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

REPORT

Freedom of Expression on the Internet

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

The report has been commissioned by the Office of the OSCE Representative on Freedom of the Media. It was prepared by Professor Yaman Akdeniz, Faculty of Law, Istanbul Bilgi University, Turkey.[*]

This report presents the conclusions of the first comprehensive research on Internet content regulation in the OSCE region. A preliminary report was prepared and published in view of the OSCE review conference and OSCE Astana Summit 2010.

The information contained in this report is based on data received from OSCE participating States as well as bona fide sources in response to a questionnaire sent out on 23 September 2010. As most of the answers were received only recently and as legislation and practices change, the study and country sections in part II remain open for updates and additions in the months to come.

[*] 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/>. Akdeniz can be contacted at yaman.akdeniz@bilgi.edu.tr.

TABLE OF CONTENTS

Introduction

Whenever new communication and media platforms have been introduced, their innovation and application was met with scepticism, fear or outright banning by the ruling parties and authorities who feared the unknown medium, and their capacity to oust them from power. Therefore, new (mass) media historically face suspicion, and are liable to excessive regulation as they spark fear of potential detrimental effects on society, security and political power structures. This has proven true in the publication and transmission of certain types of content from the printing press through the advent of radio, television and satellite transmissions, as well as other forms of communication systems. During the 1990s, as attention turned to the Internet and as access to this borderless new communication platform increased, the widespread availability of various content, including sexually explicit content and other types of content deemed to be harmful for children, stirred up a 'moral panic'[1] shared by many states and governments and certain civil-society representatives and concerned citizens.

Prior to the 1990s, information and content was predominantly within the strict boundaries and control of individual states, whether through paper-based publications, audio-visual transmissions limited to a particular area or even through public demonstrations and debates. Much of the media content made available and the discussions it triggered remained confined within territorially defined areas. Today, however, information and content with its digital transmission and widespread availability through the Internet, do not necessarily respect national rules nor territorial boundaries. This dissolution of the "sovereignty" of content control, coupled with the globalization of information, comes along with an increased multilingualism observable in many countries. The increasing popularity of user driven interactive Web 2.0 applications and services such as YouTube, Facebook and Twitter seem to eliminate virtual Internet borders even further by creating a seamless global public sphere. This, inevitably complicates state-level efforts to find an appropriate balance between the universal right to freedom of opinion and expression, which includes the right to receive and impart information, and the prohibition on certain types of content deemed illegal by nation-state authorities or intergovernmental organizations. With the widespread availability of the Internet, and increasing number of users, online content regulation became an important focus of governments and supranational bodies across the globe.

Today, many OSCE participating States feel the need to react to the development of the Internet as a major media and communication platform. Governments think that, it is on the one hand the infrastructure that requires protective measures, and on the other hand content made available that necessitates regulation. The past few years have shown that more people access the Internet, more content is made available online and more states feel obliged to regulate online content. A number of countries across the OSCE region have introduced new legal provisions in response to the availability and dissemination of certain types of (illegal or unwanted) content Governments are particularly concerned about the availability of terrorist propaganda,[2] racist content,[3] hate speech, sexually explicit content, including child

---

1 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.

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

3 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.

pornography,[4] as well as state secrets and content critical to certain governments or business practices. However, the governance of illegal as well as harmful (which falls short of illegality) Internet content may differ from one country to another and variations are evident within the OSCE participating States.[5] "Harm criteria" remain distinct within different jurisdictions with individual states deciding what is legal and illegal based upon different cultural, moral, religious, and historical differences and constitutional values.

Typically, the stance taken by many states is that what is illegal and punishable in an offline form must at least 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 and problematic. 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 when content hosted or distributed from outside the jurisdiction is deemed illegal in another.[6] Therefore, the question of jurisdiction over content adds to the challenges faced by the governments and regulators. Which country's laws should apply for content providers or for Web 2.0 based platform providers? Should the providers be liable in the country where the content has been uploaded, viewed, downloaded or where the server is placed or where the responsible providers reside? Many of these questions remain unanswered. Some countries fear the Internet could undermine their judicial sovereignty; others embrace the Internet and praise its global nature. However, the Internet certainly has created challenges for governments and these challenges are particulary visible when analyzing measures aimed at regulating online content.

Based on the limited effectiveness of state laws and lack of harmonization at international level (despite some efforts at regional level that will be addressed in this study)[7] a number of states, including some in the OSCE region, introduced policies to block access to Internet content, websites deemed illegal, and Web 2.0 based social media platforms which are outside their jurisdiction. In short, the new trend in Internet regulation seems to entail blocking access to content if state authorities are not in a position to reach the perpetrators 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.

Furthermore, in certain countries, governments went further and developed 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 increased piracy and intellectual property infringements on the Internet. These developments, as well as new policy trends in Internet content regulation are detailed in this study.

---

4 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.

5 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.

6 See generally Akdeniz, Y,. *Racism on the Internet*, Council of Europe Publishing, 2010, pp 21-31.

7 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).

While the intention of states to combat illegal activity over the Internet and to protect their citizens from harmful content is legitimate, there are also significant legal and policy developments which directly or indirectly and sometimes unintendedly have a negative impact on freedom of expression and the free flow of information on the Internet. Recent laws or certain legal measures currently under development have provoked much controversary over the past few years.

Concerned with such developments, the OSCE Representative on Freedom of the Media commissioned a report to assess whether and how access to and content on the Internet are regulated across the OSCE region by examining existing laws and practices related to freedom of expression, the free flow of information and media pluralism on the Internet. This first OSCE-wide Internet content regulation study also provides a comprehensive overview of existing international legal provisions and standards relating to media freedom and freedom of expression on the Internet. The study aims to assess whether and how these provisions are incorporated into national legislation by the OSCE participating States. [8]

The report also assesses the compliance of applicable national Internet legislation and practices with existing OSCE media freedom commitments, Article 19 of the Universal Declaration of Human Rights, Article 19 of the International Covenant on Civil and Political Rights, Article 10 of the European Convention on Human Rights (where applicable) as well as the case-law of the European Court of Human Rights.

[8] The study focuses on Internet content regulation. Therefore, certain policy considerations involving Internet's technical infrastructure which may affect the development of the Internet are left outside the scope of this study.

OSCE Commitments

The Organization for Security and Co-operation in Europe is the world's largest regional security organization and comprises 56 states of Europe, Asia and North America. Founded in 1975 on the basis of the Helsinki Final Act of the Conference on Security and Co-operation in Europe, the OSCE has assumed the tasks of identifying the potential for the outbreak of conflicts and of their prevention, settling and dealing with their aftermaths. The development of democratic institutions and the protection of human rights are among the OSCE's main means for guaranteeing stability and security in its participating States.

In various documents, the OSCE participating States committed themselves to uphold freedom of the media and guarantee their citizens the right to free expression. In the Helsinki Final Act, the participating States decided to "act in conformity with the purposes and principles of the […] Universal Declaration of Human Rights." They agreed to recognize "the importance of the dissemination of information from the other participating States", "make it their aim to facilitate the freer and wider dissemination of information of all kinds" and "encourage co-operation in the field of information and the exchange of information with other countries".[9]

At the Budapest Summit in 1994, the participating States reaffirmed "that freedom of expression is a fundamental human right and a basic component of a democratic society. In this respect, independent and pluralistic media are essential to a free and open society and accountable systems of government. They take as their guiding principle that they will safeguard this right."[10] This was echoed by the 1996 Lisbon Summit where the OSCE participating States declared that "[f]reedom of the press and media are among the basic prerequisites for truly democratic and civil societies. In the Helsinki Final Act, we have pledged ourselves to respect this principle."[11]

Only three years later, in the 1999 Charter for European Security, the participating States reaffirmed "the importance of independent media and the free flow of information as well as the public's access to information. We commit ourselves to take all necessary steps to ensure the basic conditions for free and independent media and unimpeded transborder and intra-State flow of information, which we consider to be an essential component of any democratic, free and open society."[12]

This was further defined to explicitly include the Internet by the OSCE Permanent Council Decision No. 633 where the participating States pledged to "take action to ensure that the Internet remains an open and public forum for freedom of opinion and expression, as enshrined in the Universal Declaration of Human Rights, and to foster access to the Internet both in homes and in schools." The OSCE PC Decision 633 further asks the participating States to "study the effectiveness of laws and other measures regulating Internet content".[13]

---

9 Final Act of the Conference on Security and Cooperation in Europe, Helsinki, 1 August 1975. See the full official text at http://www.osce.org/documents/mcs/1975/08/4044_en.pdf.

10 Budapest Summit Declaration, 21 December 1994. See the full official text at http://www.osce.org/mc/39554.

11 Lisbon Summit Document, 3 December 1996. See the full official text at http://www.osce.org/mc/5869.

12 Charter for European Security, adopted at the OSCE Istanbul Summit, November 1999. The full official text is available at http://www.osce.org/documents/mcs/1999/11/4050_en.pdf.

13 OSCE PC.DEC/633 on Promoting Tolerance and Media Freedom on the Internet, endorsed by MC.DEC/12/04 at the OSCE Ministerial Council in Sofia, 7 December 2004. See at http://www.osce.org/mc/23133.

Methodology

The purpose of the present study is twofold: First, it aims to provide an overview of existing legislative provisions on Internet content regulation, including governmental practices related to freedom of expression and freedom of the media across the OSCE region. Second, the study assesses the impact these regulations and practices have on the free flow of information and the freedom of expression on the Internet.

The study is a compilation of a comprehensive OSCE-wide legal matrix of legal provisions related to freedom of expression, freedom of the media and the free flow of information on the Internet. The study assesses how these provisions are applied by the OSCE participating States. Furthermore, the study assesses 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 such as Article 19 of the Universal Declaration of Human Rights, Article 19 of the International Covenant on Civil and Political Rights as well as the case-law of the European Court of Human Rights.

For this purpose, the OSCE Office of the Representative on Freedom of the Media conducted a survey of all 56 OSCE participating States by means of a questionnaire (annexed to this study). The 20 questions (and 101 sub-questions) were prepared during the summer of 2010 and distributed to all OSCE participating States on 23 September 2010.[14] Responses to the questionnaire were expected by 15 November, 2010. However, the majority of the responses were received in January and February 2011. The latest response was received in mid-May 2011.

The study assessed data collected on 46 OSCE participating States. It should be noted that 14 participating States did not provide official responses, however, information on five of those participating States was obtained from bona fide sources.

The intention was to analyse data officially obtained from the OSCE participating States, but also to encourage the states to embark on an "inventory" of their own Internet legislation applicable to online content.

The OSCE questionnaire aimed at gathering information related to general access provisions, the regulation of specific content, blocking and filtering requirements, and information related to the role and liability of Internet service providers (ISPs).

In detail, this study includes four parts based on the questions[15] and assessments related to:

A. Internet access
B. Internet content regulation
C. Blocking, content removal, and filtering
D. Licensing and liability

Based on the data gathered[16] on 46 OSCE participating States,[17] and with the assessment of the efficiency and applicability of existing international legal provisions as well as their

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

transposition into national law, the study intends to serve as an OSCE-wide legal reference tool to monitor further development in the area of Internet content regulation.

A preliminary report published on 26 November 2010[18] aimed to set forth the first findings 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, the 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.[19]

Disclaimer: For the present report and assessment, use has been made of the replies in the form in which they were received. Neither the author nor the Office of the OSCE Representative on Freedom of the Media assumes responsibility for the completeness, correctness and exhaustiveness of the information submitted. Not all replies were concise and some needed translation into English. Although the utmost has been done to convey the content of the replies correctly, it cannot be excluded that occasionally the representation of answers may not correspond to the intention of the respondent States. In these cases, the author did his utmost to interpret the provided response in the best interest of the responding State.

16 Where relevant the author conducted independent research and made use of publicly available and verifiable information in addition to making use of the information obtained from the OSCE participating States.

17 Albania, Armenia, Austria, Azerbaijan, Belarus, Bosnia and Herzegovina, Bulgaria, Canada, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Ireland, Italy, Kazakhstan, Kyrgyzstan, Latvia, Liechtenstein, Lithuania, Luxembourg, the former Yugoslav Republic of Macedonia, Moldova, Montenegro, Netherlands, Norway, Poland, Portugal, Romania, Russian Federation, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey, Turkmenistan, Ukraine, United Kingdom.

18 http://www.osce.org/fom/73725

19 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: Preliminary Report, OSCE Representative on Freedom of the Media, FOM.GAL/4/10, November 2010, at <http://www.osce.org/item/47857.html>.

FINDINGS, CONCLUSIONS AND RECOMMENDATIONS

The preparation of this report showed that despite the responsiveness of the OSCE participating States to take part in the survey, many governments expressed major difficulties in collecting the requested data. Be it for the reason that reliable or recorded information was not available, particularly pertaining to questions on prosecution and blocking statistics or the fact that several governmental institutions and ministries are responsible for the different aspects of the Internet. Hence, replying to the survey would have required high logistical efforts of co-ordinating the answers. Almost no participating State has in place an institutional focal point for Internet-related legal and policy matters.

The OSCE study includes four sections based on the questions[20] and assessments related to:

A. Internet access
B. Internet content regulation
C. Blocking, filtering and content removal
D. Licensing and liability and Internet hotlines

Part I of the study provides the summary of main findings, conclusions for each of the above sections and includes overall recommendations. Part II consists of a detailed and in depth overview of each issue addressed in the questionnaire. Information and data received from the participating States, as well as independent research conducted for this study, are provided for each question. A detailed assessment for each of the sections is also included.

A. Internet Access

The Internet is increasingly becoming indispensable for people to take part in cultural, social and political discourse and life. The number of Internet users is expected to more than double in 10 years and will reach five billion worldwide. While more than 60% of the citizens of the OSCE area are Internet users, only 30% of the participating States stated that they recognize access to the Internet as a basic human right or as implied in the fundamental right to freedom of expression. At the same time, in more than 12% of the participating States access to the Internet can legally be restricted, primarily to protect national security, public health or in times of state emergencies. As will be seen below, some OSCE states that do not have provisions on general access restrictions may nevertheless restrict users' Internet access in certain cases, such as repeated copyright infringments or when criminal content, such as child pornography, is evident.

Everyone should have a right to participate in the information society and states have a responsibility to ensure citizens' access to the Internet is guaranteed. Furthermore, Internet access policies, defined by governments, should be in line with the requirements of Article 19 of the Universal Declaration of Human Rights as well as Article 19 of the International Covenant on Civil and Political Rights and (where applicable) with Article 10 of the European Convention on Human Rights. While certain countries and international organizations, such as the United Nations, may recognize Internet access as inherent to the right to free expression and as such to be a fundamental and universal human right, a number

[20] See Appendix I.

of governments are considering adopting content and access blocking measures.[21] Countries such as Finland and Estonia already have ruled that access is a fundamental human right for their citizens. According to a 2010 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."[22]

Asked **whether there are specific legal provisions on the right to access the Internet (Question 1)**, only 17 (30.3%) participating States confirmed that they have such provisions while 29 States (51.8%) stated that no such provisions exist. No data was obtained from 10 participating States (17.9%).

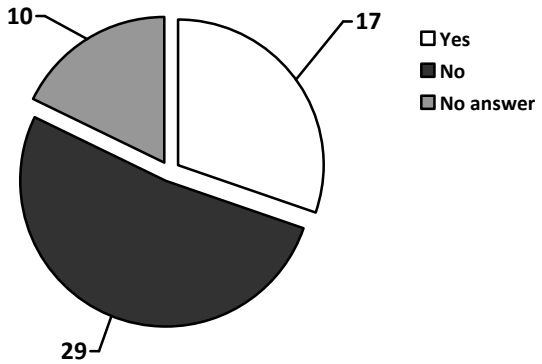


Figure 1. OSCE participating States' responses regarding the presence of specific legal provisions on the right to access the Internet (Question 1)

In some of the countries that responded positively, the right to access the Internet is interwoven with the right to information and communication, which is constitutionally protected in most cases.[23] In some states, the right to access the Internet is quaranteed by specific laws, usually within telecommunication laws or regulations.[24]

Asked whether **there are general legal provisions which could restrict users' access to the Internet (Question 2)**, 39 (69.6%) of the participating States stated "no", while only seven[25]

---

21 Note also the report by Frank La Rue, the United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, presented to the UN Human Rights Council on 3 June 2011.

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

23 Cyprus, Estonia, Georgia, Greece, Portugal, Russia, and Ukraine.

24 **Albania** (Law No. 9918 (19.05.2008) "On electronic communications in the Republic of Albania"); **Estonia** (Public Information Act § 33: Access to data communication network stipulates the right to have access to the Internet (access to data communication network). Every person shall be afforded the opportunity to have free access to public information through the Internet in public libraries, pursuant to the procedure provided for in the Public Libraries Act); **Finland** (Communications Market Act (393/2003), chapter 6 contains provisions concerning universal service. Persons residing in Finland have been granted a connection of at least 1 Mbit/s); **France** (French Constitutional Council Decisions 2009-580 DC Code for Post and Electronic Communications); **Germany** (Section 78 of the Telecommunications Act (Telekommunikationsgesetz, TKG)); **Hungary** (Universal Service Obligation, Act C of 2003, Section 117); **Montenegro** (Law on Electronic Communications ("Official Gazette of Montenegro no. 50/08), Article 102); **Spain** (Spanish General Telecommunications Act 32/2003, of 3 November, article 22, includes Internet access as a Universal Service); **Turkey** (Universal Service Law No. 5369 dated 16.06.2010); **Turkmenistan** (Article 38 (The Regulations on Internet Services Provision) of the Law of Turkmenistan "On Communications" of March 12, 2010).

25 These are Azerbaijan, France, Latvia, Lithuania, Portugal, Ukraine, and Turkmenistan.

(12.5%) responded that they have general legal provisions which could restrict users' online access. No data was obtained from 10 (17.9%) of the participating States.

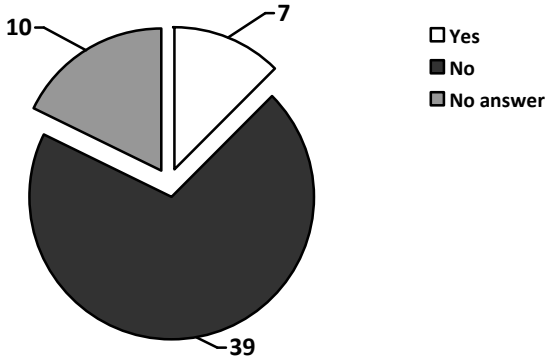


Figure 2. OSCE participating States' responses regarding the presence of general legal provisions which could restrict users' access to the Internet (Question 2)

Asked whether **there are specific legal provisions guaranteeing or regulating "net neutrality" (Question 3)** in their jurisdiction, only **Finland** responded 'yes' (1.8%), while 45 States responded 'no' (80.4%). No data was obtained from 10 (17.9%) of the participating States. In **Finland**, since July 2010, subject to section 60(3) of the Communications Market Act,[26] all Finnish citizens have a legal right to access a one megabit per second broadband connection, reportedly making Finland the first country to accord such a right.[27]

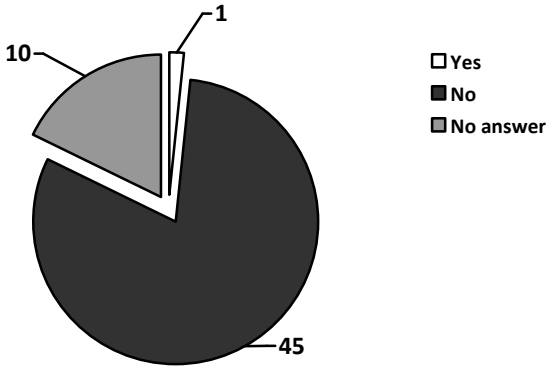


Figure 3. OSCE participating States' responses regarding specific legal provisions guaranteeing or regulating "net neutrality" (Question 3)

---

[26] See Section 60 c (331/2009) Universal service obligation concerning the provision of universal telephone services of the Finnish Communications Market Act at <http://www.finlex.fi/en/laki/kaannokset/2003/en20030393.pdf>: "Provisions on the minimum rate of a functional Internet access…. are issued by a decree of the Ministry of Transport and Communications. Prior to the issuance of the decree, the Finnish Communications Regulatory Authority shall examine the data transfer service markets, prevailing access rates available to the majority of subscribers and level of technological development, and estimate the financial impacts of the regulation on telecommunications operators.

[27] Finnish Ministry of Transport and Communications Press Release, 1 Mbit Internet access a universal service in Finland from the beginning of July, 29.06.2010, at <http://www.lvm.fi/web/en/pressreleases/view/1169259>: "The Ministry of Transport and Communications has defined the minimum rate of downstream traffic of a functional Internet access to be 1 Mbit/s, and the Finnish Communications Regulatory Authority, FICORA, has defined 26 telecom operators across Finland as universal service operators."

Network neutrality is an important prerequisite for the Internet to be equally accessible and affordable to all. It is, therefore, troubling that more than 80% of the participating States do not have legal provisions in place to guarantee net neutrality. Finland and Norway stand out as best practice examples with Finland having anchored network neutrality in its corpus of laws while Norway, together with the industry and Internet consumers, developed workable guidelines. While it is commendable that several EU countries are planning to introduce rules on network neutrality by implemtning the European Union's Telecoms Reform Package, participating States should consider legally strengthening users' rights to an open Internet. Users should have the greatest possible access to Internet-based content, applications or services of their choice without the Internet traffic they use being managed, prioritized or discriminated against by the network operators.

B. Internet Content Regulation

Undoubtedly differences 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. Usually, the difference between illegal and harmful content is that the former is criminalized by national laws, while the latter is considered offensive, objectionable, or undesirable by some but is generally not legally criminalized. While child pornography could be regarded as a clear example of content being criminalized in most, if not all the participating States, Internet content that is often labelled as "harmful" may include sexually explicit or graphically violent material. Strong or extreme political or religious views may also be regarded as harmful by states. Although this type of content falls short of the "illegality threshold", concern remains about possible access to this type of content by children. Highlighting this fundamental difference, in 1996 the European Commission stated:

> "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".[28]

More recently, the European Court of Human Rights argued that:

> "…. the Internet is an information and communication tool particularly distinct from the printed media, in particular as regards the capacity to store and transmit information. The electronic network serving billions of users worldwide is not and potentially cannot be subject to the same regulations and control. The risk of harm posed by content and communications on the Internet to the exercise and enjoyment of human rights and freedoms, … is certainly higher than that posed by the press."[29]

Policy and legal developments regarding the Internet in the OSCE region have shown that states differ in terms of categorizing or labelling certain types of content as illegal or "harmful". Harm is a criterion that depends upon various fundamental differences, which is recognized within the jurisprudence of the European Court of Human Rights.[30] Such state-level differences undoubtedly complicate harmonization of laws and approaches at the international level.

---

28 European Commission Communication on Illegal and Harmful Content on the Internet (1996), p. 10.

29 See *Editorial Board of Pravoye Delo and Shtekel v. Ukraine*, Application no. 33014/05, Jusdgment of 05.05.2011, para 63.

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

Regarding speech and content related laws and legal measures, any restriction must meet the strict criteria under international and regional human rights law. According to the European Court of Human Rights jurisprudence, a strict three-part test is required for any content-based restriction. The Court notes that the first and most important requirement of Article 10 of the Convention is that any interference by a public authority with the exercise of the freedom of expression should be lawful.[31] The second paragraph of Article 10 clearly stipulates that any restriction on expression must be "prescribed by law". If the interference is in accordance with law, the aim of the restriction should be legitimate based on the Article 10(2) – and concern limitations in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health of morals, or for the protection of the rights and freedoms of others. Furthermore, any restrictions need to be necessary in a democratic society,[32] and the state interference should correspond to a "pressing social need".[33] The state response and the limitations provided by law should be "proportionate to the legitimate aim pursued".[34] Therefore, the necessity of the content-based restrictions must be convincingly established by the state.[35] The Article 10 compatibility criteria as set out by the European Court of Human Rights should be taken into account while developing content related policies and legal measures by the participating States.

Asked whether whether **there are specific legal provisions outlawing racist content (or discourse), xenophobia and hate speech** in their jurisdiction **(Question 4)**, 45 (80.4%) of the participating States stated that there are such legal provisions in their country. The only country which responded negatively was **Kyrgyzstan**[36]. No data was obtained from 10 (17.9%) of the participating States.

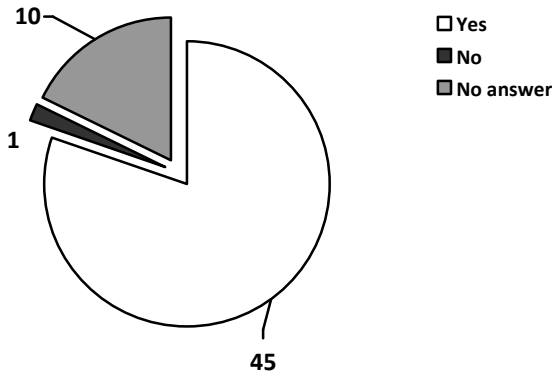


Figure 4. OSCE participating States' responses regarding specific legal provisions outlawing racist content, xenophobia and hate speech (Question 4)

---

31 Note also Article 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights within this context. See Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, A/HRC/17/27, 16 May 2011, at <http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf>.

32 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.

33 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.

34 See *Bladet Tromsø and Stensaas v. Norway* [GC], no. 21980/93, ECHR 1999-III.

35 *The Observer and The Guardian v. the United Kingdom*, judgment of 26 November 1991, Series A no. 216, pp. 29-30, § 59.

36 However, it has to be noted that Article 31 of the Kyrgyzs Constitution and Article 299 of the Kyrgyzs Criminal Code contain general provisions outlawing racist content and hate speech.

Asked whether **there are specific legal provisions outlawing the denial, gross minimisation, approval or justification of genocide or crimes against humanity** in their country **(Question 5),** 23 (41.1%) of participating States responded that they have such legal provisions in place. The same number of countries (23 - 41.1%) stated that they do not have such legal provisions, and 10 (17.9%) of the participating States did not provide a reply.

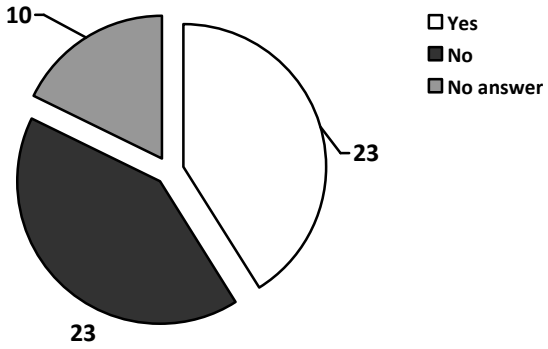


Figure 5. OSCE participating States' responses regarding specific legal provisions outlawing the denial, gross minimisation, approval or justification of genocide or crimes against humanity (Question 5).

As will be seen in Part II of this study, some countries provide criminal sanctions for publishing, dissemination, and even for possession of content related to the denial, gross minimisation, approval or justification of genocide or crimes against humanity.

Asked whether **they have in place specific legal provisions outlawing incitement to terrorism, terrorist propaganda and/or terrorist use of the Internet (Question 6)**, 40 (71.4%) participating States responded positively, while only six (10.7%) stated that they do not have such legal provisions.[37] No data was obtained from 10 (17.9%) of the participating States.

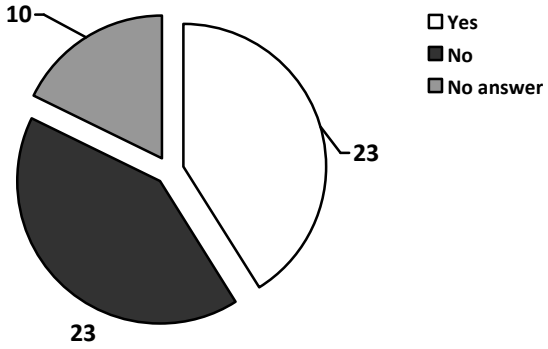


Figure 6. OSCE participating States' responses regarding specific legal provisions outlawing incitement to terrorism, terrorist propaganda and/or terrorist use of the Internet (Question 6)

Asked whether **there are specific legal provisions criminalizing child pornography** in their country **(Question 7)**, the overwhelming majority of participating States (43 - 76.8%) stated that they have such laws in place. Only three (5.4%) (Azerbaijan,[38] Kyrgyzstan,[39] and

[37] Armenia, Bulgaria, Hungary, Liechtenstein, Romania, Serbia.

[38] The legislation of the Azerbaijan Republic has no specific legal provisions criminalizing child

Turkmenistan[40]) answered negatively. No data was obtained from 10 (17.9%) of the participating States.

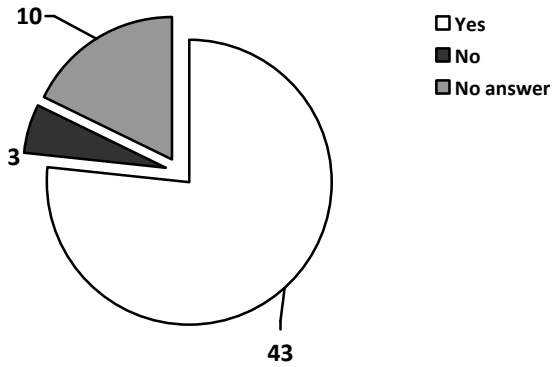


Figure 7. OSCE participatibg States' responses regarding specific legal provisions criminalizing child pornography (Question 7)

Asked whether there are **specific legal provisions outlawing obscene and sexually explicit (pornographic) content** exist in their jurisdiction **(Question 8)**, 41 (73.2%) of participating States stated that they have such laws in place. In only five (8.9%) countries (Bosnia and Herzegovina, Croatia,[41] Hungary, Liechtenstein, and Moldova) no such provisions exist. No data was obtained from 10 (17.9%) of the participating States.

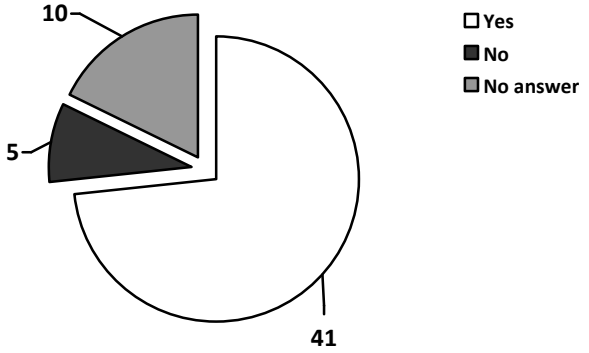


Figure 8. OSCE participating States' responses regarding specific legal provisions outlawing obscene and sexually explicit (pornographic) (Question 8)

Most legal provisions outlaw making available or showing obscene and sexually explicit (pornographic) content to children.[42] In some states, the production, manufacture,

---

pornography. The Azerbaijan Republic is a signatory to the Optional Protocol to the Convention on the Rights of the Child concerning the trafficking in children, child prostitution, and child pornography.

39 Although, there are no specific child pornography laws in Kyrgyzstan, Articles 157 and 262 of the Criminal Code contain general legal provisions on the ban of pornography.

40 Although there are no specific child pornography laws in Turkmenistan, Article 29 (Protection of the Child from Obscenities) of the Law "On the Guarantees of the Rights of the Child" states that the production and dissemination of pornographic printed publications, films or any pornographic items shall be prohibited in Turkmenistan, and the state shall guarantee the protection of children from any sexual abuse. See also Article 164 of the Criminal Code.

41 Obscene and sexually explicit (pornographic) content, except for content constituting child pornography, is not sanctioned by law in Croatia.

42 For example this is the case in Albania and in Germany (Section 184 German Criminal Code: 333

dissemination or advertisement of pornographic content are criminalized per se.[43] Sanctions vary from administrative fines[44] to criminal sanctions. Possession of such content is generally not criminalized.

The OSCE participating States were further asked whether **there are specific legal provisions outlawing Internet piracy** in their country **(Question 9)**. 44 (78.6%) of the participating States confirmed the existence of such legal provisions. Only **Turkmenistan** stated that it does not outlaw Internet piracy specifically. No data was obtained from 11 (19.6%) of the participating States.

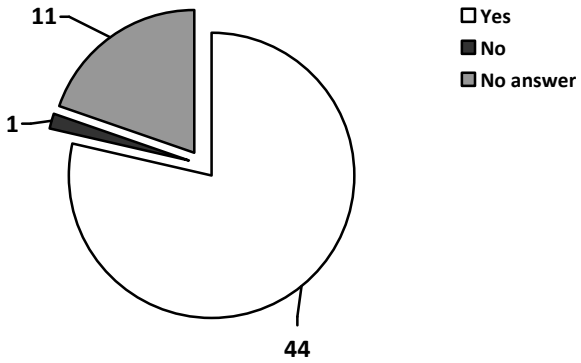


Figure 9. OSCE participating States' responses regarding specific legal provisions outlawing Internet piracy (Question 9)

The responses received show that almost all participating States have general intellectual property laws that may be used to combat Internet piracy. Liability and sanctions may be

convictions in 2007, 264 in 2008, and 214 in 2009). In Lithuania, Article 4(3) of the Law on the Protection of Minors against the Detrimental Effect of Public Information states that except for the cases provided for in Article 7 of this Law, making available to the public or dissemination of public information that may be detrimental to physical, intellectual or moral development of minors, especially the portrayal of pornography and/or gratuitous violence shall be prohibited. Note also Article 186 of the Spanish Criminal Code, and Article 226 of the Turkish Penal Code regarding the provision of sexually explicit content to children.

[43] For example see Article 263 of the Armenian Criminal Code, Article 242 of the Criminal Code of Azerbaijan, and Article 343 of the Criminal Code (introduced into the Criminal Code by Law of the Republic of Belarus on 10 November 2008). During the period from 2007 through 2009, 176 people were convicted under this article of the Criminal Code in the Republic of Belarus. Note also Article 159 of the Bulgarian Penal Code, Article 255(1) (Illicit Production or Sale of a Pornographic Piece or Other Object) of the Georgian Criminal Code. The maximum term of imprisonment for acts envisaged by Article 255(1) is two years. In Kazakhstan, Article 273 (Illegal Distribution of Pornographic Materials or Objects) of the Criminal Code states that illegal manufacture for the purposes of distribution or advertisement or distribution and advertisement of pornographic materials or objects, as well as illegal trade in publications, cinema or video materials, pictures, or other objects of pornographic nature, shall be punishable by a fine in the amount from 500 to 1,000 monthly calculation indices, or in the amount of the salary or other income of the convicted person for a period of five months to one year, or by correctional work for up to two years, or by deprivation of liberty for a term of up to two years with confiscation of the pornographic materials or objects, as well as the means of their production or reproduction. Note also Article 262 of the Criminal Code of the Kyrgyz Republic, and Article 164 (The Production or Dissemination of Pornographic Items) of the Criminal Code of Turkmenistan

[44] Article 1732(1) of the Latvian Administrative Violations Code provides for administrative liability in the case of violation of the requirements regarding the importation, manufacture, distribution, public demonstration or advertising of erotic and pornographic materials (essays, magazines, images, computer programs, films, video recordings and audio recordings, television and radio broadcasts). The sanctions involve issuing a warning or imposing a fine with or without a confiscation of these materials.

provided in the form of administrative, civil, and criminal liability. Graduated response mechanisms to limit users' access to the Internet for alleged copyright violations have been also developed in a few participating States.

Asked whether **they have specific legal provisions outlawing libel and insult (defamation) on the Internet (Question 10)**, 36 (64.3%) of the participating States responded with "yes", while eight states[45] (14.3%) do not have criminal law provisions outlawing libel. However, although there are no criminal law provisions on libel and insult within these states, civil law provisions that could be applied to the Internet do exist. No data was obtained from 12 (21.4%) of the participating States.

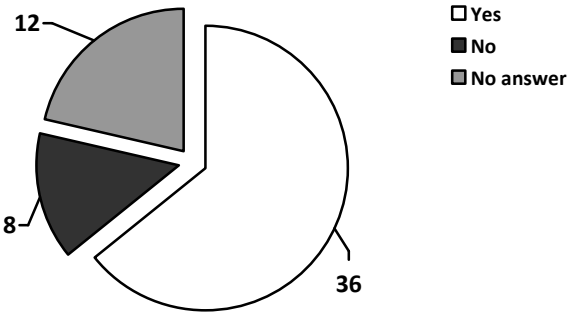


Figure 10. OSCE participating States' responses regarding specific legal provisions outlawing libel and insult (defamation) on the Internet (Question 10)

As will be shown in Part II of this report, although few states have decriminalized defamation, the decriminalization process still continues and several states are currently in the process of abolishing criminal defamation provisions.

In some OSCE participating States legal provisions on "extremism" or "extreme speech" exist. Asked whether **there are specific legal provisions outlawing the expression of views perceived to be encouraging extremism** in their country **(Question 11)**, 20 (35.7%) of the participating States answered with "yes", 26 (46.4%) with "no", and no data was obtained from 10 (17.9%) participating States.

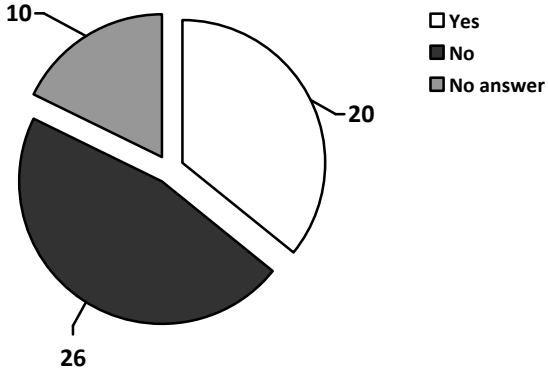


Figure 11. OSCE participating States' responses regarding specific legal provisions outlawing the expression of views perceived to be encouraging extremism (Question 11)

[45] It should be noted that eight States answered this question as "No": Bosnia and Herzegovina, Bulgaria, Canada, Croatia, France, Luxembourg, Romania and the United Kingdom.

Asked whether **they have specific legal provisions outlawing the distribution of "harmful content" (i.e. content perceived to be "harmful" by law)** in place **(Question 12)**, 19 (33.9%) participating States responded that there are such laws in their jurisdiction. However, in 26 (46.5%) countries no such legal provisions exist. No data was obtained from 11 (19.6%) participating States.

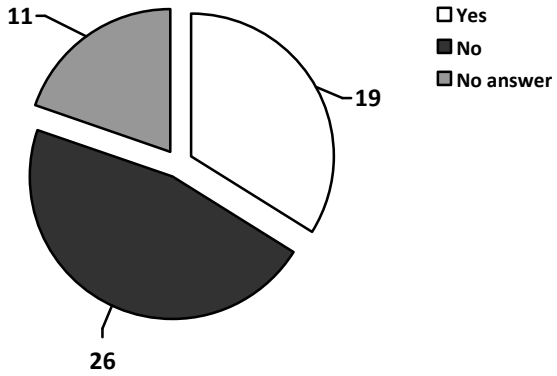


Figure 12. OSCE participating States' responses regarding specific legal provisions outlawing the distribution of "harmful content" (Question 12)

Asked whether there are **specific legal provisions outlawing any other categories of Internet content (Question 13)**, 15 (26.8%) OSCE participating States responded positively, while so such legal provisions exisit in 30 (53.6%) participating States. No data was obtained from 11 (19.6%) participating States.

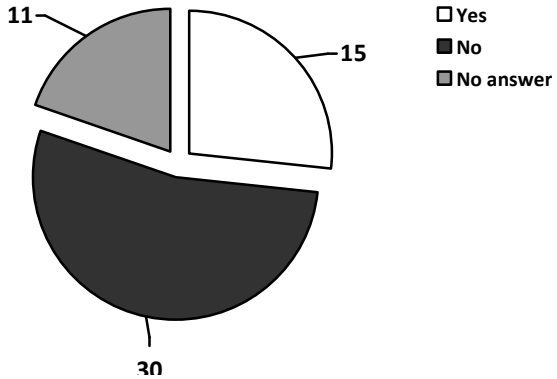


Figure 13. OSCE participating States' responses regarding specific legal provisions outlawing any other categories of Internet content (Question 13)

Legal provisions that criminalize racism and hate speech, the denial, gross minimisation or justification of crimes against humanity, incitement to terrorism, child pornography, obscene and sexually explicit content, libel and insult, and the expression of views perceived to be encouraging extremism, exist in many participating States. A considerable number of legal provisions have been introduced and existing provisions have been amended within the past few years.

Most of the legal provisions criminalizing content are applicable to any medium and are not specific to the Internet. Therefore, legal measures and criminal sanctions can also be used to regulate online content and conduct. However, content regulation developed for traditional media cannot and should not simply be applied to the Internet. Recognizing this,

some participating States have developed new legal provisions specifically designed for online content; yet often without recognizing that freedom of expression and freedom of information equally apply to the Internet. This increased legislation of online content has led to challenging restrictions on the free flow of information and the right to freely impart and receive information on and through the Internet.

Definitional problems and inconsistencies exist regarding certain speech-based restrictions. Clarifications are needed to specify what amounts for example to "extremism", "terrorist propaganda", "harmful" or "racist content", and "hate speech". As set forth in Article 19 of the Universal Declaration and in 10 of the European Convention on Human Rights, freedom of expression is subject to exceptions. These must be construed strictly, and the need for any restrictions must be established convincingly by the states.[46] Under the established principles of the European Court of Human Rights, citizens must be able to foresee the consequences which a given action may entail,[47] and sufficient precision is needed to enable the citizens to regulate their conduct.[48] At the same time, while certainty in the law is highly desirable, it may bring excessive rigidity as the law must be able to keep pace with changing circumstances. The level of precision required of domestic legislation[49] – which cannot in any case provide for every eventuality – depends to a considerable degree to the content in question, the field it is designed to cover and to the number and status of those to whom it is addressed.[50]

Furthermore, a considerable number of participating States have yet to decriminalize defamation. Harsh prison sentences and severe financial penalties continue to exist in defamation suits. The European Court of Human Rights recalled in a number of its judgments that while the use of criminal law sanctions in defamation cases is not in itself disproportionate,[51] the nature and severity of the penalties imposed are factors to be taken into account.[52] Within this context, it is important to remember that the Council of Europe's Parliamentary Assembly urges those member states which still allow incarceration for defamation, even if they are not actually imposed,[53] to abolish them without delay.[54] Criminal defamation lawsuits continue to present a serious threat to and a chilling effect for media freedom in the OSCE region. In the Internet age, decriminalization of defamation becomes a prerequisite for free media to report without fear of criminal prosecution about issues of public importance – beyond national borders and jurisdictions. In countries where a free media scene is yet to be established, it is often foreign correspondence assuming the watchdog functions. If, however, journalists face criminal charges for online publications outside their

---

46 See, among several other authorities, *Nilsen and Johnsen v. Norway* [GC], no. 23118/93, § 43, ECHR 1999-VIII, and *Fuentes Bobo v. Spain*, no. 39293/98, § 43, 29 February 2000.

47 *Lindon, Otchakovsky-Laurens and July v. France* [GC], nos. 21279/02 and 36448/02, § 41, ECHR 2007-XI. See further *Kafkaris v. Cyprus* [GC], no. 21906/04, § 140, ECHR 2008.

48 *Groppera Radio AG and Others v. Switzerland*, 28 March 1990, § 68, Series A no. 173.

49 See the *Sunday Times* v. the United Kingdom (no. 1) judgment of 26 April 1979, Series A no. 30, p. 31, § 49; the Larissis and Others v. Greece judgment of 24 February 1998, *Reports* 1998-I, p. 378, § 40; *Hashman and Harrup v. the United Kingdom* [GC], no. 25594/94, § 31, ECHR 1999-VIII; and *Rotaru v. Romania* [GC], no. 28341/95, § 52, ECHR 2000-V

50 See generally in this connection, *Rekvényi v. Hungary* [GC], no. 25390/94, § 34, ECHR 1999-III.

51 See *Radio France and Others v. France*, no. 53984/00, § 40, ECHR 2004-II; *Lindon, Otchakovsky-Laurens and July v. France* [GC], nos. 21279/02 and 36448/02, § 59, ECHR 2007-XI; *Długołęcki v. Poland*, no. 23806/03, § 47, 24 February 2009; and *Saaristo and Others v. Finland*, no. 184/06, § 69 *in limine*, 12 October 2010.

52 See *Cumpănă and Mazăre v. Romania* [GC], no. 33348/96, § 111, ECHR 2004.

53 Note case of *Sabanovic v. Montenegro and Serbia*, Application no. 5995/06, Judgment of 31.05.2011.

54 See Parliamentary Assembly of the Council of Europe, Resolution 1577: Towards decriminalisation of defamation, 2007, at <http://assembly.coe.int/main.asp?Link=/documents/adoptedtext/ta07/eres1577.htm>.

home countries, the journalistic freedom to report freely and unhindered will be severely hampered. Journalists might be subject to defamation charges in many countries where their stories have been read or downloaded.

The increased use of so-called "three-strikes" legal measures to combat Internet piracy is worrisome given the growing importance of the Internet in daily life. "Three-strikes" measures provide a "graduated response" resulting in restricting or cutting off the users' access to the Internet in cases where a user has attempted to download pirated material. The third strike usually leads to the user's access to the Internet being completely cut off. This disproportionate response is most likely to be incompatible with OSCE commitment on the "freedom to hold opinions and to receive and impart information and ideas withouth interference by public authority and regardless of frontiers."[55] In the Charter for European Security, the participating States in 1999 "reaffirmed the importance of independent media and the free flow of information as well s the public's access to information [and committed] to take all necessary steps to ensure the basic conditions for free and independent media and unimpeded transborder and intra-State flwo of information, which [they] consider the be an essential component of any democratic, free and open society."[56] Any interference with such a fundamental human right, as with any other human right, must be motivated by a pressing social need, whose existence must be demonstrated by the OSCE participating States and must be proportionate to the legitimate aim pursued.[57] Access to the Internet must be recognized as a human right, and therefore "graduated response" mechanisms which could restrict users' access to the Internet should be avoided by the OSCE participating States.

Finally, it should be noted that a considerable number of OSCE participating States did not provide statistical information on convictions under relevant law(s) pertaining to online content regulation. In the absence of reliable statistical data, or any data with regards to prosecutions and convictions involving the above mentioned content related legal provisions, it is not possible to reach conclusions on whether content related crimes were committed over the Internet. Participating States should therefore study the effectiveness of laws and other measures regulating Internet content, improve their data gathering and keeping and make such data publically available.

C. Blocking, Filtering, and Content Removal

Despite the introduction of new laws or amendments to existing laws, and the criminalization of the publication or distribution of certain types of content, in almost all instances extraterritoriality remains a major problem for Internet content regulation. Content is often hosted or distributed from outside the jurisdiction in which it is considered illegal. Laws are not necessarily harmonized at the OSCE level, let alone on a wider scale. What is considered illegal in one state may be perfectly legal in another. Different rules, laws, and regulations exist based upon different cultural, moral, political, constitutional and religious values. These differences will continue to exist and undoubtedly complicate efforts to find an appropriate

---

55 Paragraph 9.1. of the Final Act of the Copenhagen Meeting of the Conference on the Human Dimension of the CSCE, June 1990. http://www.osce.org/documents/odihr/2006/06/19392_en.pdf

56 Paragraph 26 of the Charter for European Security adopted at the OSCE Istanbul Summit 1999. See at http://www.osce.org/mc/17502.

57 See Paragraph 26 of the Final Document o fthe Moscow Meeting of the Conference on the Human Dimension of the CSCE, at http://www.osce.org/fom/item_11_30426.html. See also *Olsson v. Sweden (No. 1)*, judgment of 24 March 1988, Series A no. 130, § 67, and *Bladet Tromsø and Stensaas v. Norway* [GC], no. 21980/93, ECHR 1999-III.

balance between the right to freedom of expression and the prohibition of certain types of content deemed to be illegal by state authorities.

Based on the limited effectiveness of state laws, and lack of harmonization at international level a number of states started to block access to Internet websites and social media platforms that allegedly contain illegal content which are situated outside their legal jurisdiction. Blocking access to content seems to be faster, easier and a more convenient solution in cases where state authorities are unable to reach the perpetrators for prosecution, where mutual legal assistance agreements are not in place, or where the request for removal of such content is rejected by hosting or content providers in the countries in which the allegedly illegal content is hosted.

However, as will be seen below, blocking measures are not always provided by law, nor are they always subject to due process principles. Furthermore, blocking decisions are not necessarily taken by the courts of law, and often administrative bodies or Internet hotlines run by the private sector single handedly decide which content, website or platform should be blocked. Blocking policies often lack transparency and administrative bodies (including hotlines) lack accountability. Appeal procedures are either not in place or where they are in place, they are often not efficient. Therefore, increasingly, the compatibility of blocking with the fundamental right of freedom of expression must be questioned.

Part C of this report assesses relevant policy developments in the OSCE region, the Council of Europe and the European Union with regards to blocking, filtering, and content removal policies that are adopted and implemented.

Asked about **specific legal provisions which require closing down and/or blocking access to websites or any other types of Internet content (Question 14)**, 28 (50%) of the participating States stated that no such legal provisions exisit while 17 (30.4%) of the participating States do have laws in place which could be used to block access to websites. No data was obtained from 11 (19.6%) of the participating States.

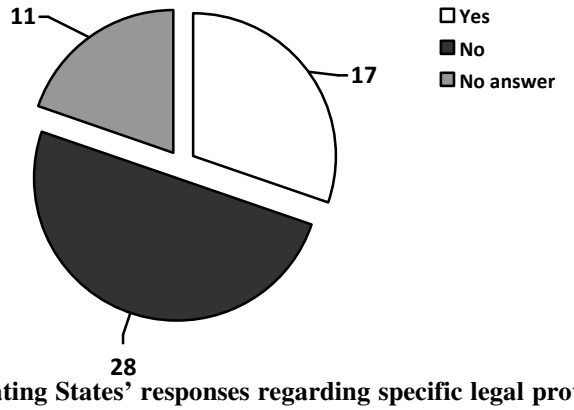


Figure 14. OSCE participating States' responses regarding specific legal provisions which require closing down and/or blocking access to websites or any other types of Internet content (Question 14)

The participating States were also asked whether they have **specific legal provisions which require blocking access to web 2.0 based applications and services such as YouTube, Facebook, or Blogger** in place **(Question 15)**. Only **Italy** responded positively to this question. 44 (78.6%) states responded negatively and **Albania**, **Azerbaijan**, **Belarus**, **Kazakhstan**, **Kyrgyzstan**, **Latvia**, **Lithuania**, **Norway**, and **Poland** explicitly stated that

there are no specific provisions which require blocking access to web 2.0 based applications and services. No data was obtained from 11 (19.6%) of the participating States.

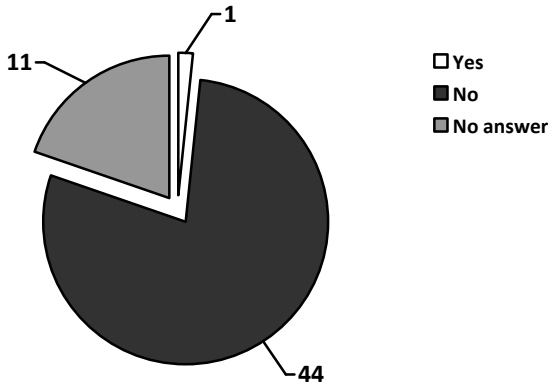


Figure 15. OSCE participating States' responses regarding specific legal provisions which require blocking access to web 2.0 based applications (Question 15)

Based on the responses received, there were no general legal provisions involving blocking in 10 participating States. These are **Austria**, **the Czech Republic**, **Germany**, **Luxembourg**, **the former Yugoslav Republic of Macedonia**, **Moldova**, **Montenegro**, **Poland**, **Serbia**, and **Slovakia**. However, there may be some removal provisions or other sanctions provided for in those countries. Furthermore, some participating States have **specific legal provisions** in the absence of **general legal provisions** which require closing down and/or blocking access to websites regarding individuals.

As will be detailed in Part II, several international organizations have recognized the need to protect children from harmful content. The European Commission developed an Action Plan on safer use of the Internet, the CoE Parliamentary Assembly recommended to address the needs and concerns of children online without undermining the benefits and opportunties offered to them on the Internet[58] and the Committee of Ministers also recommended that safe and secure spaces similar to walled gardens should be developed for children on the Internet. In 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."[59] The need to protect children from harmful content was highlighted and the development of a pan-European trustmark and labelling system[60] was encouraged. However, the CoE Committee decided not to recommend state level blocking or filtering mechanisms for the protection of children but allowed for exceptions for the protection of minors and member states can consider the installation and use of filters in places accessible to children such as schools or libraries.[61] The need to limit

[58] 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

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

[60] 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.

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

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

Asked whether **specific legal provisions requiring schools, libraries, and Internet cafes to use filtering and blocking systems and software (Question 18)** exist in their countries, 38 (67.9%) participating States responded with "no" while legal provisions do exist in 6 (10.7%) states.[62] No data was obtained from 12 (21.4%) of the participating States.

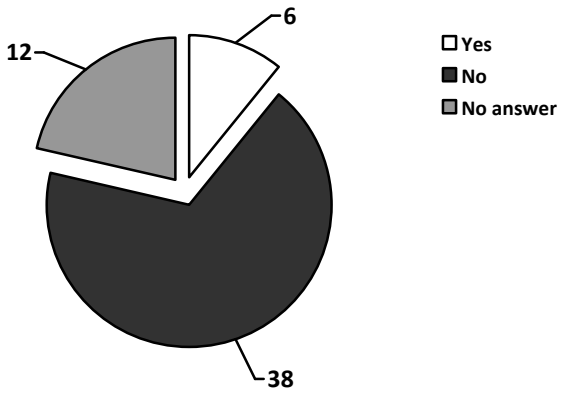


Figure 16. OSCE participating States' responses regarding specific legal provisions requiring schools, libraries, and Internet cafes to use filtering and blocking systems and software (Question 18)

The assessment of blocking, filtering and content removal provisions and policies revealed that complete suspension of communication services, including Internet access related services is possible in some OSCE participating States in times of war, states of emergency, as well as in the case of an imminent threat to national security. Although there is no so-called 'Internet kill switch' mechanisms in those countries, legal provisions may allow the authorities to switch off completely all forms of communications, including Internet communications, under certain circumstances. An 'Internet kill switch' idea was considered by the **United States** where it was envisaged that the President can authorize the shutdown of critical computer systems in the event of a national cyber emergency, however, the U.S. Senate did not act on the proposed measure.[63]

In several participating States the legal remedy provided for allegedly illegal content is removal or deletion; other participating States provide access blocking measures in addition to the removal measures. In some participating States such as in **Belarus** and the **Russian Federation** "prohibited information lists" maintained by government authorities exist. Access may be blocked if "prohibited information" appears on the Internet. Some countries also started to develop country level domain name blocking or seizure policies (**Czech Republic, Moldova**, **Switzerland**, and **United Kingdom**).

Turkey provides the broadest legal measures for blocking access to websites by specifying eleven different content related crimes, but does not reveal the number of websites blocked under the law.

Legal provisions for blocking access to child pornography exist in **Bulgaria**, **Finland**, **Italy, Liechtenstein, Romania, Turkey**, and **Ukraine**. At EU level, "mandatory blocking" of

62 Azerbaijan, Belarus, Croatia, Lithuania, Poland, and Turkey.

63 Note Protecting Cyberspace as a National Asset Act of 2010. See Cnet News, Internet 'kill switch' bill will return, 24 January, 2011, at <http://news.cnet.com/8301-31921_3-20029282-281.html>.

websites containing child pornography was not recommended but the member states "may take the necessary measures in accordance with national legislation to prevent access to such content in their territory".[64] However, in a number of countries, so-called 'voluntary blocking measures' to block access to known child pornography websites exist. **Canada**, **Denmark**, **France**, **Finland**, **Netherlands**, **Norway**, **Sweden**, **Switzerland** and the **United Kingdom** are among the participating States where such voluntary arrangements exist. While **Canada** and the **United Kingdom** rely on the British Telecom developed Cleanfeed system for ISP-level blocking, other ISP-level blocking systems are used in other participating States where voluntary blocking measures exist. In almost all instances, blocking lists and blocking criteria are not made public. Only in **Italy** the blacklist for blocking access to international or unlicensed gambling websites is transparently made available.

There is concern that voluntary blocking mechanisms and agreements do not respect due process principles within the states in which they are used. In the absence of a legal basis for blocking access to websites, platforms and Internet content, the compatibility of such agreements and systems with OSCE commitments, Article 19 of the Universal Declaration and Article 10 of the European Convention on Human Rights is arguably problematic. Although the auhorities' good intentions to combat child pornography and other types of illegal content is legitmate, in the absence of a valid legal basis in domestic law for blocking access to websites, the authority or power given to certain organizations and institutions to block, administer, and maintain the blacklists remains problematic. Such a "voluntary interference" might be contradictory to the conclusions of the Final Document of the Moscow Meeting of the Conference on the Human Dimension of the CSCE and in breach of Article 19 and Article 10 of the European Convention on Human Rights unless the necessity for interference is convincingly established.[65] Both, the 1994 Budapest OSCE Summit Document and the European Court of Human Rights reiterated the importance of freedom of expression as one of the preconditions for a functioning democracy. In Budapest "[t]he participating States reaffirm[ed] that freedom of expression is a fundamental human right and a basic component of a democratic society. In this respect, independent and pluralistic media are essential to a free and open society and accountable systems of government." Genuine, "effective" exercise of this freedom does not depend merely on the state's duty not to interfere, but may require positive measures to protect this fundamental freedom.[66] Therefore, a blocking system based exclusively on self-regulation or "voluntary agreements" risks being a non-legitimate interference with fundamental rights.

Independent courts of law are the guarantors of justice which have a fundamental role to play in a state governed by the rule of law. In the absence of a valid legal basis, the issuing of blocking orders and decisions by public or private institutions other than independent courts of law is therefore inherently problematic from a human rights perspective. Even provided that a legal basis exists for blocking access to websites, any interference must be proportionate to the legitimate objective pursued. Within this context, it is submitted that the domain-based blocking of websites and platforms carrying legal content such as YouTube, Facebook, Wordpress and Twitter could be incompatible with OSCE commitments, namely the conclusions of the Final Act of Copenhagen and the conclusions of the Final Document of

---

64 Committee on Civil Liberties, Justice and Home Affairs, Press Release: Delete child pornography web pages across the EU, says Civil Liberties Committee, 14.02.2011.

65 See Paragraph 26 of the Final Document o fthe Moscow Meeting of the Conference on the Human Dimension of the CSCE, at http://www.osce.org/fom/item_11_30426.html. See also *Observer and Guardian v. the United Kingdom*, 26 November 1991, § 59, Series A no. 216.

66 See *Özgür Gündem v. Turkey*, no. 23144/93, §§ 42-46, ECHR 2000-III, and *Fuentes Bobo v. Spain*, no. 39293/98, § 38, 29 February 2000.

the Moscow Meeting as well as with Article 10 of the European Convention on Human Rights, and regarded as a serious infringement on freedom of speech. Such a disproportionate measure would be more far-reaching than reasonably necessary in a democratic society.[67]

The Internet started to play an essential role as a medium for mass communication, especially through the development of Web 2.0 based platforms, enabling citizens to actively participate in the political debate and discourse. These platforms provide a venue popular across the world for alternative and dissenting views. Therefore, banning access to entire social media platforms carries very strong implications for political and social expression.

State-level blocking policies undoubtedly have a serious impact on freedom of expression, which is one of the founding principles of democracy. Blocking orders that are issued and enforced indefinitely on websites could result in "prior restraint". Although the European Court of Human Rights does not prohibit prior restraint on publications, the dangers inherent in prior restraint are such that they call for the most careful scrutiny on the part of the court.[68] This is particularly valid for the press as news is a perishable commodity and delaying its publication, even for a short period, may well deprive it of all its value and interest.[69] The same principles also apply to new media and Internet publications. Prior restraint and other bans imposed on the future publication of entire newspapers, or for that matter websites and Internet content are incompatible with the rights stipulated in the European Convention on Human Rights. The Strasbourg Court requires the consideration of less draconian measures such as the confiscation of particular issues of publications, including newspapers or restrictions on the publication of specific articles.[70] Arguably, the practice of banning access to entire websites, and the future publication of articles thereof (whose content is unknown at the time of access blocking) goes beyond "any notion of 'necessary' restraint in a democratic society and, instead, amounts to censorship".[71]

It is worth noting that litigation in **Belgium** triggered an application to the European Court of Justice regarding ISP-level blocking and filtering of websites containing copyright infringement. Advocate General Cruz Villalón of the Court of Justice of the European Union indicated that a measure ordering an ISP to install a system for filtering and blocking electronic communications in order to protect intellectual property rights in principle infringes on fundamental human rights.[72] The decision of the European Court of Justice will shed further light into blocking measures and their implications for fundamental human rights. Similarly, the European Court of Human Rights is currently considering two applications (regarding the blocking of Google sites and Last.fm) from **Turkey**. Both of these applications involve blocking measures. The European Court of Human Rights, therefore, may establish principles with regards to Internet and freedom of expression, and may comment on the issue

---

67 *Khurshid Mustafa and Tarzibachi v. Sweden*, App. no. 23883/06, judgment of 16 December, 2008.

68 *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.

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

70 *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.

71 *Cumpănă and Mazăre 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.

72 Court of Justice of the European Union, Press Release: Advocate General's Opinion in Case C-70/10 Scarlet Extended v Société belge des auteurs compositeurs et éditeurs (Sabam), No 37/11, Luxembourg, 14 April 2011.

of blocking access to websites. A decision surrounding these issues will certainly have broader implications for the Council of Europe member states.

On issues related to search engine providers, the CoE Committee of Experts on New Media published a draft "Guidelines for Search Engine Providers" during 2010.[73] The Committee stated that "search engine providers must promote transparency about systematic nationwide blocking or filtering about certain types of content and adhere to the principle of due process when removing specific search results from their index and provide access to redress mechanisms"[74] regardless whether the origin of removal requests is governmental, co-regulatory or private.[75]

Filtering software is mostly used in schools, libraries and Internet cafes within the OSCE region. In most cases, there are no legal requirements for their use but the laws of some participating States, such as **Belarus**, **Croatia**, **Lithuania**, **Poland** and **Turkey,** require filtering software to be used in academic institutions, libraries, and Internet cafes. In other states, such as **Canada**, **the Czech Republic**, **Hungary** and **Norway,** the use of filters is voluntary and not subject to any laws or legal provisions. The International Federation of Library Associations and Institutions, in conclusion to its 2010 annual report, warned that "filtering could, however, very easily develop into general Internet censorship and any developments should be carefully monitored by library communities and other interested parties, so as to ensure that legitimate information needs of the general public can be satisfied. Finally, "upstream filtering" of the Internet is a matter of serious concern."[76] Here it should be noted that **Turkey** decided to introduce a country-wide mandatory filtering system that will go into effect on 22 August 2011. If realized, this will lead to the first government controlled and maintained mandatory filtering system within the OSCE region.

D. Licensing and Liability related issues, and Hotlines to report Illegal Content

The final part of this study analyzes licensing and legal liability provisions related to information society service providers including access, content, platform, and search engine providers. Regarding liability for carrying third party content, in most instances liability will only be imposed upon information society service providers (including ISPs, 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[77] provides a limited and notice-based liability with takedown procedures for illegal content. The EU Directive suggests that "it is in the interest of all parties involved in the provision of information society services to adopt and implement procedures"[78] to remove and disable access to illegal information. Therefore, the service providers based in the European Union are not immune from prosecution and liability, and they are required to act expeditiously

---

73 See CoE Committee of Experts on New Media (MC-NM), draft Guidelines for Search Engine Providers, MC-NM(2010)009_en, Strasbourg, 5 October 2010.

74 *Ibid*.

75 See further CoE Committee of Experts on New Media (MC-NM), Draft Recommendation on the protection of human rights with regard to search engines, MC-NM(2010)004_en, Strasbourg, 11 March 2010

76 See *Ibid*, pp. 49-50.

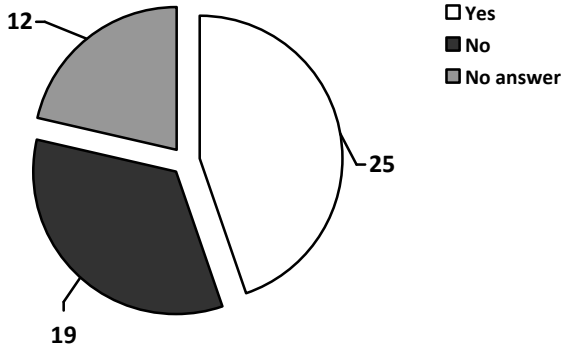
77 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, Official Journal of the European Communities, vol. 43, OJ L 178 17 July 2000 p. 1.

78 *Ibid*.

"upon obtaining actual knowledge" of illegal activity[79] or content, and "remove or disable access to the information concerned".[80] 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".[81]

A European Commission analysis of practice on notice and take-down 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".[82] A further review was subsequently commissioned in 2007, and the study disclosed all but harmonised implementation policies because "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."[83] Some further studies showed that ISPs based in Europe tend to remove and take-down content without challenging the notices they receive.[84] In 2010, the European Commission announced that it had found that the interpretation of the provisions on liability of intermediaries is frequently considered necessary in order to solve problems, and subsequently launched a consultation.[85]

The survey asked whether **specific legal liability provisions and licensing requirements for Internet Service Providers** are in place in participating States. **(Question 19)** While in 19 (33.9%) states no such legal provisions exist, 25 (44.7%) responded positely to the question. No data was obtained from 12 (21.4%) of the participating States.



79 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.

80 *Ibid*., para. 46.

81 *Ibid*.

82 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, section 4.7.

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

84 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.

85 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. The result of this work will be taken into account in the Commission's deliberations with a view to the adoption in the first half of 2011 of a Communication on electronic commerce, including on the impact of the Electronic Commerce Directive .

Figure 17 . OSCE participating States' responses regarding specific legal provisions and licensing requirements for Internet Service Providers (Question 19)

Similarly, the participating States were also asked whether **there are specific legal liability provisions and licensing requirements for Internet Search Engines or Content Providers** (e.g. Google, Yahoo, etc. **Question 20)**. While four (7.1%) of the states responded posititely, no such legal provisions exist in 38 (67.9%) of the participating States. No data was obtained from 14 (25%) of the participating States.

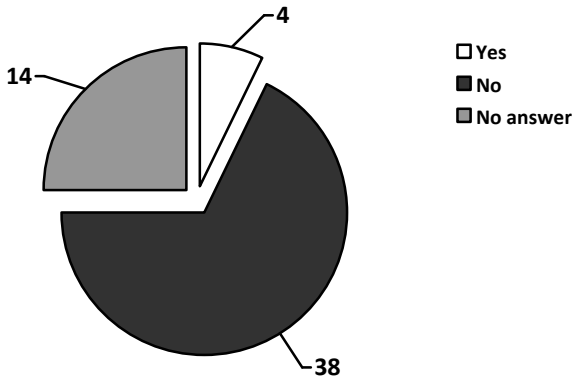


Figure 18. OSCE participating States' responses with regards to specific legal liability provisions and licensing requirements for Internet Search Engines or Content Providers (Question 20)

As can be seen above almost none of the OSCE participating States provide for any separate legal liability regime or licensing requirements for Internet search engines and content providers.

The survey also asked whether **specific legal provisions based on the "notice and take-down" principle** exist in the OSCE participating States **(Question 16)**. No such provisions are in place in 27 (48.2%) participating States while legal provisions do exist in 18 (32.2%) states. No data was obtained from 11 (19.6%) of the participating States.

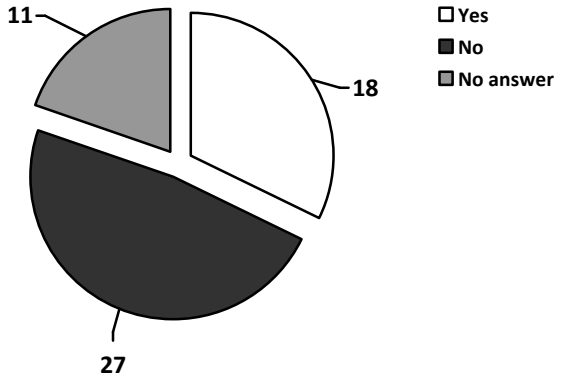


Figure 19. OSCE participating States' responses regarding specific legal provisions based on the "notice and take-down" principle (Question 16)

Finally, some participating States (where applicable) were asked **whether the EU E-Commerce Directive 2000/31 has been implemented into national law in their country** (Question 19c). In 32 (57.1%) of the participating States the EU Directive is implemented into

national law.[86] 10 (17.9%) states responded negatively and no data was obtained from 14 (25%) of the participating States.

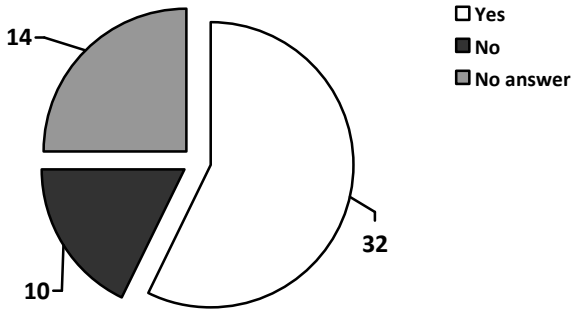


Figure 20. OSCE participating States' responses regarding the implementation of the EU E-Commerce Directive 2000/31 (Question 19c)

In addition to notice-based liability systems, hotlines to which allegedly illegal Internet content can be reported to have been developed in Europe and extended to other regions, too. The majority of the existing hotlines try to tackle the problem of child pornography and most of the hotlines based in the European Union are co-financed by the EU Safer Internet Action Plan.[87] 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 hotlines.[88] The survey results seem to indicate a rather low public awareness of the existence and purpose of these hotlines.[89]

The survey asked whether **specific (public or private) hotlines to report allegedly illegal content** to exist in the OSCE participating States **(Question 17).** Eight (14.3%) of the states replied negatively to this question. Hotlines exist in 37 (66.1%) of the participating States. No data was obtained from 11 (19.6%) the participating States. Public hotlines exist in 13 OSCE participating States. Equally, 13 participating States have private hotlines and 11 have both public and private hotlines to which illegal Internet content can be reported to.

---

86 It has to be noted, however, that only 27 of the 56 OSCE participating States are members of the European Union. The 32 countries that implemented the Directive include also EU candidate and potential candidate countries.

87 This includes INHOPE, the International Association of Internet Hotlines, an umbrella organization, which was set up in 1999 with the aim of establishing a network of Internet hotlines. As of today, it includes 39 national hotlines.

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

89 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.

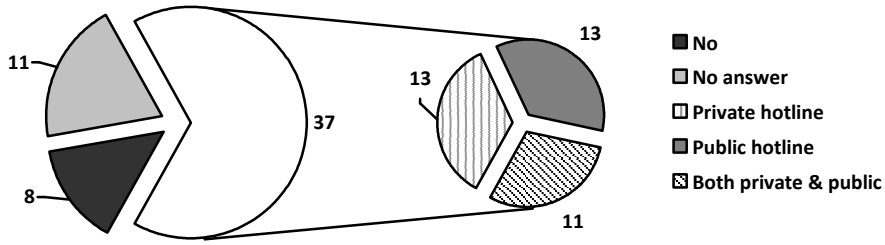


Figure 21. OSCE participating States' responses regarding the presence of specific (public or private) Hotlines to report allegedly illegal content (Question 17)

Part D of this study has shown that a number of participating States have general licensing requirements for the information society service providers while others require only some level of activity notification to the relevant authorities. It should also be highlighted that in certain countries there are no licensing requirements at all.

Liability provisions for service providers are not always clear and complex notice and take-down provisions exist for content removal from the Internet within a number of participating States. Approximately 30 participating States have laws based on the EU E-Commerce Directive. However, the EU Directive provisions rather than aligning state level policies, created differences in interpretation during the national implementation process. These differences emerged once the provisions were applied by the national courts. Aware of such issues, the European Commission launched a consultation during 2010 on the interpretation of the intermediary liability provisions. A review report is expected during 2011.[90] Furthermore, a case was filed with the European Court of Human Rights coming from **Estonia**. The case is significantly important as the Court will have the opportunity to scrutinize the "notice based liability" measures of the E-Commerce Directive with regards to Article 10 of the European Convention on Human Rights as well as issues surrounding third-party comments published on news portals and social media platforms.

Regarding the formation of public or private hotlines, it should be noted that although hotlines could potentially play an important role in relation to illegal Internet content, there remain significant questions on their operation. Private hotlines are often criticized as there remain serious concerns regarding the "policing" role they might play. It is argued that decisions involving illegality should remain a matter for the courts of law to ensure the due process principle, rather than left to hotlines operating outside a legal framework. This concern was recognised in the Martabit Report to the UN stating 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".[91] The operation of private hotlines formed through self-regulatory means should be consistent with the principles underlying the European Convention on Human Rights. States may have a positive obligation to guarantee that hotlines

[90] Public consultation on the future of electronic commerce in the internal market and the implementation of the Directive on Electronic commerce (2000/31/EC).

[91] 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.

respect due process principles, and their functions and practice do not contravene the the principles underlying the European Convention.[92] States must furthermore provide adequate and effective safeguards against abuse. These should include procedures for effective judicial scrutiny of the decisions taken by the hotlines.[93]

Furthermore, the lack of transparency with regarding the work of hotlines often attracts accusations of censorship. Leaked "child pornography" blocking blacklists maintained by hotlines from Finland,[94] Denmark,[95] and Italy[96] (as well as from China,[97] Thailand,[98] Australia,[99]) that were published on the whistleblower website Wikileaks have demonstrated that most of the hotlines also block access to adult pornographic content and even political content. In the absence of openness and transparency of the work of the hotlines and by creating secrecy surrounding the blocking criteria and keeping the list of blocked websites confidential, concerns will continue to exist regarding the work of such hotlines. The hotlines can only refute such criticism if they are established within a regulatory framework that is compatible with the requirements of the European Convention on Human Rights and other internationally applicable standards, including OSCE commitments.

E. Conclusions and Recommendations

The analysis of the data and information provided by the OSCE participating States on Internet content regulation leads to the following conclusions and recommendations:

The open and global nature of the Internet should be ensured

Participating States need to take action to ensure that the Internet remains as an open and public forum for freedom of opinion and expression, as guaranteed by OSCE commitments, enshrined in the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and the European Convention on Human Rights. OSCE participating States should keep in mind the borderless nature of the Internet when developing online content regulation policies. The preservation of the global nature of the Internet requires participating States to consider regional and alternative approaches to online content regulation.

---

92 See *Özgür Gündem v. Turkey*, no. 23144/93, §§ 42-46, ECHR 2000-III, and *Fuentes Bobo v. Spain*, no. 39293/98, § 38, 29 February 2000.

93 See *Lupsa v. Romania*, no. 10337/04, § 34, 8 June 2006.

94 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>.

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

96 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>.

97 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>.

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

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

Access to the Internet should be regarded as a human right and recognized as implicit to the right to free expression and free information

Access to the Internet remains the most important pre-requisite 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 should be recognized as a fundamental human right.

The right to freedom of expression is universal – also in regards to the medium and technology

The right to freedom of expression and freedom of the media were not designed to fit a particular medium, technology or platform. Freedom of expression applies to all means of communications, including the Internet. Restrictions to this right are only acceptable if in compliance with international norms and standards. Any restriction should be weighed against the public interest.

New technologies require new approaches

Typically, the stance taken by the participating States is that what is illegal and punishable in an offline form must at least be treated equally online. There are, however, several features of the Internet which fundamentally affect approaches to its governance. While rules and boundaries still exist, enforcement of existing laws, rules and regulations to digital content becomes evidently complex, problematic and at times impossible to enforce on the Internet. Participating States should develop alternative approaches adapted to the specific nature of the Internet. Participating States should also place more emphasis on Internet and media literacy projects for vulnerable groups, particularly children.

Network neutrality should be respected

Legal or technical measures 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 the free flow of information. Online information and traffic should be treated equally regardless of the device, content, author, origin or destination. Service providers should make their information management practices of online data transparent and accessible.

