure to contest such a notification**. Therefore, a contradiction with the safeguards as to freedom of expression is potentially possible in this context. However, it has to be noticed that the procedure appears to be formally in conformity with the text of the Directive 2011/92/EU, which does not presuppose that a prior judicial evaluation of such measures is necessary. Nonetheless, the Directive provides that "these measures must be set by transparent procedures and provide adequate safeguards, in particular to ensure that the restriction is limited to what is necessary and proportionate, and that users are informed of the reason for the restriction" and that "those safeguards shall also include the possibility of judicial redress".[61] Cypriot law does not impose such an obligation and no specific mechanisms or procedures safeguarding the proportionality and the transparency of the measures taken have been established.

Furthermore, in respect of the possibility for an injunction on the grounds of article 13 of Law no. 59/1976 on **copyright protection** and of section 32 of the Courts of Justice law 14/1960, **the order is made by the competent court** after assessment of the specific circumstances of the case. Nonetheless, it shall be noted that all the injunctions awarded by the Court on the basis of this provision concern mainly the stop of use, disclosure, exploitation of illegal or harmful content by the defendant in the frame of a civil action, while the adjudication of the main civil action is still pending. So, since **blocking/take down of illegal online content may only be carried out after the competent Cypriot courts have made an evaluation of the specific case**, the requirements for foreseeability, accessibility, clarity and precision as developed by the European Court of Human Rights are deemed to be met.

In any event, in any case the decision concerns only the blocking/filtering of specific sites (so the decision is targeted) and cannot be understood or used as a means of wholesale blocking. The significant protections afforded to the rights of freedom of expression, privacy and the secrecy of communications by the Cypriot Supreme Court could possibly counterbalance any tendency to restrict these fundamental rights.

Nicosia, 30 July 2015
Author:
Tatiana-Eleni Synodinou,
Associate Professor,
Law Department,

[61] Article 25 par. 2 of Directive of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA.