FOM.GAL/4/10
26 November 2010

ENGLISH only

Organization for Security and Co-operation in Europe
The Representative on Freedom of the Media

PRELIMINARY REPORT

Study of legal provisions and practices related to freedom of expression, the free flow of information and media pluralism on the Internet in the OSCE participating States

This preliminary report has been commissioned by the Office of the OSCE Representative on Freedom of the Media and prepared by Dr. Yaman Akdeniz, Associate Professor of Law, Faculty of Law, Istanbul Bilgi University, Turkey.*

It presents the initial stage of research into the first comprehensive study of legal provisions and practices related to freedom of expression, the free flow of information and media pluralism on the Internet in the OSCE participating States. This preliminary report was prepared in view of the OSCE review conference and OSCE Astana Summit 2010. The final study is expected to be concluded in early 2011 and will be published in English and Russian.

* Yaman Akdeniz' recent publications include Internet Child Pornography and the Law: National and International Responses (London: Ashgate, 2008: ISBN: 0 7546 2297 5), *Racism on the Internet*, Council of Europe Publishing, 2010 (ISBN 978-92-871-6634-0). For further information about his work see <http://cyberlaw.org.uk/about/>. Yaman Akdeniz can be contacted at yaman.akdeniz@bilgi.edu.tr.

Foreword

By Dunja Mijatović, the OSCE Representative on Freedom of the Media

This preliminary report was prepared in anticipation of the OSCE review conference and the OSCE Astana Summit. It aims to present an overview of existing international legal measures and provisions as well as their efficiency and enforceability related to the global or regional regulation of content available on the Internet.

Over the past years my Office has seen many OSCE participating States enacting laws aimed at regulating, among others, cybercrime, online hate speech and racist content, the protection of minors from harmful content on the Internet, as well as the fight against international threats including the terrorist use of the Internet. This increased legal regulation of online content has led to restrictions on the free flow of information and the right to freely receive and impart information through the Internet. Online journalists and media are facing mounting difficulties and uncertainties when performing their duties. Law enforcement agencies at times seem equally unsure about which measures apply when addressing the publishing or availability of potentially illegal content. The fast evolving nature of the Internet for its very complexity and flexibility seems to provoke fear and a concern that the Internet is a medium difficult to control leading to the impression that legislation designed to regulate offline content is not adequate enough to regulate online content. In fact, it seems that some policymakers regard the Internet as another world – rather than a new technical platform – and are therefore of the opinion that content on the Internet is not comparable to offline content and therefore needs not only special but especially restrictive legislation.

The number of legal reviews my Office commissioned over the last years in the area of online content regulation has increased significantly. While the number of adopted international legal provisions is well defined, it became increasingly difficult to maintain an overview of the numerous national laws and regulations applying to online media, free expression, the free flow of information and media pluralism on the Internet.

As a result, my Office decided to commission the first OSCE Internet regulation study and OSCE-wide Internet legal matrix. Our aim is threefold: The study will provide an overview of existing international legal provisions related to free expression and the free flow of information on the Internet. Second, the study will assess how national Internet legislation and practices comply with existing OSCE media freedom commitments, Article 10 of the European Convention on Human Rights (where applicable) and other relevant international standards. Third, with the help of OSCE participating States, we hope to establish a comprehensive database of applicable laws which will not only lists respective laws but which shall serve as a basis to assess future development in the area of Internet regulation, thus becoming a reference tool for national legislatures.

This preliminary report tackles our first objective by providing a first overview of existing international legal measures and provisions as well as their efficiency and enforceability related to the global or regional regulation of content available on the Internet.

Executive Summary

Today, many OSCE participating States are reacting to the availability and dissemination of certain types of (illegal or unwanted) content through the Internet by trying to regulate or control its dissemination. There is particularly major concern about the availability of terrorist propaganda, racist content, sexually explicit content including child pornography, as well as content defined as hate speech on the Internet.

This OSCE-wide Internet content regulation study involves a comprehensive overview of existing international legal provisions and standards relating to media freedom and freedom of expression on the Internet. The study will assess whether and how these are incorporated into national legislation and applied by the OSCE participating States.

Furthermore, the final study will assess the compliance of applicable national Internet legislation and practices with existing OSCE media freedom commitments, Article 10 of the European Convention on Human Rights (where applicable) and other relevant international standards. For this purpose the study will involve the compilation of a comprehensive OSCE-wide legal matrix of all legal provisions related to freedom of the media, the free flow of information and media pluralism on the Internet. A survey questionnaire was prepared during the summer of 2010 and distributed to all OSCE participating States on 23 September 2010.[1] Responses to the questionnaire were expected by 15 November, 2010. Depending on timely submissions, the study is expected to be concluded in early 2011.

This preliminary report aims to lay out the first findings of the OSCE Internet Regulation Study based 1) on the review and presentation of major international legal provisions related to the subject; 2) on the examination and assessment of the efficiency, advantages and disadvantages of various international and national content regulation measures – particularly vis-à-vis fundamental rights of free expression and media freedom; and 3) by taking into account international as well as national academic and policy discussions on the matter. This report also includes preliminary conclusions which will be further developed based on the responses to be received from the OSCE participating States to the questionnaire.

This report argues that access-blocking measures show their inadequacy as an efficient and proportionate method to combat illegal Internet content, and raises concern about the possibility of using blocking measures or upstream filtering tools at national level to silence politically motivated speech on the Internet. The report shows that international organizations such as the Council of Europe and the European Union have recognized the inefficiency of blocking to fight serious crimes. Furthermore, the report warns that blocking access to any Web 2.0 based applications and services such as YouTube, WordPress, Facebook, and Twitter, to mention a few, may have extreme side effects and strong implications for political expression.

Regarding the protection of children from accessing online content deemed to be harmful, the report states that participating States should encourage the application of end-user based filtering software programs on home computers and in schools if their use is deemed necessary. The deployment of state-level upstream filtering systems should be avoided at all costs.

In concluding, this preliminary report calls for the OSCE participating States to respect OSCE commitments and other international human rights principles when developing their Internet content-related policies and regulations. The states' response should be proportional, correspond to a "pressing social need", and be in line with the requirements of democracy with regard to content-based restrictions. Internet access should be regarded as a fundamental human right and network neutrality should not only be respected but upheld by the OSCE participating States.

[1] See OSCE FOM.GAL/3/10, 23 September, 2010 and Appendix I.

Introduction

When new media platforms were introduced in the past, their innovation and application was met with scepticism, fear or outright banning by ruling parties and authorities who feared the non-controllability of the unknown medium and their capacity to oust them from power. Therefore, new media historically face suspicion and are liable to excessive regulation as they spark fear of potential detrimental effects on society, security, political power structures, or all three. This has proved true of the publication and transmission of certain types of content not only through the printing press, but also through the radio, television and satellite transmissions and other forms of communication systems. During the 1990s, as attention turned to the Internet, the widespread availability of sexually explicit content and other types of content deemed to be harmful for children stirred up a 'moral panic'[2] shared by many states and governments.

Prior to the 1990s, information and content was predominantly within the strict boundaries and control of individual states, whether through paper-based publications (such as pamphlets, local newspapers and even books), or through audio-visual transmissions limited to a particular area (such as local radio and television), or even through public demonstrations, discussions and information sharing. However, currently, information and content, with its digital transmission and widespread availability through the Internet, does not necessarily respect national rules or territorial boundaries. This globalization of information is paired with an increased multilingualism observable in many countries. Today, the increasing popularity of user-driven interactive Web 2.0 applications and services such as YouTube, Facebook and Twitter seem to break down virtual Internet borders even further. This undoubtedly complicates efforts to find an appropriate balance between the universal right to freedom of opinion and expression and to receive and impart information, and the prohibition on certain types of content deemed illegal by national authorities or international organizations. Thus, Internet content regulation became an important focus of governments, supranational bodies and international organisations across the globe.

Today, many OSCE participating States are reacting to the availability and dissemination of certain types of (illegal or unwanted) content through the Internet by trying to regulate or control its dissemination. There is major concern about the availability of sexually explicit content including child pornography,[3] racist content,[4] and terrorist propaganda[5] as well as content defined as hate speech on the Internet.

This OSCE-wide Internet content regulation study involves a comprehensive overview of existing international legal provisions related to free expression and the free flow of information on the Internet, and the study will assess whether and how these are incorporated into national legislation and applied by the OSCE participating States.

---

2 Cohen, S., Folk Devils and Moral Panics: Creation of Mods and Rockers, Routledge: 30th Anniversary edition, 2002; Jenkins, P., Intimate Enemies: Moral Panics in Contemporary Great Britain, Aldine De Gruyter, 1992.

3 For a detailed assessment of legal issues surrounding child pornography see Akdeniz, Y., *Internet Child Pornography and the Law: National and International Responses*, Ashgate, 2008.

4 For a detailed assessment of legal issues surrounding racist content and hate speech on the Internet see Akdeniz, Y., *Racism on the Internet*, Council of Europe Publishing, 2010 (ISBN 978-92-871-6634-0); Akdeniz, Y., "Introduction," in *Legal Instruments for Combating Racism on the Internet*, Council of Europe Publishing, Human Rights and Democracy Series, 2009, pp 7-37.

5 See generally Weimann, G., *Terror on the Internet: The New Arena, the New Challenges* (Washington: US Institute of Peace, 2006).

Furthermore, the study will assess how national Internet legislation and practices comply with existing OSCE media freedom commitments, Article 10 of the European Convention on Human Rights (where applicable) and other relevant international standards. For this purpose the study will involve the compilation of a comprehensive OSCE-wide legal matrix of all legal provisions related to freedom of the media, the free flow of information and media pluralism on the Internet. A **survey questionnaire** was prepared during the summer of 2010 and was distributed to all OSCE participating States on **23 September 2010**.[6] Responses to the questionnaire were expected by **15 November, 2010**. Depending on timely submissions, the study is expected to be concluded in early 2011.

Preliminary Findings of the OSCE Internet Regulation Study

The governance of illegal as well as harmful (which falls short of illegal) Internet content may differ from one country to another, and variations exist within the OSCE participating States.[7] "Harm criteria" remain distinct within different jurisdictions with individual states deciding what is legal and illegal based upon cultural, moral, religious, historical, and legal differences and constitutional values.

Once within the strict boundaries and control of individual states, whether through paper-based publications (such as pamphlets, local papers and even books), or audio-visual transmission limited to a particular area (such as local radio), content which is digitally transmitted and availability through the Internet neither respects national rules nor boundaries. Many states say that what is illegal and punishable in an offline form must at least also be treated equally online. There are, however, several features of the Internet which fundamentally affect approaches to its governance, and while rules and boundaries still exist, enforcement of existing laws, rules and regulations to digital content becomes evidently complex, problematic and at times difficult to enforce on the Internet.

Therefore, despite the introduction of new laws, or amendments to existing laws criminalizing publication or distribution of certain types of content, in almost all instances extraterritoriality remains as a major problem with regard to the availability of Internet content hosted or distributed from outside the jurisdiction in which the content is deemed illegal.

Based on the limited effectiveness of state laws and lack of harmonization at international level (despite some efforts at regional level)[8] a number of states, including some in the OSCE region, started to introduce policies to block access to Internet content, websites deemed illegal and Web 2.0 based social-media platforms which are located outside their jurisdiction.

In short, the new trend in Internet regulation seems to be blocking access to content if state authorities are not in a position to reach the perpetrators or criminals for prosecution or if their request for removal or "take down" of such content is rejected or ignored by foreign law enforcement authorities or hosting and content providers are outside their jurisdiction.

---

6 See OSCE FOM.GAL/3/10, 23 September, 2010.

7 Harm is a criterion which depends upon cultural differences and this is accepted within the jurisprudence of the European Court of Human Rights. See for example *Handyside v UK*, App. no. no. 5493/72, Ser A vol.24, (1976) 1 EHRR 737. Nevertheless, the availability of harmful Internet content is a politically sensitive area and a cause for concern for European regulators.

8 Note the Council of Europe Convention on Cybercrime (ETS No. 185), and the Additional Protocol Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems (ETS No. 189).