Furthermore, information society service provision should not be subject to governmental barriers and strict licensing regimes.

Internet 'kill switch' plans should be avoided

Existent legal provisions allow several OSCE participating States to completely suspend all Internet communication and "switch off" Internet access for whole populations or segments of the public during times of war, states of emergency and in cases of imminent threat to national security. Reaffirming the importance of fully respecting the right to freedom of opinion and expression, the OSCE participating States should refrain from developing, introducing and applying "Internet kill switch" plans as they are incompatible with the fundamental right to information.

OSCE participating States should avoid vague legal terminology in speech-based restrictions

Definitional problems and inconsistencies exist with regards to certain speech based restrictions. Clarifications are needed to define what amounts to “extremism”, “terrorist propaganda”, “harmful” and “racist content” and “hate speech”. Legal provisions are often vague and open to wide or subjective interpretation. Any restriction must meet the strict criteria under international and regional human rights law. The necessity for restricting the right to speak and receive information must be convincingly established to be compatible with international human rights standards.

OSCE participating States should refrain from mandatory blocking of content or websites

Given the limited effectiveness of national laws and the lack of harmonization at international level to prosecute criminal online content, a number of OSCE participating States started to block access to online content deemed illegal and Web 2.0 based social media platforms situated outside their legal jurisdiction. As blocking mechanisms are not immune from significant deficiencies, they may result in the blocking of access to legitimate sites and content. Further, blocking is an extreme measure and has a very strong impact on freedom of expression and the free flow of information. Participating States should therefore refrain from using blocking as a permanent solution or as a means of punishment. Indefinite blocking of access to websites and Internet content could result to “prior restraint” and by suspending access to websites indefinitely states can largely overstep the narrow marginof appreciation afforded to them by international norms and standards.

Blocking of online content can only be justified if in accordance with these standards and done pursuant to court order and where absolutely necessary. Blocking criteria should always be made public and provide for legal redress.

Voluntary blocking and content removal arrangements should be transparent and open to appeal

Voluntary blocking measures and agreements exist in a number of OSCE participating States. However, private hotlines do not always have legal authority to require ISPs to block access to websites or to require removal of content. Any blocking system based exclusively on self-regulation or voluntary agreements between state actors and private actors have to be conceived in a way as not to interfere with fundamental rights. Furthermore, blocking criteria of hotlines and private actors are not always transparent or open to appeal. Any blocking or removal system based on self-regulation and voluntary agreements should be transparent, compatible with international norms and standards and provide for redress mechanisms and judicial remedies.

Filtering should only be encouraged as an end-user voluntary measure

OSCE participating States should encourage the use of end-user filtering software on individual home computers and in schools if their use is deemed necessary. However, the deployment of state-level upstream filtering systems, as well as government-mandated filtering systems, should be avoided. If the use of filters is encouraged by the states, users should be made aware of the potential limitations of filtering software as there are serious questions about the reliability of such tools as stand-alone solutions for child protection.

‘Three-strikes’ measures to protect copyright are incompatible with the right to information

The development of so-called “three-strikes” legal measures to combat Internet piracy in a number of participating States is worrisome. While countries have a legitimate interest to combat piracy, restricting or cutting off users’ access to the Internet is a disproportionate response which is incompatible with OSCE commitments on the freedom to seek, receive and impart information, a right which in fact should be strengthened by the Internet. Participating States should refrain from developing or adopting legal measures which could result restricting citizens’ access to the Internet. A discussion on whether or not current international standards on intellectual property protection are suited for our information society might be necessary.

Reliable information on applicable legislation and blocking statistics needs to be made available

Despite the high responsiveness of the participating States to take part in the survey, many governments expressed major difficulties in collecting the requested data, because reliable or recorded information was not available or different governmental institutions and ministries are responsible for the different aspects of the Internet. Almost no participating State had an institutional focal point on Internet matters to fall back to. It is recommended that participating States put mechanisms in place that allow for the maintenance of reliable information on Internet content regulation and statistical data pertaining to questions on blocking statistics and prosecutions for speech-related offenses committed on the Internet. These statistics and information should be made available to the public.

Participating States should also increase their efforts to better coordinate and share information on Internet content regulation.

PART II

OVERVIEW OF LAWS AND PRACTICES ON INTERNET CONTENT REGULATION IN THE OSCE AREA

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 to recognize Internet access as inherent to the right to free expression and as such to be a fundamental and universal human right, on the other hand, a number of governments are considering adopting content and access blocking measures.[100] Countries such as Finland and Estonia have already ruled that access is a fundamental human right for their citizens, and according to a 2010 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."[101]

Within 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 the purposes and principles of the Charter of the United Nations and respecting fully and upholding the Universal Declaration of Human Rights."[102]

By taking these important policy developments into account the OSCE survey asked the participating States whether they have

- specific legal provisions on the right to access the Internet (**Question 1**)
- general legal provisions which could restrict users' access to the Internet (**Question 2**)
- specific legal provisions guaranteeing or regulating "net neutrality" (**Question 3**)

Asked whether there are specific legal provisions on the right to access the Internet (Question 1), only 17 (30.3%) of the participating States answered positively to this question while 29 States (51.8%) stated that no such provisions exist. No data was obtained from 10 participating States (17.9%).

---

100 Note also the report by Frank La Rue, the United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, presented to the UN Human Rights Council on 3 June 2011.

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

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

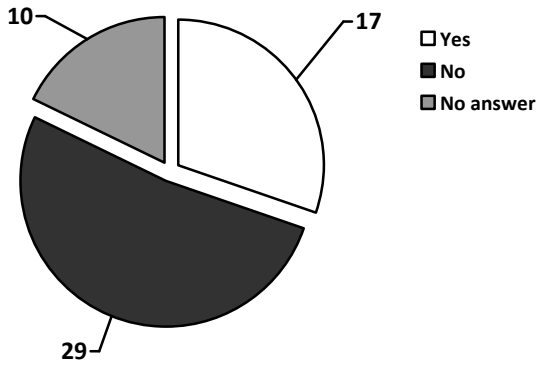


Figure 22. OSCE participating States' responses with regards to the presence of specific legal provisions on the right to access the Internet (Question 1)

Among the States which have access related provisions, a number of responses stated that the right to access the Internet is a right interwoven with the right to access to information and communication, protected by the state constitutions. This includes that everyone has the right to participate in the information society and, in turn, the state has a responsibility to assist in the advancement of it.[103] In some states, the right to access the Internet is provided by specific laws, usually within universal access laws or regulations.[104]

Legal provisions which could restrict users' access to the Internet

The OSCE survey also asked the participating States whether **there are general legal provisions which could restrict users' access to the Internet (Question 2)** in their country. 39 (69.6%) of the participating States stated "no", while only 7 participating States[105] (12.5%) stated that they have general legal provisions which could restrict users' access to the Internet. No data was obtained from ten (17.9%) of the participating States.

[103] Cyprus, Estonia, Georgia, Greece, Portugal, Russia, and Ukraine.

[104] **Albania** (Law No. 9918 (19.05.2008) "On electronic communications in the Republic of Albania"); **Estonia** (Public Information Act § 33: Access to data communication network stipulates the right to have access to the Internet (access to data communication network). Every person shall be afforded the opportunity to have free access to public information through the Internet in public libraries, pursuant to the procedure provided for in the Public Libraries Act); **Finland** (Communications Market Act (393/2003), chapter 6 contains provisions concerning universal service. Persons residing in Finland have been granted a connection of at least 1 Mbit/s); **France** (French Constitutional Council Decisions 2009-580 DC Code for Post and Electronic Communications); **Germany** (Section 78 of the Telecommunications Act (Telekommunikationsgesetz, TKG)); **Hungary** (Universal Service Obligation, Act C of 2003, Section 117); **Montenegro** (Law on Electronic Communications ("Official Gazette of Montenegro no. 50/08), Article 102); **Spain** (Spanish General Telecommunications Act 32/2003, of 3 November, article 22, includes Internet access as a Universal Service); **Turkey** (Universal Service Law No. 5369 dated 16.06.2010); **Turkmenistan** (Article 38 (The Regulations on Internet Services Provision) of the Law of Turkmenistan "On Communications" of March 12, 2010).

[105] These are Azerbaijan, France, Latvia, Lithuania, Portugal, Ukraine, and Turkmenistan.

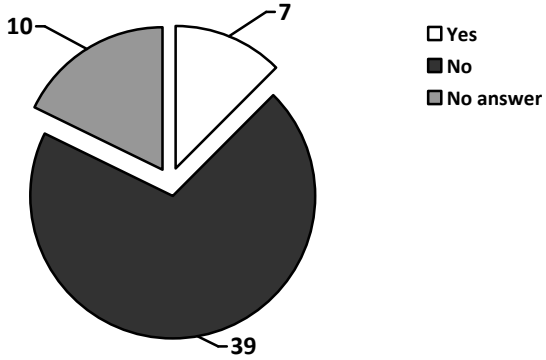


Figure 23. OSCE participating States' responses with regards to the presence of general legal provisions which could restrict users' access to the Internet (Question 2)

Based on the information received from the participating States, in certain countries access to the Internet can be restricted to all users subject to various legal provisions, in certain countries access can be restricted to individual users, and in others restrictions apply to specific types of Internet content only as will be outlined later in this study.

For example, in **Azerbaijan**, according to Clause 3 of the "Order of the Azerbaijan Republic Ministry of Communications and Information Technologies" issued on 24 February, 2000, a provider can suspend delivery of Internet services in certain circumstances including in times of war or state of emergency, in events of natural disaster, or other catastrophe, or when services are provided to third parties without the appropriate license, and in cases where systems that are either defective or uncertified are connected to the network. Delivery of Internet services can also be suspended in cases that run against the rules established by the legislation of the Azerbaijan Republic and the law "On Telecommunications".

The official response provided by **France** referred to Law No. 2009-669 of 12 June, 2009 on promoting the dissemination and protection of creation on the Internet which includes a flexible response mechanism. The provisions may entail restricting Internet access of users after a judicial decision.[106] In **Latvia**, Section 9(1)(5) of the Law on Information Technologies Security[107] stipulates that upon a request from the Institution on Prevention of Security Incidents a user's access to the electronic communication networks may be temporally restricted up to 24hrs if the user substantially endangers the rights of other users, or the information system itself, or the security of the electronic communication networks. In **Lithuania**, access can only be restricted upon the expiry of the service credit limit, or in case the subscriber violates the conditions of the terms of service subject to certain regulations.[108] The **Russian Federation**, in its response, stated that although Russia does not generally restrict access to the Internet, restriction of access to information can be provided by federal laws in order to protect the foundations of the constitutional system, morality, health, rights

106 See further assessment with regards to question 9 of the survey on legal provisions outlawing Internet piracy later in this report.

107 Section 9 of the Law on Information Technologies Security is entitled 'On the security of public electronic communication nets'. Article 9 came into force on 1 May 2011 and the relevant Cabinet of Ministers' regulatory rules on its implementation shall be issued until that date.

108 Paragraph 28 of The Rules for Provision of Electronic Communications Services approved by Order No. 1V-1160 of the Director of the Communications Regulatory Authority of the Republic of Lithuania of 23 December 2005.

and lawful interests of other persons, and ensure the country's defence and state security.[109] In **Turkey**, access to websites including social media platforms can be blocked subject to Law No. 5651, entitled "Regulation of Publications on the Internet and Suppression of Crimes Committed by means of Such Publication," and subject to Law No. 5846 on "Intellectual & Artistic Works" with regards to intellectual property infringements. In **Ukraine**, in the context of copyright protection, Article 38(9)(1) of the Law "On Telecommunications" provides for the communications operators and Internet providers to disconnect, pursuant to a court decision, the terminal equipment of the user if it is used for unlawful acts.[110] In **Turkmenistan**, access restrictions may apply through the government-owned Turkmen Telecom, and users can only use "terminal equipment" that has been officially certified.[111] Users are prevented from "the use of terminal equipment to commit unlawful acts that affect the national security, defence, law and order".[112]

Based on the positive considerations to recognize Internet access as a fundamental human right, the adoption or consideration of measures to restrict access by certain governments is worrisome.

Legal provisions guaranteeing or regulating "Net 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 type or destination, so that the Internet users "should have the greatest possible access to Internet-based content."[113] Users should be able to use 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, the network, or the device used for Internet connectivity. As declared by the Council of Europe Committee of Ministers in 2010, "access to infrastructure is a prerequisite for the realisation of this objective".[114] More importantly, 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."[115]

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."[116] Therefore, there is

---

109 Note Article 9 (1) of Federal Law No. 149-FZ of 27 July 2006 "On Information, Information Technologies and Information Protection".

110 Unlawful acts in this case refer to a violation of the Law of Ukraine "On Copyright and Related Rights".

111 The official text reads: "terminal equipment that has the document of conformity with requirements". Article 42(2) (The Obligations of Telecommunications Service Users) of the Law of Turkmenistan "On Communications". Note further US Bureau of Democracy, Human Rights, and Labor, 2009 Country Reports on Human Rights Practices, March 11, 2010, at <http://www.state.gov/g/drl/rls/hrrpt/2009/index.htm>.

112 *Ibid*, Article 42(3).

113 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.

114 *Ibid*.

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

116 *Ibid*.

"growing international interest as to whether, and to what extent, traffic management should be subject to regulation."[117] According to a discussion paper issued by OFCOM, the independent regulator and competition authority for the UK communications industries, "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"[118] thus in fact giving preference to certain data-heavy services, such as Voice-over-IP or video-streaming services.

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

With regards to this debate, 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."[119]

The 2009 EU Regulatory Framework lays down net neutrality as a policy objective and states that end-users should be able to access and distribute information or run applications and

---

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

118 *Ibid*.

119 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, Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.

services of their choice. The revised EU Universal Service Directive (2002/22/WE)[120] requires operators through Article 22 to be transparent on minimum quality of service (QoS) levels[121] offered, and enables national regulatory authorities to set minimum QoS requirements on public electronic communications network providers. Although there is no set definition of 'net neutrality', Article 8(§4)(g) of the Framework Directive[122] requires national regulatory authorities to promote the interests of the citizens of the European Union by fostering the ability of end-users to access and distribute information or run applications and services of their choice. This is supported by new transparency requirements vis-à-vis consumers.[123] Subject to these provisions, consumers will need to be informed about certain issues when subscribing to a service. These include conditions under which a EU member state may limit access to and/or use of services and applications, the procedures put in place by the provider in order to measure and shape traffic so as to avoid filling or overfilling a network link, and how these measures may impact on service quality. All these provisions, contained in the revised EU regulatory framework, had to be transposed into national legislation by the EU member states by 25 May 2011.

Furthermore, the European Commission launched a public consultation on "the open Internet and net neutrality in Europe", conducted between 30 June and 30 September 2010.[124] In a Communication paper published in April 2011,[125] the Commission referred to a survey conducted by the Body of European Regulators for Electronic Communications (BEREC)[126] in early 2010 to assess the state of play with regards to net neutrality in the different member states. According to the Commission, "BEREC noted that there have been instances of unequal treatment of data by certain operators."[127] According to the BEREC survey limits on the speed (so called 'throttling') of peer-to-peer (P2P) file-sharing or video streaming by certain providers in France, Greece, Hungary, Lithuania, Poland and the United Kingdom were witnessed. Furthermore, BEREC survey also found that blocking of or additional charging for the provision of VoIP services in mobile networks are applied by certain mobile

120 Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services.

121 National regulatory authorities may specify, inter alia, the quality of service parameters to be measured, and the content, form and manner of information to be published, in order to ensure that end-users have access to comprehensive, comparable and user-friendly information. Where appropriate, the parameters, definitions and measurement methods given in Annex III could be used. For the definition of quality-of-service parameters, definitions and measurement methods referred in Article 22, see Annex III: Quality of Service Parameters, EU Universal Service Directive (2002/22/WE).

122 Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 (Framework Directive).

123 Article 21 of the Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, commonly referred to as EU Universal Service Directive.

124 The consultation attracted over 300 responses from a wide range of stakeholders, including network operators, Internet service providers, member states, consumer and civil society organizations as well as a number of individuals.

125 See the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of Regions on The Open Internet and Net Neutrality in Europe, Com(2011) 222 final, Brussels, 19.04.2011.

126 BEREC replaced the European Regulators Group (ERG), the group through which National Regulatory Authorities (NRAs) exchange expertise and best practice and delivered opinions on the functioning of the telecoms market in the EU.

127 Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of Regions on The Open Internet and Net Neutrality in Europe, Com(2011) 222 final, Brussels, 19.04.2011., pp 5-6.

phone operators in Austria, Germany, Italy, the Netherlands, Portugal and Romania.[128] The European Commission will publish, by the end of 2011, further findings and analysis to be conducted by BEREC including any instance of blocking or throttling certain types of traffic. On the basis of the evidence and the implementation of the telecom framework provisions, the European Commission announced that it will decide, as a matter of priority, on the issue of additional guidance on net neutrality.[129]

While the 27 member states of the European Union had time until 25 May 2011 to transpose the Telecoms Reform Package into national legislation,[130] the American Civil Liberties Union called with an October 2010 report on the US government to act to preserve the free and open Internet arguing that net neutrality is "one of the "foremost free speech issues of our time."[131] In December 2010, the Federal Communications Commission (FCC) issued the "Open Internet Order" to preserve the Internet as an open platform for "innovation, investment, job creation, economic growth, competition, and free expression".[132] To provide greater clarity and certainty regarding the continued freedom and openness of the Internet, the FCC decided to adopt three basic rules that are grounded in broadly accepted Internet norms:

> i. **Transparency.** Fixed and mobile broadband providers must disclose the network management practices, performance characteristics, and terms and conditions of their broadband services;
> ii. **No blocking.** Fixed broadband providers may not block lawful content, applications, services, or non-harmful devices; mobile broadband providers may not block lawful websites, or block applications that compete with their voice or video telephony services; and
> iii. **No unreasonable discrimination.** Fixed broadband providers may not unreasonably discriminate in transmitting lawful network traffic.[133]

According to the FCC, the framework adopted "aims to ensure the Internet remains an open platform— one characterized by free markets and free speech—that enables consumer choice, end-user control, competition through low barriers to entry, and the freedom to innovate without permission."[134]

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

---

128 The European Commission does not have evidence to conclude that these concerns are justified at this stage but this should be borne in mind in a more exhaustive fact-finding exercise. See the Communication fro the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of Regions on The Open Internet and Net Neutrality in Europe, Com(2011) 222 final, Brussels, 19.04.2011.

129 *Ibid*., p. 9.

130 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.

131 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-

132 See Article 1 of the Open Internet Order, Federal Communications Commission, FCC 10-201, 21 December, 2010, at <http://www.fcc.gov/Daily_Releases/Daily_Business/2010/db1223/FCC-10-201A1.pdf>.

133 *Ibid*.

134 *Ibid*.

by non-transparent traffic management, content and services' discrimination or impeding connectivity of devices."[135] 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 the Committee of Ministers to member states on measures to promote the respect for freedom of expression and information with regard to Internet filters."[136]

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."[137]

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."[138]

The OSCE participating States were asked whether **there are specific legal provisions guaranteeing or regulating "net neutrality" (Question 3)** in their jurisdiction. Only **Finland** responded 'yes' (1.8%), while 45 States responded 'no' (80.4%). No data was obtained from ten (17.9%) of the participating States.

In **Finland**, since July 2010, subject to section 60(3) of the Communications Market Act,[139] all Finnish citizens have a legal right to access a one megabit per second broadband connection, reportedly making Finland the first country to accord such a right.[140]

---

135 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

136 *Ibid*., para 6.

137 *Ibid*., para 8.

138 *Ibid*., para 9.

139 See Section 60 c (331/2009) Universal service obligation concerning the provision of universal telephone services of the Finnish Communications Market Act at <http://www.finlex.fi/en/laki/kaannokset/2003/en20030393.pdf>: "Provisions on the minimum rate of a functional Internet access…. are issued by a decree of the Ministry of Transport and Communications. Prior to the issuance of the decree, the Finnish Communications Regulatory Authority shall examine the data transfer service markets, prevailing access rates available to the majority of subscribers and level of

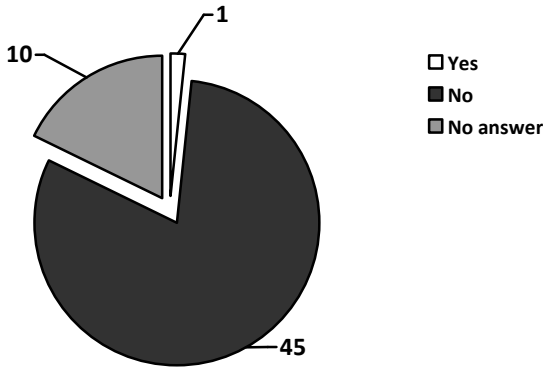


Figure 24. OSCE participating States' responses with regards to specific legal provisions guaranteeing or regulating "net neutrality" (Question 3)

It is also worth noting that although there are no legal provisions as such in **Norway**, the Norwegian Post and Telecom Authority (NPT) has developed a set of guidelines for network neutrality together with the Norwegian Internet service providers, content providers, industry associations and consumer authorities. According to the guidelines:

- Internet users are entitled to an Internet connection with a predefined capacity and quality.
- Internet users are entitled to an Internet connection that enables them to
    - Send and receive content of their choice
    - Use services and run applications of their choice
    - Connect hardware and use software of their choice that does not harm the network.
- Internet users are entitled to an Internet connection that is free of discrimination with regard to type of application, service or content or based on sender or receiver address.[141]

For the time being, this arrangement seems adequate in **Norway** to meet the challenges of network neutrality or lack of thereof, because the national regulator has a set of tools to set minimum standards. Similarly in **Canada**, there is no specific legal provision on net neutrality in the Telecommunications Act. However, section 36 of the Telecommunications Act prohibits a Canadian telecommunications carrier from controlling the content or influencing the meaning or purpose of telecommunications carried by it for the public, unless the Canadian Radio-television and Telecommunications Commission (CRTC)[142] approves otherwise. The CRTC in 2009 reviewed the Internet traffic management practices of Internet service providers.[143] In its decision, the CRTC established a principled approach that aimed to

---

technological development, and estimate the financial impacts of the regulation on telecommunications operators.

140 Finnish Ministry of Transport and Communications Press Release, 1 Mbit Internet access a universal service in Finland from the beginning of July, 29.06.2010, at <http://www.lvm.fi/web/en/pressreleases/view/1169259>: "The Ministry of Transport and Communications has defined the minimum rate of downstream traffic of a functional Internet access to be 1 Mbit/s, and the Finnish Communications Regulatory Authority, FICORA, has defined 26 telecom operators across Finland as universal service operators."

141 See Norwegian Post and Telecom Authority, The Norwegian approach to net neutrality, 07.10.2010, at <http://goo.gl/fzT2X>. See further Network Neutrality: *Guidelines for Internet neutrality,* Version 1.0 24 February 2009, at <http://goo.gl/c4rhn>.

142 The Canadian Radio-television and Telecommunications Commission (CRTC) is an independent public organization that regulates and supervises the Canadian broadcasting and telecommunications systems.

143 Telecom Regulatory Policy CRTC 2009-657: Review of the Internet traffic management practices of Internet service providers at <http://www.crtc.gc.ca/eng/archive/2009/2009-657.htm>.

balance the freedom of Canadians to use the Internet for various purposes with the legitimate interests of ISPs to efficiently manage the traffic thus generated on their networks, consistent with legislation, including privacy legislation. The CRTC based its determinations in this matter on the following four considerations:

> **1. Transparency**
> Where any Internet traffic management practices (ITMPs) are employed, ISPs must be transparent about their use. Consumers need this information to make informed decisions about the Internet services they purchase and use.
> Economic practices are the most transparent ITMPs. They match consumer usage with willingness to pay, thus putting users in control and allowing market forces to work.
> **2. Innovation**
> Network investment is a fundamental tool for dealing with network congestion and should continue to be the primary solution that ISPs use; however, investment alone does not obviate the need for certain ITMPs. The Commission recognizes that some measures are required to manage Internet traffic on ISP networks at certain points in the network at certain times.
> Where ITMPs are employed, they must be designed to address a defined need, and nothing more.
> **3. Clarity**
> ISPs must ensure that any ITMPs they employ are not unjustly discriminatory nor unduly preferential. The Commission has established an ITMP framework that provides clarity and a structured approach to evaluating whether existing and future ITMPs are in compliance with subsection 27(2) of the Telecommunications Act (the Act).
> **4. Competitive neutrality**
> For retail services, ISPs may continue to employ ITMPs without prior Commission approval. The Commission will review such practices, assessing them against the framework, based upon concerns arising primarily through complaints by consumers.[144]

Furthermore, it should be noted that in several OSCE participating States there are plans to introduce rules and regulations with regards to net neutrality. **Austria**,[145] **Estonia,**[146] **Luxembourg,** and **Poland** intended to implement the EU Telecoms Reform Package which contains several provisions relating to net neutrality by 25 May 2011. Similarly, **France** is planning to set down this principle, however, a deadline has not been set. In **Germany**, an amendment of the Telecommunications Act (TKG) is currently in the legislative process, and it is intended to take account of aspects of net neutrality in the provisions serving to regulate the national telecommunications market.[147] In **Hungary**, the net neutrality issue is planned to be addressed in the Act on Electronic Communication during 2011 when implementing the revised EU regulatory framework for electronic communications. In **Latvia**, amendments to

---

144 For wholesale services there will be additional scrutiny. When an ISP employs more restrictive ITMPs for its wholesale services than for its retail services, it will require Commission approval to implement those practices. Furthermore, the CRTC also decided to take steps to ensure that personal information collected for the purpose of managing Internet traffic is not used for other purposes and is not disclosed. In Telecom Decision CRTC 2010-445, Modifications to forbearance framework for mobile wireless data services, the CRTC determines that the policy framework established for Internet traffic management practices applies to the use of mobile wireless data services to provide Internet access.

