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 359-385

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.

ITALY

1. Legal Sources

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

1.1.1. Relevant International Rules in force in Italy

Italy has implemented many international instruments regulating internet websites, electronic commerce and freedom of expression on the web.

The most important are the following:

- the **European Directive** 1995/46/EU on the protection of individuals with regard to the processing of personal data and on the free movement of such data;[1]
- the **European Directive 2000/31/EC** on electronic commerce (E-Commerce-Directive);[2]
- the **European Directive** 2002/58/EU concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications);[3]
- the European 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/EC;[4]
- the **European Directive 2011/93/UE** on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA[5]
- the **CoE Convention on Cybercrime;**[6]

---

1 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. Legge del 06/10/1998 n. 344, differimento del termine per l'esercizio della delega prevista dalla legge 31 dicembre 1996, n. 676, in materia di trattamento dei dati personali. See also http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4443361 .

2 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market. Decreto Legislativo 9 aprile 2003, n. 70.

3 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 (Directive on privacy and electronic communications). Decreto legislativo 30/6/2003, n. 196-Codice in materia di protezione dei dati personali. GURI n° 174 del 29/7/2003 p. 11.

4 Even though the Directive has been declared invalid with the DRI judgment (C-293/12 e C-594/12, Digital Right Ireland and Sietlinger) the decision of the Court of Justice does not automatically determine the invalidity of the national rules on data retention by the Member States. Pursuant to art. 267 of the Treaty on the Functioning of the European Union, the jurisdiction of the Court can have direct effect only on European legislation and not on the national ones implementing it. For these reasons the DECRETO LEGISLATIVO 30 maggio 2008, n. 109, Attuazione della direttiva 2006/24/CE riguardante la conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2008-05-30;109! vig= is still in force.

5 See DECRETO LEGISLATIVO 4 marzo 2014, n. 39, Attuazione della direttiva relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, che sostituisce la decisione quadro 2004/68/GAI http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2014-03-04;39!vig= ().

- the **CoE Convention** on the Protection of Children against Sexual Exploitation and Sexual Abuse, signed in **Lanzarote**, on the 25.X.2007;[7]
- the CoE Convention for the Protection of Individuals with regard to **Automatic Processing of Personal Data**.[8]

Other international instruments have not yet completed their "*iter parlamentare*".

These are:

- the CoE **Convention on the Prevention of Terrorism**, signed in Warsaw, on 16.V.2005;[9]
- the "Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a **racist and xenophobic nature** committed through computer systems":[10] this instrument needs coordination with existent Italian bodies such as the UNAR;[11]
- the **Framework decision 2008/913/JI** on combating certain forms and expressions of **racism and xenophobia** by means of criminal law of the Council of the European Union.[12]

The majority of available measures preventing the illegal use of the internet, deal essentially with the **liability of the different types of internet service providers**[13] and users, an issue that is, in its general terms, outside of the scope of the present research.
As regards the blocking, filtering and taking down of illegal internet content, the only specific measures within the Italian legal system are aimed at promptly responding to **child abuse and exploitation** by granting certain powers to the police. These powers are derived from the Convention of Lanzarote that acknowledges that, in cases of child abuse and exploitation, timely prevention is of the essence**.** It is commonly acknowledged that a child is abused every single time that an internet user watches a video displaying the child.

---

6 LEGGE 18 marzo 2008 n.48 (in Suppl. ordinario n. 79 alla Gazz. Uff., 4 aprile, n. 80). - Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalita' informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno. See http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2008-03-18;48!vig=.

7 Legge 172 del 1 ottobre 2012 http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2012-10-01;172.

8 LEGGE 21 febbraio 1989, n. 98, Ratifica ed esecuzione della convenzione n. 108 sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale, adottata a Strasburgo il 28 gennaio 1981. (GU n.66 del 20-3-1989 - Suppl. Ordinario n. 19): http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:1989-02-21;98!vig=.

9 http://www.senato.it/service/PDF/PDFServer/BGT/00280603.pdf.

10 http://www.camera.it/_dati/leg17/lavori/stampati/pdf/17PDL0031740.pdf.

11 See www.unar.it (National Union Anti-discriminations based on Racism).

12 http://www.senato.it/service/PDF/PDFServer/BGT/00703064.pdf

13 See OCSE, The Economic and Social Role of Internet Intermediaries, 2010, 9, http://www.oecd.org/internet/ieconomy/44949023.pdf See, recently, App. Milano, sez. spec. impresa, 7 gennaio 2015, n. 29, with the comment by Deborah Bianchi, Responsabilità nell'Internet. Parametri inscindibili: hoster attivo e bilanciamento dei diritti, in *RIDARE* (http://ridare.it/articoli/giurisprudenza-commentata/responsabilit-nellinternet-parametri-inscindibili-hoster-attivo-e). The case law is abundant: Corte appello Milano Sez. spec. Impresa 07/01/2015 n. 29, Tribunale Milano sez. I 25/05/2013, Corte appello Milano sez. I 27/02/2013 n. 8611, Tribunale Firenze 25/05/2012, Tribunale Roma sez. IX 20/10/2011, Tribunale Milano 09/09/2011 n. 10893, Tribunale Roma Sez. Proprieta' Industriale e Intellettuale 11/07/2011,,Tribunale Milano 31/03/2011, Tribunale Roma 22/03/2011,,Tribunale Roma Sez. Proprieta' Industriale e Intellettuale 20/03/2011, Tribunale Roma Sez. Proprieta' Industriale e Intellettuale 14/04/2010 Tribunale Milano sez. IV 12/04/2010 n. 1972, Tribunale Firenze Sez. Proprieta' Industriale e Intellettuale 14/07/2006, Tribunale Milano sez. XI 09/03/2006, Tribunale Napoli Sez. Proprieta' Industriale e Intellettuale 30/05/2005, Tribunale Napoli 26/02/2002.

1.2. National rules allowing filtering, blocking and/or taking down of illegal internet content

The most relevant Italian rules, in order to prevent and impede **cybercrimes or the display of illegal internet content**, are the following:

- Title XII "crimes against the person", Chapter III "crimes against **individual freedom**", Section IV "crimes against the **inviolability of domicile**" of the Italian Criminal Code.[14]
- Italian Law **633/1941** (as amended by law n. **248/2000**, and most recently by Legislative Decree no. 21 February 2014, n. 22 and LD. November 10, **2014, n. 163**)[15] protecting **copyright** and other rights relating to its exercise.
- The decree on electronic commerce n. 70/2003, for copyright violations online implementing Directive 2000/31 / EC on information society services.
- The Consolidated Text (Testo Unico) on audiovisual media services, Law n. **177/2005**,[16] as amended by law no. **44/2010**,[17] regarding specifically the broadcasting services.
- Annexe A to the **Resolution AGCOM** (*Italian Authority for Media communications*) **no. 680/13/CONS of 12 December 2013** establishing the rules for the protection of copyright in electronic communications networks and procedures for the implementation of legislative decree, April 9, 2003.[18]
- Title IX of Book Five of the Civil Code on **intellectual property rights** and on **industrial inventions.**[19]
- **Art. 700 of the Italian Code of Civile Procedure. Injunctive reliefs** may be granted by the civil judge. In particular, the Article has been used to block illegal internet content in the areas of **copyright, trademark and unfair competition law**.
- Art. 2 bis, Law **895/1967**,[20] introduced by art. 8 of Law 155/2005 prohibits the training or delivery of instructions concerning **manufacturing or use of explosive materials**, and **weapons**.[21]
- Law n. **547/1993**,[22] which amended and added rules on computer crimes otherwise absent from the Criminal Code and the Code of Criminal Procedure. The law contains different kinds of

---

14 http://pluris-cedam.utetgiuridica.it/main.html#mask=main,id=05AC00011263,pos=0,ds_name=LEGGI,opera=05,hl=true,_menu=normativa,_npid=376822077,__m=bd.

15 http://www.iusexplorer.it/FontiNormative/Leggi?idDocMaster=4094130&idDataBanks=7&idUnitaDoc=27342288&nVigUnitaDoc=1&pagina=1&loadTreeView=True&NavId=1402754455&pid=19&IsCorr=False.

16 www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2005-07-31;177!vig=.

17 www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2010-03-15;44!vig=.

18 See the resolution: http://www.agcom.it/documentazione/documento?p_p_auth=fLw7zRht&p_p_id=101_INSTANCE_kidx9GUnIodu&p_p_lifecycle=0&p_p_col_id=column-1&p_p_col_count=1&_101_INSTANCE_kidx9GUnIodu_struts_action=%2Fasset_publisher%2Fview_content&_101_INSTANCE_kidx9GUnIodu_assetEntryId=771920&_101_INSTANCE_kidx9GUnIodu_type=document . It is possible to download the rules from the same webpage.

19 http://pluriscedam.utetgiuridica.it/main.html#_menu=normativa,mask=main,opera=05,_npid=377522713,__m=bd_search,__dk=0.

20 http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:1967-10-02;895!vig=.

21 "Whoever, outside the cases allowed by legal provisions of Acts or regulations, trains someone or delivers instructions in any form, also anonymously, or through electronic transmission, relating to the manufacturing or use of explosive materials, war weapons, chemical aggressors or harmful or dangerous bacteriological substances and other lethal devices shall be punished, unless the offence is a more serious one, with imprisonment from one to six years". Translation provided by the OSCE Comparative Study 2010, p. 132, note 671.

provisions on “computer crimes”: the protection against **infringements to the confidentiality of data and of communications**, data protection, information systems. In addition, it extends to electronic documents the provisions against **fraud and falsity in acts**.[23]

- Art. 143 lit. c) ff. and Art. 154, c) and d), **Law n. 196/2003**, Code on the protection of personal data (*Codice in materia di protezione dei dati personali).*[24] These contemplate, among the powers of the National Data Protection Authority that the latter may: prescribe to those entities treating data any measure considered either necessary or convenient to align the treatment of data to the provisions in force; prohibit, even *ex officio*, totally or in part, the treatment of data when illegitimate or incorrect; decide to block the treatment of data, in accordance with Art. 143. (Lgs Decree No. 196/2003, available in English, at: http://194.242.234.211/documents/10160/2012405/Data ProtectionCode-2003.pdf)
- Art. 1, par. 50 of **Law 296/2006** on "**virtual betting**", allowing the *Agenzia delle Dogane e dei Monopoli* to exert targeted actions to combat illegal practices.[25]
- Annex 2 to the **General Decree n. 1034/2007** implementing Law 296/2006 and establishing rules on the blocking and filtering of websites offering illegal betting and gambling.
- Art. 2 of the **Legislative Decree n. 7/2015** prescribing the creation of a black list of websites among the measures implementing the Convention and Protocols of the United Nations **Convention against Transnational Organized Crime**, adopted by the General Assembly on Nov. 15, 2000 and May 31, 2001. [26]

2. Legal Framework

Italy **has not enacted any specific law** on the blocking, filtering and taking down illegal internet content. There are different laws with varying legal functions and objectives that provide for such measures. These measures may be of preventive character or of a punitive nature. They may be used to stop the **commission of a crime**, to avoid the **infringement of administrative regulations** or to ensure that **rights of private persons** are respected. Accordingly, the extent of the powers of Italian authorities varies in this respect, although all these measures are taken under the preventive control of the **judiciary**, with the notable exception of **virtual betting**.

---

22 LEGGE 23 dicembre 1993, n. 547, Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica. (GU n.305 del 30-12-1993) http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:1993-12-23;547.

23 G.Cassano, Diritto nell’Internet, Cedam (ed.), pp. 513-514.

24 www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2003-06-30;196!vig= .

25 http://www.agenziadoganemonopoli.gov.it/wps/wcm/connect/Internet/ed/LAgenzia/Chi+siamo/La+missione/.

26 LEGGE 17 aprile 2015, n. 43, Conversione in legge, con modificazioni, del decreto-legge 18 febbraio 2015, n. 7, recante misure urgenti per il contrasto del terrorismo, anche di matrice internazionale, nonché proroga delle missioni internazionali delle Forze armate e di polizia, iniziative di cooperazione allo sviluppo e sostegno ai processi di ricostruzione e partecipazione alle iniziative delle Organizzazioni internazionali per il consolidamento dei processi di pace e di stabilizzazione. (15G00060) (GU n.91 del 20-4-2015). See www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2015-04-17;43!vig= for the law and www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legge:2015-02-18;7!vig= for the decree.

The present section first examines a system based on the establishment of a black-list and, second, the legal framework of take down or removal of internet content endangering or actually offending citizens' rights.

2.1. Blocking and/or filtering of illegal Internet content

2.1.1. Prevention and Prosecution of Grave Abuses on Children

Italy is a member of the **CIRCAMP Project** to fight child abuse material that acts through the **Child Sexual Abuse Anti Distribution Filter** (CSAADF) originally developed in Norway[27]. In Italy, the Filter is under the control of the **Centro nazionale per il contrasto della pedopornografia**,[28] created by art. 14-*bis* of the Law 3 August 1998, n. 269,[29] subsequently modified by law 6 February 2006, n. 38.[30]

The **operation of the Filter** is described by the Decreto 8 gennaio 2007 of the Ministero delle comunicazioni, titled "Requisiti tecnici degli strumenti di filtraggio che i fornitori di connettivita' alla rete Internet devono utilizzare, al fine di impedire, con le modalita' previste dalle leggi vigenti, l'accesso ai siti segnalati dal Centro nazionale per il contrasto alla pedopornografia".[31] These provisions respect and implement art. 25 of the Directive 2011/92/EU of the European Parliament, which prescribes that:

"1. Member States shall take **the necessary measures to ensure the prompt removal of web pages** containing or disseminating child pornography hosted in their territory and to endeavour to obtain the removal of such pages hosted outside of their territory.

2. Member States may take measures to **block access to web pages** containing or disseminating child pornography towards the Internet users within their territory. 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. Those safeguards shall also include the possibility of **judicial redress**."

A. Legal basis of the *Centro*

Law n° 38/2006[32] has modified law n. 269/1998[33] with the introduction of a series of new articles (Art. 14 *bis* to art. 14 *quinquies*). It has established the National Center for the prevention and prosecution of child pornography on the internet which has been tasked with the gathering of reports from the police, from foreign entities and public and private actors working to combat child pornography. These reports concern sites that disseminate material that uses and abuses children on network internet and other networks of communication, as well as managers and recipients of related payments.[34]

---

27 https://www.europol.europa.eu/content/joint-action-22-european-countries-against-online-child-sexual-abuse-material-internet.

28 http://www.poliziadistato.it/articolo/455Centro_nazionale_per_il_contrasto_alla_pedo_pornografia_su_Internet/.

29 http://www.camera.it/parlam/leggi/98269l.htm.

30 www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:1998-08-03;269!vig=.

31 GU n. 23 del 29 gennaio 2007. See http://www.interlex.it/testi/dm070108.htm

32 LEGGE 6 febbraio 2006, n. 38 Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet. (GU n.38 del 15-2-2006), http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2006-02-06;38!vig=

33 LEGGE 3 agosto 1998, n. 269 Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di riduzione in schiavitu'. (GU n.185 del 10-8-1998) www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:1998-08-03;269!vig=

34 "1. Presso l'organo del Ministero dell'interno di cui al comma 2 dell'articolo 14, e' istituito il Centro nazionale per il contrasto della pedopornografia sulla rete INTERNET, di seguito denominato "Centro",

In addition, it prescribes that "without prejudice to the initiatives and determinations of judicial authorities, in case of identification of a criminal website, such website, as well as the names of its operators and of the beneficiaries of the relevant payments, are included in a list, which is constantly updated".

> Art. 14 quarter: (Use of technical tools to prevent the access to sites which disseminating child pornography) "The suppliers of connectivity to the internet, in order to prevent access to sites identified by the Centre, are obliged to use the filtering tools and related technology solutions meet the requirements identified by the Minister of Communications, in consultation with the Minister for Innovation and Technology, and after hearing the most representative associations of suppliers of network connectivity internet. By the same decree it shall also state the period within which suppliers of network connectivity internet must give itself the means of filtering."

B. Functions of the *Centro nazionale per il contrasto della pedopornografia*

The fight against Child Abuse and Exploitation is based both on research and on prosecution.

As regards to **research**, the Center provides all available information to the Italian Presidency of the Council of Ministers - Department for Equal Opportunities. This information is used to produce **statistical data related to online child pornography**, to prepare a **national plan to combat the phenomenon** as well as the annual report.

As regards to **prosecution**, the Center has two main functions. The first one is to **monitor the web** and the second one is to collect **reports from private persons, public authorities, as well as by providers**. L. n. 38 of 2006 obliges both public authorities *and* internet providers to report any information on these topics to the Center. All reports are checked by the Center. Eventually, all cybercrimes against children lead the Center to take many kind of measures, including **protective measures** consisting in the blocking, filtering and taking down of internet content and the **sanctions against the author of the cybercrime** and/or the crimes against the child or the children involved.

C. The black list

Based on the information available, the Center on a daily basis compiles a black list of criminal DNS. The black list is sent to the prosecutor in charge of monitoring activities at the Center with a request to block the access to the DNS figuring in the list or more precisely to "fornitori di connettività". **ISPs** are required to redirect users trying to access black listed sites in a STOP PAGE explaining the reasons of the inaccessibility of the website. Compliance with the public authorities' orders is monitored by the police. The Center has a duty to erase from the black list the addresses of websites that do not display anymore child pornography.

> con il compito di raccogliere tutte le segnalazioni, provenienti anche dagli organi di polizia stranieri e da soggetti pubblici e privati impegnati nella lotta alla pornografia minorile, riguardanti siti che diffondono materiale concernente l'utilizzo sessuale dei minori avvalendosi della rete INTERNET e di altre reti di comunicazione, nonche' i gestori e gli eventuali beneficiari dei relativi pagamenti. Alle predette segnalazioni sono tenuti gli agenti e gli ufficiali di polizia giudiziaria. Ferme restando le iniziative e le determinazioni dell'autorita' giudiziaria, in caso di riscontro positivo il sito segnalato, nonche' i nominativi dei gestori e dei beneficiari dei relativi pagamenti, sono inseriti in un elenco costantemente aggiornato. 2. Il Centro si avvale delle risorse umane, strumentali e finanziarie esistenti. Dall'istituzione e dal funzionamento del Centro non devono derivare nuovi o maggiori oneri a carico del bilancio dello Stato. 3. Il Centro comunica alla Presidenza del Consiglio dei ministri - Dipartimento per le pari opportunita' elementi informativi e dati statistici relativi alla pedopornografia sulla rete INTERNET, al fine della predisposizione del Piano nazionale di contrasto e prevenzione della pedofilia e della relazione annuale di cui all'articolo 17, comma 1."

The black list cannot be published since it is covered by the *segreto istruttorio* - the criminal procedural principle of confidentiality of investigations - ex art. 329 c.p.p.[35] However, an example of blacklist, that includes 287 blocked websites, has been published – in violation of Italian laws on the secrecy of investigations – by the website Wikileaks.[36]

Procedural aspects are explained *infra.*

D. Collaboration with Europol and Interpol

In order to identify the authors of the cybercrime as well as the internet surfers seeking obscene images of children, **information is shared with service providers and cooperation of banks, the Italian Post Office and financial intermediaries** is also sought.

The names of operators and beneficiaries of payments related to Child Abuse and Exploitation are included in a list which is constantly updated. In addition, this information is also shared with **Europol** and **Interpol**. All this information is also covered by the *segreto istruttorio* (confidentiality of investigations) ex art. 329 c.p.p.[37]

If the illegal internet content is uploaded from a **hardware located abroad**, the website is filtered in such a way that it becomes impossible, within the Italian boundaries, to access the page. Filtering consists of **redirecting the internet surfer seeking the criminal image to a stop-page**. If the illegal internet content is uploaded from a **hardware located within the Italian boundaries**, the hardware is confiscated and the images are immediately taken down and destroyed.

E. Other entities working with the Center

The Center is assisted by an entity called U.A.C.I. (**Unit of Analysis of Computer Crime**), created in order to **assist police officers in the investigation** of high-tech crimes. The UACI designs new investigation techniques and provides the Center with the necessary **backup required by the monitoring** of the repugnant obscene material uploaded on the web. UACI's **psychologists** and criminologists of the State Police, in addition, trace the **psychological profiles, compulsions and behaviours** of the authors of these kind of crimes and of "consumers", in collaboration with universities, companies and research institutions.[38]

F. Targets of the Center

The General Legal Framework for fighting Child abuses addresses the speed and transnationality of the internet.

---

35 The Italian Criminal Code at art. 329 prescribes: "1. Gli atti di indagine compiuti dal pubblico ministero e dalla polizia giudiziaria sono coperti dal segreto fino a quando l'imputato non ne possa avere conoscenza e, comunque, non oltre la chiusura delle indagini preliminari. 2. Quando è necessario per la prosecuzione delle indagini, il pubblico ministero può, in deroga a quanto previsto dall'articolo 114, consentire, con decreto motivato, la pubblicazione di singoli atti o di parti di essi. In tal caso, gli atti pubblicati sono depositati presso la segreteria del pubblico ministero. 3. Anche quando gli atti non sono più coperti dal segreto a norma del comma 1, il pubblico ministero, in caso di necessità per la prosecuzione delle indagini, può disporre con decreto motivato: a) l'obbligo del segreto per singoli atti, quando l'imputato lo consente o quando la conoscenza dell'atto può ostacolare le indagini riguardanti altre persone; b) il divieto di pubblicare il contenuto di singoli atti o notizie specifiche relative a determinate operazioni".

36 https://wikileaks.org/wiki/Italian_secret_internet_censorship_list,_287_site_subset,_21_Jun_2009.

37 See footnote 33.

38 See Chiesa R. Ciappi S. Ducci S. Hackers profiling Project La scienza del Criminal profiling Applicata al mondo del Hacking di N. Bressan.

In Italy, the Criminal Code criminalizes in art. 528 the display and publication of **obscene material**, whether resulting from writings, drawings, images, or other obscene objects.[39] As a consequence, it criminalises the diffusion of such material on the internet.

Virtual images are also criminalized under the Italian Criminal Code.[40] Virtual images are those images produced using a graphic software and do not involve the exploitation of real children. However, the quality of the images makes them appear real and their criminalization aims at **preventing any possible risk of emulation**, in order to prevent possible victimizations of children.

According to art. 15 of Law no. **47/1948**: [41] "The provisions of art. 528 of the Criminal Code also apply in the case of publication of events that have really happened or even of only imaginary events, whenever these disturb the common sense of morality or the family order or whenever they may cause the spread of suicides or murders."

Under these provisions, the "public" distribution of pornographic images on the Internet is allowed provided that two conditions are respected: i*)* minors (under eighteen years of age) shall not be involved and ii*)* access to the website is conscious and voluntary.

In sum, pornographic images may only be displayed by sites that are clearly identifiable by third persons as sites that diffuse pornographic images and that do not provide images of children under 18 years.

---

39 Criminal Code section 528: "Chiunque, allo scopo di farne commercio o distribuzione ovvero di esporli pubblicamente, fabbrica, introduce nel territorio dello Stato, acquista, detiene, esporta, ovvero mette in circolazione scritti, disegni, immagini od altri oggetti osceni di qualsiasi specie, è punito con la reclusione da tre mesi a tre anni e con la multa non inferiore a lire duecentomila. Alla stessa pena soggiace chi fa commercio, anche se clandestino, degli oggetti indicati nella disposizione precedente, ovvero li distribuisce o espone pubblicamente. Tale pena si applica inoltre a chi: 1. adopera qualsiasi mezzo di pubblicità atto a favorire la circolazione o il commercio degli oggetti indicati nella prima parte di questo articolo; 2. dà pubblici spettacoli teatrali o cinematografici, ovvero audizioni o recitazioni pubbliche, che abbiano carattere di oscenità. Nel caso preveduto dal n. 2 la pena è aumentata se il fatto è commesso nonostante il divieto dell'Autorità." See also the deontological code of journalists stating: "(Il giornalista) non deve inoltre pubblicare immagini o fotografie particolarmente raccapriccianti di soggetti coinvolti in fatti di cronaca, o comunque lesive della dignità della persona; né deve soffermarsi sui dettagli di violenza o di brutalità, a meno che non prevalgano preminenti motivi di interesse sociale.
Carta dei doveri del giornalista (CNOG e FNSI 8 luglio 1993)", http://www.odg.it/content/carta-dei-doveri-del-giornalista.

40 Criminal Code sections 600bis (Juvenile prostitution), 600ter (Juvenile pornography), 600quater (possession of pornographic material), 600quinquies (Tourism initiatives aimed at juvenile prostitution exploitation), and 600septies (Aggravating and mitigating circumstances). The latter was introduced in sections 2, 3, 4, 5, 6 and 7 of Act 269/98 to punish exploitation through the Internet. Note that Section 600quater in subsection 1 envisages virtual pedophilia and provides a definition of it and also Section 600ter punishes virtual images.

41 Art. 15 Law 47/1948: "Le disposizioni dell'art. 528 del Codice penale si applicano anche nel caso di stampati i quali descrivano o illustrino, con particolari impressionanti o raccapriccianti, avvenimenti realmente verificatisi o anche soltanto immaginari, in modo da poter turbare il comune sentimento della morale o l'ordine familiare o da poter provocare il diffondersi di suicidi o delitti", http://www.iusexplorer.it/FontiNormative/Leggi?IdDatabanks=7&IdUnitaDoc=6206705&IdDocMaster=2045273&NVigUnitaDoc=1&num=15&tipo=ART&NavId=2034084568&pid=19&IsCorr=False.

2.1.2. Prevention and Prosecution of Terrorism

New rules aimed at counteracting terrorism in line with the Convention and Protocols of the United Nations **Convention against Transnational Organized Crime**, adopted by the General Assembly on Nov. 15, 2000 and May 31, 2001 have been enacted through **Legislative Decree n. 7 of 2015 and Law n. 43 of 2015** validating the Decree.[42]

Art. 15 of a previous Decree of 27 July 2005, no. 144, ratified with amendments by Law 31 July 2005, n. 155, had introduced the following article to the Italian Criminal Code:

> Art. 270 *sexies*: "Are considered to be related to terrorism those conducts that, by their nature or context, may seriously damage a country or an international organization and are carried out in order to intimidate a population or compel a government or an international organization to perform or refrain from performing any act or in order to destabilize or destroy the fundamental political, constitutional, economic and social structures of a country or an international organization, as well as other activities characterized as terrorism or as actions with terrorist objectives by international conventions or other international law rules to the respect of which Italy is bound."[43]

Internet is a very potent medium that that can be used to reach a growing number of potential fighters - as shown by the recent investigations into the phenomenon of so-called "Lone wolves" (*lupi solitari*). Thus online tools were developed to combat the use of computer networks to incite and proselytize terrorism. The penalty of imprisonment for the offense of instigation of terrorism is thus increased whenever the internet is used as a medium (Articles 302 and 414, fourth paragraph, of the Criminal Code), given the unique danger involved.

The same law introduced measures to combat the activities of the so called "**foreign fighters**", terrorists using the internet for proselytizing purposes. In this case too, the punishment is increased when acts of incitement and justification of terrorism or terrorism itself are committed through the web. New procedural rules have been introduced to ease the investigation of terrorism related crimes committed with the use of technology or telecommunications. These rules address the acquisition of documents and computer data held abroad, including those not available to the public.

In this respect, the 2015 Decree introduces measures very similar to those of articles 14 *ter* and 14 *quater* of the law 3 August 1998, n. 269, introduced by Article 19 of the Law on Feb. 6, 2006,[44] n. 38, in light of the positive experience as regards to combating child pornography on the web:

> "For the purposes of conducting the activities [of prosecution of terrorism] carried out by police officers therein, and the prevention and suppression of terrorist activities or facilitation of terrorism, […], the organ of the Ministry of the Interior for the safety and regularity of telecommunications services, subject to the actions and decisions of the court, **constantly updates a list of sites** used for the activities and conduct referred to in Articles 270-bis and 270-e of the Criminal Code, […]. The Minister reports on the measures taken pursuant to this paragraph and paragraphs 3 and 4 of this article in a special section of the annual report referred to in Article 113 of the Law of 1 April 1981, n. 121.

---

42 See supra at para 2 for quotes.

43 "Sono considerate con finalità di terrorismo le condotte che, per la loro natura o contesto, possono arrecare grave danno ad un Paese o ad un'organizzazione internazionale e sono compiute allo scopo di intimidire la popolazione o costringere i poteri pubblici o un'organizzazione internazionale a compiere o astenersi dal compiere un qualsiasi atto o destabilizzare o distruggere le strutture politiche fondamentali, costituzionali, economiche e sociali di un Paese o di un'organizzazione internazionale, nonché le altre condotte definite terroristiche o commesse con finalità di terrorismo da convenzioni o altre norme di diritto internazionale vincolanti per l'Italia."

44 See supra at para 2.1.

3. The suppliers of connectivity, on request of the judicial authority, preferably made through an order of the judicial police under paragraph 2 of Article 7-bis of the Decree-Law of 27 July 2005, no. 144, ratified with amendments by Law 31 July 2005, n. 155, inhibit access to the sites included in the list referred to in paragraph 2, in the manner, timing and the technical solutions identified and defined by the decree provided for in Article 14-quater, paragraph 1 of Law August 3, 1998 , n. 269.

4. In proceedings for offenses under Articles 270-bis [Associations for purposes of terrorism, including international terrorism or subversion of the democratic order], 270-ter [Assistance to such kind of association], 270-c [Recruitment for the purposes of terrorism, including international terrorism] and 270-d [Training for the purposes of terrorism, including international] of the Criminal Code committed with the purpose of terrorism in Article 270-sexies of the Criminal Code, and there are concrete elements making it possible to believe that some of these activities over the Internet, the public order ministry, by reasoned decree, preferably by means of the judicial police under paragraph 2 of Article 7-bis of the Decree-Law of 27 July 2005 n. 144, ratified with amendments by Law 31 July 2005, n. 155, service providers referred to in Article 16 of Legislative Decree 9 April 2003, n. 70, or to persons still providing input and management, through which the content relating to the same activities is made accessible to the public, to provide for the removal. In the case of user-generated content and hosted on platforms due to third parties, will the removal of only the specific illegal content. The recipients fulfill the order immediately and no later than forty-eight hours of receipt of the notification. In case of default, you have the prohibition of access to the Internet domain in the forms and in the manner provided for in Article 321 of the Criminal Procedure Code, while ensuring, where technically possible, the use of content unrelated to misconduct.[45]