Furthermore, in certain countries, governments went further and started to develop policies and legal measures which could restrict users' access to the Internet. This new blocking trend has been triggered in a number of countries as a result of substantially increased piracy and intellectual property infringement through and on the Internet. These developments, as well as new policy trends in Internet content regulation, will be detailed in this study

The final version of this commissioned study will include four parts based on the questionnaire[9] sent to the all Delegations of the OSCE participating States and include assessments related to:

A. Internet Access
B. Internet Content Regulation
C. Blocking, content removal, and filtering and
D. Licensing and liability

Based on the responses to be received from the OSCE participating States, and with the assessment of the efficiency and applicability of existing international legal provisions as well as their translation into national law and practice, the study will serve as an OSCE-wide Internet Legal Matrix. Preliminary findings are provided below.

Given that this report focuses on international provisions and challenges in regard to their enforceability and the fact that only few questionnaires had been returned answered at the point of writing of this preliminary report, it is indispensable to emphasize the provisional nature of its findings.

A. Internet Access

Internet Access – A Fundamental Human Right

While on the one hand, certain countries and international organizations such as the United Nations are considering recognizing Internet access to be a fundamental and universal human right, on the other hand, a number of governments are considering adopting content and access blocking measures. Countries such as Finland and Estonia have already ruled that access is a human right for their citizens and, according to a poll by the BBC World Service involving 27,000 adults across 26 countries, "almost four in five people around the world believe that access to the Internet is a fundamental right."[10]

In this context, it is important to recall one of the most important declarations of principles of the World Summit on the Information Society (Geneva 2003 – Tunis 2005). The participants declared their

> "common desire and commitment to build a people-centred, inclusive and development-oriented Information Society, where everyone can create, **access**, utilize and share information and knowledge, enabling individuals, communities and peoples to achieve their full potential in promoting their sustainable development and improving their quality of life, premised on

[9] See Appendix I.

[10] BBC News, Internet access is 'a fundamental right' 08 March, 2010, at http://news.bbc.co.uk/2/hi/8548190.stm

the purposes and principles of the Charter of the United Nations and respecting fully and upholding the Universal Declaration of Human Rights."[11]

Based on the positive considerations to recognize Internet access as a fundamental human right, the adoption or consideration of access-blocking measures by certain governments – as will be outlined below - is worrisome.

Network Neutrality

Network neutrality is defined as the principle that all Internet data traffic should be treated equally based on an "end-to-end" principle. In practice, this means that network operators or Internet access providers treat data packets equally, regardless of origin, content or destination, so that users "should have the greatest possible access to Internet-based content."[12] Users should have any applications or access any services of their choice without the traffic related to the services they use being managed, prioritized or discriminated by the network operators. This general principle, "commonly referred to as network neutrality, should apply irrespective of the infrastructure or the network used for Internet connectivity. Access to infrastructure is a prerequisite for the realisation of this objective,"[13] as declared by the Council of Europe Committee of Ministers. Similarly, a recent European Commission document recognized that "this architectural feature is considered by many to have been a key driver of the growth of the Internet to date, and to have facilitated an open environment conducive to the spectacular levels of innovation seen in online applications, content and services networks."[14]

However, "a number of cases have emerged involving the differentiated treatment by network operators of services or traffic which have led some interested parties to question whether the principle of the openness or neutrality of the Internet may be at risk."[15] Therefore, there is "growing international interest as to whether, and to what extent, traffic management should be subject to regulation."[16] According to a discussion paper issued by OFCOM in the United Kingdom "the debate ranges widely including questions such as whether citizens have a 'fundamental right' to a neutral Internet, or whether 'net neutrality' promotes economic competitiveness and growth."[17]

From a users' perspective there is concern that network operators may place restrictions on the access and use of certain applications and services over the Internet. Examples include restrictions on 'voice over Internet Protocol' (VoIP) services such as Skype and speed restrictions with regard to the use of peer-to-peer (P2P) networks and applications for downloading and sharing digital content, including pirated content.

---

11 Declaration of Principles for the first phase of the World Summit on the Information Society, Geneva, 10-12 December 2003.

12 CoE Declaration of the Committee of Ministers on Network Neutrality, adopted on 29 September 2010 at the 1094th meeting of the Ministers' Deputies. See https://wcd.coe.int/ViewDoc.jsp?id=1678287&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383, para 4.

13 *Ibid*.

14 European Commission, Questionnaire for the Public Consultation on the Open Internet and Net Neutrality in Europe, 30 June, 2010.

15 *Ibid*.

16 OFCOM (UK), Traffic Management and 'net neutrality": A Discussion Document, 24 June, 2010, p.1, para 1.5.

17 *Ibid*.

It is also important to note the EU Telecommunications Reform Package of November 2009 which addressed access related concerns from a human rights perspective:

> "Measures taken by Member States regarding end-users' access to or use of services and applications through electronic communications networks shall respect the fundamental rights and freedoms of natural persons, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and general principles of Community law.
>
> "Any of these measures regarding end-users' access to, or use of, services and applications through electronic communications networks liable to restrict those fundamental rights or freedoms may only be imposed if they are appropriate, proportionate and necessary within a democratic society, and their implementation shall be subject to adequate procedural safeguards in conformity with the European Convention for the Protection of Human Rights and Fundamental Freedoms and with general principles of Community law, including effective judicial protection and due process. Accordingly, these measures may only be taken with due respect for the principle of the presumption of innocence and the right to privacy. A prior, fair and impartial procedure shall be guaranteed, including the right to be heard of the person or persons concerned, subject to the need for appropriate conditions and procedural arrangements in duly substantiated cases of urgency in conformity with the European Convention for the Protection of Human Rights and Fundamental Freedoms. The right to effective and timely judicial review shall be guaranteed."[18]

While the 27 Member States of the European Union have time until June 2011 to transpose the package into national legislation,[19] the American Civil Liberties Union in an October 2010 report called on the U.S. government to preserve the free and open Internet arguing that net neutrality is "one of the "foremost free speech issues of our time."[20]

The Council of Europe also recognized, in a September 2010 Committee of Ministers Declaration on Network Neutrality, that the "users' right to access and distribute information online and the development of new tools and services might be adversely affected by non-transparent traffic management, content and services' discrimination or impeding connectivity of devices."[21] According to the CoE Declaration

> "traffic management should not be seen as a departure from the principle of network neutrality. However, exceptions to this principle should be considered with great circumspection and need to be justified by overriding public interests. In this context, member states should pay due attention to the provisions of Article 10 of the European Convention on Human Rights and the related case law of the European Court of Human Rights. Member states may also find it useful to refer to the guidelines of Recommendation CM/Rec(2008)6 of

---

18 See Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services, Article 1.

19 Note also the Report on the EU public consultation on 'The open internet and net neutrality in Europe', at http://ec.europa.eu/information_society/policy/ecomm/doc/library/public_consult/net_neutrality/report.pdf Digital Agenda: Consultation reveals near consensus on importance of preserving open Internet, Ref: IP/10/1482 Date: 09/11/2010.

20 America Civil Liberties Union, *Network Neutrality 101: Why the Governments Must Act to preserve the Free and Open Internet*, October 2010, at http://www.aclu.org/free-speech-technology-and-liberty/network-neutrality-101-why-government-must-act-preserve-free-and-

21 CoE Declaration of the Committee of Ministers on Network Neutrality, adopted on 29 September 2010 at the 1094th meeting of the Ministers' Deputies. See https://wcd.coe.int/ViewDoc.jsp?id=1678287&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383

> the Committee of Ministers to member states on measures to promote the respect for freedom of expression and information with regard to Internet filters."[22]

Furthermore, the Committee of Ministers declared its commitment to the principle of network neutrality and recommended that

> "Users and service, application or content providers should be able to gauge the impact of network management measures on the enjoyment of fundamental rights and freedoms, in particular the rights to freedom of expression and to impart or receive information regardless of frontiers, as well as the right to respect for private life. Those measures should be proportionate, appropriate and avoid unjustified discrimination; they should be subject to periodic review and not be maintained longer than strictly necessary. Users and service providers should be adequately informed about any network management measures that affect in a significant way access to content, applications or services. As regards procedural safeguards, there should be adequate avenues, respectful of rule of law requirements, to challenge network management decisions and, where appropriate, there should be adequate avenues to seek redress."[23]

The Declaration pointed out that issues surrounding net neutrality should be explored further within a "Council of Europe framework with a view to providing guidance to member states and/or to facilitating the elaboration of guidelines with and for private sector actors in order to define more precisely acceptable management measures and minimum quality-of-service requirements."[24]

B. Internet Content Regulation

Undoubtedly differences do exist between approaches adopted to regulate content on the Internet. Content regarded as harmful or offensive does not always fall within the boundaries of illegality in all OSCE participating States. Usually, the difference between illegal and harmful content is that the former is criminalized by national laws, while the latter is considered offensive, objectionable, unwanted or undesirable by some but is generally not considered criminal. While child pornography could be regarded as a clear example of content being outlawed in most, if not all, 56 OSCE participating States, Internet content that is often labelled as "harmful" may include sexually explicit material, graphically violent material, and content advocating illegal activity such as drug use, bomb-making instructions or underage drinking, and gambling. Certain harsh or extreme political views or religious views are also regarded as harmful by many state regulators. Although this type of content falls short of the "illegality threshold," there remains concern about children's access to this type of content. Highlighting this fundamental difference, the European Commission stated that:

> "These different categories of content pose radically different issues of principle, and call for very different legal and technological responses. It would be dangerous to amalgamate separate issues such as children accessing pornographic content for adults, and adults accessing pornography about children".[25]

Furthermore, nations differ in terms of categorizing or labelling certain types of content. For example, content advocating hateful or racist views and content involving terrorist

---

22 *Ibid*., para 6.
23 *Ibid*., para 8.
24 *Ibid*., para 9.
25 European Commission Communication on Illegal and Harmful Content on the Internet (1996), p, 10.

propaganda may be treated differently by different states. The reason is that in many states "freedom of expression extends not only to ideas and information generally regarded as inoffensive but even to those that might offend, shock, or disturb. Such are the demands of that pluralism, tolerance and broadmindedness without which there is no 'democratic society'."[26] Across the pan-European region, the member states of the Council of Europe have a certain margin of appreciation[27] in assessing whether a "pressing social need" exists to introduce speech-based restrictions to their national laws based on Article 10 of the European Convention on Human Rights. Nevertheless, the state action is subject to European supervision through the European Court of Human Rights and the necessity of the content-based restrictions must be convincingly established by the contracting states.

Harm is, therefore, a criterion which depends upon various fundamental differences and this is recognized within the jurisprudence of the European Court of Human Rights.[28] Such state-level differences undoubtedly complicate harmonization of laws and approaches at the international level.

A number of issues of concern and subject to regulation at state level will be discussed under separate headings below.

Internet Child Pornography

Harmonization efforts to combat illegal Internet content, even for universally condemned content such as child pornography, have been protracted and are ongoing[29] despite the adoption of several legal instruments including the European Union's Framework Decision on combating the sexual exploitation of children and child pornography,[30] the Council of Europe's Cybercrime Convention 2001[31] which through Article 9 includes a provision on child pornography, the Council of Europe's more recent Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse[32] and the United Nations' Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.[33] These legal instruments require member states to criminalize the production, distribution, dissemination or transmission of child pornography, supplying or making available and the acquisition or possession of child pornography among other child pornography related crimes.

---

26 *Handyside v. UK* (1976), App. No. 5493/72, Ser A vol. 24; *Castells v. Spain* (1992), App. No. 11798/85, Ser. A vol. 236. Note also *Lingens v. Austria*, judgment of 8 July 1986, Series A, No. 103.

27 *Ibid*.

28 See *Handyside v UK*, App. no. 5493/72, Ser A vol.24, (1976) 1 EHRR 737.

29 Rights of the Child: Report submitted by Mr. Juan Miguel Petit, Special Rapporteur on the sale of children, child prostitution and child pornography, E/CN.4/2005/78, 23 December, 2004. Note also the Addendum to this report: E/CN.4/2005/78/Add.3, 8 March, 2005. Note further Akdeniz, Y., *Internet Child Pornography and the Law: National and International Responses*, 2008, Ashgate.