145 Austria is in the process of implementing the new European framework for electronic communications networks- and services. This will lead to an amendment to the Telecommunications Act. "Net neutrality" itself will not be regulated as a specific principle (more than the regular regulatory principles), but the concept will be dealt within the amended Act. So, in order to prevent the degradation of service and the hindering or slowing down of traffic over networks, the national regulatory authority will be able to set minimum quality of service requirements on an undertaking or undertakings providing public communications networks.

146 The Estonian Communications Act changes are currently in preparation phase.

147 Note sections 2, 20, 43a, 45n, 45o of the draft amendment of the TKG.

the Electronic Communications Law have been drafted to transpose the provisions contained in the EU Telecoms Reform Package into national legislation. In **Lithuania**, a draft bill of legislative amendments is under preparation in order to ensure full implementation of the Telecoms Reform Package.[148] The **Swedish** government intends to present a bill to be presented to the Parliament in the course of 2011 to address net neutrality and possibly to implement the EU Telecoms Reform Package. **Italy** stated in its response to the OSCE survey that "Italy participated in the public consultation promoted by the European Commission on this issue and it expressed its view about the general need to guarantee net neutrality, unless verified and specific traffic congestion problems suggest a different need, as sometimes can be in the case of mobile networks" but did not mention any plans to regulate net neutrality. **Croatia** is also planning to implement the relevant provisions of the EU regulatory framework in the field of electronic communications in the process of its alignment with the EU acquis. In **Portugal**, there are no specific legal provisions that explicitly address net neutrality issues. However, Article 39(1) of the Electronic Communications Law which provides the users of publicly available electronic communications networks and services equal access implicitly guarantees "net neutrality". Specific provisions on net neutrality may be adopted in the context of the revision of Portuguese legislation in the scope of the transposition of the European Union directives on electronic communications.

Conclusion to Part A

The Internet is increasingly becoming indispensable for people to partake in cultural, social and political discourse and life. In only ten years from now, the number of Internet users is expected to more than double, and will reach five billion worldwide. While over 60% of the citizens of the OSCE area are Internet users, only 30% of the participating States stated that they recognize access to the Internet as a basic human right or as implied to the fundamental right to freedom of expression. At the same time, in at least over 12% of the participating States access to the Internet can legally be restricted, mostly to protect national security, public health or in times of state emergencies. Everyone should have a right to participate in the information society, and the states have a responsibility to ensure citizens' access to the Internet is guaranteed. Furthermore, Internet access policies, defined by governments, should be in line with the requirements of Article 19 of the Universal Declaration of Human Rights as well as Article 19 of the International Covenant on Civil and Political Rights and (where applicable) with Article 10 of the European Convention on Human Rights.

Network neutrality is an important prerequisite for the Internet to be equally accessible and affordable to all. It is, therefore, concerning that over 80% of the OSCE participating States do not have legal provisions in place yet to guarantee net neutrality. Finland and Norway stand out as best practice examples with Finland having anchored network neutrality in its corpus of laws while Norway together with the industry and Internet consumers developed workable guidelines. While it is commendable that several EU countries are planning to introduce rules on network neutrality by implemtning the European Union's Telecoms Reform Package, OSCE participating States should consider legally strengthening users' rights to an open Internet. Users should have the greatest possible access to Internet-based content, applications, or services of their choice without the Internet traffic they use being managed, prioritized, or discriminated by the network operators.

---

148 The Lithuanian Bill will cover 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 (OJ L 337/37 (18.12.2009)) including the provisions concerning net neutrality (Commission Declaration on Net Neutrality).

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 criminalized by national laws. While child pornography could be regarded as a clear example of content being criminalized in most if not all the 56 OSCE participating States, Internet content that is often labelled as "harmful" may include sexually explicit, or graphically violent material and content advocating illegal activity such as drug use, bomb making instructions, underage drinking, and gambling. Certain strong or extreme political or religious views may also be regarded as harmful by many states, and although this type of content falls short of the "illegality threshold", concern remains about possible access to this type of content by children. Highlighting this fundamental difference, in 1996 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".[149]

More recently, the European Court of Human Rights argued that:

> "…. the Internet is an information and communication tool particularly distinct from the printed media, in particular as regards the capacity to store and transmit information. The electronic network serving billions of users worldwide is not and potentially cannot be subject to the same regulations and control. The risk of harm posed by content and communications on the Internet to the exercise and enjoyment of human rights and freedoms, … is certainly higher than that posed by the press."[150]

Policy and legal developments with regards to the Internet in the OSCE region have shown that states differ in terms of categorizing or labelling certain types of content. For example, content advocating hate or racist views and content involving terrorist propaganda may be treated differently by different states. The reason for this 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'."[151] 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.[152] Such state-level differences undoubtedly complicate harmonization of laws and approaches at the international level.

---

149 European Commission Communication on Illegal and Harmful Content on the Internet (1996), p. 10.

150 See *Editorial Board of Pravoye Delo and Shtekel v. Ukraine*, Application no. 33014/05, Jusdgment of 05.05.2011, para 63.

151 *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, and *Vogt v. Germany,* 26 September 1995, § 52, Series A no. 323.

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

As far as speech and content related laws and legal measures are concerned, any restriction must meet the strict criteria under international and regional human rights law. According to the European Court of Human Rights jurisprudence, a strict three-part test is required for any content-based restriction. The European Court notes that the first and most important requirement of Article 10 of the Convention is that any interference by a public authority with the exercise of the freedom of expression should be lawful. Article 10 of the Convention stipulates that:

> 1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.
> 2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.[153]

The second paragraph of Article 10 clearly stipulates that any restriction on expression must be "prescribed by law". In order to comply with this important requirement, interference does not merely have to have a basis in domestic law. The law itself must correspond to certain requirements of "quality". In particular, a norm cannot be regarded as a "law" unless it is formulated with sufficient precision to enable the citizen to regulate his conduct.[154] The degree of precision depends, to a considerable extent on the content of the instrument at issue, the field it is designed to cover, and the number and status of those to whom it is addressed.[155] The notion of foreseeability applies not only to a course of conduct, but also to "formalities, conditions, restrictions or penalties," which may be attached to such conduct, if found to be in breach of the national laws.[156] If the interference is in accordance with law, then secondly the aim of the restriction should be legitimate based on the Article 10(2) limitations in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health of morals, or for the protection of the rights and freedoms of others. Finally, the restrictions need to be necessary in a democratic society,[157] and the state interference should correspond to a "pressing social need".[158] The state response and the limitations provided by law should be "proportionate to the legitimate aim pursued".[159] The European Court of Human Rights requires the reasons given by the national authorities to be relevant and sufficient.[160]

---

153 Note also Article 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights within this context. See Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, A/HRC/17/27, 16 May 2011, at <http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf>.

154 See, for example, *Lindon, Otchakovsky-Laurens and July v. France* [GC], nos. 21279/02 and 36448/02, § 41, ECHR 2007-XI.

155 See *Groppera Radio AG and Others v. Switzerland*, 28 March 1990, § 68, Series A no. 173.

156 See see, *Kafkaris v. Cyprus* [GC], no. 21906/04, § 140, ECHR 2008.

157 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.

158 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.

159 See *Bladet Tromsø and Stensaas v. Norway* [GC], no. 21980/93, ECHR 1999-III.

160 The Court notes that the nature and severity of the penalty imposed, as well as the "relevance" and "sufficiency" of the national courts' reasoning, are matters of particular significance when it comes to

Within the pan-European region, member states of the Council of Europe have a certain margin of appreciation 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.[161] The Court is therefore empowered to give the final ruling on whether a "restriction" is reconcilable with freedom of expression as protected by Article 10.[162] The Court's supervision will be strict because of the importance given to freedom of expression. While the measure taken need not be shown to be "indispensable", the necessity for restricting the right must be convincingly established.[163] According to the Council of Europe Committee of Experts for the Development of Human Rights (DH-DEV) "at the core of the examination of any interference in the exercise of freedom of opinion is therefore a balancing of interests, in which the Court takes account of the significance of freedom of opinion for democracy".[164]

The Article 10 compatibility criteria as set out by the European Court of Human Rights should be taken into account while developing content related policies and legal measures by the OSCE participating States.

In terms of the OSCE RFOM study, the OSCE participating States were asked questions about specific legal provisions

- outlawing racist content (or discourse), xenophobia, and hate speech (**Question 4**);
- outlawing the denial, gross minimisation, approval or justification of genocide or crimes against humanity (**Question 5**);
- outlawing incitement to terrorism, terrorist propaganda and/or terrorist use of the Internet (**Question 6**);
- criminalizing child pornography (**Question 7**);
- outlawing obscene and sexually explicit (pornographic) content (**Question 8**);
- outlawing Internet piracy (**Question 9**);
- outlawing libel and insult (defamation) on the Internet (**Question 10**);
- outlawing the expression of views perceived to be encouraging "extremism" (**Question 11**);
- outlawing the distribution of "harmful content" (**Question 12**);
- outlawing any other categories of Internet content (**Question 13**);

The OSCE RFOM questionnaire, for each of the above questions, requested the participating States to provide statistical information in relation to convictions under relevant law(s) for the

---

assessing the proportionality of an interference under Article 10(2): See *Cumpănă and Mazăre v. Romania* [GC], no. 33348/96, § 111, ECHR 2004, and *Zana v. Turkey*, 25 November 1997, § 51, *Reports of Judgments and Decisions* 1997-VII. The Court also reiterates that Governments should always display restraint in resorting to criminal sanctions, particularly where there are other means of redress available. See further *Başkaya and Okçuoğlu* judgment of 8 July 1999, Reports 1999.

161 *The Observer and The Guardian v. the United Kingdom*, judgment of 26 November 1991, Series A no. 216, pp. 29-30, § 59.

162 *Lingens v. Austria*, 8 July 1986, Series A No. 103, p. 26, § 41; *Perna v. Italy* [GC], no. 48898/99, § 39, ECHR 2003-V; and *Association Ekin v. France*, no. 39288/98, § 56, ECHR 2001-VIII.

163 Autronic AG judgment of 22 May 1990, Series A No. 178, § 61.

164 Council of Europe Steering Committee For Human Rights (CDDH), Committee of Experts for the Development of Human Rights (DH-DEV), Working Group A, Report on "Hate Speech", document GT-DH-DEV A(2006)008, Strasbourg, 9 February 2007, para. 22. Note further the Handyside judgment of 7 December 1976, Series A No. 24, §49.

reporting period from 1 January 2007 until 30 June 2010. The questionnaire also sought to establish whether the relevant provisions prescribe blocking access to websites or any other types of Internet content as a sanction for these offences. These issues and the individual official responses are assessed below.

Legal provisions outlawing racist content, xenophobia, and hate speech on the Internet

There is strong documented evidence that racist organisations and individuals are currently using the Internet to disseminate racist content. As free-to-use Web 2.0 based platforms and applications have grown popular, racist organisations and individuals have started to use platforms such as YouTube, 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 February 2011, the Simon Wiesenthal Center announced that there are approximately 14,000 (compared to 11,500 in 2010) hate and terrorism related websites, social network pages, chat forums and micro-blogs.[165] The Center's report stated that they witnessed a 12% increase compared to 2010. [166]

However, efforts to harmonise laws to combat racist content on the Internet have proved to be problematic.[167] Since the finalisation of the Cybercrime Convention the Council of Europe also developed the first additional protocol to the Cybercrime Convention on the criminalisation of acts of a racist or xenophobic nature committed through computer systems.[168] The Additional Protocol which came into force in March 2006 requires the signatories to criminalize the dissemination[169] of racist and xenophobic material[170] through computer systems, as well as racist and xenophobic-motivated threats,[171] racist and xenophobic-motivated insults,[172] and the denial, gross minimisation, approval or justification

---

165 European Jewish Post, "Wiesenthal Center 2011 Digital Terror/Hate Report Confirms: Escalating Online Threats against Religious Minorities in Middle East, Recruitment of 'Lone Wolf' Terrorists," 25 February, 2011.

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

167 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.

168 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.

169 Article 3 (Dissemination of racist and xenophobic material through computer systems): Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: distributing, or otherwise making available, racist and xenophobic material to the public through a computer system.

170 Article 2 of the Additional Protocol defines *racist and xenophobic material* as "any written material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors."

171 Article 4 (Racist and xenophobic motivated threat): Each Pay shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: threatening, through a computer system, with the commission of a serious criminal offence as defined under its domestic law, (i) persons for the reason that they belong to a group, distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors, or (ii) a group of persons which is distinguished by any of these characteristics.

172 Article 5 (Racist and xenophobic motivated insult): Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: insulting publicly, through a computer system, (i)

of genocide or crimes against humanity, particularly those that occurred during the period 1940-45.[173] 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 April 2011.[174]

In terms of the OSCE participating States, 15 States (26.8%) signed (but not ratified) the Additional Protocol, and 18 States (32.1%) ratified the Additional Protocol. 23 (41.1%) participating States of the OSCE did not sign or ratify the Additional Protocol.[175]

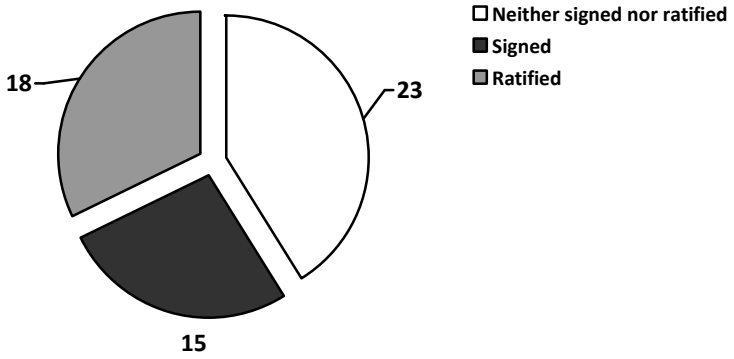


Figure 25. Status of OSCE participating States with regards to signing and ratification of the CoE Additional Protocol.

Furthermore, there are also significant policy developments at the European Union level to encounter racism and xenophobia. 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.[176] 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

---

persons for the reason that they belong to a group distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors; or (ii) a group of persons which is distinguished by any of these characteristics.

173 Article 6 (Denial, gross minimisation, approval or justification of genocide or crimes against humanity): Each Party shall adopt such legislative measures as may be necessary to establish the following conduct as criminal offences under its domestic law, when committed intentionally and without right: distributing or otherwise making available, through a computer system to the public, material which denies, grossly minimises, approves or justifies acts constituting genocide or crimes against humanity, as defined by international law and recognised as such by final and binding decisions of the International Military Tribunal, established by the London Agreement of 8 August 1945, or of any other international court established by relevant international instruments and whose jurisdiction is recognised by that Party.

174 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.

175 It should be noted that nine OSCE Participating States are not members of the Council of Europe. These are Belarus, Canada, Holy See, Kazakhstan, Kyrgyzstan, Tajikistan, Turkmenistan, United States of America, and Uzbekistan.

176 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.

crimes of genocide, crimes against humanity and war crimes.[177] Article 1 of the Framework Decision describes the offences concerning racism and xenophobia as follows:

> 1. Each Member State shall take the measures necessary to ensure that the following intentional conduct is punishable:
> (a) publicly inciting to violence or hatred directed against a group of persons or a member of such a group defined by reference to race, colour, religion, descent or national or ethnic origin;
> (b) the commission of an act referred to in point (a) by public dissemination or distribution of tracts, pictures or other material;
> (c) publicly condoning, denying or grossly trivialising crimes of genocide, crimes against humanity and war crimes as defined in Articles 6, 7 and 8 of the Statute of the International Criminal Court, directed against a group of persons or a member of such a group defined by reference to race, colour, religion, descent or national or ethnic origin when the conduct is carried out in a manner likely to incite to violence or hatred against such a group or a member of such a group;
> (d) publicly condoning, denying or grossly trivialising the crimes defined in Article 6 of the Charter of the International Military Tribunal appended to the London Agreement of 8 August 1945, directed against a group of persons or a member of such a group defined by reference to race, colour, religion, descent or national or ethnic origin when the conduct is carried out in a manner likely to incite to violence or hatred against such a group or a member of such a group.

The specific crimes covered within the Framework Decision also apply to the Internet, and the Member States of the European Union had time until 28.11.2010 to transpose[178] the Framework Decision into national law.

At the UN level, Article 4 of the International Convention on the Elimination of All Forms of Racial Discrimination (ICERD) "condemn(s) 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,[179] the ICERD provisions remain the most important normative basis upon which international efforts to eliminate racial discrimination could be built.[180] Nonetheless, there is no unified approach to this issue and there remain different interpretations and legal practice pertinent to Article 4. To date, 19 states have announced reservations and/or interpretative declarations in respect of Article 4.

In terms of OSCE commitments, the demand within the OSCE to enhance its work in the area of action against racism, xenophobia, discrimination, and anti-Semitism has increased in recent years.[181] The 11th Ministerial Council meeting of Maastricht in December 2003

---

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

178 There is no detailed information yet on whether all the EU Member States transposed the Directive, and how this Directive was implemented into national laws.

179 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.

180 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.

181 See generally OSCE Office for Democratic Institutions and Human Rights (ODIHR), *International Action Against Racism, Xenophobia, Anti-Semitism and Tolerance in the OSCE Region: A Comparative Study* (September 2004), at www.osce.org/ publications/odihr/2004/09/12362_143_en.pdf. See also: ODIHR, *Combating Hate Crimes in the OSCE Region: An Overview of statistics, legislation, and national initiatives* (June 2005), at www.osce.org/publications/odihr/2005/09/16251_452_en.pdf; and ODIHR, *Challenges and Responses to Hate-Motivated Incidents in the OSCE Region* (October 2006), at www.osce.org/ documents/odihr/2006/10/21496_en.pdf.

encouraged the participating states to collect and keep records and statistics on hate crimes, including forms of violent manifestations of racism, xenophobia, discrimination and anti-Semitism. The Ministerial Council also gave concrete responsibilities to the OSCE Institutions, including the Office for Democratic Institutions and Human Rights, which was tasked to gather information and statistics collected by the participating States in full co-operation with, *inter alia*, the CERD, the ECRI, and the European Monitoring Centre on Racism and Xenophobia,[182] as well as with relevant non-governmental organisations. Since then the OSCE has organised a number of high-level conferences and meetings to address the problems of racism, xenophobia, discrimination, and anti-Semitism.[183] The need to combat hate crime, which can be fuelled by racist, xenophobic and anti-Semitic propaganda on the Internet, was explicitly recognised by a decision of the 2003 Maastricht Ministerial Council.[184] This was reinforced by the OSCE Permanent Council Decision on Combating anti-Semitism (PC.DEC/607)[185] and its Decision on Tolerance and the Fight against Racism, Xenophobia and Discrimination (PC.DEC/621)[186] in 2004. In November 2004, the OSCE also published a Permanent Council Decision on Promoting Tolerance and Media Freedom on the Internet (PC.DEC/633).[187]

The Maastricht Decision stated that the participating States should investigate and, where applicable, fully prosecute violence as well as criminal threats of violence motivated by racist, xenophobic, anti-Semitic or other related bias on the Internet.[188] Alongside the decision, the OSCE Representative on Freedom of the Media was given the task of actively promoting both freedom of expression on and access to the Internet. Therefore, the Representative continues to observe relevant developments in all participating States. This involves monitoring and issuing early warnings when laws or other measures prohibiting speech motivated by racist or other bias are enforced in a discriminatory or selective manner for political purposes, which can lead to impeding expression of alternative opinions and views.[189]

The European Court of Human Rights also referred to "hate speech" in a number of its judgments. In the case of *Gündüz v. Turkey*[190] the Court emphasised that tolerance and respect for the equal dignity of all human beings constitute the foundations of a democratic, pluralistic society. The Court also stated that "as a matter of principle it may be considered

---

182 Now taken over by the European Union Agency for Fundamental Rights (FRA). See http://fra.europa.eu/.

183 Conference on Anti-Semitism, Vienna (19 June 2003); Conference on Racism, Xenophobia and Discrimination, Vienna (4 September 2003); Conference on Anti-Semitism, Berlin (28 April 2004); Meeting on the Relationship between Racist, Xenophobic and Anti-Semitic Propaganda on the Internet and Hate Crimes, Paris (16 June 2004); Conference on Tolerance and the Fight Against Racism, Xenophobia and Discrimination, Brussels (13 September 2004); and Conference on Anti-Semitism, and other forms of Intolerance, Cordoba (8 June 2005).

184 See Maastricht Ministerial Council, *Decision No. 4/03 on Tolerance and Non-Discrimination* (2003) at para. 8.

185 See www.osce.org/documents/pc/2004/04/2771_en.pdf.

186 See www.osce.org/documents/pc/2004/07/3374_en.pdf.

187 See www.osce.org/documents/pc/2004/11/3805_en.pdf. Note also the Ministerial Council Decision No. 12/04 on Tolerance and Non-Discrimination, December 2004, at www.osce.org/documents/mcs/2004/12/3915_en.pdf, as well as the Cordoba Declaration, CIO.GAL/76/05/Rev.2, 9 June 2005, at www.osce.org/documents/cio/2005/06/15109_ en.pdf.

188 See Maastricht Ministerial Council, *Decision No. 633: Promoting Tolerance and Media Freedom on the Internet* (2004), at decision No. 2, at www.osce.org/documents/mcs/2004/12/ 3915_en.pdf.

189 *Ibid*. at decision No. 4.

190 *Gündüz v. Turkey,* Application No. 35071/97 judgment of 4 December 2003, § 40. With regard to hate speech and the glorification of violence, see *Sürek v. Turkey (No. 1)* No. 26682/95, § 62, ECHR 1999-IV. See further Akdeniz, Y., *Racism on the Internet*, Council of Europe Publishing, 2010 (ISBN 978-92-871-6634-0); and *Legal Instruments for Combating Racism on the Internet*, Council of Europe Publishing, Human Rights and Democracy Series, 2009.

necessary in certain democratic societies to sanction or even prevent all forms of expression which spread, incite, promote or justify hatred based on intolerance (including religious intolerance), provided that any 'formalities', 'conditions', 'restrictions' or 'penalties' imposed are proportionate to the legitimate aim pursued".[191] According to the Court, "only statements which promote a certain level of violence qualify as hate speech",[192] but "there can be no doubt that concrete expressions constituting 'hate speech', which may be insulting to particular individuals or groups, are not protected by Article 10 of the Convention".[193]

In relation to the OSCE RFOM study, the OSCE participating States were asked whether **they have in place specific legal provisions outlawing racist content (or discourse), xenophobia, and hate speech (Question 4)**.[194] 45 (80.4%) of the participating States stated that there are legal provisions outlawing racist content (or discourse), xenophobia, and hate speech in their country. The only country which responded negatively was **Kyrgyzstan**. No data was obtained from ten (17.9%) of the participating States.

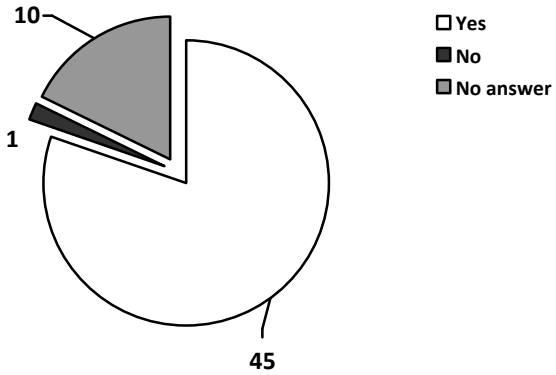


Figure 26. OSCE participating States' responses with regards to specific legal provisions outlawing racist content, xenophobia, and hate speech (Question 4)

In terms of data and information provided by the responding states, as it will be shown below, some variations exist between the OSCE participating States' laws and regulations on racist content (or discourse), xenophobia, and hate speech on the Internet.

By way of example, in **Albania** the distribution of racial or xenophobic content through the Internet is criminalized,[195] as well as insults based on racial or xenophobic motives distributed through the Internet.[196] Albania also criminalizes racist and xenophobic threats through the Internet.[197] In **Austria**, Section 283(1) of the Austrian Criminal Code[198] criminalizes public

191 *Ibid*.

192 *Ibid*.

193 *Ibid*., para. 41. See similarly *Jersild v. Denmark*, judgment of 23 September 1994 para. 35. Note further *Ergin v. Turkey*, judgment of 4 May 2006, para. 34; *Alinak and Others v. Turkey*, judgment of 4 May 2006, para. 35; *Han v. Turkey*, judgment of 13 September 2005, para. 32.

194 The participating States were also asked to provide information on relevant and applicable laws and regulations, information on how offences related to these types of content are defined by law, information on whether the law criminalizes possession and/or distribution of such content, information on what sort of sanctions are available at state level, and information on the maximum prison term envisaged by law for such offences.

195 According to Article 119/a of the Albanian Criminal Code, this offence is sanctioned with a maximum of 2 years of imprisonment.

196 According to Article 119/b of the Albanian Criminal Code, this offence is sanctioned with a maximum of 2 years of imprisonment.

197 According to Article 84/a of the Albanian Criminal Code, this offence is sanctioned with a maximum of 3 years of imprisonment.

racist incitement to commit hostile acts against specific religious communities, churches or groups determined by race, people, tribe or state, if the nature of the incitement is suited for endangering the public order. According to Section 283(2), public agitation (call for hate and contempt), as well as verbal abuse or decrying someone, if committed in a manner violating human dignity, is also criminalized.