---

[45] See art. 2, para. 3 ff. of the DECRETO-LEGGE 18 febbraio 2015 n. 7 (in Gazz. Uff., 19 febbraio 2015, n. 41). - Decreto convertito, con modificazioni, dalla Legge 17 aprile 2015, n. 43. - Misure urgenti per il contrasto del terrorismo, anche di matrice internazionale, nonché' proroga delle missioni internazionali delle Forze armate e di polizia, iniziative di cooperazione allo sviluppo e sostegno ai processi di ricostruzione e partecipazione alle iniziative delle Organizzazioni *internazionali* per il consolidamento dei processi di pace e di stabilizzazione: "2. Ai fini dello svolgimento delle attività di cui all'articolo 9, commi 1, lettera b), e 2, della legge 16 marzo 2006, n. 146, svolte dagli ufficiali di polizia giudiziaria ivi indicati, nonché' delle attività di prevenzione e repressione delle attività terroristiche o di agevolazione del terrorismo, di cui all'articolo 7-bis, comma 2, del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155, l'organo del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione, fatte salve le iniziative e le determinazioni dell'autorità giudiziaria, aggiorna costantemente un elenco di siti utilizzati per le attività e le condotte di cui agli articoli 270-bis e 270-sexies del codice penale, nel quale confluiscono le segnalazioni effettuate dagli organi di polizia giudiziaria richiamati dal medesimo comma 2 dell'articolo 7-bis del decreto-legge n. 144 del 2005, convertito, con modificazioni, dalla legge n. 155 del 2005. Il Ministro dell'interno riferisce sui provvedimenti adottati ai sensi del presente comma e dei commi 3 e 4 del presente articolo in un'apposita sezione della relazione annuale di cui all'articolo 113 della legge 1° aprile 1981, n. 121 (5). 3. I fornitori di connettività, su richiesta dell'autorità giudiziaria procedente, preferibilmente effettuata per il tramite degli organi di polizia giudiziaria di cui al comma 2 dell'articolo 7-bis del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155, inibiscono l'accesso ai siti inseriti nell'elenco di cui al comma 2, secondo le modalità, i tempi e le soluzioni tecniche individuate e definite con il decreto previsto dall'articolo 14-quater, comma 1, della legge 3 agosto 1998, n. 269. 4. Quando si procede per i delitti di cui agli articoli 270-bis, 270-ter, 270-quater e 270-quinquies del codice penale commessi con le finalità di terrorismo di cui all'articolo 270-sexies del codice penale, e sussistono concreti elementi che consentano di ritenere che alcuno compia dette attività per via telematica, il pubblico ministero ordina, con decreto motivato, preferibilmente per il tramite degli organi di polizia giudiziaria di cui al comma 2 dell'articolo 7-bis del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155, ai fornitori di servizi di cui all'articolo 16 del decreto legislativo 9 aprile 2003, n. 70, ovvero ai soggetti che comunque forniscono servizi di immissione e gestione, attraverso i quali il contenuto relativo alle medesime attività è reso accessibile al pubblico, di

2.1.3. Prevention of illegal gambling and ludomania (gambling addiction)

In Italy, gambling is allowed only via licence granted by the Autonomous Administration of State Monopolies (AAMS). This license is required for online gambling as well and internet service providers may be asked to block access to non-licensed online gambling sites.[46]

The drafting of the blacklist was first decided in Article 1 of the 2006 Budget Law, with the aim to combat online fraud related to gambling. Recently, through the Decree Balduzzi (dl 158/2012 converted into Law 189/2012), the AAMS created an official "Observatory designed to assess the most effective measures to fight the spread of pathological gambling and the phenomenon of addiction".

The Italian model has been followed by numerous other European countries.

The first black-list was published on Friday, 24 February 2006, and led to the blocking of more than 500 sites. The decision to put together a black list of illegal gambling sites was aimed at combating "increasing instances of illegality related to the distribution of online games with cash prizes." With a Decree of 7 February 2006, the measure was implemented.

In substance, the Decree aims at removing gambling sites operating "without the concession, authorization or other proof of authorization or qualifying or otherwise in violation of laws or regulations or limits or requirements defined by AAMS, performing in Italy the collection of games reserved to the State, through the Internet or other electronic networks or telecommunications."

In practice, the AAMS creates a black list, which is publicly available, that orders ISPs to redirect users trying to reach the non-authorised operators to a STOP PAGE.[47]

---

provvedere alla rimozione dello stesso. In caso di contenuti generati dagli utenti e ospitati su piattaforme riconducibili a soggetti terzi, è disposta la rimozione dei soli specifici contenuti illeciti. I destinatari adempiono all'ordine immediatamente e comunque non oltre quarantotto ore dal ricevimento della notifica. In caso di mancato adempimento, si dispone l'interdizione dell'accesso al dominio internet nelle forme e con le modalità di cui all'articolo 321 del codice di procedura penale, garantendo comunque, ove tecnicamente possibile, la fruizione dei contenuti estranei alle condotte illecite (7).

46 This black-list is publicly accessible and is constantly updated. See https://www1.agenziadoganemonopoli.gov.it/files_siti_inibiti/elenco_siti_inibiti.txt.

47 The STOP PAGE provides users with the following information (translation by the reporter):
WARNING - SITE CANNOT BE REACHED - Under Decree of the Autonomous Administration of State Monopolies (AAMS) of 2 January 2007, governing the removal of websites offering games, lotteries, betting or pools with cash prizes without the prescribed authorisations, in order to implement art. 1, paragraph 50, of the Law of 27 December 2006 n. 296, the requested site is not accessible because it lacks the necessary permissions to operate in Italy. The list of authorized operators of electronic games is available on the corporate website www.agenziadoganemonopoli.gov.it.

2.2. The take down order of internet content offending citizen's rights

2.2.1. Copyright violations

In order to react to the so called "digital piracy", the illegal consumption of content protected by copyright, many kinds of online law-enforcement solutions have been discussed. These solutions involve internet intermediaries as providers.[48]

In a recent case, an Italian broadcasting company had asked *Yahoo!*, in addition to the removal of TV programs displayed in breach of her copyright (through file-sharing in Yahoo's 2.0 platform), to implement an **automatic filtering system**. The Milanese judges, however, considered the measure of "automatic filtering" a **disproportionate sacrifice to the provider** as well as a **violation of the right to information and freedom of expression** of users and the Data Protection (importance of IP and identity of netizens).[49]

According to the judiciary, in cases of violation of any personal rights online (copyright, publication of confidential data etc.) the request to the judge should always be detailed and **may not consist of asking for an automatic filtering of contents**.

Both the URLs of pages that contain the content causing damage needs to be made explicit as well as the remedy foreseen.
In case of a breach of copyright, the remedy shall consist of the removal of an URL in order to **disable any possible access** to all channels controlled by the provider diffusing the illegal content.
The **legal basis for the take down process** is provided by the national regulatory framework for electronic commerce, in conformity with the European Union regulatory framework.[50]

According to such rules, no system of monitoring and filtering *ex ante* internet content is legal, since it would adversely affect the role of the Internet as a free space for communication and information system.

In particular, a decision adopted on February 28, 2008 by the national Authority and known as **"Peppermint" case**[51] stipulates the illegitimacy of data treatment consisting in a systematic monitoring of the web, with the purpose of identifying web users exchanging music or games protected by copyright on the internet. The same decision clearly inhibits any private companies' treatment of such personal data and orders to the two companies involved to delete the existing ones.

This rule ensures that the principle of freedom of expression and movement of services that the European directive on electronic commerce seeks to protect is upheld.[52]

Copyright violations through the internet are punished under the **general rules of liability** in force in Italy (art. 2043 of the Italian civil code) and through the **general procedural instruments** available in Italy.[53]

---

48 See Bertoni, Montagnani, Il ruolo degli intermediari Internet tra tutela del diritto d'autore e valorizzazione della creatività in rete, in XL Giur. Comm., 2013, 537 ss.

49 App. Milano, sez. spec. impresa, 7 gennaio 2015, n. 29.

50 Art. 16 and 17 of the decree on electronic commerce n. 70/2003, for copyright violations online implementing Directive 2000/31 / EC on information society services. A translation of the latter is given *infra* at par. 3.2.1.

51 http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1495246.

52 Arts 1 and 3 Directive 2000/31 / EC on information society services.

2.2.2. Internet content of defamatory character or in breach of confidential data

In the field of **infringement of confidential data** or **defamation,**[54] **the leading case is the case** *Google Vivi down*: judgment **no. 1972/2010 of the Fourth Criminal Chamber of the Milan** of 24 February to 12 April 2010. This was a case regarding **cyber-bullying.** It started after a video had been uploaded on a Google site showing a young boy suffering from Down syndrome being roughed up and insulted by some peers. In this case, the Milan court sentenced three leaders of the popular search engine, with headquarters in Mountain View, Silicon Valley, to six months of imprisonment on grounds of the unlawful processing of personal data relating to the health of the boy(under Article. 167 d.lg. n. 196 of 2003). On that occasion, the Court of Milan established a distinction between **content providers and service providers. Liability of *Google* managers arose from the** lack of **communication** regarding the legal obligations of the uploader and the goal to make economic profits through the displaying of videos uploaded on its platform.[55]

The Court of Appeal of Milan subsequently acquitted those managers stating that the provider that offers uploading services benefits from the limitations of liability provided for in Articles. 16 and 17 of Legislative Decree no. 70/2003.

The attorney general's appeal to the Supreme Court was based, *inter alia*, on the circumstance that *Google* was not merely offering space for uploading video, but was actually performing activities of indexing and cataloguing of the material loaded (as an "active" host provider, a figure that, according to the prosecution, did not fall in the scope of Article. 16). The Supreme Court, however, rejected any accusation because it would **not be realistic to impose upon *Google* a duty to monitor** whatever content was posted by users in accordance with Art. 17 of Legislative Decree 70/2003. In addition, the Supreme Court observed that *Google* was not aware of the offense and collaborated with the competent authorities by immediately removing the video from its platform.[56]

---

53 See point 54 ff. of App. Milano, sez. spec. impresa, 7 gennaio 2015, n. 29

54 Defamation is still a crime in Italy, however, a bill is going to be approved in order to decriminalise defamation through the press, as requested by the Council of Europe (most recently in December 2013, after the decision Belpietro v. Italy, C . Edu September 24, 2013, Appl. no. 43612/10). The bill will provide the abolition of imprisonment for libel (see Montanari in www.penalecontemporaneo of 28 October 2013 on the first version of the bill).

55 See, for example Cass., sez. II, sent. n. 36721 (21.2.2008 - ud. 21.2.2008), B.M.I. (rv. 242085); Cass., sez. V, sent. n. 4741 27.12.2000 (cc. 17.11.2000), (rv 217745). Picotti, I diritti fondamentali nell'uso ed abuso dei social network. Aspetti penali, Giurisprudenza di Merito,,2012, 2522; Corrias Lucente, Ma i network providers, i service providers e gli access providers rispondono degli illeciti penali commessi da un altro soggetto mediante l'uso degli spazi che gestiscono?, Giurisprudenza di Merito, 2004, 2526; Lotierzo, Il caso Google-Vivi Down quale emblema del difficile rapporto degli internet providers con il codice della privacy, in Cass. pen., 2010, 1288 ss.; Manna, I soggetti in posizione di garanzia, in Dir. inf., 2010, 779 ss.; Ingrassia, Il ruolo dell' internet service provider nel ciberspazio: cittadino, controllore o tutore dell'ordine? Risposte attuali e scenari futuribili di una responsabilità penale dei provider, in www.penalecontemporaneo.it, Ingrassia, La Corte d'Appello assolve i manager di Google anche dall'accusa di illecito trattamento dei dati personali, in www.penalecontemporaneo.it .

56 Cass. pen., Sez. III, 17 dicembre 2013 (dep. 3 febbraio 2014), n. 5107, Pres. Mannino, Rel. Andronio. See http://www.penalecontemporaneo.it/area/3-/19-/-/2817-la_sentenza_della_cassazione_sul_caso_google/#sdfootnote1sym (28.10.2015).

2.2.3. Blocking and filtering websites on grounds of unfair competition

Unfair competition is prohibited and punished in Italy, *inter alia*, by art. 2598 n. 3 of the Italian civil code. This article served as the basis for an injunction by Italian judges to several "Uber" companies,[57] ordering them to stop provision of their services in violation of Italian unfair competition rules: *uber* drivers had the opportunity to avoid certain costs related to taxi services and consequently could offer such services at prices significantly lower than the rates charged by operators of the public service.[58]

Despite the injunction, **the company had continued to operate**. A request for a relief was then made by the plaintiffs of the first proceeding, on the basis of art. 700 of the Italian civil procedure code – an article serving as a legal basis for protective measures of various content[59] – and led the judges to order the blocking of the web application.

A subsequent request by the American company to suspend the blocking of the application 'Uber-pop' was rejected by the Tribunale of Milan.[60]

In its decision the judge also decided that "the **publication of the operative part of this measure for thirty days on the home page of the site www.uber.com** in its section on Italian territory in a legible signature and direct (no need to return the form of additional links) within fifteen days from the notification of the present order at the expenses of the respondents".

The Italian Ministro dell'interno subsequently asked the Italian authority regulating competition and the market (Autorità garante per la concorrenza e per il mercato, AGCM) to deliver an opinion on this matter. The opinion was released in September 29 and published on the website of the AGCM in November 2nd.[61] In his opinion, the President of AGCM, Giovanni Pitruzzella, stresses that it is necessary to draw the "right balance between **the competitive advantages arising from the development of this type of digital platforms** (and protection of public interest related to them) and the **protection of individual categories of workers**, following an interpretation of the rules respectful of the constitutional principle recognising the **freedom of private economic initiatives** - referred to in Article 41 of the Constitution". In addition, the AGCM President argued that Italian laws regulating taxi services (in particular law n. 21/92), because of their date, should not be applied to "services which connect professional drivers on the one hand and **demand for mobility** on the other".

In this respect, the Authority invites both the Italian Parliament and Italian judges to take action: the first to review the laws on taxi services, the seconds to read the obsolete rules on taxi services with a

---

57 UBER INTERNATIONAL B.V., UBER INTERNATIONAL HOLDING B.V., UBER B.V., RAISER OPERATIONS B.V., UBER ITALY s.r.l. and a private person.

58 The request for an art. 700 injunction was presented jointly by TAXIBLU s.e. - Taxiblu Consorzio Radiotaxi Satellitare soc. coop., SOCIETÀ COOPERATIVA PRONTO TAXI s.e. a r.l., COOPERATIVA RADIO TAXI TORINO s.e., COOPERATIVA RADIOTAXI GENOVA s.e., ITALTAXI SERVICE s.r.l.), ASSOCIAZIONE SINDACALE S.A.T.M./C.N.A. - Sindacato Artigiano Taxisti di Milano e provincia, ASSOCIAZIONE UNICA MILANO E LOMBARDIA, T.A.M. - Tassisti Artigiani Milanesi, UNIONE ARTIGIANI DELLA PROVINCIA DI MILANO, FEDERAZIONE NAZIONALE UGL TAXI, ASSOCIAZIONE TUTELA LEGALE TAXI and other persons.

59 See *infra* at 3.3.3.

60 Tribunale Sez. spec. Impresa Milano, 25/05/2015. See Ridare NEWS - Vincono le società radio taxi – il Tribunale di Milano, con provvedimento d'urgenza, inibisce l'utilizzo di "Uber pop".

61 http://www.google.ch/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CB0QFjAAahUKEwiux9aij5rJAhXEPBQKHZiyDFQ&url=http%3A%2F%2Fwww.agcm.it%2Fsegnalazioni%2Fsegnalazioni-e-pareri%2Fdownload%2FC12563290035806C%2F3CC2F83F8C3AD6C4C1257EDD0048E769.html%3Fa%3DAS1222.pdf&usg=AFQjCNHZ73d24PKELd-jHwP-zWXWK4K5og.

view to adapt these to the new realities created by the services named **UberBlack**, **UberVan (both still functioning in Italy) but also UberPop (blocked).**

2.2.4. Deindexisation as a means of implementing the right to be forgotten

A "right to erasure" will be included in the future **EU Regulation on data protection** (Art. 17 of the existing draft)[62]. The origin of the article, in its present state, lie in the position of **Art. 29 Group** and, in particular, in its "**Guidelines** on the implementation of the Court of Justice of the European Union's judgment Google Spain and inc. v. Agencia EspaÑola de protección de datos (AEPD) and Mario Costeja González C-131/12",[63] adopted on 26 November 2014.[64]

At the domestic level, the **National Authority on Data Protection** has decided several cases, following specific requests from citizens, and ordered to delete news resulting from a web research considered harmful. Rather obviously, these decisions are all taken on the basis of a case-by-case analysis, with the aim of identifying and balancing, *case by case*, the freedom of the press[65] with the right to the protection of private data.[66]

As regards to the right to be forgotten, instead of taking down the internet content, the remedy typically consists of **deindexisation** of the URL by the search engine: "*IL GARANTE: prescrive, ai sensi degli articoli 143, comma 1, lett. b) e 154, comma 1, lett. c) a Google Inc., con sede in Mountain View, USA, di cancellare dal risultato dei motori di ricerca la seguente url http://....* ".[67]

3. Procedural Aspects

As any other medium, the world wide web is monitored in a limited manner, solely for **determinate purposes** and to the extent that may be necessary to respect public order in a democratic society as well as individual rights of citizens.

The nature of rights deserving protection by way of limiting access to the internet **influences the procedural means for enacting and enabling such protection**. Thus, the procedures for such limitation vary based on the gravity and seriousness of the threat to individual rights of citizens.

---

62 http://www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-inofficial-consolidated-LIBE.pdf

63 See ECJ Costeja, 13 May 2014 and ECJ, Vuitton/Google, 23 March 2010. http://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX%3A62012CJ0131.

64 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf

65 Seven out of nine decisions did not recognise the right of the persons involved "to be forgotten". See doc. web nn. 3623819, 3623851, 3623897, 3623919, 3623954, 3624003 and 3624021.

66 In two cases: n. 501 of 6th November 2014 - http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3623877 - and n. 581 of 11th December 2014 - http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3623978 the Authority ordered deindexisation.

67 *Ibidem*.

3.1. Administrative orders to ISPs to redirect users from black listed DNS to STOP pages

3.1.1. Procedural Aspects of the Black List aimed at counteracting crimes against minors

In conformity with the **CIRCAMP Project** to fight child abuse material and art. 25 of the Directive 2011/92/EU of the European Parliament, Italy implements the **Child Sexual Abuse Anti Distribution Filter** (CSAADF) originally developed in Norway.[68]

As previously observed, the Filter is under the control of the **Centro nazionale per il contrasto della pedopornografia** and its operation is based on the daily update of a black list: the internet surfer browsing websites displaying obscene images of children abuses and exploitation is redirected to a stop page.

The Decreto 8 gennaio 2007 of the Ministero delle comunicazioni, titled "*Requisiti tecnici degli strumenti di filtraggio che i fornitori di connettivita' alla rete Internet devono utilizzare, al fine di impedire, con le modalita' previste dalle leggi vigenti, l'accesso ai siti segnalati dal Centro nazionale per il contrasto alla pedopornografia*" contains the technical requirement allowing the operation of the filter.[69]

The *Centro* may report to the judiciary, make inquiries on its own but under the control of the judiciary, order the seizure or filtering of websites etc. All these activities are carried out under the control of the judiciary and reported to the headquarters of Interpol.

The technical instrument used for filtering from Italy is the **notification of the order to filter a website given to a supplier of connectivity** (fornitore di connettività, as stated by the decree quoted above).[70]

There are about 90 suppliers in Italy: these suppliers are identified by the Minister of Communication. The Minister equips the suppliers with a "web client certificate". The certificate allows them access to the blacklist.

Every day the black list is updated and every day the filters are adjusted.

From a technical point of view, blocking of content is done through DNS servers.

According to *Wikileaks*: "when request for blocked site is made, user is redirected to IP 212.48.170.80 instead of original address. Two name servers involved in the blocking are 212.48.160.5 and 212.48.160.6".[71] Please note however, this information has not been verified.[72]

---

68 https://www.europol.europa.eu/content/joint-action-22-european-countries-against-online-child-sexual-abuse-material-internet.

69 GU n. 23 del 29 gennaio 2007. See http://www.interlex.it/testi/dm070108.htm.

70 *Ibidem.*

71 http://wikileaks.org/wiki/Italian_secret_internet_censorship_list%2C_287_site_subset%2C_21_Jun_2009.

72 According to *Wikileaks* it is easy to access the list : « The list can be reproduced by using the Unix "dig" utility, using a command such as "dig @212.48.160.6 -f list +noall +answer" where "list" is a file containing list of domains to be checked (one per line). We then search for results which lead to IP 212.48.170.80, the site which displays the "censorship page". This is a universal method, which can be applied to all DNS based blocking systems."

Wikileaks has published one of the blacklists created by the *Centro* and has made it publicly available.[73]

According to *Wikileaks* "The majority of sites on the Italian list seem to be unrelated to child pornography. While some do appear to relate to the images of teenagers, the vast majority of sites are related to what appears to be legal young-adult pornography. Some sites are unrelated to any type of pornography."