30 Council Framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography (see OJ L 013 20.01.2004, p. 0044-0048), at <http://register.consilium.europa.eu/pdf/en/03/st10/st10748en03.pdf>. For a summary of the Framework Decision see <http://europa.eu/scadplus/leg/en/lvb/l33138.htm>.

31 Convention on Cybercrime, ETS No: 185, at <http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm>.

32 Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, CETS No.: 201

33 Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, New York, 25 May 2000, Fifty-fourth session (97th plenary meeting), Agenda item 116 (a), Distr. General A/RES/54/263, 26 June 2000. Not yet in force (the Optional Protocol will enter into force three months after the date of deposit of the tenth instrument of ratification or accession with the Secretary-General of the United Nations, in accordance with its article 14).

In terms of ratification and implementation, the EU Council Framework Decision came into force in January 2004 and the EU Member States implemented the provisions of the Framework Decision into their nations' laws by January 2006. However, the EU is currently considering to amend the 2004 Framework Decision with a new proposal,[34] and among other issues the EU is for the first time discussing whether to introduce regulations demanding the blocking of access to websites known to carry child pornography as will be discussed later in this report.

At the Council of Europe level, 30 member states (as well as the United States)[35] implemented the Convention provisions into national legislation. Andorra, Monaco, Russia, and San Marino are the member states which have yet to sign the Convention, and 16 Council of Europe member states that signed the convention are yet to ratify. Furthermore, in March 2010, during its 5th annual conference on cybercrime, the Council of Europe called for a worldwide implementation of its Cybercrime Convention to sustain legislative reforms already underway in many countries and a global capacity-building initiative to combat web-based crimes and to enhance trust in information and communication technologies. This could result in further support for the Convention.

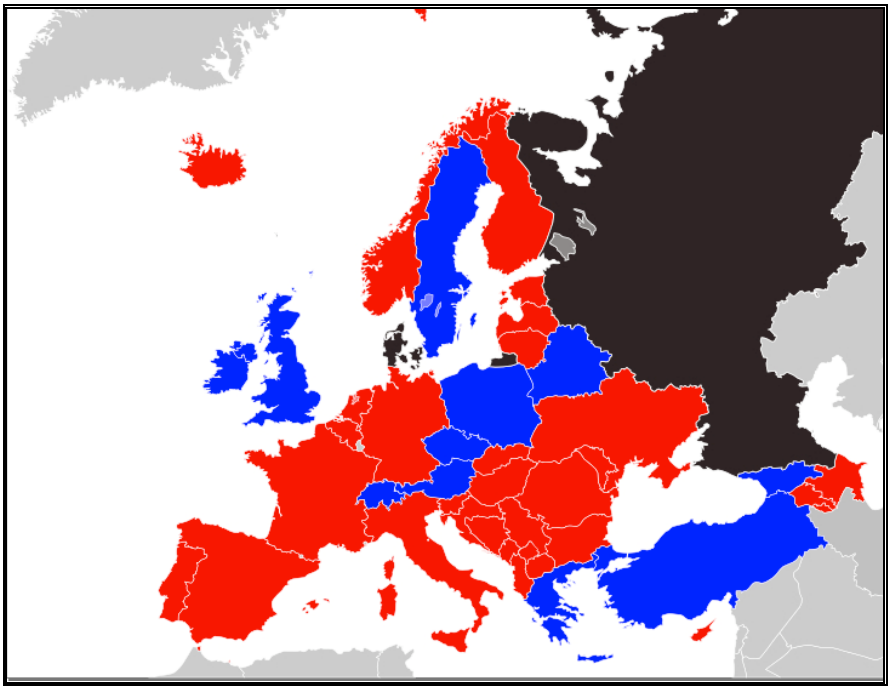

Figure 1: Member states in Red ratified the Convention, member states in blue signed but not ratified the Convention, and member states in black are yet to sign or ratify the Convention.

34 See Proposal for a Council Framework Decision on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA.

35 The full list of member states which ratified the Cybercrime Convention as of **November 2010** are: Albania, Armenia, Azerbaijan, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Denmark, Estonia, Finland, France, Germany, Hungary, Iceland, Italy, Latvia, Lithuania, Moldova, Montenegro, the Netherlands, Norway, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Ukraine, the United States of America,[35] and "the former Yugoslav Republic of Macedonia".

The Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse[36] which was opened to signature in October 2007 came into force in July 2010. So far, 41 contracting states signed the Convention but only nine have ratified it.

At the UN level, the Optional Protocol on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography entered into force on 18 January, 2002. As of October 2010, 118 UN member states signed the Optional Protocol, and 141 members have ratified or acceded to the Optional Protocol.[37]

Racist Content on the Internet

There is strong documented evidence to show that organizations and individuals are using the Internet to disseminate racist content. Following the extreme popularity of free-to-use Web 2.0 based platforms and applications, racist organisations and individuals have started to use platforms such as YouTube and other on-demand video and file sharing and social networking sites such as Facebook and Twitter to disseminate content involving hatred and to dynamically target young people. Furthermore, several controversial publications of a racist nature and publications which encourage violence are currently disseminated through a number of websites, social media platforms, blogs and discussion forums. In March 2010, the Simon Wiesenthal Center announced that[38] there are approximately 11,500 hate- and terrorism-related websites, social network pages, chat forums and micro-blogs. The Center's report stated that they witnessed a 20 percent increase compared to 2009.

However, efforts to harmonize laws to combat racist content have proved to be problematic.[39] Since the finalization of the Cybercrime Convention, the Council of Europe also developed the first Additional Protocol to the Convention on the criminalization of acts of a racist or xenophobic nature committed through computer systems.[40] The Additional Protocol, which came into force in March 2006, requires the signatories to criminalize the dissemination of racist and xenophobic material through computer systems, as well as racist and xenophobic-motivated threat and insult including the denial, gross minimization, approval or justification of genocide or crimes against humanity, particularly those that occurred during the period 1940-45. It also defines the notion of this category of material and establishes the extent to which its dissemination violates the rights of others and criminalizes certain conduct accordingly. Although the Additional Protocol intended to harmonize substantive criminal law in the fight against racism and xenophobia on the Internet, only thirty-four contracting states (including the external supporters Canada and South Africa) have signed the Additional Protocol since it was opened to signature in January 2003. Eighteen signatories have ratified the Additional Protocol as of November 2010.[41]

---

36 CETS No. 201.

37 For details see http://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-11-c&chapter=4&lang=en

38 See the Simon Wiesenthal Center, *Digital Terrorism and Hate Report*, 2010.

39 Akdeniz, Y., *Racism on the Internet*, Council of Europe Publishing, 2010 (ISBN 978-92-871-6634-0); and Akdeniz, Y., "Governing Racist Content on the Internet: National and International Responses," (2007) *University of New Brunswick Law Journal* (Canada), Vol. 56, Spring, 103-161.

40 Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, CETS No.: 189.

41 Albania, Bosnia and Herzegovina, Croatia, Cyprus, Denmark, France, Latvia, Lithuania, Montenegro, Netherlands, Norway, Portugal, Romania, Serbia, Slovenia, Ukraine, and the former Yugoslav Republic of Macedonia.

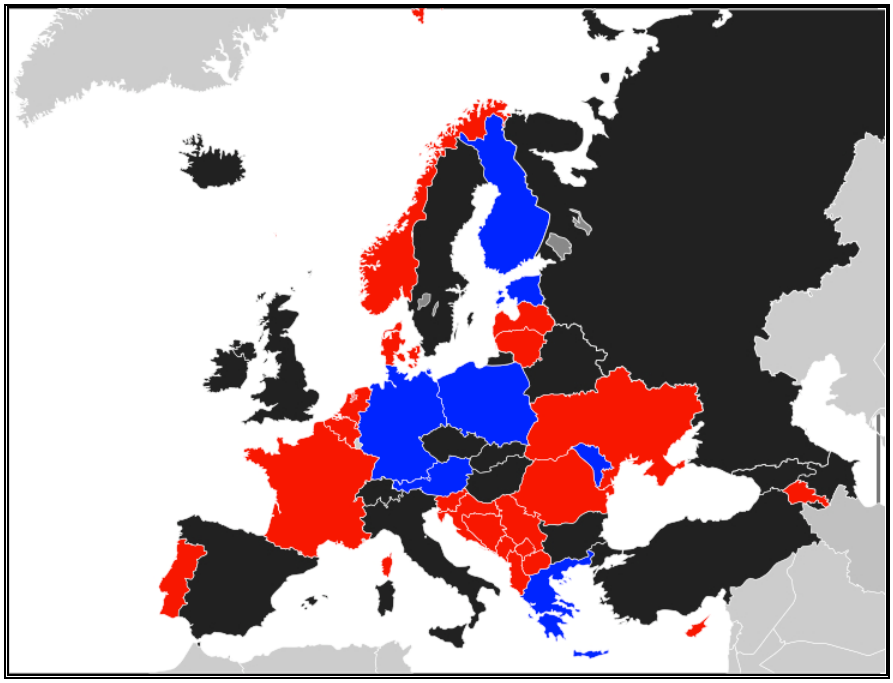

Figure 2: Member states in Red ratified the Additional Protocol (AP), member states in blue signed but not ratified the AP, and member states in black are yet to sign or ratify the AP.

In terms of aligning its policy to combat racism and xenophobia, the European Union adopted a Framework Decision on combating racism and xenophobia on 28 November, 2008.[42] The Framework Decision is designed to ensure that racism and xenophobia are punishable in all EU Member States by effective, proportionate and dissuasive criminal penalties. The Framework Decision includes such crimes as incitement to hatred and violence and publicly condoning, denying or grossly trivializing crimes of genocide, crimes against humanity and war crimes.[43] The specific crimes covered within the Framework Decision also apply to the Internet and the Member States of the European Union had time until 28 November 2010 to transpose the Framework Decision into national law.

At UN level, States Parties to the International Convention on the Elimination of All Forms of Racial Discrimination (ICERD), through Article 4, "condemn all propaganda and all organisations which are based on ideas or theories of superiority of one race or group of persons of one colour or ethnic origin, or which attempt to justify or promote racial hatred and discrimination in any form". Currently, with 173 ratifications by member states as of November 2010,[44] the ICERD provisions remain the most important normative basis upon which international efforts to eliminate racial discrimination could be built.[45] Nonetheless, harmonization has not been established and there remain different interpretations and applications of Article 4. To date, 19 states have entered reservations or interpretative declarations in respect of Article 4.

---

42 Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law, OJ L 328 of 6.12.2008, at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32008F0913:EN:NOT

43 *Ibid*., section 1(d).

44 See Note by the Secretariat, Efforts by the Office of the United Nations High Commissioner for Human Rights for universal ratification of the International Convention on the Elimination of All Forms of Racial Discrimination, E/CN.4/2006/13, 15 February 2006, at http://daccessdds.un.org/doc/UNDOC/GEN/G06/107/92/PDF/G0610792.pdf.

45 See Report of the Committee on the Elimination of Racial Discrimination, Sixty-fourth session (23 February to 12 March 2004) Sixty-fifth session (2-20 August 2004), No: A/59/18, 1 October 2004.

Extremism, Glorification of Violence and Terrorist Propaganda on the Internet

The availability of glorification of violence and terrorist propaganda[46] on the Internet and content which may encourage terrorist activities,[47] such as bomb-making instructions, including the infamous *Anarchist's Cookbook* or the often cited *Encyclopaedia of the Afghan Jihad, The Al-Qaeda Manual*,[48] *The Mujahideen Poisons Handbook*, *The Terrorists Handbook*, *Women in Jihad*, and *Essay Regarding the Basic Rule of the Blood, Wealth and Honour of the Disbelievers* are easily obtainable through the Internet. In certain countries downloading these types of content can potentially lead to a possession charge under terrorism laws. The availability of such content closely associated with terrorist activity triggered policy action at the international level and new laws and policies are being developed to combat the availability of such content on the Internet.

With regard to this issue, the Council of Europe Convention on the Prevention of Terrorism (CETS No. 196) which came into force in June 2007 provides for a harmonized legal basis to prevent terrorism and to counter, in particular, public provocation to commit terrorist offences[49] and recruitment[50] and training[51] for terrorism, including through the Internet. If signed and ratified by the member states of the CoE, the distribution and publication of certain types of content deemed to be facilitating terrorist activity could be criminalized. While 43 member states signed the Convention, only 26 of them ratified it as of November 2010.

Similarly, the EU has been trying since June 2006 to formulate a harmonized policy to combat the terrorist use of the Internet. The European Commission proposed to criminalize the public provocation to commit terrorist offences, recruitment for terrorism and training for terrorism by amending the Framework Decision on combating terrorism.[52] The deadline for transposition by the signatories is 9 December 2010.

Internet Piracy, 3-strikes-out provisions, and the Draft ACTA

---

46 Note articles 5-7 of the Council of Europe Convention on the Prevention of Terrorism (CETS No. 196), which came into force in June 2007.

47 Note "Terror law vague, accused to argue", *The Globe and Mail* (Canada), 30 August 2006 and "Abu Hamza trial: Islamic cleric had terror handbook, court told", *The Guardian*, London, 12 January 2006.

48 The US Department of Justice made available an English version as a PDF document a few years back. See *The Register*, "Download al Qaeda manuals from the DoJ, go to prison?" 30 May 2008, at www.theregister.co.uk/2008/05/30/notts_al_qaeda_manual_case/.

49 For the purposes of this Convention, "public provocation to commit a terrorist offence" means the distribution, or otherwise making available, of a message to the public, with the intent to **incite** the commission of a terrorist offence, where such conduct, whether or not directly advocating terrorist offences, causes a danger that one or more such offences may be committed. See Article 5 of the Council of Europe Convention on the Prevention of Terrorism (CETS No. 196).

50. For the purposes of this Convention, "recruitment for terrorism" means to solicit another person to commit or participate in the commission of a terrorist offence, or to join an association or group, for the purpose of contributing to the commission of one or more terrorist offences by the association or the group. See Article 6 of the Council of Europe Convention on the Prevention of Terrorism (CETS No. 196).

51. For the purposes of this Convention, "training for terrorism" means to provide instruction in the making or use of explosives, firearms or other weapons or noxious or hazardous substances, or in other specific methods or techniques, for the purpose of carrying out or contributing to the commission of a terrorist offence, knowing that the skills provided are intended to be used for this purpose. See Article 7 of the Council of Europe Convention on the Prevention of Terrorism (CETS No. 196).

52 See Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism, Official Journal of the European Union, L 330/21, 09.12.2008.

Predominantly private sector concerns involving the availability and circulation of pirated content have been witnessed in the recent years. The entertainment industry complains that their business has been "decimated by piracy on the Internet."[53] It claims that rather than purchasing copyright-protected content legally, Internet users download large quantities of pirated content. The entertainment industry also argues that piracy not only includes downloading music or movies but also television episodes, software, books, newspapers, magazines, comics and even adult pornography. Live television sports transmission is also subject to piracy through various streaming websites and platforms. The entertainment industry is therefore pressuring governments and international organizations to address the problem of Internet piracy and the distribution of pirated content through the Internet.

While access related limitations have been addressed under Section A of this report, this section will briefly outline the legal measures incorporated to the Draft Anti-Counterfeiting Trade Agreement (ACTA), a multilateral agreement which has the purpose of establishing international standards on intellectual property rights enforcement. The scope of ACTA, among other things, includes copyright infringement on the Internet. The development of ACTA in secrecy has been heavily criticized by civil liberties organizations. Leaked versions of the draft Agreement appeared online prior to an official draft release for discussion in April 2010.

The draft Agreement proposes a notice-based liability regime for online service providers with regard to third-party intellectual property rights infringements. Upon receiving legally sufficient notice of alleged infringement, the online service providers may remove or disable access to infringing material under the draft Agreement. This notice-based procedure included in the draft Agreement as a possible measure, as in the case of the more broad provisions of the EU E-Commerce Directive, "shall not affect the possibility for a judicial or administrative authority, in accordance with the Parties legal system, requiring the service provider to terminate or prevent an infringement, nor does it affect the possibility of the Parties establishing procedures governing the removal or disabling of access to information."[54]

As in the case of the E-Commerce Directive (see below) the Parties to ACTA shall not impose a general monitoring requirement on providers if the notice-based procedures are followed. The proposed measures, however, also include provisions for rights holders to obtain information from online providers on the identity of the relevant subscriber who has allegedly downloaded or distributed infringing content. In March 2010, a European Parliament resolution on the transparency and state of play of the ACTA negotiations[55] stated that

> "any agreement reached by the European Union on ACTA must comply with the legal obligations imposed on the EU with respect to privacy and data protection law, notably as set out in Directive 95/46/EC, Directive 2002/58/EC and the case-law of the European Court of Human Rights and the Court of Justice of the European Union (CJEU)"[56]

---

53 EMI Records (Ireland) Limited, Sony Music Entertainment Ireland Limited, Universal Music Ireland Limited, Warner Music Ireland Limited and WEA International Incorporated vs. UPC Communications Ireland Limited, The High Court (Ireland – Commercial), [2009 No. 5472 P], judgment dated 11 October, 2010.

54 See Article 2.18 [Enforcement Procedures in the Digital Environment] of the Draft ACTA.

55 European Parliament resolution of 10 March 2010 on the transparency and state of play of the ACTA negotiations, Strasbourg, P7_TA(2010)0058, at http://www.europarl.europa.eu/sides/getDoc.do?type =TA&reference=P7-TA-2010-0058&language=EN&ring=P7-RC-2010-0154

56 *Ibid*.

The European Parliament resolution, in order to respect fundamental rights, such as the right to freedom of expression and the right to privacy, while fully observing the principle of subsidiarity, considered that:

> "the proposed agreement should not make it possible for any so-called 'three-strikes' procedures to be imposed, in full accordance with Parliament's decision on Article 1.1b in the (amending) Directive 2009/140/EC calling for the insertion of a new paragraph 3(a) in Article 1 of Directive 2002/21/EC on the matter of the 'three strikes' policy; considers that any agreement must include the stipulation that the closing-off of an individual's Internet access shall be subject to prior examination by a court".[57]

Despite such strong statements, certain states have or started to develop legal measures which are often referred as "**three-strikes**" and provide a "**graduated response**" resulting in restricting or cutting off the user's access to the Internet after the user has allegedly committed three intellectual property infringements and received two warnings. While some political actors consider this "three-strike" approach to dealing with copyright infringement as a legitimate means to addressing the problem, it has been met with reservations and criticism by others who either recognize access to the Internet as a fundamental right or the fact that a considerable amount of copyright infringements on the Internet is committed by children and minors who are often not aware of the legal implications of their action.

So far, three-strikes measures are yet to be put in place in the countries in which they are being developed. It is important to note within this context that a high court in Ireland ruled, by respecting the doctrine of separation of powers and the rule of law, that a court "cannot move to grant injunctive relief to the recording companies against internet piracy, even though that relief is merited on the facts."[58] According to the Irish court "in failing to provide legislative provisions for blocking, diverting and interrupting Internet copyright theft, Ireland is not yet fully in compliance with its obligations under European law. Instead, the only relevant power that the courts are given is to require an Internet hosting service to remove copyright material."[59]

Libel on the Internet

The terms defamation are most commonly referred to in the OSCE participating States' legislation to describe false statements of facts and opinions which harm the reputation of the other person and/or are insulting or offensive.[60] The multi-purpose hybrid Internet, especially with the development of Web 2.0 based technologies and platforms, provides the possibility to any user to publish extensively whether through blogs, micro-blogging platforms such as Twitter, or through social media platforms such as Facebook, and YouTube. This results in the daily turnover of publications on the Internet not being globally and statistically

---

57 *Ibid*.

58 EMI Records (Ireland) Limited, Sony Music Entertainment Ireland Limited, Universal Music Ireland Limited, Warner Music Ireland Limited and WEA International Incorporated vs. UPC Communications Ireland Limited, The High Court (Ireland – Commercial), [2009 No. 5472 P], judgment dated 11 October, 2010.

59 *Ibid*.

60 The Office of the OSCE Representative on Freedom of the Media, *Libel and Insult Laws: A Matrix on Where We Stand and What We Would Like to Achieve*, Vienna, 2005, p. 5.

ascertainable. This user-driven activity can also lead into the publication of defamatory content on such platforms.[61]

OSCE participating States usually regulate defamation through civil or criminal measures and Internet defamation is treated as any other type of publication.

There is a persistent debate over whether Internet Service Providers, hosting companies and Web 2.0 based social media platform operators are primary publishers or only distributors of third-party content. The providers may be the target of defamation claims as secondary parties for publishing or republishing defamatory statements. This is particularly crucial considering that many of the defamatory statements over the Internet come from "anonymous sources". In terms of service provider liability, in most instances liability will only be imposed upon the providers if there is "knowledge and control" over the information which is transmitted or stored by a provider. Based on the "knowledge and control" principle, notice-based takedown procedures have been developed in Europe. For example, the EU Directive on Electronic Commerce[62] provides for limited and notice-based liability with takedown procedures for illegal content, as will be discussed later in this report.

However, by way of contrast it is important to note that U.S.- based service providers have more protection from liability for third-party content regardless of their "knowledge" of it,[63] This issue will also be addressed below under the heading of "D. Licensing and liability related issues."

Unlike in the United States, in many nations notice-based liability measures represent the liability regime for Internet service providers, hosting companies, as well as for social media platforms. While actions against content providers, bloggers or users are usually decided on their merits under state laws, notice-based liability regimes place secondary publishers such as web hosting companies or Internet service providers under some pressure to remove material from their servers without considering whether the allegedly defamatory content is true or whether it is in the public interest. Therefore, there could be a "possible conflict between the pressure to remove material, even if true, and the emphasis placed upon freedom of expression under the European Convention of Human Rights."[64] The final OSCE-wide study will assess this issue further.

Children's Access to Harmful Content over the Internet

Another area which is subject to debate without harmonized solutions involves the availability of content deemed to be harmful to minors. The main (but not exclusive) concern has been the availability of sexually explicit (pornographic) content over the Internet. While state level laws generally do not criminalize possession and viewing for adults, states, however, remain concerned about children's access to sexually explicit content. Variations do certainly exist in terms of how to tackle the problem of children accessing sexually explicit content or any other types of content deemed to be harmful.

---

61 On YouTube, for example, 35 hours of video material are uploaded every minute. See http://youtube-global.blogspot.com/2010/11/great-scott-over-35-hours-of-video.html

62. 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, Official Journal of the European Communities, vol. 43, OJ L 178 17 July 2000 p. 1.

63 Note section 230(c)(1) of the Communications Decency Act. Note also the decision in *Zeran v. America Online Inc.*, 129 F.3d 327 at 330 (4th Cir. 1997), *certiorari* denied, 48 S. Ct. 2341 (1998).

64 Law Commission (Engşand and Wales), Defamation and the Internet: A Preliminary Investigation, (Scoping Paper: Dec 2002), at http://www.lawcom.gov.uk/docs/defamation2.pdf.

Regarding the safer use of the Internet by children, self-regulatory initiatives involving the development of end-user filtering mechanisms, as well as education and the strengthening of media and textual Internet literacy, offer solutions. For example, the EU Action Plan on safer use of the Internet advocates measures to increase awareness among parents, teachers, children and other consumers of available options to help these groups use the networks safely by choosing the right control tools. In October 2008, the European Commission's Safer Internet programme was extended for the 2009-2013 period with an aim to improve safety for children surfing the Internet, promote public awareness, and create national centres for reporting illegal online content with a €55 million budget.[65] Encouraging self-regulatory solutions are also supported at the Council of Europe level. The Declaration on Freedom of Communication on the Internet adopted by the Committee of Ministers of the Council of Europe on 28 May 2003 notably encouraged self-regulation and co-regulatory initiatives regarding Internet content. Similar recommendations were made in Council of Europe Recommendation Rec(2001)8 on self-regulation concerning cyber-content.[66]

Regarding the protection of children from harmful content, the Council of Europe's Committee of Ministers recommended in July 2009[67] that member states of CoE, in co-operation with private sector actors and civil society, develop and promote coherent strategies to protect children against content and behaviour carrying a risk of harm. The needs and concerns of children online, according to a Parliamentary Assembly Recommendation on the promotion of Internet and online media services appropriate for minors[68] should be addressed without undermining the benefits and opportunities offered to them on the Internet.