Azerbaijan[199] criminalizes through Article 10 of the Media Act,[200] making use of the mass media including the Internet and other forms of dissemination for purposes of advocating violence and brutality, fomenting of national, racial or social discord or intolerance or for committing other unlawful acts.[201] **Bulgaria** criminalizes explicitly the propagation of hatred on religious grounds through electronic information systems.[202] Furthermore, the Bulgarian Ministry of Justice has elaborated draft laws for the amendment of the Penal Code, with a view of implementing the EU Council Framework Decision 2008/913/JHA on combating certain forms and expressions of racism and xenophobia by means of criminal law.

In **Canada**, under the Criminal Code,[203] and by section 13(1) of the Canadian Human Rights Act,[204] hate speech is prohibited and hate propaganda is not tolerated.[205] Section 13(2) stipulates that these provisions clearly apply to the Internet.[206] Section 13(3) of the Canadian

---

198 Strafgesetzbuch – StGB.

199 Azerbaijan is not a signatory to the Council of Europe's Additional Protocol to the Convention on Cybercrime. However, according to Clause 1.8 of the "Action Plan to Form an Electronic Government," approved by Order No. 163s of the Cabinet of Ministers on 14 May 2010, it is expected that measures will be taken to sign the Additional Protocol.

200 Media Act of 7 December 1999.

201 Article 283 of the Azeri Criminal Code, which criminalises acts intended to arouse national, racial, social or religious hatred or enmity or belittle national dignity, and acts intended to restrict the rights of citizens, or to establish superiority among citizens on the basis of national, racial or social status or their attitude to religion.

202 Article 164, Section II "Crime against the religion" of the Bulgarian Penal Code: Who propagates hatred on religious grounds through speeches, publications, activities or in any other way shall be punished by imprisonment of up to three years or by corrective labour. Eight (8) persons were convicted between 2007 and first half of 2010 under this provision.

203 See section 318 (Advocating Genocide); section 319(1) (Public Incitement to Hatred); section 319(2) (Willful Promotion of Hatred). All of these offences require the consent of the Attorney General before a proceeding can be instituted.

204 If following a fair hearing the Canadian Human Rights Tribunal finds that a complaint related to a discriminatory practice described in Section 13 is substantiated, the Tribunal may order that the communicator cease the discriminatory practice and take measures to redress the practice or to prevent the same or a similar practice from occurring in the future; that the communicator compensate a victim specifically identified in the communication that constituted the discriminatory practice with an amount not exceeding twenty thousand dollars; and that the communicator pay a penalty of not more than ten thousand dollars; or a combination of these orders. It should be noted that the Canadian Human Rights Tribunal in *Warman v. Lemire* (2009) CHRT 26 decided that s.13 in conjunction with its associated monetary penalty provision is inconsistent with s. 2(b) of the Canadian Charter of Rights and Freedoms which guarantees the freedom of thought, belief, opinion and expression. The Federal Court of Canada will soon review this decision and may quash this decision if it is found to be incorrect.

205 Section 13(1) of the Canadian Human Rights Act states that "it is a discriminatory practice for a person or a group of persons acting in concert to communicate telephonically or to cause to be so communicated, repeatedly, in whole or in part by means of the facilities of a telecommunication undertaking within the legislative authority of Parliament, any matter that is likely to expose a person or persons to hatred or contempt by reason of the fact that that person or those persons are identifiable on the basis of a prohibited ground of discrimination". Note *Canada (Human Rights Commission) v. Taylor*, [1990] 3 S.C.R. 892.

206 Section 13(2) states that "For greater certainty, subsection (1) applies in respect of a matter that is communicated by means of a computer or a group of interconnected or related computers, including the Internet, or any similar means of communication, but does not apply in respect of a matter that is

Human Rights Act provides protection to ISPs or web-hosting companies from liability for content involving hatred posted to their servers by third parties.[207] Furthermore, the Canadian Criminal Code prohibits inciting hatred against an "identifiable group" by communicating in a public place statements which are likely to lead to a breach of peace (subsection 319(1)),[208] and communicating statements, other than in private conversation, to wilfully promote hatred against an "identifiable group" (subsection 319(2)).[209] With regards to hate propaganda on the Internet, Section 320.1 of the Criminal Code authorizes a judge to order the deletion, from a computer system within the jurisdiction of the court, of publicly available hate propaganda material. This provision makes it possible to remove hate propaganda material from the Internet in cases where the person who posted the material is unknown or is outside the Canadian jurisdiction. The Code also provides for the seizure and forfeiture of hate propaganda kept on premises for distribution or sale (subsections 320(1) and (4)).

Croatia criminalizes in its Penal Code (as amended in July 2004) the direct spreading of racist or xenophobic materials by using computer systems.[210] Furthermore, the Electronic Media Act[211] prohibits the distribution of hate speech through electronic publications.[212] Furthermore, upon signing the Additional Protocol to the Convention on Cybercrime concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems in 2003, Croatia made amendments to its Criminal Code in 2004.[213]

In **Denmark**, the criminal law provisions that specifically address racist statements and other crimes of a racist nature are also applicable to crimes committed through the use of the Internet. Section 266(b) of the Danish Criminal Code prohibits dissemination of racist statements and racist propaganda.[214] Section 266(b)(2) states that in determining the penalty

---

communicated in whole or in part by means of the facilities of a broadcasting undertaking."

207 Section 13(3) states that "For the purposes of this section, no owner or operator of a telecommunication undertaking communicates or causes to be communicated any matter described in subsection (1) by reason only that the facilities of a telecommunication undertaking owned or operated by that person are used by other persons for the transmission of that matter."

208 The offences under section 319 of the Criminal Code of inciting or wilfully promoting hatred are dual procedure offences, punishable by two years imprisonment on indictment and up to six months imprisonment and/or up to a $2,000.00 fine when proceeded with by way of summary conviction.

209 Subsection 319(2), which prohibits the wilful promotion of hatred against an identifiable group, has come under the most direct scrutiny by our courts. In considering a charge under s. 319(2), a trial judge must consider not only the words used by the accused, but the circumstances and context in which they were spoken. See *R. v. Ahenakew*, 2008 SKCA 4 (CanLII), and *R. v. Keegstra*, [1990] 3 S.C.R. 697. Note further that in July 2010, Mr. Salman An-Noor Hossain was charged by the Ontario Provincial Police after a five-month investigation revealed that a website and blog operated by Mr. Hossain contained information that, among other things, wilfully promoted hatred and advocated genocide of the Jewish community. The specific charges were: Wilfully promoting hatred against an identifiable group (Section 319(2)), advocating or promoting genocide against an identifiable group (Section 318(1)).

210 The Croatian provisions include distribution or otherwise making available of content that denies, significantly diminishes, approves or justifies the criminal act of genocide or crimes against humanity, with the aim of spreading racial, religious, gender-based, national or ethnic hatred based on the colour of skin, sexual orientation or other characteristics, or with the aim of slighting.

211 Official Gazette 153/09.

212 Article 12 of the Electronic Media Act stipulates as follows: "In audio and/or audiovisual services it is prohibited to promote, favour the promotion of and spreading of hatred or discrimination based on race or ethnic affiliation or colour, gender, language, religion, political or other belief, national or social origin, property, trade union membership, education, social status, marital or family status, age, health condition, disability, genetic heritage, native identity, expression or sexual orientation, as well as anti-Semitism and xenophobia, ideas of the fascist, nationalist, communist and other totalitarian regimes."

213 Note Article 174, paragraph 3 of the Croatian Criminal Code: Official Gazette 105/04.

214 For example, in February 2003 the Eastern High Court found the editor of a website guilty of violating section 266(b)(1) and (2) of the Danish Criminal Code for publishing an article named "Behind Islam"

the court shall consider if the conduct is in the nature of propaganda, which shall be a particularly aggravating circumstance. A fine or imprisonment for any term not exceeding two years is the appropriate penalty provided by law, and a total of 12 convictions were recorded between 2007-2009 in Denmark with regards to Section 266.

According to ECRI, the situation in **France** concerning racism on the Internet is a serious cause for concern.[215] The French law of 29 July 1881 defines a number of offences deriving from the verbal (oral or written) and non-verbal expression of various forms of racism, specifically racial defamation; racial insult; incitement to racial discrimination, hatred, or violence; denial or justification of crimes against humanity. Furthermore, Section 6.7 of Law No. 2004-575 on confidence in the digital economy[216] aims to prevent and penalise the dissemination of racist content on the Internet.[217] The law obliges French ISPs and hosting companies to help combat incitement to racial hatred by implementing a notification procedure which makes it easy for Internet users to draw their attention to this sort of content.[218] Once made aware of the existence of such content on their servers, the ISPs and the hosting companies must then report suh content to the public authorities. The companies are also obliged to publicise the ways in which they endeavour to counter such phenomena on the Internet.

In **Germany**, there has been an increase in the so-called 'propaganda crimes' during the last 10 years, provoked by the growth of the Internet use.[219] The German Penal Code (StGB) includes provisions on propaganda offences. Section 86 of the Penal Code regulates the distribution of propaganda material of unconstitutional organisations (or of the former National Socialist party). This provision criminalises the distribution of Nazi slogans, flyers, and other propaganda materials, including music. The provision covers materials and data, including those distributed through the Internet. The maximum sentence for the Section 86 offence is three years' imprisonment. The mere possession of propaganda materials is not criminalised by this section.

Similarly, Section 86a of the German Penal Code criminalises the public use of certain symbols (such as swastikas, flags, military insignia, Hitler salutes, or other Nazi symbols)

---

which included several degrading statements about Muslims in December 1999. The court also regarded the publication of the article on the Internet as propaganda, and ruled that it was in violation of section 266(2)(b). The website editor was sentenced to 20 day-fines of DKK 300 (reported in the *Danish Weekly Law Journal* 2003 page 751, U.2003.751/2Ø). Taken from Documentation and Advisory Centre on Racial Discrimination (DACoRD), *National Analytical Study on Racist Violence and Crime: RAXEN Focal Point for Denmark* (2003), compiled for the National Focal Point of the European Monitoring Centre on Racism and Xenophobia (EUMC).

215 ECRI strongly recommended that the French authorities pursue and reinforce their efforts to combat forms of racist expression propagated via the Internet in its 2010 report on France. ECRI, Report on France (Fourth Monitoring Cycle), CRI(2010)16, 15 June, 2010.

216 Dated 21 June 2004.

217 See ECRI, Third Report on France, CRI (2005) 3, adopted on 25 June 2004 and made public on 15 February 2005.

218 ECRI notes that following the entry into force of the 2004 law on confidence in the digital economy, which it welcomed in its previous report, on 19 June 2008 the Court of Cassation dismissed an appeal on points of law against a decision requiring Internet service providers to block access from French territory to a site hosted abroad which was offering to supply brochures with antisemitic and Holocaust-denial content. See further ECRI, Report on France (Fourth Monitoring Cycle), CRI(2010)16, 15 June, 2010.

219 Note Akdeniz, Y., *Racism on the Internet*, Council of Europe Publishing, 2010 (ISBN 978-92-871-6634-0), and European Forum for Migration Studies (EFMS), Institute at the University of Bamberg, *National Analytical Study on Racist Violence and Crime: RAXEN Focal Point for Germany*, written by Rühl, S., and Will, G., 2004, compiled for the National Focal Point of the European Monitoring Centre on Racism and Xenophobia (EUMC).

associated with unconstitutional organisations in a meeting or in publications. As in the case of Section 86, this offence is also sanctioned with a maximum of three years' imprisonment sentence. Furthermore, Section 130(1) of the German Penal Code criminalises the agitation of the people, and anyone who incites or advocates hatred against segments of the population including national, racial or religious groups, or against a group defined by national customs and traditions (for example non-Germans or Jewish people), or calls for violent or arbitrary measures against them, or assaults the human dignity of others by insulting, maliciously maligning or defaming segments of the population. This provision, in its Section 130(2), extends to writings which incite hatred or call for violent or arbitrary measures against segments of the population, or which assault the human dignity of others by insulting, maliciously maligning or defaming segments of the population. The production, dissemination, public display, or making accessible of such content through, for example, the Internet is therefore criminalised.

The maximum custodial sentence for actions as defined by Section 130(1) of the Criminal Code is five (5) years; and for the dissemination of writings pursuant to Section 130(2) of the Criminal Code (StGB) it is three (3) years. A total of 859 convictions were registered for the Section 130(1) offence, while 190 convictions were recorded for the Section 130(2) offence between 2007 and 2009, as shown below.

Year	Section 130(1) of the Criminal Code (StGB) Total number of convictions	Section 130(2) of the Criminal Code (StGB) Total number of convictions
2007	318	62
2008	287	60
2009	254	68
Total	859	190

Table 1. Section 130 convictions under the German Criminal Code

An exemption from the criminal liability established by Section 130(2) of the Criminal Code has been set out in Section 130(6) in conjunction with Section 86(3) of the Criminal Code. According to this provision of the law, the dissemination of the corresponding writings is not punishable if it serves to educate people as citizens of the state, to defend against efforts to disrupt the constitutional order, if it is made for artistic or scientific purposes, or for purposes of research or education, as well as for reporting on current or historical events or for similar purposes.

The manufacture, possession, import, and transportation on the territory of the Republic of **Kazakhstan** of media products containing information aimed at propaganda of or advocating a forced change of the constitutional system, violation of the integrity of the Republic of Kazakhstan, undermining state security, unleashing war, inciting social, racial, national, religious, class or tribal strife, the cult of cruelty, violence and pornography is punished with an administrative fine under Article 344[220] of the Code of Administrative Offences of the Republic of Kazakhstan.[221] The same provision also covers the distribution on the territory of the Republic of Kazakhstan of media products containing information and materials aimed at the propaganda of or advocating a forced change of the constitutional system, violation of the integrity of the Republic of Kazakhstan, undermining state security, unleashing war, inciting social, racial, national, religious, class or tribal strife, supporting and justifying extremism or

220 Article 344 is entitled "Manufacture, Possession, Import, Transportation, and Dissemination in the Territory of the Republic of Kazakhstan of Media Products and Other Products".

221 Code of Administrative Offences of the Republic of Kazakhstan No. 155-II of 30 January 2001 (with amendments and addenda of 6 October 2010).

terrorism, as well as revealing the techniques and tactics of antiterrorist operations during their implementation. Furthermore, incitement of Social, national, Tribal, racial, or religious enmity is criminalized by Article 164 of the Criminal Code of the Republic of Kazakhstan.[222]

In **Lithuania**, distribution of racist content, xenophobia and hate speech is prohibited by the provisions of the Criminal Code,[223] and under the Law on Provision of Information to the Public (the law regulating mass media).[224] 173 persons were investigated in criminal proceedings between 2007 and 2010 in Lithuania for these offences.[225]

In **Montenegro**, the Constitution of Montenegro prohibits encouraging or inducing hatred or intolerance on any grounds and any direct or indirect discrimination on any grounds. The Criminal Code prescribes a set of criminal offences against the rights and freedoms of people and citizens. In the narrow sense, racism and xenophobia mean any spreading of ideas based on racial superiority and hatred, any incitement to racial discrimination, as well as racial violence. Racism and xenophobia are sanctioned in the Criminal Code by offences such as incitement of national, racial and religious hatred, causing national, racial and religious hatred,[226] and racial and other forms of discrimination.[227] These offences are sanctioned with a prison term from six months to five years. The official response provided by Montenegro to the OSCE RFOM questionnaire state that the acts committed through the Internet would require a stricter treatment due to a higher level of vulnerability and injury of a protected good.

---

222 No. 167-I of 16 July 1997 (with amendments and addenda as of 6 October 2010). Note also Article 54 "Circumstances Aggravating Criminal Liability and Punishment". Article 164 states that: (1) Deliberate actions aimed at the incitement of social, national, tribal, racial, or religious enmity or antagonism, or at offense to the national honour and dignity, or religious feelings of citizens, as well as propaganda of exclusiveness, superiority, or inferiority of citizens based on their attitude towards religion, or their genetic or racial belonging, if these acts are committed publicly or with the use of the mass information media, shall be punished by a fine in an amount up to one thousand monthly assessment indices, or in an amount of wages or other income of a given convict for a period of up to ten months, or by detention under arrest for a period of up to six months, or by correctional labour for a period of up to two years or deprivation of freedom for period of up to five years. (2) The same acts committed by a group of persons or committed repeatedly, or combined with violence or a threat to apply it, as well as committed by a person with the use of his official position, or by the head of a public association, shall be punished by a fine in an amount from five hundred to three thousand [monthly assessment indices, or in an amount of wages or other income of a given convict for a period from, five months up to one year or by restriction of freedom for a period up to four years, or by imprisonment for a period from two to six years with deprivation of the right to hold certain positions or to engage in certain types of activity for a period up to three years, or without it. (3) The acts stipulated by the first and second parts of this Article which entailed serious consequences shall be punished by imprisonment for a period from three to ten years with deprivation of the right to hold certain positions or to engage in certain types of activity for a period of up to three years, or without it.".

223 Articles 169, 170 and 170.1. The terms of imprisonment vary depending on the gravity of crime. Pursuant to paragraphs of Articles 170 and 170.1 of the Criminal Code, they may vary from one to three years. Administrative fines are also available under these provisions.

224 Subparagraph 3 of Para 1 of Article 19: It is "prohibited to publish in the media information which (…) instigates war or hatred, ridicule, humiliation, instigates discrimination, violence, physical violent treatment of a group of people or a person belonging thereto on grounds of sex, sexual orientation, race, nationality, language, descent, social status, religion, convictions or views".

225 Majority of these investigations were Internet-related.

226 Article 370 of the Criminal Code: Anyone who publicly invites to violence or hatred towards a group or member of a group defined on the basis of race, skin color, religion, origin, national or ethnic affiliation, shall be punished by an imprisonment sentence for a term of six months to five years.

227 Article 443 of the Criminal Code. This Article prescribes punishments for a person who, on the basis of differentiation of race, skin colour, nationality, ethnic or some other personal characteristic, violates fundamental human rights and freedoms guaranteed by generally accepted rules of international right, persecutes organizations or individuals who advocate human equality, spreads the ideas on superiority of one race over another or promotes racial hatred or incites to racial discrimination.

In the **Netherlands**, prosecutions can be launched against authors of discriminatory material on the Internet under the anti-discrimination provisions of the Criminal Code.[228] Subject to theses provisions, making insulting remarks about a group of people on the grounds of their race, religion or belief, sex, sexual orientation or disability is a criminal offence.[229] Similarly, incitement to hatred or violence against, or discrimination of a group of people on the grounds of their race, religion or belief, sex, sexual orientation or disability is also criminalized.[230] The dissemination of material or objects containing material insulting to a group of people on the grounds of their race, religion or belief, sexual orientation or disability or constituting incitement to hatred or violence against, or discrimination against a group of people on the grounds of their race, religion or belief, sexual orientation or disability is also subject to criminal liability.[231] In the Netherlands, many criminal complaints are lodged by the Internet Discrimination Hotline (MDI).[232] The MDI liaises with the prosecutors dealing with cases involving such offences, providing tips for the local police on the detection of online crime.

In **Norway**, Section 135a of the General Civil Penal Code of 1902 prohibits publicly uttered discriminatory or hateful expressions. The provision applies to any public distribution of racist, xenophobic and hateful statements, including actions where such material is posted on the Internet.[233] The maximum penalty for a violation of this section is three years' imprisonment. The offender may also be sentenced to pay compensation.[234]

Article 13 of the Constitution of the Republic of **Poland** prohibits the existence of organizations and political parties which refer in their programs to totalitarian methods and procedures, such as nazism, fascism and communism, and whose program or activity assumes or allows racial and national hatred, the use of violence to obtain power or to influence the state policy or provide for the concealment of their structure or membership.[235]

---

228 Articles 137c to 137e of the Criminal Code.

229 Article 137c of the Criminal Code.

230 Article 137d of the Criminal Code.

231 Article 137e of the Criminal Code. The maximum penalties in case of article 137c(1) and 137d(1) are a prison sentence of of one year or a fine of the third category (7.600 euros). Aggravated circumstances are laid down in articles 137c(2) and 137d(3) in case (a) the act is committed by a person who has done so professionally or as a habit, or (b) the act is committed by two or more persons jointly. In that case the maximum penalty is a prison sentence of two years or a fine of the fourth category (19.000 euro). The maximum penalty in article 137e (1) is a prison sentence of 6 months or a fine of the third category (7.600 euro). Aggravated circumstances are stipulated in article 137e (2): (a) the fact is committed by a person who has done so professionally or as a habit, or (b) the fact is committed by two or more persons jointly. In that case the maximum penalty is a prison sentence of a year or a fine of the fourth category (19.000 euro).

232 Several dozen cases were brought over the period under review.

233 Section 135a second subsection, states that the term "discriminatory or hateful statement" shall mean (in translation) "threatening or insulting anyone, or inciting hatred or persecution or contempt for anyone because of his or her a) skin colour or national or ethnic origin, b) religion or life stance, or c) homosexuality, lifestyle or orientation." Section 135a covers statements uttered orally, in writing or through symbols. Section 135a provides that statements suitable to reach a large number of persons shall be deemed equivalent to publicly uttered statements. This means that section 135a is applicable to statements posted on an open Internet site, without reference to the number of people actually visiting the site.

234 The Norwegian General Civil Penal Code of 2005 implies a total upgrade of the Penal Code of 1902. The current provisions concerning discriminatory and hateful statements are maintained in the Penal Code 2005 sections 185 and 186. The regulation has not yet entered into force.

235 The Polish Penal Code in its article 119(1) criminalizes violence, illegal threat towards a group or an individual due to, *inter alia,* their racial identity. Article 119(2) criminalizes public incitement to commit a crime defined in article 119(1)). Article 256 criminalizes public promotion of fascist and other totalitarian state systems or inciting hatred based on national, ethnic, racial or religious differences. Article 257 criminalizes public insult of a group within the population or individual persons because of their national, ethnic, racial or religious affiliation.

In **Sweden,** the Penal Code criminalizes racial agitation, and provides that "a person who, in a disseminated statement or communication, threatens or expresses contempt for a national, ethnic or another group of persons with the allusion to their race, colour, national or ethnic origin" has committed a crime.[236] This particular provision also covers Internet publications and distribution.

Spain also criminalises the dissemination of racist ideas, and its Criminal Code prohibitions extend to the Internet. The Spanish Criminal Code prohibits racial agitation, and this covers statements or communications which threaten or express contempt for a national, ethnic or another group of persons with the allusion to their race, colour, national or ethnic affiliation, or religious belief.[237] These provisions also cover images or gestures. The Spanish Supreme Court ruled in 1996 that "the bearing of symbols that can be associated with the Nazi persecution of the Jews and other persons can constitute racial agitation".[238]

In the **Russian Federation,** the distribution of extremist materials, as well as their production or possession for the purpose of distribution is prohibited.[239] The Russian Law "On Extremism"[240] defines extremist materials as documents intended for publication or information on other carriers inciting to extremist activities, or substantiating or justifying the need for performing such activities, including works by the leaders of the National Socialist Workers' Party of Germany, the Fascist Party of Italy, publications substantiating, or justifying national and/or racial superiority, or justifying the commitment of military or other crimes aimed at complete or partial destruction of any ethnic, social, racial, national or religious group. The propaganda and public show of Nazi attributes or symbols or attributes or symbols that are so similar to Nazi attributes or symbols that could be mistaken for them are also covered within the definition of "extremist materials". The federal list of banned extremist materials must be posted on the Internet on the website of the federal state registration agency. This list must also be published in the media. A decision to include a specific item on the federal list of banned extremist materials may be appealed in court as envisaged by the Russian Federation law.

Furthermore, in compliance with Article 280 of the Russian Federation Criminal Code, public incitement to extremist activity is punishable by a fine, or by arrest for a term of four to six months, or by deprivation of liberty for a term of up to three years. The same deeds committed through media are punishable by deprivation of liberty for a term of three to five years, along with deprivation of the right to hold specified offices or engage in specified activities for a term up to three years. According to Article 282 of the Russian Federation Criminal Code, actions aimed at the incitement of hatred or enmity, as well as denigration of

---

236 Chapter 16, section 8. The number of persons found guilty of agitation against a national or ethnic group in Sweden were: in 2007: 28; in 2008: 29; in 2009: 33.

237 See Chapter 16, section 8 of the Spanish Criminal Code.

238 OSCE/ODIHR, Combating Hate Crimes in the OSCE Region: An Overview of Statistics, Legislation, and National Initiatives, OSCE, 2005, at <http://www.osce.org/odihr/16405> as cited in Akdeniz, Y., *Racism on the Internet*, Council of Europe Publishing, 2010.

239 See Arts. 280 and 282 of the Russian Federation Criminal Code. Note further Article 16 of the Media Law and Article 13 of Federal Law No. 114-FZ of 25 July 2002 "On Counteraction of Extremist Activity". Incitement to extremist activities is also punishable under Articles 280 and 282.

240 Federal Law No. 114-FZ of 25 July 2002 "On Counteracting Extremist Activity," the Russian Federation Code of Administrative Offences, and the Russian Federation Criminal Code. Article 1 of Federal Law No. 114-FZ of 25 July 2002 "On Counteracting Extremist Activity". Moreover, according to Article 13 of the Law "On Extremism", the distribution of extremist materials, as well as their production or possession for the purpose of distribution, is prohibited in the Russian Federation.

dignity of a person or a group of persons on the grounds of sex, race, nationality, language, origin, attitude to religion, as well as of affiliation to any social group, if these actions have been committed in public or with the use of media, may be punishable by deprivation of liberty for a term of up to two years. The same actions committed under aggravating circumstances may be punishable by deprivation of liberty for a term of up to five years.