The *Centro* has a duty to verify the persistent existence of the illegal content and, if it determines that the website is now publishing legal content, it has a duty to erase the address from the list.

3.1.2. Procedural Aspects of the Black List aimed at counteracting Terrorism

This list will probably function in a very similar manner to the black list established to counteract child-pornography. Similar to the child pornography black list, this list too is kept confidential for investigation purposes. It is likely that this list will be the **responsibility of the Italian intelligence**.[74]

3.1.3. Procedural Aspects of the Black List aimed at counteracting illegal gambling

The procedure necessary to obtain the black list of websites offering illegal gambling in Italy is very different, despite the existence of certain similarities. The competent administrative body (AAMS) monitors the internet autonomously and receives indications from the police (in particular the Italian "Guardia di finanza"[75]), from her technologic partner (SOGEI[76]) and from any interested stakeholder (citizens). Whistleblowing is done through a dedicated e-mail address.[77]

The administrative body processes the information acquired, in particular considering if the website is, in fact, offering gambling without the prescribed authorisations and establishes, roughly on a monthly basis, a black list. However, different from the blacklists of child pornography and terrorism, the illegal gambling black list is published and publicly available.[78]

In addition to the publication of the black list, AAMS issued an **administrative decree to the 19 Italian major ISPs** – identified by the Italian Ministry of Economic Development – **containing the order to redirect users trying to access those website to their Stop page**.[79]

Non-compliance by the ISPs of the administrative order is punished through the ordinary administrative rules provided for by Law 689/1981.

This procedure is governed by the **General Decree n. 1034/2007** implementing Law 296/2006 and establishing rules on the blocking and filtering of websites offering illegal betting and gambling.

---

73 *Supra* note 28.

74 See http://www.sicurezzanazionale.gov.it/sisr.nsf/chi-siamo/organizzazione/aise.html and http://www.sicurezzanazionale.gov.it/sisr.nsf/tag/cyber.html.

75 http://www.gdf.gov.it The Guardia di Finanza is responsible, in particular, for cybercrime, fraud, and trafficking.

76 http://www.sogei.it.

77 Monopoli.segnalazionesiti@aams.it.

78 https://www1.agenziadoganemonopoli.gov.it/siti_inibiti.htm The last black list, published on October 2nd, contains 5525 illegal websites.

79 See supra footnote 45.

3.2. Administrative *ad hoc* orders to ISPs to take down illegal internet content on grounds of copyright violations, defamation or the right to be forgotten

3.2.1. Description of the administrative procedure and of the liability regime of internet services providers

The administrative procedure is described in art. 5, [80] 14 par. 3, 16 par. 3[81] and 17[82] of the legislative Decree n. 70/2003. These rules are clear in establishing the liability regime of Internet intermediaries, as acknowledged by the most recent case law.[83] These rules establish an **absence of any obligation of the hosting provider** to verify ***ex ante*** through a screening, the non-violation of copyrights by individuals who upload videos in its platforms. Liability of ISPs arise when it can be proven that the hosting provider had been informed of the illegal character of the content of videos uploaded by its users and has not ***ex post*** removed such illegal content from its portal – either voluntarily or under an **explicit administrative or judicial order**.[84]

---

80 A translation of art. 5 would read as follows: ""1. The free movement of a given information society service **from another Member State may be limited, by decision of the judicial or administrative bodies or supervisory authorities independent of the involved sector**, for reasons of: a) public order, for the prevention, investigation, detection and prosecution of crime, in particular the protection of minors and the fight against incitement to racial hatred, sex, religion or nationality, and violation of human dignity Human; b) protection of public health; c) public security, including the safeguarding of national security and defense; d) the protection of consumers, including investors. 2. The measures referred to in paragraph 1 shall be permitted if, in this case, are: a) necessary for a given information society service which prejudices the objectives aimed at protecting public interests referred to in paragraph 1, or which constitutes a serious and grave risk of prejudice to the same objectives; b) Proportionate to those objectives. 3. Without prejudice to the prosecution acting in a criminal investigation, the competent authority, through the Ministry of Industry or the independent sector, must, before adopting the measure: a) Require the Member State referred to in paragraph 1 to take measures and ensure that they were not taken or were inadequate; b) Notify the European Commission and the Member State referred to in paragraph 1 of its intention to take such measures. The measures taken by the independent authority, is given periodically to the Ministry responsible. 4. In urgent cases, the person referred to in paragraph 3 may derogate from the conditions imposed by the article. The measures, in this case, shall be notified in the shortest possible time to the Commission and to the Member State, together with the reasons for the urgency".

81 A translation of art. 14, par 3, would read as follows: "The court or the administrative authority having supervisory functions, may, in urgent cases, request the service provider, exercising the activities [of mere conduit], to prevent or stop violations committed". Similar provisions, in an almost identical drafting, refer to the activities of "caching" – art. 15, para 2, and "hosting", art. 16 para 3.

82 A translation of art. 17 would read as follows: "In providing the services referred to in Articles 14, 15 and 16, the **lender is neither subject to a general obligation to monitor the information that transmits or stores**, **nor to a general obligation to actively seek facts or circumstances indicating the presence of illegal activities**. 2. However, taken into account Articles 14, 16, 15th, the lender is obliged: a) to **immediately inform** the competent judicial or administrative authority responsible for the supervision, whenever he has **become aware of alleged illegal activities** or information regarding its service recipient of the information society; b) to **provide, without delay, at the request of the competent authorities, any information in its possession** to enable identification of the recipient of its services with which it has agreements for data storage, in order to **detect and prevent illegal activity**. 3. The lender is **civilly liable** for the content of such services in case of non-compliance with the requests by the judicial or administrative authority responsible for supervision, if he did **not act promptly** to prevent access to such content, or if, having had knowledge of the unlawful or prejudicial character to third persons of the contents of a service, has **failed to inform** the competent authority."

83 *Supra* at 2.2.3. and footnotes.

84 *Infra* par. 3.

EU legislation currently in force, as well as the national legislature, is interpreted as excluding any kind of general obligation of prior surveillance by ISPs, in order to ensure maximum respect for the principle of freedom of expression and information in the network Internet.[85]

A **specific obligation** for the ISPs arises only in connection with the **general rules on liability** (art. 2043 Italian civil code) in the following cases: if the ISP has not removed the illegal internet content **despite an order by a the competent judiciary or administrative body**; if the ISP is aware of the specific copyright violation, because it has been informed by the person who owns the copyright or by the guarantor of it, and has not promptly **informed the competent authorities of the illegal character** of the internet content uploaded in its platform.[86]

3.2.2. The Competent regulatory bodies and their powers

A. - The Authority for Communications, *Autorità Garante per le Comunicazioni*, AGCOM, is the main regulatory body for telecommunications. It is an independent agency, accountable to the Parliament, responsible for protecting intellectual property rights, regulating advertisements and monitoring public broadcasting.

AGCOM adopted **resolution no. 680/13 / CONS of 12 December 2013** whose annex contains "Regulations concerning the protection of copyright on electronic communications networks and implementation procedures under the Legislative Decree 9 April 2003, n. 70". The resolution enables **AGCOM to order ISPs to remove content upon review by an internal panel but without prior judicial approval, if a copyright violation is detected**.

Despite the fact that the measure was approved after three public consultations[87] and a workshop,[88] and that it takes into account the different legislative approaches and regulations adopted worldwide, the resolution is strongly criticized by users' organizations and ISP representatives and it is now **under the exam of the Italian Constitutional Court**.

According to the administrative judges that have referred the prejudicial question to the Constitutional Court: "The use of the network marked a new frontier of freedom of expression: information previously inaccessible, such as the exercise of powers by States, have reached every corner of the globe […] today's society of information, wired together in real time by the network, has added the role of the Internet to that of the press as an essential mode of exercising the "freedom of expression", the right to inform and to be informed, democratic pluralism and freedom of economic initiative under conditions of full competition. Internet thus, at least as of the "quantity" of the number of "sources", the circularity of the information permitted by the possibility of immediate feedback and by the number of "users" (…) is now one of the main tools for implementing the "freedom' of expression" enshrined in Article. 21 of the Constitution".[89]

The Court further quotes the relevant judgements of the European Court of Justice in this field: C 70/10 SABAM against SCARLET[90] **precluding indiscriminate filtering of internet content** and C

---

85 See points 18 ff. of App. Milano, sez. spec. impresa, 7 gennaio 2015, n. 29.

86 Art. 17 of the decree on electronic commerce n. 70/2003.

87 See http://www.agcom.it/tutela-del-diritto-d-autore.

88 "Copyright online: model comparison", held on May 24, 2013 at the Hall of the Globe of the Chamber of Deputies, *ibidem.*

89 T.A.R. Lazio Roma Sez. I, Ordinanza di remissione 26-09-2014, n. 1 at 22 (translation by the reporter).

90 On line at http://curia.europa.eu/juris/document/document.jsf?text=&docid=115202&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=457681.

324/09, L'Oreal and others[91] stating: "The third sentence of Article 11 of Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights must be interpreted as requiring the Member States to **ensure that the national courts with jurisdiction in relation to the protection of intellectual property rights are able to order the operator of an online marketplace to take measures which contribute, not only to bringing to an end infringements of those rights by users of that marketplace, but also to preventing further infringements of that kind**. Those injunctions must be effective, proportionate, and dissuasive and must not create barriers to legitimate trade".

In addition, the Court of Justice has furthered observed that the European rules permit "an internet service provider in civil proceedings to be ordered to give a copyright holder or its representative information on the subscriber to whom the internet service provider provided an IP address which was allegedly used in an infringement" (decision C - 461/10 Section III, Bonnier Audio AB and Others v Perfect Communication Sweden).[92] Moreover, the Italian judges refer to the judgment of the Court of Justice (Section IV) of 27 March 2014 C - 314/12 - UPC Telekabel Vien Gmbh against Constantin Film Verleih Gmbh[93] to stress that "The fundamental rights recognised by EU law must be interpreted as not precluding a court injunction prohibiting an internet service provider from allowing its customers access to a website placing protected subject-matter online without the agreement of the rightholders when that injunction does not specify the measures which that access provider must take and when that access provider can avoid incurring coercive penalties for breach of that injunction by showing that it has taken all reasonable measures, provided that (i) the measures taken do not unnecessarily deprive internet users of the possibility of lawfully accessing the information available and (ii) that those measures have the effect of preventing unauthorised access to the protected subject-matter or, at least, of making it difficult to achieve and of seriously discouraging internet users who are using the services of the addressee of that injunction from accessing the subject-matter that has been made available to them in breach of the intellectual property right, that being a matter for the national authorities and courts to establish."