The Committee of Ministers also recommended that safe and secure spaces similar to walled gardens should be developed for children on the Internet. While doing so the Committee of Ministers noted that "every action to restrict access to content is potentially in conflict with the right to freedom of expression and information as enshrined in Article 10 of the European Convention on Human Rights."[69]

Therefore, while the need to protect children from harmful content was highlighted, and the development of "walled gardens or gated communities – which are accessible to an identifiable group of users only"[70] as well as the development of a pan-European trustmark and labelling system[71] was encouraged, the CoE Committee did not recommend state level

---

65 European Parliament legislative resolution of 22 October 2008 on the proposal for a decision of the European Parliament and of the Council establishing a multiannual Community programme on protecting children using the Internet and other communication technologies (COM(2008)0106 – C6-0092/2008 – 2008/0047(COD)).

66 Council of Europe Rec(2001)8, 5 September 2001.

67 Recommendation CM/Rec(2009)5 of the Committee of Ministers to member states on measures to protect children against harmful content and behaviour and to promote their active participation in the new information and communications environment, adopted by the Committee of Ministers on 8 July 2009 at the 1063rd meeting of the Ministers' Deputies.

68 Parliamentary Assembly Recommendation 1882 (2009) on the promotion of Internet and online media services appropriate for minors, adopted by the Assembly on 28 September 2009 (28th Sitting). See http://assembly.coe.int/main.asp?Link=/documents/adoptedtext/ta09/erec1882.htm

69 See Guidelines 7, Recommendation CM/Rec(2009)5 of the Committee of Ministers.

70 See Paragraph 11 of the Recommendation 1882 (2009), The promotion of Internet and online media services appropriate for minors.

71 To be prepared in full compliance with the right to freedom of expression and information in accordance with Article 10 of the European Convention on Human Rights. See Guidelines 12, Recommendation CM/Rec(2009)5 of the Committee of Ministers.

blocking or filtering mechanisms for the protection of children. Similarly, the Committee stated that "online content which is not labelled should not however be considered dangerous or less valuable for children, parents and educators."[72] In terms of the use of the filters, the Steering Committee on Media and New Communication Services (CDMC), in response to the Parliamentary Assembly Recommendation on the promotion of Internet and online media services appropriate for minors recalled that

> "children's access to filters should be age appropriate and "intelligent" as a means of encouraging access to and confident use of the Internet and as a complement to strategies which tackle access to harmful content. The use of such filters should be proportionate and should not lead to the overprotection of children in accordance with Recommendation CM/Rec(2008)6 on measures to promote the respect for freedom of expression and information with regard to Internet filters."[73]

Some of the mechanisms currently discussed for protecting children from harmful content such as blocking and filtering will be assessed further in this preliminary report as well as in the final report as the issues surrounding protection of children sometimes serves as a catalyst for the development of policies associated with state level blocking and filtering without distinguishing between the rights of adult and child users.

C. Blocking, Filtering, and Content Removal

Based on the limited effectiveness of state laws, and lack of harmonization at the international level (despite some efforts at regional level) a number of states started to introduce policies to block access to Internet content and websites deemed illegal and which are often situated outside their legal jurisdiction. In short, the new trend in Internet regulation seems to be blocking access to content if state authorities are not in a position to reach the perpetrators or criminals for prosecution or if their request for removal or take down of such content is rejected or ignored by hosting or content providers outside their jurisdiction.

However, blocking policies are not always subject to due process principles, decisions are not necessarily taken by the courts of law and often administrative bodies or Internet hotlines run by the private sector unilaterally decide which content or website should be subject to blocking. Often blocking policies lack transparency, the administrative bodies lack accountability and appeal procedures are either not in place or not functioning. Therefore, increasingly, the compatibility of blocking action is questioned not only with regard to the fundamental right of freedom of expression but also with regard to rule of law principles.

EU Perspectives on Blocking Access to Allegedly Illegal Content

The development of policies and measures to detect misuse of the Internet by extremist websites, and to enhance co-operation of states against terrorist use of the Internet was included within the context of the European Union's May 2006 revised Action Plan on Terrorism.[74] The adoption of "legal measures obliging Internet service providers to remove or

---

72 See Guidelines 13, Recommendation CM/Rec(2009)5 of the Committee of Ministers.

73 See Recommendation 1882 (2009), The promotion of Internet and online media services appropriate for minors. Reply from the Committee of Ministers, adopted at the 1088th meeting of the Ministers' Deputies (16 June 2010 - Doc. 12297).

74 Council of the European Union, *Revised Action Plan on Terrorism*, 10043/06, Brussels, 31 May, 2006.

disable access to the dissemination of terrorist propaganda they host"[75] was considered within the context of the revised Action Plan. However, this policy option has been ruled out during the Impact Assessment work done by the European Commission with regards to the proposal for a Council Framework Decision amending Framework Decision 2002/475/JHA on combating terrorism.[76]

Speedy Re-apparition of Websites and Inefficiency of Blocking

The Commission ruled out "encouraging blocking through the industry's self-regulation or through agreements with industry, without the previous adoption of legal measures outlawing the dissemination of terrorist propaganda and terrorist expertise."[77] The European Commission cited "the issue of the speedy re-apparition of websites that have been closed down" as the main reason for not recommending a blocking policy with regards to the dissemination of terrorist propaganda over the Internet. The Commission argued that blocking policies are ineffective as in most cases blocked websites reappear under another name outside the jurisdiction of the European Union in order to avoid the eventuality of being closed down or blocked once more.[78] The Commission also acknowledged that existing methods of filtering can be circumvented,[79] and they are designed specifically for websites and are not capable of blocking the distribution of objectionable content through other Internet services such as P2P networks.

The European Commission in its assessment concluded that the removal or disabling access to terrorist propaganda or terrorist expertise by Internet service providers hosting such information, without the possibility to open an investigation and prosecute the one responsible behind such content appears inefficient. The Commission reached the conclusion that the dissemination of such content would only be hindered rather than eliminated.[80] The Commission expressed that

> "the adoption of blocking measures necessarily implies a restriction of human rights, in particular the freedom of expression and therefore, it can only be imposed by law, subject to the principle of proportionality, with respect to the legitimate aims pursued and to their necessity in a democratic society, excluding any form of arbitrariness or discriminatory or racist treatment."[81]

The European Commission also expressed concern regarding the cost of implementing blocking and filtering systems by ISPs and concluded that the implementation of such a system would have direct economic impact not only on ISPs but also on consumers.[82]

Furthermore, the EU Check the Web (Monitoring) Project was launched in May 2006 by the German EU Council Presidency with the aim of intensifying EU co-operation on monitoring and analyzing Internet sites in the context of counter-terrorism, and to prevent terrorist use of

---

75 European Commission Staff Working Document, Accompanying document to the proposal for a Council Framework Decision amending Framework Decision 2002/475/JHA on combating terrorism: Impact Assessment, 14960/07 ADD1, Brussels, 13 November, 2007, para 4.2, pp 29-30.

76 *Ibid*.

77 Ibid.

78 See *ibid*. See further Communication from the Commission to the European Parliament, the Council and the Committee of the Regions "Towards a general policy on the fight against cyber crime" of 22 May, 2007 - COM(2007) 267.

79 *Ibid*., p 41.

80 See further European Commission Staff Working Document, section 5.2, pp 41-42.

81 *Ibid*., p 29.

82 *Ibid*, p 42-45.

the Internet. The project carried out by Europol monitors websites advocating terrorism (mainly Islamist extremist terrorism). Initial proposals for the Check the Web Project considered blocking as an option, and it was stated that "only a rigorous effort to fight terrorist use of the Internet can strike at the backbone of terrorism. To do so, numerous Internet sites in a wide variety of languages must be monitored, evaluated and, if necessary, blocked or closed down."[83] However, partially declassified documents in relation to the EU Check the Web Project state that "Member States will not be obliged to monitor, interrupt or shut down specific Internet sites"[84] in the fight against terrorist use of the Internet. Therefore, blocking access to websites and Internet content is not a common policy adopted within the European Union region, and there are no EU policies actively encouraging blocking access to websites.[85]

Blocking Considered by the EU with regards to Combating Child Pornography

However, recently, the European Commission – in view of amending its policy framework with regards to combating the sexual abuse, sexual exploitation of children and child pornography – proposed to have EU-wide mechanisms to block access from the Union's territory to Internet websites identified as containing or disseminating child pornography.[86] The draft provision[87] would require Member States to take necessary measures to enable the competent judicial or police authorities to order or obtain the blocking of access to Internet websites containing or disseminating child pornography, subject to adequate safeguards. Such safeguards according to the draft provisions would in particular "ensure that the blocking is limited to what is necessary, that users are informed of the reason for the blocking and that content providers are informed of the possibility of challenging it."[88] In November 2010, the Civil Liberties, Justice and Home Affairs Committee of the European Parliament doubted the effectiveness of blocking measures during a debate of the draft Council Framework Decision.[89]

Compatibility of blocking with ECHR Questioned

While this blocking measure regarding child pornography was proposed, a European Commission Staff Working Document referred to the risks of blocking access to content without a legal basis, and emphasized that in order to respect fundamental rights such as the

---

83 Note from the German Delegation to the Article 36 Committee, Proposals of the German Delegation regarding EU co-operation to prevent terrorist use of the Internet ("Check the Web"), 9496/06 LIMITE, ENFOPOL 96 JAI 261, 18 May 2006

84 Council of the European Union, document no. 13930/06 RESTREINT UE, 13930/06, EXT 2, ENFOPOL 169, Brussels, 10 November, 2008, Conclusions of the Kick-off conference "Check the Web" - Berlin, 26-27 September 2006.

85 The Commission, however, proposed to criminalize the public provocation to commit terrorist offences, recruitment for terrorism and training for terrorism by amending the Framework Decision on combating terrorism. It is expected that the amendments will take place during 2008. See Proposal for a Council Framework Decision amending Framework Decision 2002/475/JHA on combating terrorism, 2007/0236 (CNS), COM(2007) 650 final, Brussels, 6 November, 2007, at <http://ec.europa.eu/commission_barroso/frattini/archive/COM(2007)650%20EN.pdf>.

86 See Proposal for a Council Framework Decision on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA, paragraph 12 and draft Article 18 entitled Blocking access to websites containing child pornography.

87 *Ibid*.

88 *Ibid*.

89 European Parliament Civil Liberties, Justice and Home Affairs Committee, Press Release: Child pornography: MEPs doubt effectiveness of blocking web access, 22.11.2010, at http://www.europarl.europa.eu/sides/getDoc.do?type=IM-PRESS&reference=20101115IPR94729&secondRef=0&language=EN The Committee will vote on its report on the draft Council Framework Decision in February 2011.

right to freedom of expression, any interference would need to be prescribed by law and be necessary in a democratic society.[90] The European Commission Staff Working Document argued that the "proportionality of the measure would be ensured, as the blocking would only apply to specific websites identified by public authorities as containing such material."[91] The Commission document also warned that there is "a risk, depending on the technology used, that the systems in place may occasionally block legitimate content too"[92] which raises further concerns of proportionality.

CoE Perspectives on Blocking Access to Allegedly Illegal Content

The content specific crimes within the Cybercrime Convention and the Additional Protocol, namely, the offences related to child pornography (Article 9), and the dissemination of racist and xenophobic material through computer systems (AP, Article 3), as well as offences related to child pornography (Article 20) within the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse do not include any blocking provisions. Similarly the provisions of the Convention on the Prevention of Terrorism do not provide for blocking, and instead – as in any offline environment – cover the criminal activity of dissemination and publication.

Access and hosting providers are protected under the provisions of these CoE Conventions.[93] Serving as a conduit, or for hosting a website or newsroom containing above-mentioned material would not lead to criminal liability for the service providers without the required intent under domestic law.[94] Moreover and it is important to stress, as provided by the EU E-Commerce Directive, a service provider is not required to monitor conduct to avoid criminal liability under the CoE provisions.