According to the decisions of district and city courts of the Russian Federation constituent entities, within the reporting period 115 guilty verdicts were issued for the distribution on the Internet of extremist materials that are on the federal list of banned extremist materials published on the official website of the Russian Federation Ministry of Justice. Moreover, the Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communications (Roskomnadzor) issued 11 warnings between 1 January 2007 and 30 June 2010 to the editorial boards of electronic media for breaches of Article 4 of the Media Law.

In the **United Kingdom**, Section 17 of the Public Order Act 1986 makes it an offence for a person to use threatening, abusive or insulting words or behavior, or to display any written material which is threatening, abusive or insulting, intending to stir up racial hatred, or where having regard to all the circumstances racial hatred is likely to be stirred up.[241] The related offences include distribution, broadcasting, performance, and public display of inflammatory material under the 1986 Act.[242] The possession of racially inflammatory material (written material or a recording) with a view to displaying, publishing, distributing, showing, playing or broadcasting it for the purpose of stirring up racial hatred is also an offence.[243] A person guilty of any of these offences may be sentenced to imprisonment for a term not exceeding seven years, or a fine, or both. Furthermore, the Schedule to the Racial and Religious Hatred Act 2006[244] entitled "Hatred against Persons on Religious Grounds" became Part 3A of the Public Order Act 1986, and the new provisions introduced offences involving stirring up hatred against persons on racial or religious grounds. Section 29A defines religious hatred as hatred against a group[245] of persons defined by reference to religious belief or lack of religious belief.[246] These offences need to be balanced with the right to freedom of expression, and therefore section 29J entitled "Protection of freedom of expression" states that "nothing in this Part shall be read or given effect in a way which prohibits or restricts discussion, criticism or

---

241 Section 17 of the 1986 Act (Amended by the Anti-Terrorism, Crime and Security Act 2001 ss 37, 125, Sch 8 Pt 4.) defines "racial hatred" as hatred against a group of persons defined by reference to colour, race, nationality (including citizenship) or ethnic or national origins.

242 **Ireland** has similar legislation in place: Section 2 of the Prohibition of Incitement to Hatred Act 1989 defines the offence of publishing or distributing written material that is likely to stir up hatred. It is also an offence to publicly use words, display materials or behave in a manner which is likely to stir up hatred. In addition, this section provides for the offence of distributing, showing or playing a recording of visual images or sounds likely to incite hatred. Persons convicted of this offence may be sentenced to imprisonment for the maximum term of two years and/or the maximum fine of €12,500.

243 Section 23, 1986 Public Order Act: The possession becomes an offence if the material is possessed with a view to distributing it with intent to stir up racial hatred.

244 The 2006 Act came into force on 1 October 2007.

245 Religious group means any group of people defined by reference to their religious belief or lack of religious belief. For example, this includes Muslims, Hindus and Christians, and different denominations and branches within those religions. It would also include people with no religious belief at all. See the Crown Prosecution Service Racist and Religious Crime Prosecution Policy, March 2008, at www.cps.gov.uk/publications/prosecution/rrpbcrbook.html.

246 Similar to the Part 3 offences under the 1986 Act section 29B criminalises the use of words or behaviour or display of written material, section 29C criminalises the publication or distribution of written material, section 29E criminalises the distribution, showing, or playing a recording, and section 29G criminalises the possession of inflammatory material. The penalties for these offences are the same as for the 1986 offences.

expressions of antipathy, dislike, ridicule, insult or abuse of particular religions or the beliefs or practices of their adherents, or of any other belief system or the beliefs or practices of its adherents, or proselytising or urging adherents of a different religion or belief system to cease practising their religion or belief system".

Legal provisions outlawing the denial, gross minimisation, approval or justification of genocide or crimes against humanity

In a number of states legal provisions criminalizing the denial, gross minimisation, approval or justification of genocide or crimes against humanity exist for historical reasons. Article 6[247] of the CoE Additional Protocol requires the criminalisation of expressions which deny, grossly minimise, approve or justify acts constituting genocide or crimes against humanity as defined by international law and recognised as such by final and binding decisions of the International Military Tribunal, established by the London Agreement of 8 April 1945. Furthermore, the scope of Article 6 is not limited to the crimes committed by the Nazi regime during the Second World War and established as such by the Nuremberg Tribunal, but also to genocides and crimes against humanity established by other international courts set up since 1945 by relevant international legal instruments (such as United Nations Security Council Resolutions, multilateral treaties, etc.). Such courts may be, for instance, the International Criminal Tribunals for the former Yugoslavia, for Rwanda, and also the Permanent International Criminal Court.

The CoE Additional Protocol provision intends to make it clear that "facts of which the historical correctness has been established may not be denied, grossly minimised, approved or justified in order to support these detestable theories and ideas".[248] This provision is supported by the European Court of Human Rights, which made it clear in its judgment in *Lehideux and Isorni*[249] that the denial or revision of "clearly established historical facts – such as the Holocaust (whose negation or revision) would be removed from the protection of Article 10 by Article 17" of the European Convention on Human Rights. The Court stated that "there is no doubt that, like any other remark directed against the Convention's underlying values,[250] the justification of a pro-Nazi policy could not be allowed to enjoy the protection afforded by Article 10".[251] The Court, and previously, the European Commission of Human Rights, have found in a number of cases that freedom of expression guaranteed under Article 10 of the Convention may not be invoked in conflict with Article 17, in particular in cases concerning Holocaust denial and related issues.[252]

---

247 Denial, gross minimisation, approval or justification of genocide or crimes against humanity.

248 Para. 41 of the explanatory report for the CoE Additional Protocol.

249 Judgment of 23 September 1998. Note within this context also *Garaudy v. France*, 24 June 2003, inadmissible, Application No. 65831/01.

250 See, *mutatis mutandis*, the *Jersild v. Denmark* judgment of 23 September 1994, Series A No. 298, p. 25, § 35.

251 Note also that the United Nations Resolution rejected any denial of the Holocaust as an historical event, either in full or part, in October 2005. See UN General Assembly Resolution on Holocaust Remembrance, A/60/L.12, 26 October 2005,. Additionally, on 26 January 2007, the UN General Assembly adopted Resolution No. A/RES/61/255 (GA/10569) condemning any denial of Holocaust (<www.un.org/News/Press/docs/2007/ga10569.doc.htm>).

252 Note the cases of *Glimmerveen and J. Hagenbeek v. the Netherlands*, Nos. 8348/78 and 8406/78, Commission decision of 11 October 1979, Decisions and Reports (DR) 18, p. 187; *Kühnen v. Germany*, No. 12194/86, Commission decision of 12 May 1988, DR 56, p. 205; *B.H., M.W., H.P. and G.K. v. Austria*, No. 12774/87, Commission decision of 12 October 1989, DR 62, p. 216; *Ochsenberger v. Austria*, No. 21318/93, Commission decision of 2 September 1994; *Walendy v. Germany*, No. 21128/92, Commission decision of 11 January 1995, DR 80, p. 94; *Remer v. Germany*, No. 25096/94, Commission decision of 6 September 1995, DR 82, p. 117; *Honsik v. Austria*, No. 25062/94, Commission decision of 18 October 1995, DR 83-A, p. 77; *Nationaldemokratische Partei Deutschlands, Bezirksverband München-Oberbayern*

Furthermore, as mentioned above Article 1 of the EU Framework Decision on combating racism and xenophobia[253] also criminalizes publicly condoning, denying or grossly trivializing crimes of genocide, crimes against humanity and war crimes.[254]

In terms of the OSCE RFOM study, the OSCE participating States were asked whether **there are specific legal provisions outlawing the denial, gross minimisation, approval or justification of genocide or crimes against humanity** in their country **(Question 5).**[255] In contrast to Question 4 on specific legal provisions outlawing racist content (or discourse), xenophobia, and hate speech, 23 (41.1%) of the participating States have laws and legal provisions outlawing the denial, gross minimisation, approval or justification of genocide or crimes against humanity. Equally, 23 (41.1%) participating States stated that they do not have such legal provisions, and 10 (17.9%) of the participating States did not provide a reply.

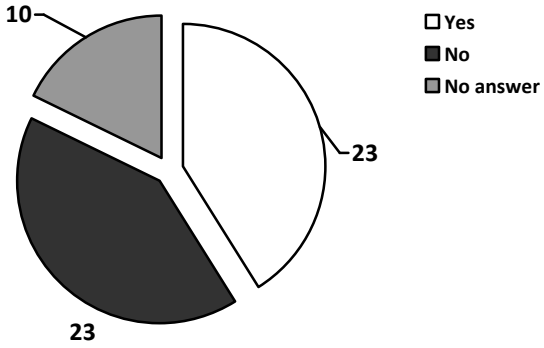


Figure 27. OSCE participating States' responses with regards to specific legal provisions outlawing the denial, gross minimisation, approval or justification of genocide or crimes against humanity (Question 5).

As will be seen below criminal sanctions are provided for publishing, dissemination, and even for possession of content related to the denial, gross minimisation, approval or justification of genocide or crimes against humanity within certain OSCE participating States which responded to the OSCE RFOM questionnaire.

---

v. Germany, No. 25992/94, Commission decision of 29 November 1995, DR 84, p. 149; *Rebhandel v. Austria*, No. 24398/94, Commission decision of 16 January 1996; *Nachtmann v. Austria*, No. 36773/97, Commission decision of 9 September 1998; *Witzsch v. Germany* (dec.), No. 41448/98, 20 April 1999; *Schimanek v. Austria* (dec.), No. 32307/96, 1 February 2000; *Garaudy v. France* (dec.), No. 65831/01, ECHR 2003-IX; *Norwood v. United Kingdom* (dec.), 23131/03, 16 November 2004.

253 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.

254 Article 1(d) states that "publicly condoning, denying or grossly trivialising the crimes defined in Article 6 of the Charter of the International Military Tribunal appended to the London Agreement of 8 August 1945, directed against a group of persons or a member of such a group defined by reference to race, colour, religion, descent or national or ethnic origin when the conduct is carried out in a manner likely to incite to violence or hatred against such a group or a member of such a group" should be criminalized by the EU Member States.

255 The participating States of the OSCE were also asked how these offences are defined by law, whether the possession of such content is criminalized, which sanctions (criminal, administrative, civil) are envisaged by law, the maximum prison term envisaged by law for such offences, any statistical information in relation to convictions under such provisions for the reporting period of 1 January 2007 – 30 June 2010, and whether the law (or relevant regulations) prescribes blocking access to websites or any other types of Internet content as a sanction for these offences.

In **Albania**, the Criminal Code since November 2008 includes a stipulation outlawing the distribution of materials pro-genocide or pro-crimes against humanity through the Internet.[256] Article 74/a of the Criminal Code defines the distribution of materials pro-genocide or pro-crimes against humanity through the Internet as public provision or intentional distribution to public through the Internet of materials that deny significantly minimize, approve or justify acts constituting genocide or crimes against humanity. The possession and/or distribution of content involving pro-genocide or pro-crimes against humanity are criminalized, and the maximum prison term is 6 years. In **Austria**, the denial, gross minimisation, approval or justification of the Nazi genocide or other Nazi crimes against humanity is a criminal act punishable by the courts according to the Prohibition Act.[257] In 2007 a total of 10 persons were convicted because of criminal acts falling under the Prohibition Act. In 2008, 28 persons were convicted, and in 2009, 34 persons were convicted.

In **Canada**, the Criminal Code prohibits inciting hatred against an "identifiable group" by communicating in a public place statements which are likely to lead to a breach of the peace,[258] and communicating statements, other than in private conversation, to wilfully promote hatred against an "identifiable group".[259] Advocating or promoting genocide is an indictable offence punishable by a maximum of five years imprisonment.[260] In **Croatia**, Article 12 of the Electronic Media Act prohibits to promote, favour the promotion of and spreading of ideas of the fascist, nationalist, communist and other totalitarian regimes.[261] Furthermore, the Croatian Criminal Code was amended in 2004 subsequent to signing the CoE Additional Protocol. Therefore, under Article 174(3) anyone who in order to spread racial, religious, gender, national, ethnic hatred, or hatred based on colour or sexual orientation or other characteristics, or in order to belittle, publicly presents or propagates ideas of superiority or inferiority of a race, ethnic or religious community, gender, nation, or ideas of superiority or inferiority based on colour or sexual orientation or other characteristics, shall

---

256 Article 74/a. Since the recent adoption of the relevant legal provisions in 2008, there have been no recorded cases of convictions.

257 Section 3g of the Prohibition Act (Verbotsgesetz): Whoever acts in a national-socialist way other than the ways mentioned in sections 3a to 3f is to be punished with a prison sentence of a minimum of one year up to a maximum of ten years, unless the criminal act is to be punished more severely according to another provision of the law. If the perpetrator or the way of perpetration is especially dangerous, the maximum prison sentence is twenty years. Section 3h of the Prohibition Act (Verbotsgesetz): Whoever denies, grossly minimizes, approves of or tries to justify the Nazi genocide or other Nazi crimes against humanity in print works, broadcasting services or in any other media or otherwise in such a public way that it becomes accessible for many people, is also to be punished according to section 3g.

258 Section 319(1) of the Canadian Criminal Code.

259 Section 319(2) of the Canadian Criminal Code.

260 With regard to the offence of "counseling" another to commit an offence Canadian criminal law criminalizes this act generally, and more specifically in relation to crimes against humanity and genocide. Note therefore section 464 of the Criminal Code. It should also be noted that under the Crimes Against Humanity and War Crimes Act, the following offences could be said to apply, with the right set of facts, to the approval or justification of genocide and crimes against humanity: Anyone (whether in or out of Canada) who counsels a genocide or crime against humanity is guilty of an indictable offence (s. 4(1.1) and 6(1.1)). Furthermore, anyone who counsels a military commander or superior to commit an offence (whether in or out of Canada) in relation to their responsibilities for ensuring genocide and crimes against humanity are not committed (s. 5(2.1) and 7(2.1)) is guilty of an indictable offence. The maximum sentence for these offences is life imprisonment.

261 Article 12 stipulates in full, as follows: "In audio and/or audiovisual services it is prohibited to promote, favour the promotion of and spreading of hatred or discrimination based on race or ethnic affiliation or colour, gender, language, religion, political or other belief, national or social origin, property, trade union membership, education, social status, marital or family status, age, health condition, disability, genetic heritage, native identity, expression or sexual orientation, as well as anti-Semitism and xenophobia, ideas of the fascist, nationalist, communist and other totalitarian regimes."

be punished by a prison term from three months to three years.[262] İt follows that anyone who with such a goal distributes or in any other way makes available to the public through a computer system materials that deny, considerably downplay, condone or justify the crime of genocide or the crime against humanity, shall be punished by a prison term of six months to three years.[263]

In the **Czech Republic** the denial, questioning, approval and justification of genocide is criminalized.[264] Whoever publicly denies, questions, approves or tries to justify Nazi, communist or any other genocide or other crimes of the Nazis and Communists against humanity shall be punished by imprisonment from six months to three years. In **France**, Law no. 90-615 of 13 July 1990 ("the *loi Gayssot*") amended the Freedom of the Press Act by adding Section 24 *bis* which makes it a crime to "deny the existence of one or more crimes against humanity as defined in Article 6 of the Statute of the International Military Tribunal annexed to the London agreement of 8 August 1945 which have been committed either by the members of an organisation declared criminal pursuant to Article 9 of the Statute or by a person found guilty of such crimes by a French or international court". This crime is sanctioned by one year's imprisonment and/or a fine.

In **Germany**, the denial, minimization, approval or justification of genocide or crimes against humanity is sanctioned by the Criminal Code.[265] Section 130(3) provides for a maximum of five year's imprisonment for whoever approves of or denies or renders harmless an act committed under the rule of National Socialism of the type indicated in section 220a(1) of the Criminal Code (Genocide) in a manner capable of disturbing the public peace. Holocaust denial crimes under Section 130(3) can also be committed in writing. The maximum term of imprisonment for denial pursuant to Section 130(3) of the Criminal Code (StGB) amounts to five (5) years, and for the dissemination of the corresponding writings pursuant to section 130(5) in conjunction with Section 130(2) of the Criminal Code (StGB), it amounts to three (3) years.

Year	Section 130(3) of the Criminal Code (StGB) Total number of convictions
2007	53
2008	45
2009	44
Total	142

Table 2. Section 130(3) convictions under the German Criminal Code

As can be seen from the above table, there were a total of 142 convictions between 2007 and 2009 with regards to Section 130(3) crimes under the German Criminal Code.

In **Latvia**, Article 741 of the Criminal Code[266] imposes criminal liability for public glorification of genocide, crime against humanity, crime against peace or war crime or public denial or acquittal of implemented genocide, crime against humanity, crime against peace or

262 Article 174(3)(3).
263 Article 174(3)(4).
264 Article 405, Penal Code Act. No. 40/2009 Coll.
265 Note section 140(2) of the Criminal Code (StGB) (Approving of offences), sections 185 et seq. of the Criminal Code (StGB) (Insult), as well as section 130 (1) of the Criminal Code (StGB) (Incitement to hatred); a special provision was created in 1994 penalizing the denial of the genocide perpetrated under National Socialist rule (section 130(3) of the Criminal Code (StGB)).
266 This article is entitled "Acquittal [i.e., justification] of Genocide, Crimes against Humanity".

war crime. The applicable sentence is deprivation of liberty for a term up to five years or community service.[267] In **Lithuania**, Article 1702(1) of the Criminal Code states that:[268]

> A person who publicly justifies genocide or other crimes against humanity or war crimes as recognised by the legal acts of the Republic of Lithuania, European Union or binding decisions of courts of the Republic of Lithuanian or the international courts, denies and grossly minimizes them if such acts are committed in a threatening, insulting or abusive way or if they violate public order; as well as a person who publicly approves aggression committed against the Republic of Lithuania by the USSR or Nazi Germany, genocide or other crimes against humanity or war crimes committed by the USSR or Nazi Germany within the territory of the Republic of Lithuania or against the population of the Republic of Lithhuania, or other serious crimes or grave crimes committed in the years 1990–1991 by the persons who carried out or participated in the aggression against the Republic of Lithuania or grave crimes against the population of the Republic of Lithuania, denies them or grossly minimizes them, if such acts are committed in a threatening, insulting or abusive way or if they violate public order shall be punished by a fine or by restriction of liberty or by arrest or by imprisonment for a term of up to two years.
> 2. A legal entity shall also be held liable for the acts provided for in this Article.

Similarly, in **the former Yugoslav Republic of Macedonia**, the Criminal Code in its Article 407-a criminalizes the approving or justifying genocide, crimes against humanity or military crime.[269] In **Montenegro**, Article 370(2) of the Criminal Code criminalizes anyone who publicly approves, renounces the existence or significantly reduces the gravity of criminal offences of genocide, crimes against humanity and war crimes committed against a group or member of a group member defined based on race, skin color, religion, origin, national or ethnic affiliation, in the manner which can lead to violence or cause hatred against a group of persons or a member of such group, if those criminal offences have been determined by a final and enforceable judgment of a court in Montenegro or of the international criminal tribunal. Imprisonment sentence for a term of six months to five years is provided for such an offence in Montenegro.

In **Norway**, section 108 of the Penal Code 2005[270] includes a separate provision on public incitement to genocide, crimes against humanity and war crimes. The provision also applies when the incitement is done through the Internet. The penalty for violating section 108 is 10 years' imprisonment, and is considered as a serious crime. In **Poland**, Article 55 of the Act on the Institute of National Remembrance – Commission for the Prosecution of Crimes against the Polish Nation[271] makes it an offence to publicly deny crimes referred in Article 1(1),[272] and

---

267 Should the offence qualify as a public incitement to genocide, the offender is subject to a more severe criminal sanctions, namely, under Article 711 of the Criminal Law on Incitement to Genocide, the applicable sentence is deprivation of liberty for a term up to eight years.

268 This article is entitled "Public Justification of International Crimes, Crimes of the USSR or Nazi Germany against the Republic of Lithuania or its Population, Their Denial or Gross Minimisation".

269 (1) Anyone who will publicly negate, roughly minimize, approve and justify the crimes stipulated in the articles 403 through 407, through an information system, shall be sentenced with imprisonment of one to five years. (2) If the negation, minimizing, approval or the justification is performed with intention to instigate hate, discrimination or violence against a person or group of persons due to their national, ethnic or racial origin or religion, the perpetrator, shall be sentenced with imprisonment of at least four years.

270 See chapter 16, passed by law on 7 March 2008.

271 Dated 18 December, 1998.

272 Article 1: The act regulates: (1) the recording, collecting, storing, processing, securing, making available and publishing of the documents of the state security authorities, produced and accumulated from July 22, 1944 until July 31, 1990, as well as the documents of the security authorities of the Third Reich and the Soviet Union relating to: a) - the Nazi crimes, - the communist crimes, - other crimes against peace, humanity or war crimes, perpetrated on persons of Polish nationality or Polish citizens of other nationalities

this offence is subject to a fine or the penalty of imprisonment of up to 3 years. In **Romania**, the denial, gross minimization, approval or justification through any means, in public, of the Holocaust, genocide and crimes against humanity or its effect are punished with imprisonment from 6 months to 5 years or fine.[273] In **Slovenia**, Article 297(2) of the Criminal Code[274] criminalizes the public dissemination of "ideas on the supremacy of one race over another, or provides aid in any manner for racist activity or denies, diminishes the significance of, approves, disregards, makes fun of, or advocates genocide, holocaust, crimes against humanity, war crime, aggression, or other criminal offences against humanity." This offence is punished by imprisonment of up to two years. In **Ukraine**, in accordance with the Law of Ukraine "On the Famine of 1932-1933 in Ukraine", the Famine is recognized as a genocide against the Ukrainian people. Article 2 of this Law envisages that public denial of Famine of 1932-1933 in Ukraine is an abuse of millions of Famine victims' memory, humiliation of the Ukrainian people and is therefore unlawful.

Legal provisions outlawing incitement to terrorism, terrorist propaganda and/or terrorist use of the Internet

The availability of glorification of violence and terrorist propaganda[275] on the Internet, and content which may encourage terrorist activities[276] such as bomb-making instructions including the infamous *Anarchist's Cookbook*, or the often cited *Encyclopaedia of the Afghan Jihad, The Al-Qaeda Manual*,[277] *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. 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. According to the European Commission, the "Internet is used to inspire and mobilise local terrorist networks and individuals in Europe and also serves as a source of information on terrorist means and methods, thus functioning as a 'virtual training camp'. Activities of public provocation to commit terrorist offences, recruitment for terrorism and training for terrorism have multiplied at very low cost and risk."[278] Therefore, in certain countries the distribution of content related to terrorism is already criminalized, and in certain countries downloading such content can potentially lead to a possession charge under terrorism laws. Many states have criminalized or starting to criminalize public provocation to commit terrorist offences.

---

between September 1, 1939 until July 31, 1990, b) other politically motivated reprisals, instigated by the officers of the Polish law enforcement agencies or the judiciary or persons acting on their order which were disclosed in the contents of the rulings made on the strength of the Act, dated February 23, 1991, on considering as invalid the rulings made in the cases of persons oppressed for their activities for the cause of an independent Polish State (Journal of Laws No. 34, item 149, with later amendments).

273 See article 6 of the Emergency Ordinance No. 31 of March 13, 2002.

274 Criminal Code (Official Gazette Republic of Slovenia No 55/2008). Public Incitement to Hatred, Violence or Intolerance.

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

276 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.

277 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/.

278 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.

With regards to this issue, the Council of Europe Convention on the Prevention of Terrorism (CETS No. 196) which entered into force in June 2007 provides for a harmonised legal basis to prevent terrorism and to counter, in particular, public provocation to commit terrorist offences,[279] recruitment[280] and training[281] for terrorism including through the Internet. Therefore, 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 criminalised. While 43 member states signed the Convention, only 27 of them ratified it as of April 2011. Four Member States of the CoE (Czech Republic, Liechtenstein, Monaco and Switzerland) neither signed nor ratified the Convention. As far as the OSCE participating States are concerned, all of the CoE ratifying States are also members of the OSCE, while 13 OSCE participating States neither signed nor ratified the Convention.

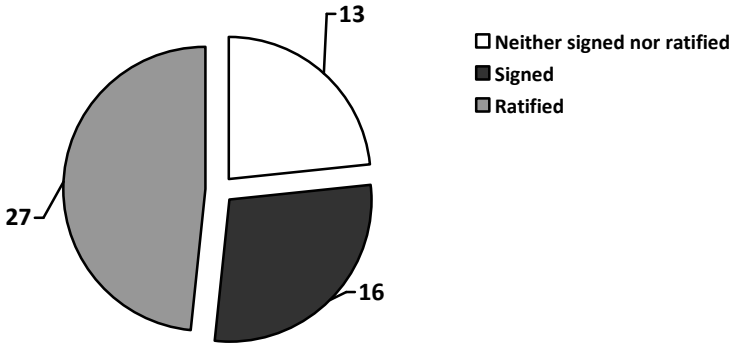


Figure 28. Status in regard to signing and ratifying the CoE Convention on the Prevention of Terrorism

In terms of combating the use of the Internet for terrorist purposes, the OSCE, at the Sofia Ministerial Council in 2004, decided that "participating States will exchange information on the use of the Internet for terrorist purposes and identify possible strategies to combat this threat, while ensuring respect for international human rights obligations and standards, including those concerning the rights to privacy and freedom of opinion and expression."[282] This was followed up by a decision on countering the use of the Internet for terrorist purposes in 2006 during the OSCE Brussels Ministerial Council.[283] The OSCE Decision invited the

---

279 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).