In light of the former indications, it is important, according to the judges, to find a fair balance between the protection of intellectual property rights, enjoyed by the owners of copyright, and that of the other fundamental rights at stake. In other words, the limitations of access to the Internet for the protection of copyright need to be subject to prior scrutiny by national courts, provided that the implementation of those directives into Italian law cannot bypass the protection provided by our Constitution to the potentially conflicting fundamental rights at stake.[94]

B. - The competent administrative body for Personal Data Protection is the *Garante per la protezione dei dati personali* or Data Protection Authority (DPA) or *Garante privacy*. Set up in 1997, the DPA supervises compliance by all stakeholders and entities treating personal data with data protection laws. Art. 143, para 1, lett. c), 144 and 154, para 1, lett. d), of Law 196/2003 allows the authority to ban and block operations that are liable to cause serious harm to individuals. In this respect, the National Authority has published Guidelines on Emails and the Internet at Workplace where the use of preventive filters in order to target the access to websites not related to the job is evaluated more

---

91 On line at http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30dd06f04afe9171464d9f909ba8575d4133.e34KaxiLc3qMb40Rch0SaxuRbN90?text=&docid=107261&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=457357.

92 On line at http://curia.europa.eu/juris/document/document.jsf?text=&docid=121743&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=458277.

93 On line at http://curia.europa.eu/juris/document/document.jsf?text=&docid=149924&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=459078.

94 T.A.R. Lazio Roma Sez. I,Ordinanza di remissione 26-09-2014, n. 1, at 23.

favourably if compared to *ex post* controls [95]. The decisions of the DPA are publicly available on its website.[96] According to the ONG Freedom House, the authority "is generally viewed as professional and fair in carrying out its duties".[97]

C. – In addition to international rules, the right to be forgotten is articulated in art. 2 and 27 of the Italian Constitution. Despite this, in most cases defamation proceedings based on the violation of this right have not been successful.[98] Recently, the Italian Corte di Cassazione has requested a **preliminary ruling by the European Court of justice** on the possible solutions to the conflict between the principle of confidentiality of personal data of art. 6, letter. e) of the Directive 4 6/95 / EC of the European Parliament and of the Council of 24 October 1995, implemented in Italy through the Legislative Decree no. 196/2003, on the one hand, and the advertising system implemented with the register of companies provided for by the First Directive 68/151 / EC of 9 March 1968 as well as by national law in art. 2188 cc, and L. 29 December 1993, n. 580, Art. 8.[99]

3.1. Blocking and/or filtering other websites displaying illegal content

In Italy, the power to order the shutdown of a website is given to the competent Judicial Authority in the forms and procedures prescribed by regulatory sources. The following measures may be taken to prevent and prosecute cybercrimes, even though not every crime may be lead to the adoption of such measures. The High Court, for instance, has stated that **seizure of a website in the context of defamation is not allowed**.[100]

3.1.1. Seizure of hardware

Seizure is the general protective measure used in criminal trials. As in most European countries, preventive and protective measures affect temporarily the sphere of the rights and powers of a person, in order to safeguard certain trial needs and/or to guarantee the effective implementation of the future final decision.

Preventive measures have the following characteristics: lawfulness (in compliance with the Constitution); legitimate aim and motivation.

Seizures are subject to art. **253** of the **Code of Criminal Procedure describing the** "object and formalities of seizure".[101]

---

95 http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1408680

96 See, for an example of non-violation of data protection laws: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4363110 and for an example of violation of data protection laws: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3457687.

97 https://freedomhouse.org/report/freedom-net/2015/italy.

98 Cassazione civile sez. VI 12 settembre 2014 n. 19327, Cassazione civile sez. III 06 giugno 2014 n. 12834 etc.

99 Cassazione civile sez. I 17/07/2015 (ud. 04/05/2015 , dep.17/07/2015) n. 15096.

100 Cassazione penale, sez. un. 29/01/2015 (ud. 29/01/2015, dep.17/07/2015) n. 31022 in a case of defamation at the expenses of a judge.

101 The Italian Code of Criminal Procedure at art. 253 prescribes: "*1. L'autorità giudiziaria dispone con decreto motivato il sequestro del corpo del reato e delle cose pertinenti al reato necessarie per l'accertamento dei fatti". 2. Sono corpo del reato le cose sulle quali o mediante le quali il reato è stato commesso nonché le cose che ne costituiscono il prodotto, il profitto o il prezzo.3. Al sequestro procede personalmente l'autorità giudiziaria ovvero un ufficiale di polizia giudiziaria delegato con lo stesso decreto. 4. Copia del decreto di sequestro è consegnata all'interessato, se presente.* http://www.iusexplorer.it/

Seizure is **mandatory** “whenever there is a risk that the free availability of a thing relevant to the criminal offense may aggravate or prolong the consequences of it or facilitate the commission of other crimes”.

It is **optional** when, despite the absence of the above-mentioned reasons, “there are things that are subject to confiscation and it is better not to leave them under the availability of the accused person while the proceedings are still pending” (art. 321 Criminal Procedure Code).[102]

Only the Public Prosecutor is entitled to request a seizure. A preventive seizure order is issued by decree "*inaudita altera parte*" in every stage of the proceedings, by the judge, at the request of the Prosecutor.

The seizure is ordered through a **motivated decree** by the judge for preliminary investigations and by the competent Court to decide on the merits, according to the stage of the procedure.

There are two necessary conditions for the application of the measure at issue:

1) the "***fumus***" of the crime, that is, we proceed in order for a fact that corresponds to an abstract case of the offense;
2) the "***periculum in mora***" that is the real possibility that the availability of the item can aggravate or prolong the consequences of it or facilitate the commission of other crimes.

The seizure is immediately revoked when one of the conditions of the injunction is not present any longer; revocation can be placed directly by the Public Prosecutor during the preliminary

---

FontiNormative/Leggi?idDocMaster=3948142&idDataBanks=10&idUnitaDoc=20113010&nVigUnitaDoc=1&pagina=1&loadTreeView=True&NavId=261144429&pid=19&IsCorr=False

102 The Italian Code of Criminal Procedure at art. 321 prescribes: “*Quando vi è pericolo che la libera disponibilità di una cosa pertinente al reato possa aggravare o protrarre le conseguenze di esso ovvero agevolare la commissione di altri reati, a richiesta del pubblico ministero il giudice competente a pronunciarsi nel merito ne dispone il sequestro con decreto motivato. Prima dell'esercizio dell'azione penale provvede il giudice per le indagini preliminari. 2. Il giudice può altresì disporre il sequestro delle cose di cui è consentita la confisca.2-bis. Nel corso del procedimento penale relativo a delitti previsti dal capo I del titolo II del libro secondo del codice penale il giudice dispone il sequestro dei beni di cui è consentita la confisca. 3. Il sequestro è immediatamente revocato a richiesta del pubblico ministero o dell'interessato quando risultano mancanti, anche per fatti sopravvenuti, le condizioni di applicabilità previste dal comma 1. Nel corso delle indagini preliminari provvede il pubblico ministero con decreto motivato, che è notificato a coloro che hanno diritto di proporre impugnazione. Se vi è richiesta di revoca dell'interessato, il pubblico ministero, quando ritiene che essa vada anche in parte respinta, la trasmette al giudice, cui presenta richieste specifiche nonché gli elementi sui quali fonda le sue valutazioni. La richiesta è trasmessa non oltre il giorno successivo a quello del deposito nella segreteria. 3-bis. Nel corso delle indagini preliminari, quando non è possibile, per la situazione di urgenza, attendere il provvedimento del giudice, il sequestro è disposto con decreto motivato dal pubblico ministero. Negli stessi casi, prima dell'intervento del pubblico ministero, al sequestro procedono ufficiali di polizia giudiziaria, i quali, nelle quarantotto ore successive, trasmettono il verbale al pubblico ministero del luogo in cui il sequestro è stato eseguito. Questi, se non dispone la restituzione delle cose sequestrate, richiede al giudice la convalida e l'emissione del decreto previsto dal comma 1 entro quarantotto ore dal sequestro, se disposto dallo stesso pubblico ministero, o dalla ricezione del verbale, se il sequestro è stato eseguito di iniziativa dalla polizia giudiziaria. 3-ter. Il sequestro perde efficacia se non sono osservati i termini previsti dal comma 3-bis ovvero se il giudice non emette ordinanza di convalida entro dieci giorni dalla ricezione della richiesta. Copia dell'ordinanza è immediatamente notificata alla persona alla quale le cose sono state sequestrate*”. http://www.iusexplorer.it/FontiNormative/Leggi?idDocMaster=3948142&idDataBanks=10&idUnitaDoc=20113103&nVigUnitaDoc=1&pagina=1&loadTreeView=True&NavId=1176230400&pid=19&IsCorr=False.

investigation, it is ordered by the Court, under request of the Public Prosecutor or the person which has interest, in the other phases or during the preliminary investigation when the Public Prosecution is wholly or partly dissenting.

In case of **urgency**, that is when the "*periculum in mora*" enables judicial intervention, a seizure may be adopted by the Public Prosecutor or even police officers. The decree of seizure, adopted "*a non iudice*", expires if it is not followed by an expedited validation order; the measure must be brought within the following forty-eight hours to the Public Prosecutor of the place where the seizure took place (art. 321 paragraphs 3bis *ter* c.p.p.).

The consequences of a seizure are said to affect constitutionally protected values less than other measures and this explains the reason why it can be adopted in some cases by the police.