Regarding the deployment and use of blocking and filtering systems the CoE Cybercrime Convention Committee (T-CY) recognized the legal difficulties that could arise when attempting to block certain sites with illegal content.[95] More importantly, a CoE Committee of Ministers Recommendation of 2007[96] called upon the member states to promote freedom of communication and creation on the Internet regardless of frontiers, in particular by not subjecting individuals to any licensing or other requirements having a similar effect, nor any general blocking or filtering measures by public authorities, or restrictions that go further than those applied to other (including traditional) means of content delivery.[97]

---

90 Commission Staff Working Document, Accompanying document to the proposal for a Council Framework Decision on combating the sexual abuse , sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA, Impact assessment, 8150/09 ADD 1, Brussels, 30 March, 2009, p 30.

91 *Ibid*.

92 *Ibid*.

93 Note the Convention on Cybercrime, ETS No. 185, Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, CETS No. 201, Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, CETS No. 189, Convention on the Prevention of Terrorism, CETS No. 196.

94 Council of Europe, Committee of Ministers, Explanatory Report of the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, (2002) at para. 25, at <http://conventions.coe.int/Treaty/en/Reports/Html/189.htm>.

95 CoE Cybercrime Convention Committee (T-CY), 2nd Multilateral Consultation of the Parties, Strasbourg, 13 and 14 June, 2007, Strasbourg, 15 June, 2007, T-CY (2007) 03, para. 29.

96 CM/Rec(2007)16 of November, 2007.

97 Recommendation CM/Rec(2007)16 of the Committee of Ministers to member states on measures to promote the public service value of the Internet: Adopted by the Committee of Ministers on 7 November, 2007 at the 1010th meeting of the Ministers' Deputies.

In March 2008, the Committee of Ministers in a new Recommendation[98] recalled the Declaration of the Committee of Ministers on Freedom of Communication on the Internet of 28 May, 2003,[99] which stressed that public authorities should not, through general blocking or filtering measures, deny access to the public information and other communication on the Internet regardless of frontiers.[100] The Committee of Ministers in its March 2008 Recommendation stated that

> "there is a tendency to block access to the population to content on certain foreign or domestic web sites for political reasons. This and similar practices of prior State control should be strongly condemned."[101]

Equally, the 2003 Declaration emphasized that exceptions must be allowed for the protection of minors, and states can consider the installation of filters for the protection of minors, in particular in places accessible to them such as schools or libraries.[102]

Furthermore, CoE Recommendation of March 2008 stated that any intervention by member states that forbids access to specific Internet content may constitute a restriction on freedom of expression and access to information in the online environment. Any such restriction would have to fulfil the conditions in Article 10(2) of the European Convention on Human Rights and the relevant case law of the European Court of Human Rights. The Recommendation noted that the voluntary and responsible use of Internet filters (products, systems and measures to block or filter Internet content) can promote confidence and security on the Internet for users, in particular for children and young people, while also noting that the use of such filters can seriously impact on the right to freedom of expression and information as protected by Article 10 of the ECHR.

The Guidelines provided within the March 2008 Recommendation[103] stated that the Internet users should have the possibility to challenge the blocking decisions or filtering of content and be able to seek clarifications and remedies.[104] The Guidelines called upon the member states to refrain from filtering Internet content in electronic communications networks operated by public actors for reasons other than those laid down in Article 10(2) of the ECHR as interpreted by the European Court of Human Rights.

The Guidelines further called upon the member states to guarantee that nationwide general blocking or filtering measures are only introduced if the conditions of Article 10(2) of the ECHR are fulfilled. According to the Guidelines, such action by the state should only be taken if filtering activity concerns specific and clearly identifiable content, a competent national authority has taken a decision on its illegality and the decision can be reviewed by an

---

98 Recommendation CM/Rec(2008)6 of the Committee of Ministers to member states on measures to promote the respect for freedom of expression and information with regard to Internet filters: Adopted by the Committee of Ministers on 26 March, 2008 at the 1022nd meeting of the Ministers' Deputies.

99 Freedom of communication on the Internet, Declaration adopted by the Council of Europe Committee of Ministers on 28 May, 2003 at the 840th meeting of the Ministers' Deputies.

100 *Ibid*, Principle 3.

101 *Ibid*.

102 Note however issues surrounding filtering through libraries: IFLA World Report 2010, August 2010, at http://www.ifla-world-report.org

103 Recommendation CM/Rec(2008)6 of the Committee of Ministers to member states on measures to promote the respect for freedom of expression and information with regard to Internet filters: Adopted by the Committee of Ministers on 26 March, 2008 at the 1022nd meeting of the Ministers' Deputies.

104 *Ibid*, Guideline I.

independent and impartial tribunal or independent regulatory body in accordance with the requirements of Article 6 of the ECHR. The Guidelines also called upon the states to ensure that all filters are assessed both before and during their implementation to ensure that the effects of the filtering are proportionate to the purpose of the restriction and thus necessary in a democratic society in order to avoid unreasonable blocking of content.

According to the CoE Guidelines, the universal and general blocking of offensive or harmful content for users who are not part of a specific vulnerable group (such as children) which a filter has been activated to protect should be avoided. This recommendation therefore distinguishes between the adults' use of the Internet and vulnerable groups' use of the Internet. Therefore, the need to limit children's access to certain specific types of Internet content deemed as harmful should not also result in blocking adults' access to the same content available on the Internet.

D. Licensing and liability related issues

Regarding the role that can be played by the information service providers industry including the Internet Service Providers, hosting companies, Web 2.0 based social media platforms and search engines, it is recognized that the service providers can contribute to the development of self-regulatory mechanisms such as industry-wide codes of conduct as well as hotlines to report illegal content.

However, although no service provider controls third-party content or all of the technical backbones of the Internet, the role service providers play in providing access has made them visible targets for the control of content on the Internet. Their responsibility as gateways to communication to the public has been brought into question, especially in relation to the availability and distribution of illegal content such as child pornography, pirated digital content, as well as racist content, terrorist propaganda and defamation. Furthermore, policy makers often consider whether service providers should be compelled to block access to certain websites and content, or whether they should be compelled to remove certain types of content from their servers.

Notice-based Liability and Takedown Procedures

Regarding liability for carrying third-party content, in most instances liability will only be imposed upon service providers (including Internet Service Providers, hosting companies, Web 2.0 based social media platforms and search engines) if there is "**knowledge and control**" over the information which is transmitted or stored by a service provider. Based on the "knowledge and control" theory notice-based liability and takedown procedures have been developed in Europe. For example, the EU Directive on Electronic Commerce[105] provides a limited and notice-based liability with takedown procedures for illegal content.

The EU Directive suggested that "it is in the interest of all parties involved in the provision of information society services to adopt and implement procedures"[106] to remove and disable access to illegal information. As far as hosting issues by information society service providers are concerned, Article 14(1) of the e-Commerce Directive required Member States to:

---

105. 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, Official Journal of the European Communities, vol. 43, OJ L 178 17 July 2000 p. 1.

106. Ibid.

> "ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:
> (a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or
> (b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information."

Therefore, the service providers based in the EU are not immune from prosecution and liability and they are required to act expeditiously "upon obtaining actual knowledge" of illegal activity[107] or content "to remove or to disable access to the information concerned".[108] Such removal or disabling of access "has to be undertaken in the observance of the principle of freedom of expression and of procedures established for this purpose at national level"[109]. Under the Directive, "notice" has to be specific and may be given by an individual complainant or by a self-regulatory hotline. In some states the notice may only be given by law-enforcement agencies or provided through court orders. However, termination or prevention of an infringement is also possible by a court or administrative authority order. Article 14(3) states that the provisions of Article 14 do not "affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information". It was decided that the notice and takedown procedures would not be regulated in the Directive itself.[110] Rather, the Directive, through Recital 40 and Article 16, encouraged self-regulatory solutions and procedures to be developed by the Internet industry to implement and bring into action the "notice and takedown procedures".[111]

In addition to the notice-based limited liability exceptions, the Directive prevents EU Member States from imposing a monitoring obligation on service providers only with respect to obligations of a general nature. However, "this does not concern monitoring obligations in a specific case, and in particular, does not affect orders by national authorities in accordance with national legislation".[112] Under Article 15, the Directive specifically requires Member States not to "impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor impose a general obligation actively to seek facts or circumstances indicating illegal activity". However, Member States "may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request".[113]

---

107. Note the decision of the European Court of Justice with regards to this issue in the case of *Google France and Google Inc. et al. v Louis Vuitton Malletier et al*., Judgment (23 March, 2010) in Joined Cases C-236/08 to C-238/08, OJ C 134 of 22.05.2010, p.2.
108. Ibid., para. 46.
109. Ibid.
110. See Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee – First report on the application of Directive 2000/31/EC on electronic commerce), COM(2003) 702 final, Brussels, 21 November 2003, at http://europa.eu.int/eur-lex/en/com/rpt/2003/com2003_0702en01.pdf, section 4.7.
111. Of those member states which have transposed the directive, only Finland has included a legal provision setting out a notice and takedown procedure concerning copyright infringements only. This information has been taken from the above-mentioned Commission Report: COM(2003) 702 final.
112. Ibid., para. 47.
113. Article 14(2).

A European Commission analysis of work on notice and takedown procedures published in 2003 claimed that "though a consensus is still some way off, agreement would appear to have been reached among stake holders in regards to the essential elements which should be taken into consideration".[114] A further review was subsequently commissioned in 2007 and revealed all but harmonized implementation policies by stating that "the manner in which courts and legal practitioners interpret the E-Commerce-Directive in the EU's various national jurisdictions reveals a complex tapestry of implementation."[115]

Some further studies showed that ISPs based in Europe tend to remove and take down content without challenging the notices they receive. A Dutch study claimed that "it only takes a Hotmail account to bring a website down, and freedom of speech stands no chance in front of the cowboy-style private ISP justice".[116] In 2010, the European Commission announced that it had found, through its contacts with various stakeholders, that the interpretation of the provisions concerning the liability of intermediaries is frequently considered necessary towards solving problems, and subsequently launched a consultation.[117]

Furthermore, a CoE Parliamentary Assembly Recommendation on the promotion of Internet and online media services appropriate for minors[118] recommends that the Committee of Ministers "initiate work towards ensuring greater legal responsibility of Internet service providers for illegal content, whether or not this originates from third parties or users,"[119] and that this work may require the drafting of a new additional protocol to the Convention on Cybercrime. However, since this call no action has been taken at the CoE level to draft such a new additional protocol.

While European policy is based on a limited liability regime, it needs to be mentioned that a contrasting approach has been adopted in the USA. In short, the US based service providers are immune from liability for third-party content regardless of their "knowledge" of it. Section 230(c)(1) of the Communications Decency Act provides that "no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider".[120] Section 230 was considered and tested

---

114. See report from the Commission to the European Parliament, the Council and the European Economic and Social Committee – First report on the application of Directive 2000/31/EC on electronic commerce, COM(2003) 702 final, Brussels, 21.11.2003, at http://europa.eu.int/eur-lex/en/com/rpt/2003/com2003_0702en01.pdf, section 4.7.

115 See Study on the Liability of Internet Intermediaries, Markt/2006/09/E (Service Contract ETD/2006/IM/E2/69), November 2007, p. 12.

116. Nas, S., (Bits of Freedom), The Multatuli Project: ISP Notice & take down, 2004, at www.bof.nl/docs/researchpaperSANE.pdf. Note also Ahlert, C., Marsden, C. and Yung, C., "How 'Liberty' Disappeared from Cyberspace: The Mystery Shopper Tests Internet Content Self-Regulation", at http://pcmlp.socleg.ox.ac.uk/text/liberty.pdf.

117 Public consultation on the future of electronic commerce in the internal market and the implementation of the Directive on Electronic commerce (2000/31/EC). Responses to the Questionnaire were due by early November 2010.

118 1882 (2009).