Against the decree of seizure issued by the judge the party opposing it may ask for a **review** within ten days from its implementation or knowledge of it (art. 324 paragraph 4 c.p.p.).[103] Implementation of seizures, in general, are governed by the provisions of the Code's implementation, which was affected by the reform introduced by Law 15.07.2009, n. 94 (so-called "pacchetto sicurezza").[104]

On these grounds, the High Court has upheld the decision of an Italian Court authorising the seizure of a platform used for copyrights violations.[105]

According to the High Court a special inhibitory power is assigned to judges by Decree of April 9, 2003, n. 70, Art. 14 to 16. Such special legislation, provides for free movement in general, but within the limits of the respect of copyright: Article. 4, paragraph 1, lett. a) - of such services, such as those operated by providers for access to the Internet network, authorises limitations aimed at the **prevention, investigation, detection and prosecution of criminal offenses**. In particular art. 14, para 3, Art. 15, paragraph 3, and art. 16, paragraph 3, provide that the judicial authorities may require in case of urgency that the service provider terminates or prevents violations. According to the Court these provisions should be read together with art. 17, which excludes a general monitoring obligation (in the sense that the provider is not required to verify that the data), notably in violation of copyright, but, together with the obligation to report unlawful activities, whenever the service provider is aware of those, and to provide direct information enabling authorities to identify the author of the unlawful activity. These provisions, according to the Court, suggest that there is an **inhibitory power enabling orders to providers of these services to foreclose access to the Internet computer network for the sole purpose of preventing the continuation of the commission of offenses**. This injunction must respect the **principle of "proportionality**" (Legislative Decree. N. 70 of 2003, Art. 5, paragraph 2, lett. B, cit.). Limiting access is possible only to the extent of allowing the objective of detection and prosecution of crimes, since the circulation of information on the computer network Internet is still a **form of expression and dissemination of thought** that lies in the constitutional guarantee of art. 21 of the Constitution as stated, in particular, by the High Court in

---

103 http://www.iusexplorer.it/FontiNormative/Leggi?idDocMaster=3948142&idDataBanks=10&idUnitaDoc=20113108&nVigUnitaDoc=1&pagina=1&loadTreeView=True&NavId=1493710218&pid=19&IsCorr=False.

104 LEGGE 15 luglio 2009, n. 94 Disposizioni in materia di sicurezza pubblica. (09G0096) (GU n.170 del 24-7-2009 - Suppl. Ordinario n. 128). http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2009-07-15;94!vig=.

105 Cassazione penale sez. III, 29/09/2009 (ud. 29/09/2009 , dep.23/12/2009) n. 49437: The original decision ordered that internet service providers (ISP) and in particular the providers operating on the Italian territory impede access to their users access to the Site web called www.thepiratebay.org, as well as aliases and domain names redirecting to that website.

the case: Cass., Sec. 3, 11 December 2008 - 10 March 2009, n. 10535 (where, with reference to a blog, a distinction between freedom of expression and freedom of the press was sketched).[106]

When elements of the offense of copyright violations (Article. 171 ter, paragraph 2, letter. a-bis) Law 633/1941) appear, a court may order the seizure of the website and, if the owner contributes in the criminal activity spreading within the Internet works protected by copyright, a court may request that ISPs preclude access to the site.

As stated above these measures must respect the **principle of proportionality**, thus **they cannot be used**, for example, **when the cybercrime consists of a defamation**.[107]

3.3.2. Confiscation of hardware

The same principles govern **confiscation of the hardware**, regulated by **Article 240 of Criminal Code**.[108]
With the legal instrument of confiscation, the State makes an expropriation of assets related to the execution of criminal acts, property that could be used to re-engage in criminal activity.

It is a security measure allowing the expropriation by the State of things used or intended to commit the crime, or representative of your product or profit.

Confiscation presents certain similarities with seizure, but while this is characterized by the temporary nature of the measure, **in the case of confiscation, the owner loses the confiscated property, that might even be destroyed.** Confiscation may be **ordered upon a discretionary evaluation of the judge** in case of things which have served or were destined to commit a crime, or things that are the product or profit of such crime. Confiscation is **mandatory** when the danger is inherent to the confiscated property because this is the price of the crime or because its use is criminal. It is however possible to revoke the measure through presentation of a **revocation order** issued by the competent authority.

---

106 Seizure of the website was accompanied by a real injunction to ISPs. This injunction was deemed "urgent" ex art. 14, para 3, Art. 15, paragraph 3, and art. 16, paragraph 3. By combining these measures with the art. 321 Criminal Procedure Code, the criminal court, in ordering the seizure of the website, has simultaneously required providers to restrict access to the site in order to preclude the activity of illegal distribution of contents protected by copyright.

107 Cassazione penale, sez. un. 29/01/2015 (ud. 29/01/2015 , dep.17/07/2015) n. 31022 *supra* note 50.

108 The Italian Criminal Code at art. 240 prescribes: "1. *Nel caso di condanna il giudice può ordinare la confisca delle cose che servirono o furono destinate a commettere il reato, e delle cose che ne sono il prodotto o il profitto.2. È sempre ordinata la confisca:1) delle cose che costituiscono il prezzo del reato; 1-bis)* ***dei beni e degli strumenti informatici o telematici che risultino essere stati in tutto o in parte utilizzati per la commissione dei reati*** *di cui agli articoli; delle cose, la fabbricazione, l'uso, il porto, la detenzione o l'alienazione delle quali costituisce reato, anche se non è stata pronunciata condanna. 3. Le disposizioni della prima parte e dei numeri 1 e 1-bis del capoverso precedente non si applicano se la cosa o il bene o lo strumento informatico o telematico appartiene a persona estranea al reato. La disposizione del numero 1-bis del capoverso precedente si applica anche nel caso di applicazione della pena su richiesta delle parti a norma dell'articolo 444 del codice di procedura penale. 4. La disposizione del numero 2 non si applica se la cosa appartiene a persona estranea al reato e la fabbricazione, l'uso, il porto, la detenzione o l'alienazione possono essere consentiti mediante autorizzazione amministrativa.*http://www.iusexplorer.it/FontiNormative/Leggi?idDocMaster=3948141&idDataBanks=10&idUnitaDoc=2011200 1&nVigUnitaDoc=1&pagina=1&loadTreeView=True&NavId=814138053&pid=19&IsCorr=False.

3.3.3. Art. 700 of the Italian Code of Civil Procedure

This article of the Italian Code of Civil Procedure offers a general preventive remedy that may be used and in fact has been used to order *ad hoc* filtering, blocking and taking down of illegal (not necessarily criminal) internet content under the control of the judiciary.[109]

4. General Monitoring of Internet

In Italy, **no entity in charge of general monitoring of internet content** has been created.

As in other countries, monitoring of internet content is related to targeted *matters* in the legal frameworks described above.

As acknowledged by the ONG Freedom House: "Monitoring of personal communications is permissible only if a judicial warrant has been issued, and widespread technical surveillance is not a concern in Italy."[110]

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

Within the case law of the ECHR, **no evidence** is found on the interference between any of the aforementioned Italian practices on the blocking, filtering or taking down of Internet Content and rights protected under the ECHR.

The requirements of foreseeability, accessibility, and clarity developed in this subject matter by the European Court of Human Rights seem to be met by the articulate Italian legislation on the matter.
It may be useful to recall that in recent years the Court discussed that any public authority interference with the peaceful enjoyment of the right of freedom of expression must be justified by the **lawfulness** of such interference (existence of a legal basis); the **legitimate aim** of the interference (protection of conflicting citizen's rights as those protected by art. 8 ECHR); its necessity in a democratic society (namely the necessity to prevent and punish criminal conducts – paedophilia in the first place).

The practice of blocking, filtering or taking down of Internet content guarantees a good balance between Article 8 and Article 10 of the European Convention on Human Rights since, as stated by the Court: "the Court has held that speech that is incompatible with the values proclaimed and guaranteed by the Convention is not protected by Article 10 by virtue of Article 17 of the Convention".[111]

No possible doubts exist as regards to the conformity of the practice of blacklist for child pornography with art. 10 ECHR: the Court explicitly affirms that **member States have specific positive obligations in the protection of the vulnerable**, since such obligations are inherent in **Articles 3 and 8 of the Convention**.[112]

---

109 Art. 700 of the Italian Code of Civil Procedure was used in the Italian "Uber" case, on which see supra at 2.2.3.

110 https://freedomhouse.org/report/freedom-net/2015/italy.

111 CASE OF DELFI AS v. ESTONIA (Application no. 64569/09), JUDGMENT, STRASBOURG, 16 June 2015.

112 K.U. v. Finland, no. 2872/02, 2 December 2008 and previously M.C. v. Bulgaria, no. 39272/98, ECHR 2003-XII.

Similar conclusions apply to the black-list established for hindering cybercrimes related to terrorism since it is a primary responsibility of the State that of protecting the life of civilians.

It is not clear if the same conclusion could apply to the publicly available black-list on gambling, whose regime **differs** to that of the black lists drafted to counteract child pornography and terrorism. In Italy, as in many countries, although gambling is not illegal, the obligation to pay a sum as a consequence of the "gambling contract" is not enforceable. Here, the balance to be found is that between the **freedom of economic initiative**, on the one hand, and the **proven use of internet gambling for money-laundering by the Italian Mafia**[113] on the other hand, taking into account the dimensions acquired by the phenomenon of *ludomania* (**pathological gambling**, in Italian *gioco d'azzardo patologico* or GAP) that may even lead to characterise ludomaniacs as "vulnerable persons".[114]

The conformity of the aforementioned Italian legislation and practices with the principle of **freedom of expression**, seems to be re-iterated by the recently released report of Freedom House that rates Italy as the **8th country in the world** for freedom of the net, the **4th within the Council of Europe** (after Iceland, Estonia and Germany).[115]

Freedom House further recalls that in Italy "An **inter-parliamentary committee** appointed in July 2014 to draft an internet bill of rights released its nonbinding "**Declaration of Internet Rights**" in July 2015.[116] The declaration makes Italy **the first European country to release** such a document, following in the footsteps of Brazil. The declaration contains language defending the **right to internet access**, **data protection, net neutrality, anonymity, and the right to be forgotten**".[117]

Report completed on 28.10.2015 by Ilaria Pretelli[118]

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

---

113 In the framework of operation "gambling", Colonel Gaetano Scilla, head of the Anti-Mafia Investigation of Reggio Calabria is quoted to have stated that "The volume of online game run by the 'Ndrangheta, [the calabrese mafia] represents 10% of Calabrian' GDP". See extensively: http://www.linkiesta.it/it/article/2015/10/07/casino-on-line-le-mille-vie-del-riciclaggio/27676/ (18.11.2015).

114 See the legislative proposal: http://www.senato.it/japp/bgt/showdoc/17/DDLPRES/769207/index.html?stampa=si&spart=si&toc=no (18.11.2015).

115 Freedom House refers to the following document: http://www.camera.it/application/xmanager/projects/leg17/commissione_internet/testo_definitivo_inglese.pdf.

116 *Ibidem.*

117 *Ibidem.*

118 I wish to thank our talented *stagiaire* Luca Ferraiuolo who has proved to have a special gift for finding, within the Italian public administration, the competent persons with primary responsibilities for enacting the laws referred to in the text.