119 *Ibid*, para 16.6., at http://assembly.coe.int/main.asp?Link=/documents/adoptedtext/ta09/erec1882.htm

120. Communications Decency Act, 47 U.S.C. (1996). Section 230(e)(2) defines "interactive computer service" as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions". Section 230(e)(3) defines "information content provider" as "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service". See however, the different policy established for copyright infringement with the passage of the *Digital Millenium Copyright Act of 1998*, Pub. L. No. 105-304, 112 Stat. 2860.

by the Fourth Circuit Court of Appeals in *Zeran v. America Online Inc.*, a defamation case where the court held that "by its plain language, section 230 created a federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service".[121] Nor did the fact that the provider had notice of the transmission of wrongful material prevent the operation of this immunity in the *Zeran* case. On the other hand, some similarities do exist with the EU regime through the Digital Millennium Copyright Act 1998 (DMCA)[122] which is the only U.S. legislation that provides a notice-based liability system for service providers within the context of intellectual property infringements. Section 512(c) of the DMCA entitled limitations on liability relating to material online provides a "safe harbor" for U.S.-based service providers and states that a provider shall not be liable for infringement of copyright if the provider

> (A)
> (i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing;
> (ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or
> (iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;
> (B) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity; and
> (C) upon notification of claimed infringement as described in paragraph (3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity.[123]

The Formation of Internet Hotlines for Reporting Allegedly Illegal Content

In addition to notice-based liability systems, hotlines to report allegedly illegal Internet content have been developed in Europe. The majority of the current hotlines try to tackle the problem of child pornography and racist content. However, according to a EuroBarometer Survey of 2008, reporting to the hotlines seems to be low, and users seem to prefer to report illegal content they come across to the police rather than to the hotlines.[124] The survey results seem to indicate a low public awareness of the existence and purpose of these hotlines. [125]

Although hotlines could potentially play an important role in relation to illegal Internet content, there remain significant question marks in terms of their operation. Hotlines are often criticized as there remain serious concerns regarding the "policing" role such organizations

---

121. *Zeran v. America Online Inc.*, 129 F.3d 327 at 330 (4th Cir. 1997), *certiorari* denied, 48 S. Ct. 2341 (1998). The plaintiff's claim, which arose out of a false bulletin board posting that the plaintiff was selling t-shirts with offensive messages about the Oklahoma City bombing, was framed as one for negligence in failing to remove the posting, but the court said that the allegations were in substance indistinguishable from a "garden variety defamation action": 129 F.3d 327 at 332.

122 Digital Millenium Copyright Act (H. R. 2281) 1998.

123 Note the joint cases of *Viacom vs. YouTube and Google; The Football Association Premier League vs. YouTube and Google*, US District Court, Southern District of New York, decided 23.06.2010 (Case 1:07-cv-02103-LLS). See generally https://www.eff.org/cases/viacom-v-youtube for further information about the case.

124 EuroBarometer Survey 2008, Summary Report, available through http://ec.europa.eu/information_society/activities/sip/eurobarometer/index_en.htm.

125 The EuroBarometer Survey 2008 was conducted in October 2008 with approximately 12 750 randomly selected parents of children aged 6-17 years old who were interviewed in the 27 EU Member States. 92% "thought of the police when asked how they would report illegal or harmful content seen on the Internet". Only four out of 10 parents (38%) said they would report such content to a hotline set up for this purpose and one-third mentioned non-profit or other associations.

play. Many maintain that decisions involving illegality should remain a matter for courts of law rather than hotline operators. It is argued that their operations might lack transparency and can "violate due process concepts that are also enshrined in international, regional, and national guarantees around the world".[126] This problem was recognised in the Martabit report to the UN which stated that "while encouraging these initiatives, States should ensure that the due process of law is respected and effective remedies remain available in relation to measures enforced".[127]

Furthermore, leaked "child pornography" blocking blacklists maintained by hotlines from Finland,[128] Denmark,[129] and Italy[130] (as well as from China,[131] Thailand,[132] Australia,[133]) that were published on Wikileaks have demonstrated that most of the hotlines also censor adult pornographic content and even political content. Secrecy and unaccountability of such private hotlines lead into blocking and censorship of content which is not deemed to be illegal. In the absence of openness, and transparency of the work of the hotlines as well as the secrecy surrounding the blocking criteria and the list of blocked websites, concerns will continue to exist about the work of such hotlines.

Preliminary Conclusions

Having addressed issues that will be analyzed further in the final version of the study, which will be based on the responses received from the OSCE participating States to the questionnaire distributed on 23 September, 2010,[134] this report naturally can draw few preliminary conclusions which are detailed below.

Participating States' Laws should respect OSCE commitments and other international human rights principles

Regulation of the Internet should respect OSCE commitments, especially the governmental duty to uphold independence and pluralism of the media, and the free flow of information, as defined in Decision No. 193 of the Permanent Council of the OSCE, 5 November 1997, and constantly developed ever since. State laws with regards to Internet content should also be in

---

126 Per Professor Nadine Strossen, from an ACLU Press Release, "ACLU Joins International Protest Against Global Internet Censorship Plans", 9 September 1999, at www.aclu.org/news/1999/n090999a.html.

127 Report of the Intergovernmental Working Group on the effective implementation of the Durban Declaration and Programme of Action on its fourth session (Chairperson-Rapporteur: Juan Martabit (Chile)), E/CN.4/2006/18, 20 March 2006, at http://daccessdds.un.org/doc/UNDOC/GEN/G06/119/23/PDF/G0611923.pdf, at para. 47.

128 Wikileaks, "797 domains on Finnish Internet censorship list, including censorship critic, 2008," 05 January, 2009, at <http://www.wikileaks.com/wiki/797_domains_on_Finnish_Internet_censorship_list%2C_including_censorship_critic%2C_2008>.

129 Wikileaks, "Denmark: 3863 sites on censorship list," February, 2008, at <http://wikileaks.org/wiki/Denmark:_3863_sites_on_censorship_list%2C_Feb_2008>.

130 Wikileaks, "Italian secret internet censorship list, 287 site subset, 21 June, 2009, at <http://wikileaks.org/wiki/Italian_secret_internet_censorship_list%2C_287_site_subset%2C_21_Jun_2009>.

131 Wikileaks, "China: censorship keywords, policies and blacklists for leading search engine Baidu, 2006-2009," 02 May, 2009, at <http://www.wikileaks.com/wiki/China:_censorship_keywords%2C_policies_and_blacklists_for_leading_search_engine_Baidu%2C_2006-2009>.

132 Wikileaks, "Thailand official MICT censorship list," 20 December, 2008, at <http://wikileaks.org/wiki/Thailand_official_MICT_censorship_list%2C_20_Dec_2008>.

133 Wikileaks, "Leaked Australian blacklist reveals banned sites," 19 March, 2009, at <http://wikileaks.org/wiki/Leaked_Australian_blacklist_reveals_banned_sites>.

134 See Appendix I.

conformity with other international human rights principles, especially freedom of expression and privacy of communications.

The European Court of Human Rights has made clear that "freedom of political debate is at the very core of the concept of a democratic society which prevails throughout the Convention".[135] Regarding content-based restrictions, the state response should be proportional, correspond to a "pressing social need",[136] and be in line with the requirements of democracy.[137] The necessity for restricting the right to speak must be convincingly established to be compatible with international human rights standards.

Internet Access and Net Neutrality

As access to the Internet remains the prerequisite to be part of and take part in the Information Society, access to the Internet is one of the basic prerequisites to the right to freedom of expression and the right to impart and receive information regardless of frontiers. As such, access to the Internet is a fundamental human right. OSCE participating States, as well as international organizations, should continue to work to close the digital divide and provide affordable Internet access to all their citizens. While doing so, network neutrality should be respected and measures taken regarding end-users' access to or use of services and applications through the Internet should respect the fundamental rights and freedoms guaranteed by international human rights principles, especially freedom of expression and privacy of communications.

Blocking is an inadequate method to combat illegal content

Although the criminalization of certain types of content is encouraged through the policies of a number of international organizations, as shown in this report, it has to be stressed that neither the EU nor the CoE encourage or regard blocking access to websites as a feasible solution to counter criminal use of the Internet. In fact, serious concerns have been raised regarding adoption of state-level blocking and filtering policies. Blocking of content as a potential solution to fight serious crimes has been found to be inadequate and was dismissed by the European Union.[138]

Blocking access to content indefinitely could also result to "prior restraint". Although the European Court of Human Rights does not prohibit the imposition of prior restraints on publications, the dangers inherent in prior restraints are such that they call for the most careful scrutiny on the part of the European Court.[139] This is especially the case as far as the press is concerned, for news is a perishable commodity and to delay its publication, even for a short period, may well deprive it of all its value and interest.[140] The same principles must also apply

---

135 *Lingens v. Austria*, Series A no. 103, 8.7.1986, para. 42.

136 See *Sürek v. Turkey* (No. 1) (application no. 26682/95), judgment of 8 July 1999, Reports 1999; *Sürek* (No. 3) judgment of 8 July 1999.

137 See *Sunday Times v. UK* (No.2), Series A no. 217, 26.11.1991, para. 50; *Okçuoğlu v. Turkey*, No. 24246/94, 8.7.1999, para. 43.

138 However, a Draft Council Framework Decision on combating the sexual abuse, sexual exploitation of children and child pornography proposed to have EU wide mechanisms to block access from the Union's territory to Internet pages identified as containing or disseminating child pornography especially where the original materials are not located within the EU. **This policy is still under consideration.** See Proposal for a Council Framework Decision on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA, paragraph 12 and draft Article 18 entitled Blocking access to websites containing child pornography.

139 *Case of Ürper and Others v. Turkey*, (Applications nos. 14526/07, 14747/07, 15022/07, 15737/07, 36137/07, 47245/07, 50371/07, 50372/07 and 54637/07), Chamber Judgment of 20.10.2009, paras 39-45.

140 Observer *and* Guardian *v. the United Kingdom*, 26 November 1991, § 59, Series A no. 216).

to new media and Internet publications. It stems from the Strasbourg principles that by suspending access to websites indefinitely the member states could largely overstep the narrow margin of appreciation afforded to them.[141] Furthermore, there could be a violation of OSCE media freedom commitments and other international provisions such as Article 10, ECHR if i) blocking measures or filtering tools are used at state level to silence politically motivated speech on the Internet, or ii) if the criteria for blocking or filtering are secret, or iii) if the decisions of the administrative bodies are not publicly made available for legal challenge.

Blocking and Web 2.0 based applications and services

It should be further highlighted that blocking access to any Web 2.0 based applications and services such as YouTube, WordPress, Facebook and Twitter may have extreme side effects and strong negative implications on political expression. These sites and platforms provide unique venues used all around the world for exchanging information (including from Vancouver to Vladivostok) and expressing alternative and dissenting views.

Blocking access to such services and platforms not only results in the blocking of access to the allegedly illegal content (usually displayed a single file or page) but also results in the blocking of millions of legitimate pages, files and content using the single domain these systems operate under. Therefore, blocking access to Web 2.0 based systems and services should be avoided at all costs as the damage caused by blocking access would be higher than the public good that would be achieved by blocking and censoring access to thousands (if not millions) of pages of legitimate content. [142]

Filtering is an inadequate method to combat harmful content

By far the most common motivation for the use of filtering and blocking software is the protection of children[143] from Internet content deemed to be harmful or inappropriate. Although the filtering tools were originally promoted as technological alternatives that would prevent the enactment of national laws regulating Internet speech, filtering systems have been shown to pose their own significant threats to free expression. If filtering solutions are deployed at the country-access level (whether index based,[144] analysis based filtering[145] or both) or used by individual ISPs, they can be used to block access to legitimate and political content. Within this context, both the EU and CoE strongly emphasize the adoption of policies which do not result in adult citizens being prevented from accessing legal content which may be deemed inappropriate for children to access. Therefore, while OSCE participating States should encourage the use of end-user filtering software on home computers, and in schools if their use is deemed necessary, the deployment of state-level upstream filtering systems should be avoided at all costs. Furthermore, users should be made aware of the potential limitations of filtering software.

---

141 *Cumpana and Mazare v. Romania*, no. 33348/96, § 119, 10 June 2003; *Obukhova v. Russia*, no. 34736/03, § 28, 8 January 2009, and *Case of Ürper and Others v. Turkey*, (Applications nos. 14526/07, 14747/07, 15022/07, 15737/07, 36137/07, 47245/07, 50371/07, 50372/07 and 54637/07), Chamber Judgment of 20.10.2009, paras 39-45.

142 The States have a positive obligation to protect their citizens' right to receive information in the absence of any plausible justification, or legitimate aim based on Article 10(2) ECHR criteria: Note *Autronic AG v. Switzerland,* 22 May 1990, §§ 47-48, Series A no. 178, and the more recent case of *Khurshid Mustafa and Tarzibachi v. Sweden*, App. no. 23883/06, judgment of 16 December, 2008.

143 IFLA World Report 2010, August 2010, at http://www.ifla-world-report.org

144 Blacklists prepared by government bodies or by commercial organizations.

145 Developed to meet a set of criteria intended to determine the acceptability of content.

Appendix I

RFoM project "Study of legal provisions and practices related to freedom of expression, the free flow of information and media pluralism on the Internet in the OSCE participating States"

Questionnaire for OSCE field presences and OSCE participating States
Deadline for submission 15 November 2010

N.B.: Regarding the inquired statistics, the reporting period for this questionnaire shall be 01 January 2007 – 30 June 2010.

We would appreciate if you could provide as much information as available. If you do not have the requested information, then please specify the reasons why the information requested is not available (e.g. not applicable, no such law or legal provision, the data is not available, etc.).

Please return your answers either in hard-copy through your OSCE Delegation or electronically via email to:

Ms Adilia Daminova, Project Officer, adilia.daminova@osce.org
Ms Ženet Mujić, Senior Adviser, zenet.mujic@osce.org

A. Access related questions

1. Are there specific legal provisions on the right to access the Internet?

- Please provide the name of the law/s, and relevant sections of these laws if such laws exist.
- If the answer is No to the above question, please state whether your country is planning to introduce such a law in the near future? Please state whether there is a draft bill involving this matter.

2. Are there general legal provisions which could restrict users' access to the Internet?

- Please provide the name of the applicable law/s, and relevant sections of these laws if such laws exist.

3. Are there specific legal provisions guaranteeing or regulating "net neutrality"?

- Please provide the name of the law/s, and relevant sections of these laws if such laws exist.
- If the answer is No to the above question, please state whether your country is planning to introduce such a law in the near future? Please state whether there is a draft bill involving this matter.

B. Content regulation related questions

4. Are there specific legal provisions outlawing racist content (or discourse), xenophobia, and hate speech?

- Please provide the name of relevant law/s and regulations, and the relevant sections of such provisions.
- Please state how these offences are defined by law.
- Please state specifically whether the possession and/or distribution of such content is criminalized.
- Please state which sanctions (criminal, administrative, civil) are envisaged by law.
- Please also state (if applicable) the maximum prison term envisaged by law for such offences.
- Please provide any statistical information in relation to convictions under relevant law/s for the reporting period of 01 January 2007 – 30 June 2010.
- Please state whether the law (or relevant regulations) prescribes blocking access to websites or any other types of Internet content as a sanction for these offences. If the answer is Yes, then please provide the blocking statistics for the reporting period of 01 January 2007 – 30 June 2010.
- Please state whether your country has signed or ratified the Additional Protocol to the CoE Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (CETS No 189).

5. Are there specific legal provisions outlawing the denial, gross minimisation, approval or justification of genocide or crimes against humanity?

- Please provide the name of relevant law/s and regulations, and the relevant sections of such provisions.
- Please state how these offences are defined by law.
- Please state specifically whether the possession of such content is criminalized
- Please state which sanctions (criminal, administrative, civil) are envisaged by law.
- Please also state (if applicable) the maximum prison term envisaged by law for such offences.
- Please provide any statistical information in relation to convictions under this law for the reporting period of 01 January 2007 – 30 June 2010.
- Please state whether the law (or relevant regulations) prescribes blocking access to websites or any other types of Internet content as a sanction for these offences. If the answer is Yes, then please provide the blocking statistics for the reporting period of 01 January 2007 – 30 June 2010.

6. Are there specific legal provisions outlawing incitement to terrorism, terrorist propaganda and/or terrorist use of the Internet?

- Please provide the name of relevant law/s and regulations, and the relevant sections of such provisions.
- Please state how these offences are defined by law.
- Please state specifically whether the possession of content involving “terrorist propaganda” is criminalized.

- Please state which sanctions (criminal, administrative, civil) are envisaged by law.
- Please also state (if applicable) the maximum prison term envisaged by law for such offences.
- Please provide any statistical information in relation to convictions under such law for the reporting period of 01 January 2007 – 30 June 2010.
- Please state whether the prescribed sanctions include blocking access to websites or any other types of Internet content. If the answer is Yes, then please provide the blocking statistics for the reporting period of 01 January 2007 – 30 June 2010.
- Please state whether your country has signed or ratified the CoE Convention on the Prevention of Terrorism (CETS No 196).

7. Are there specific legal provisions criminalizing child pornography?

- Please provide the name of relevant law/s and regulations, and the relevant sections of such provisions.
- Please state how these offences are defined by law.
- Please state which sanctions (criminal, administrative, civil) are envisaged by law.
- Please also state (if applicable) the maximum prison term envisaged by law for such offences.
- Please provide any statistical information in relation to convictions under these laws for the reporting period of 01 January 2007 – 30 June 2010.
- Please state whether the legal definition of "child pornography" includes unreal characters (drawings, paintings, cartoons, artificially created images etc.) and computer generated imagery within the concept of child pornography.
- Please state whether the prescribed sanctions include blocking access to websites or any other types of Internet content. If the answer is Yes, then please provide the blocking statistics for the reporting period of 01 January 2007 – 30 June 2010.
- Please state whether your country has signed or ratified the CoE Convention on Cybercrime (CETS No 185) which includes a provision on child pornography (Article 9).

8. Are there specific legal provisions outlawing obscene and sexually explicit (pornographic) content?

- Please provide the name of relevant law/s and regulations, and the relevant sections of such provisions.
- Please state how these offences are defined by law.
- Please state which sanctions (criminal, administrative, civil) are envisaged by law.
- Please also state (if applicable) the maximum prison term envisaged by law for such offences.
- Please provide any statistical information in relation to convictions under such law for the reporting period of 01 January 2007 – 30 June 2010.
- Please state whether the law (or relevant regulations) prescribes blocking access to websites or any other types of Internet content as a sanction for these offences. If the answer is Yes, then please provide the blocking statistics for the reporting period of 01 January 2007 – 30 June 2010.

9. Are there specific legal provisions outlawing Internet piracy?

- Please provide the name of relevant law/s and regulations, and the relevant sections of such provisions.
- Please state how these offences are defined by law.
- Please state which sanctions (criminal, administrative, civil) are envisaged by law.
- Please also state (if applicable) the maximum prison term envisaged by law for such offences.
- Please provide any statistical information in relation to convictions under such law for the reporting period of 01 January 2007 – 30 June 2010.
- Please state whether the prescribed sanctions include blocking access to websites or any other types of Internet content or the cutting off connections to the Internet. If the answer is Yes, then please provide the relevant statistics for the reporting period of 01 January 2007 – 30 June 2010.

10. Are there specific legal provisions outlawing libel and insult (defamation) on the Internet?

- Please provide the name of relevant law/s and regulations, and the relevant sections of such provisions.
- Please state how these offences are defined by law.
- Please state which sanctions (criminal, administrative, civil) are envisaged by law.
- Please also state (if applicable) the maximum prison term envisaged by law for such offences.
- Please provide any statistical information in relation to convictions under such law (for the reporting period).
- Please state whether the prescribed sanctions include blocking access to websites or any other types of Internet content. If the answer is Yes, then please provide the blocking statistics for the reporting period of 01 January 2007 – 30 June 2010.

11. Are there specific legal provisions outlawing the expression of views perceived to be encouraging "extremism"?

- Please provide the name of relevant law/s and regulations, and the relevant sections of such provisions.
- Please state how these offences are defined by law.
- If applicable please provide the legal definition of "extremism".
- Please state which sanctions (criminal, administrative, civil) are envisaged by law.
- Please also state (if applicable) the maximum prison term envisaged by law for such offences.
- Please provide any statistical information in relation to convictions under such law (for the reporting period).
- Please state whether the prescribed sanctions include blocking access to websites or any other types of Internet content. If the answer is Yes, then please provide the blocking statistics for the reporting period of 01 January 2007 – 30 June 2010.

12. Are there specific legal provisions outlawing the distribution of "harmful content" (i.e. content perceived to be "harmful" by law)?

- Please provide the name of relevant law/s and regulations, and the relevant sections of such provisions.
- Please state how these offences are defined by law.
- If applicable please provide the legal definition of "harmful content".
- Please state which sanctions (criminal, administrative, civil) are envisaged by law.
- Please also state (if applicable) the maximum prison term envisaged by law for such offences.
- Please provide any statistical information in relation to convictions under such law (for the reporting period).
- Please state whether the prescribed sanctions include blocking access to websites or any other types of Internet content. If the answer is Yes, then please provide the blocking statistics for the reporting period of 01 January 2007 – 30 June 2010.

13. Are there specific legal provisions outlawing any other categories of Internet content that have not been mentioned above?

- Please specify if any other types of Internet content is outlawed.
- Please provide the name of relevant law/s and regulations, and the relevant sections of such provisions if they exist.
- If applicable please state how these offences are defined by law.
- If applicable please state which sanctions (criminal, administrative, civil) are envisaged by law.
- If applicable please also state the maximum prison term envisaged by law for such offences.
- Please state whether the prescribed sanctions include blocking access to websites or any other types of Internet content. If the answer is Yes, then please provide the blocking statistics for the reporting period of 01 January 2007 – 30 June 2010.

C. Blocking, content removal, and filtering related questions

14. Are there general legal provisions which require closing down and/or blocking access to websites or any other types of Internet content?

- If the answer is Yes, then please provide the name of relevant law/s and regulations, and the relevant sections of such provisions.
- Please state how these provisions are defined by law.
- Please provide the blocking or any other relevant statistics for the reporting period of 01 January 2007 – 30 June 2010.

15. Are there specific legal provisions which require blocking access to web 2.0 based applications and services such as YouTube, Facebook, or Blogger?

- If the answer is Yes, then please provide the name of relevant law/s and regulations, and the relevant sections of such provisions.
- Please state how these provisions are defined by law.

- Please provide the blocking statistics for the reporting period of 01 January 2007 – 30 June 2010.

16. Are there specific legal provisions based on the "notice and take-down" principle?

- If the answer is Yes, then please provide the name of relevant applicable law/s and regulations, and relevant sections of such provisions.
- Please state whether such provisions apply to content, hosting, access providers (ISPs), web 2.0 based companies (e.g. YouTube, Facebook, etc.), and search engines (Google, Yahoo, Bing, etc.).
- Please state how these provisions are defined by law.
- Please provide statistical data with regards to such removal requests for the reporting period of 01 January 2007 – 30 June 2010.

17. Are there specific (public or private) Hotlines to report allegedly illegal content?

- If applicable please state if these hotlines are public organizations or privately run.
- If applicable please state whether they are established by law (co-regulation) or through self-regulation.
- Please also provide information on the formation/structure of such hotlines.
- Please state which types of content can be reported to these hotlines.
- Please provide statistics and Annual Reports of such hotlines if they exist (for the reporting period of 01 January 2007 – 30 June 2010).

18. Are there specific legal provisions requiring schools, libraries, and Internet cafes to use filtering and blocking systems and software?

- Please provide the name of relevant law/s and regulations, and the relevant sections of such provisions if such laws, or regulations exist.
- Please state how these provisions are defined by law.

D. Licensing and liability related questions

19. Are there specific legal liability provisions and licensing requirements for Internet Service Providers?

- Please provide the name of relevant law/s and regulations, and the relevant sections of such provisions.
- Please state how these provisions are defined by law.
- (If applicable) Please state if the EU E-Commerce Directive 2000/31 has been implemented into national law. If yes, then please provide the name of the law, and relevant sections of the law.
- Please provide statistical data with regards to prosecutions involving ISPs (for the reporting period).

20. Are there specific legal liability provisions and licensing requirements for Internet Search Engines or Content Providers (e.g. Google, Yahoo, etc.)?

- Please provide the name of relevant law/s and regulations, and the relevant sections of such provisions.

- Please state how these provisions are defined by law.
- If applicable please state any sanctions (criminal, administrative, civil) for breach of legal provisions envisaged by law.
- If applicable please also state the maximum prison term envisaged by law for any offences.
- Please provide statistical data with regards to prosecutions involving Internet Search Engines or Content Providers (for the reporting period).