280. 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).

281. 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).

282 Sofia Ministerial Council, Decision No. 3/04: Combating the use of the Internet for terrorist purposes, 2004.

283 Brussels Ministerial Council, Decision No. 7/06: Countering the use of the Internet for terrorist purposes, 2006. Note further the outcomes of the OSCE Expert Workshop on Combating the Use of the Internet for Terrorist Purposes (Vienna, 13 and 14 October 2005), and the OSCE-Council of Europe Expert Workshop on Preventing Terrorism: Fighting Incitement and Related Terrorist Activities (Vienna, 19 and 20 October 2006).

"participating States to increase their monitoring of websites of terrorist/violent extremist organizations and their supporters and to invigorate their exchange of information in the OSCE and other relevant fora on the use of the Internet for terrorist purposes and measures taken to counter it, in line with national legislation, while ensuring respect for international human rights obligations and standards, including those concerning the rights to privacy and freedom of opinion and expression, and the rule of law."[284]

Similarly, since June 2006 the EU has been trying to formulate a harmonised policy to combat the terrorist use of the Internet. The European Commission introduced provisions to criminalise the public provocation to commit terrorist offences,[285] recruitment for terrorism,[286] and training for terrorism[287] by amending the Framework Decision on combating terrorism.[288] Through Article 2 the amended Council Framework Decision states that this Framework Decision "shall not have the effect of requiring Member States to take measures in contradiction of fundamental principles relating to freedom of expression, in particular freedom of the press and the freedom of expression in other media as they result from constitutional traditions or rules governing the rights and responsibilities of, and the procedural guarantees for, the press or other media where these rules relate to the determination or limitation of liability." The deadline for the transposition of the Framework Decision by the signatories was 09.12.2010.

Furthermore, the European Commission has taken up the initiative of four Member States (Germany, Netherlands, Czech Republic, and United Kingdom),[289] and their sub-project "Exploring the Islamist Extremist Web of Europe - Analysis and Preventive Approaches" as part of the EU Check the Web (Monitoring) Project,[290] and started a public-private partnership approach to countering terrorist use of the Internet. It has started a dialogue between law enforcement authorities and service providers to reduce the dissemination of illegal terrorism-related content on the internet and organized two conferences (the first in November 2009, the second in May 2010). A European Agreement Model to facilitate public/private cooperation on the issue is under development.[291]

As part of this OSCE survey, the OSCE participating States were asked whether **they have in place specific legal provisions outlawing incitement to terrorism, terrorist propaganda**

---

284 Brussels Ministerial Council, Decision No. 7/06: Countering the use of the Internet for terrorist purposes, 2006.

285 According to Article 3(1)(a) "public provocation to commit a terrorist offence" shall mean the distribution, or otherwise making available, of a message to the public, with the intent to incite the commission of one of the offences listed in Article 1(1)(a) to (h), where such conduct, whether or not directly advocating terrorist offences, causes a danger that one or more such offences may be committed.

286 According to Article 3(1)(b) "recruitment for terrorism" shall mean soliciting another person to commit one of the offences listed in Article 1(1)(a) to (h), or in Article 2(2).

287 According to Article 3(1)(c) "training for terrorism" shall mean providing 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 committing one of the offences listed in Article 1(1)(a) to (h), knowing that the skills provided are intended to be used for this purpose.

288 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.

289 EU Counter-Terrorism Coordinator, EU Counter-Terrorism Strategy - Discussion paper, Council of the European Union, Brussels, Doc No. 15983/08, 19 November, 2008.

290 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 the Internet.

291 EU Counter-Terrorism Coordinator (CTC), EU Action Plan on combating terrorism, 15893/1/10 REV 1, Brussels, 17 January 2011.

and/or terrorist use of the Internet (Question 6).[292] 40 (71.4%) of the participating States stated that there are such laws in their countries. Only six (10.7%) stated that they do not any such legal provisions.[293] No data was obtained from ten (17.9%) of the participating States.

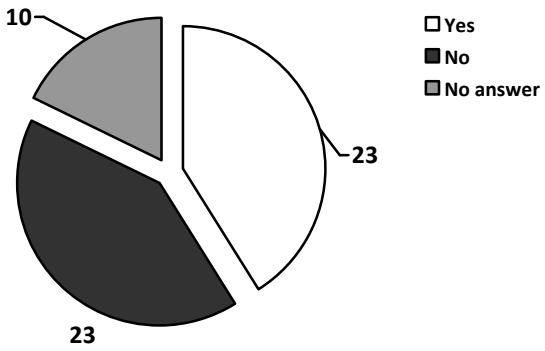


Figure 29. OSCE participating States' responses with regards to specific legal provisions outlawing incitement to terrorism, terrorist propaganda and/or terrorist use of the Internet (Question 6)

The recently amended Criminal Code of **Albania**[294] includes specific legal provisions that are relevant to electronic communications, training for acts with terrorist purposes,[295] public incitement, and to propagandize actions with terrorist purposes.[296] The possession of content involving "terrorist propaganda" materials is also criminalized. The maximum prison terms envisaged by law for such offences are ten years for public incitement, and propaganda for actions with terrorist purposes, and a minimum prison term of seven years for the crime of training acts with terrorist motives.[297] In **Austria**, section 282 of the Criminal Code (StGB) sanctions the incitement to criminal acts, and the approval of criminal acts with up to two years' imprisonment. Moreover, according to section 12 StGB, not only the immediate perpetrator is punishable, but also anyone who contributes to or instigates a criminal act.[298] However, the mere possession of propaganda material is not criminalized in Austria.

---

292 The participating States of the OSCE were also asked how these offences are defined by law, whether the possession of content involving "terrorsit propaganda" is criminalized, which sanctions (criminal, administrative, civil) are envisaged by law, the maximum prison term envisaged by law for such offences, any statistical information in relation to convictions under such provisions for the reporting period of 1 January 2007 – 30 June 2010, and whether the law (or relevant regulations) prescribes blocking access to websites or any other types of Internet content as a sanction for these offences.

293 Armenia, Bulgaria, Hungary, Liechtenstein, Romania, Serbia.

294 Law No. 9686 (26.02.2007) "On some addenda and amendments to Law No. 7895 (27.01.1995) "The Criminal Code of the Republic of Albania".

295 Article 232 of the Albanian Criminal Code: "training acts with terrorist purposes" is defined as acts involving the preparations, training and provision of all forms of instructions, including those delivered anonymously or through electronic means, for the production and utilization of explosive materials, firearms and military ammunitions, chemical, biological and nuclear weaponry and all other forms of armaments that are hazardous to people and property, as well as for the deployment of new techniques and methods for carrying out actions with terrorist purposes, including the cases when such actions are directed towards another state, international organizations or institutions.

296 Article 232/a of the Albanian Criminal Code: "public incitement and propaganda for actions with terrorist purposes" is designated as incitement, public calling and distribution of written or other forms of propaganda materials, which aim at supporting or carrying out acts with terrorist purposes, or the financing of terrorism-related activities.

297 Since the recent adoption of the relevant legal provisions in 2007, there have been no recorded cases of convictions.

298 Section 278c StGB defines terrorist criminal acts.

In **Azerbaijan,** liability for incitement to terrorism and abetting propaganda of terrorism is assigned through the simultaneous application of Articles 214 ("Terrorism") and 32 ("Conspiracy")[299] of the Criminal Code of the Azerbaijan Republic. The use of the Internet for terrorist purposes is regulated by Article 214 of the Criminal Code.[300] Possession of terrorsit propaganda material does not constitute grounds for criminal indictment, except in cases of criminal complicity.[301] Incitement[302] to carry out terrorism related acts[303] is also criminalized in **Belarus**.[304]

In **Canada**, like in most common law countries, the general modes of participation that define parties to an offence in the Criminal Code are applicable to all the offences, and establish terms through operation of law under which a person can be found to be a "party".[305] Furthermore, section 2 of the Criminal Code defines a "terrorism offence" to include any counselling (which includes inciting) in relation to a "terrorism offence". Moreover, the second branch of the definition of "terrorist activity" in subsection 83.01(1) of the Criminal Code states, in part, that an act or omission also "includes a conspiracy, attempt or threat to commit any such act or omission, or being an accessory after the fact or counselling in relation to any such act or omission …" Hence, where someone incites another (inciting being one way to counsel) to commit a terrorist activity, that incitement itself would fall within the definition of "terrorist activity".

In addition, there are a number of terrorism offences that could be considered as catching various forms of incitement to terrorism in Canada. By subsection 83.18(1) of the Criminal Code,[306] every one who knowingly participates in or contributes to, directly or indirectly, any activity of a terrorist group for the purpose of enhancing the ability of any terrorist group to facilitate or carry out a terrorist activity is guilty of an indictable offence, and liable to imprisonment for a term not exceeding ten years. The offence may be committed whether or not a terrorist group actually facilitates or carries out a terrorist activity; the participation or contribution of the accused actually enhances the ability of a terrorist group to facilitate or carry out a terrorist activity; or the accused knows the specific nature of any terrorist activity

---

299 According to Article 32.4 of the Criminal Code of Azerbaijan, incitement is defined as actions that result in one person inclining another, through persuasion, bribery, threats, or other means, to commit a crime. At the same time, criminal indictment is possible in cases where propaganda of terrorism is aimed at the commission of a terrorist act.

300 The actions of an individual performing as an agitator who conducts propaganda of terrorism in the commission of a terrorist act fall under Article 214.1, with references to Article 32 of the Criminal Code of the Azerbaijan Republic. Using the Internet for terrorist purposes is considered the commission of a crime from the moment it is first employed until it reaches a specified level and the creation of an actual threat to safety.

301 There is no statistical information in relation to convictions handed down in accordance with Article 214 of the Criminal Code of the Azerbaijan Republic during the period of 1 January 2007 to 30 June 2010.

302 Article 16 of the Criminal Code of Belarus.

303 See articles 124, 126, 289, 290, 290.1 and 359 of the Criminal Code.

304 During the period from 2007 through 2009, nobody was convicted of such a crime.

305 Pursuant to paragraph 21(1)(c) of the Criminal Code, every one is a party to an offence who abets any person in committing it. To abet within the meaning of this section includes intentionally encouraging, instigating or promoting the crime to be committed. In addition, section 22 of the Criminal Code makes a person who counsels another person to commit an offence that is thereby committed a party to that offence, and according to subsection 22(3), counselling includes incitement. By section 464 of the Code, one can also commit the offence of counselling even if the offence being counselled has not been committed. Canadian courts have found that counselling requires that the statements, viewed objectively, actively promote, advocate, or encourage the commission of the offence described in them. Unlike abetting, the mental fault element for counselling is not restricted to intention and includes recklessness.

306 Knowingly Participating in Any Activity of a Terrorist Group (Including Recruiting a Person into a Terrorist Group).

that may be facilitated or carried out by a terrorist group.[307] The maximum sentence for this crime is ten years' imprisonment.

Section 83.19 of the Criminal Code[308] provides that everyone who knowingly facilitates a terrorist activity is guilty of an indictable offence and liable to imprisonment for a term not exceeding fourteen years.[309] The maximum sentence for this crime is 14 years' imprisonment.[310] Section 83.22(1) of the Criminal Code also criminalizes knowingly instructing any person to carry out a terrorist activity.[311] These offences can be used to prosecute terrorist activity that involves the use of the Internet in Canada. The case of *R. v. Namouh*[312] is an example that illustrates the use of the Internet for incitement to terrorism.

> The accused had participated in making and disseminating various videos for the Global Islamic Media Front (GIMF). The Crown prosecutor successfully argued that Namouh spent hours creating and distributing propaganda videos, including images of the deaths of Western soldiers and suicide bombings. Cybercrime investigators extracted videos, including how-to guides for detonating suicide bombs and encrypting e-mails, from his computer. They found thousands of pages of transcripts of Namouh's posts, suggesting that he was very active in chat rooms, message boards and jihad forums. The judge decided that the GMIF was a "terrorist group", as defined the Criminal Code, because it counselled the commission of terrorist activity through its promotion of violent jihad.

In terms of possession of terrorist propaganda, mere possession of terrorist propaganda is not criminalized in Canada.

---

307 See subsection 83.18(2) of the Criminal Code. By subsection 83.18(3), "participating in or contributing to an activity of a terrorist group" includes, in part, providing, receiving or recruiting a person to receive training; providing or offering to provide a skill or an expertise for the benefit of, at the direction of or in association with a terrorist group; recruiting a person in order to facilitate or commit a terrorism offence; entering or remaining in any country for the benefit of, at the direction of, or in association with, a terrorist group; and making oneself, in response to instructions from any of the persons who constitute a terrorist group, available to facilitate or commit a terrorist offence. Factors that a court may use to determine whether an accused participates in or contributes to any activity of a terrorist group include whether the accused uses a name, word, symbol or other representation identifying the terrorist group; frequently associates with any of the persons who constitute the terrorist group; or receives any benefit from the terrorist group (subsection 83.18(4)).

308 Knowingly Facilitating a Terrorist Activity.

309 By subsection 83.19(2), a terrorist activity is facilitated whether or not the facilitator knows that a particular terrorist activity is facilitated, that any particular terrorist activity was foreseen or planned at the time it was facilitated, or that any terrorist activity was actually carried out.

310 "Knowingly Instructing any Person to Carry out Any Activity for the Benefit of a Terrorist Group" is also criminalized through subsection 83.21 (1) of the Criminal Code.

311 Every person who knowingly instructs, directly or indirectly, any person to carry out a terrorist activity is guilty of an indictable offence and liable to imprisonment for life (subsection 83.22(1) of the Criminal Code). Again, the offence may be committed whether or not: the terrorist activity is actually carried out, the accused instructs a particular person to carry out the terrorist activity, the accused knows the identity of the person whom the accused instructs to carry out the terrorist activity, or the person whom the accused instructs to carry out the terrorist activity knows that it is a terrorist activity (subsection 83.22(2)) The maximum punishment for this crime is life imprisonment.

312 *R. v. Namouh* (2010) QCCQ 943 (CanLII). Saïd Namouh, 37, was sentenced in the Court of Quebec to life in jail for conspiring to deliver, discharge or detonate an explosive or lethal device in a public place contrary to s. 431.2 of the *Criminal Code*. In addition, he was sentenced to eight years in jail for extortion of a foreign government for the benefit, at the direction and in association with a terrorist group contrary to s. 83.2 of the *Criminal Code*, eight years for facilitating terrorist activity contrary to s. 83.19 and four years for his participation in a terrorist group contrary to s. 83.18.

In **Croatia**, public instigation to terrorism is criminalized through the Criminal Code,[313] and punished by a prison term of one to ten years. In **Estonia**, public incitement for the commission of acts of terrorism is punishable by two to 10 years of imprisonment.[314] The mere possession of content involving "terrorist propaganda" is not criminalized in Estonia. In **Finland**, incitement to terrorism is criminalized in the Criminal Code,[315] but the possession of content involving terrorist propaganda is not criminalized.

In **France**, incitement of acts of terrorism is also criminalized.[316] If the acts of justification of or incitement to commit an act of terrorism result from messages or information made available to the public by an online communications service, and they constitute patently illicit unrest, the cessation of this service may be pronounced by the judge in chambers, at the request of the public prosecutor and any physical person or legal entity with an interest in the matter. Within the context of French legislation, the case of *Leroy v. France*[317] should be noted. The European Court of Human Rights held in that case that the publication of a drawing (cartoon) representing the attack on the twin towers of the World Trade Center, with a caption which parodied the advertising slogan of a famous brand: "We have all dreamt of it ... Hamas did it" provoked a certain public reaction, capable of stirring up violence and demonstrating a plausible impact on public order in a politically sensitive region, namely the Basque Country. The drawing was published in the Basque weekly newspaper *Ekaitza* on 13 September 2001, two days after the attacks of 11 September.

The applicant complained that the French courts had denied his real intention, which was governed by political and activist expression, namely that of communicating his anti-Americanism through a satirical image and illustrating the decline of American imperialism. The European Court, however, considered that the drawing was not limited to criticism of American imperialism, but supported and glorified the latter's violent destruction. In this regard, the European Court based its finding on the caption which accompanied the drawing, and noted that the applicant had expressed his moral support for those whom he presumed to be the perpetrators of the attacks of 11 September 2001. Through his choice of language, the applicant commented approvingly on the violence perpetrated against thousands of civilians and diminished the dignity of the victims. In the European Court's opinion, this factor – the date of publication – was such as to increase the applicant's responsibility in his account of, and even support for, a tragic event, whether considered from an artistic or a journalistic perspective. Therefore, no violation of Article 10 was found by the Court.[318]

---

313 Article 169.a. To institute the criminal proceedings in regard of the crime referred to in this Article it is necessary to have the approval of the Attorney General of the Republic of Croatia. Furthermore, Article 169.b criminalizes recruiting and training for terrorism.

314 Section 2372 (Preparation of and incitement to acts of terrorism) of the Estonian Penal Code.

315 Criminal Code, Chapter 34 a, Section 1 - Offences made with terrorist intent: A person who, with terrorist intent and in a manner that is conducive to causing serious harm to a State or an international organisation intentionally commits the public incitement to an offence referred to in chapter 17, section 1, shall be sentenced to imprisonment for at least four months and at most four years: Criminal Code, Chapter 17, Section 1 - Public incitement to an offence (1) A person who through the mass media or publicly in a crowd or in a generally published writing or other presentation exhorts or incites anyone into the commission of an offence, so that the exhortation or incitement (1) causes a danger of the offence or a punishable attempt being committed, or (2) otherwise clearly endangers public order or security, shall be sentenced for public incitement to an offence to a fine or to imprisonment for at most two years.

316 Article 24 of the Law of 29 July 1881 on Freedom of the Press.

317 *Leroy v. France*, Application No. 36109/03, Chamber judgment of 02.10.2008.

318 Similarly, no violation of Article 10 was found by the Court in *Orban and others v. France* (Application No. 20985/05, Chamber judgment of 15.01.2009) on account of the applicants' conviction for publicly defending war crimes, following the publication of a book named *Services Spéciaux Algérie 1955-1957* ("Special Services: Algeria 1955-1957"). According to the Court, penalising a publisher for having assisted

The **Georgian** Criminal Code through Article 324 restricts the use of the Internet by terrorists.[319] Article 330 restricts and criminalizes public incitement to terrorism and terrorism propaganda by declaring that public dissemination of information or otherwise calling upon to commit any of the crimes of terrorism, notwithstanding the fact whether it contains direct incitement to commission of crime, or whether it creates a real threat of commission of this crime shall be punishable by deprivation of liberty for three to six years.[320] In **Germany**, the provision of directions for the commission of a serious violent act endangering the state is criminalized through Section 91 of the Criminal Code (StGB).[321] The mere possession of content capable of serving as an instruction in the sense as defined by Section 91 of the Criminal Code is not penalized by law. The maximum term of imprisonment as provided for by Section 91 of the Criminal Code amounts to three (3) years.

In **Ireland**, in common law an offence of incitement to commit a criminal offence exists. Furthermore, incitement or invitation to join, inter alia, an unlawful organization is also criminalized.[322] A person found guilty of such a crime is liable on conviction on indictment to imprisonment for a term not exceeding 10 years.

In **Kazakhstan**, propaganda of terrorism[323] or public appeals to commit an act of terrorism, and/or the distribution of such materials is criminalized by deprivation of liberty for a term of

---

in the dissemination of a witness account written by a third party concerning events which formed part of a country's history would seriously hamper contribution to the discussion of matters of public interest and should not be envisaged without particularly good reason.

319 Article 324 states that "cyber terrorism, i.e. misappropriation of data, protected by the law, use of it, or threat of its use that can pose grave consequence and infringes public security, state strategic, politic and economic interests, committed for the purpose to intimidate population and/or influence governmental agency is punishable by the depravation of liberty from ten to fifteen years.

320 For the act stipulated in Article 330, criminal responsibility of a legal person is envisaged as well. According to the statistical information, during the reporting period there was no registered offence envisaged specifically by article 324 and article 330 of the Georgian Criminal Code.

321 (1) Imprisonment of up to three years or a fine shall be imposed upon anyone who
1. commends or makes accessible to another person a writing (section 11 (3), whose content is apt to serve as directions for a serious violent act endangering the state (section 89a (1), if the circumstances of its dissemination are apt to encourage or cause the willingness of others to commit a serious violent act endangering the state,
2. procures a writing of the type described in number 1 above in order to commit a serious violent act endangering the state.
(2) Subs. 1 number 1 shall not apply if
1. the act relates to civic education, to the aversion of unconstitutional movements, to art and science, research or scholarship, reporting on current events, history or similar aims, or
2. the act serves exclusively to fulfill lawful professional or official duties.
(3) If the offender's guilt is insignificant, the court may order discharge pursuant to this provision.

322 Section 3 of the Criminal Law Act 1976 provides that any person who recruits another person for an unlawful organisation or who incites or invites another person (or other persons generally) to join an unlawful organisation or to take part in, support or assist its activities shall be guilty of an offence and shall be liable on conviction on indictment to imprisonment for a term not exceeding 10 years. The Criminal justice (Terrorist Offences) Act 2005 through section 5 defines "terrorist groups": A terrorist group that engages in, promotes, encourages or advocates the commission, in or outside the State, of a terrorist activity is an unlawful organisation within the meaning and for the purposes of the Offences against the State Acts 1939 to 1998 and section 3 of the Criminal Law Act 1976.

323 Terrorism is defined in Article 1(3) of Law of the Republic of Kazakhstan No. 416-I of 13 July 1999 "On Counteracting Terrorism" as: an illegal criminally punishable act or the threat to commit such an act against individuals or organizations for the purpose of violating public security, intimidating the public, influencing decision-making by governmental bodies of the Republic of Kazakhstan, foreign countries and international organizations, or with the purpose of terminating the activity of government or public officials, or out of revenge for such activity.

up to five years.[324] The same acts committed by a person with the use of his/her official position or by the head of a public association or with the use of the media shall be punishable by deprivation of liberty for a term of three to eight years. Furthermore, the distribution of media products containing information and materials aimed at the propaganda or advocating of a forced change in the constitutional system, violation of the integrity of the Republic of Kazakhstan, undermining state security, unleashing war, inciting social, racial, national, religious, class or tribal strife, supporting and justifying extremism or terrorism, as well as revealing the techniques and tactics of antiterrorist operations during their implementation in the territory of the Republic of Kazakhstan is punished with administrative fines.[325] Furthermore, propaganda and justification of extremism or terrorism, distribution of information revealing the techniques and tactics of antiterrorist operations during their implementation is also prohibited.[326] Grounds for terminating a media publication or distributing a media product include propaganda of extremism or terrorism.[327] Furthermore, distribution of material advocating terrorism in an online resource shall entail criminal responsibility under Article 233-1 of the Criminal Code.[328]

Public incitement to terrorism or publishing terrorist propaganda is criminalized by Article 226(3) of the Criminal Code of the **Kyrgyz Republic**, and is punished with a fine in the amount of 50 to 500 specified rates or correctional labour for a term of up to one year or custodial restraint for a term of up to two years or deprivation of liberty for a term of up to two years.[329] Article 299(2) of the Criminal Code also provides for liability for acquisition, storage, transportation and sending of extremist materials for the purpose of distribution, or production and distribution of the same as well as deliberate use of the symbols or of the attributes of extremist organizations.[330] In **Latvia**, under Article 882 of the Criminal Law on Invitation [i.e., incitement] to Terrorism and Terrorism Threats, a person who commits a public incitement to terrorism or threatens to implement an act of terror can be deprived of liberty for a term up to eight years. The crime can also be committed through the Internet.[331]

---

[324] Article 233-1, Law of the Republic of Kazakhstan No. 416-I of 13 July 1999 "On Counteracting Terrorism".

[325] Article 344. Manufacture, Possession, Import, Conveyance, and Dissemination in the Territory of the Republic of Kazakhstan of Media Products and Other Products, Code of the Republic of Kazakhstan on Administrative Offences No. 155-II of 30 January 2001 (with amendments and addenda as of 6 October 2010).

[326] Article 2(3) (Freedom of Speech, Receipt and Dissemination of Information), Law of the Republic of Kazakhstan No. 451-I of 23 July 1999 "On the Media".

[327] Article 13. Termination and Suspension of a Media Publication or Distribution of a Media Product, Law of the Republic of Kazakhstan No. 451-I of 23 July 1999 "On the Media".

[328] According to the Committee on Legal Statistics and Special Accounts of the General Prosecutor's Office of the Republic of Kazakhstan, 1 person in 2008 and 2 persons for 6 months in 2010 were prosecuted under Article 233 of the CC of the RK; 2 persons in 2008, 3 persons in 2009 and 1 person for 6 months in 2010 were prosecuted under Article 233-1 of the CC of the RK; 6 persons in 2008 and 16 persons in 2009 were prosecuted under Article 233-2 of the CC of the RK.

[329] The same actions committed with the use of media shall be punishable by a fine of up to 1000 specified rates or correctional labour for a term of up to three years or custodial restraint for a term of up to five years or deprivation of liberty for a term of up to five years with debarment from holding certain positions or engaging in certain activities for a term of up to three years.

[330] Acquisition, storage, transportation and sending of extremist materials for the purpose of distribution, or production and distribution of the same as well as deliberate use of the symbols or of the attributes of extremist organizations shall be punishable by a fine in an amount of 1000 to 5000 specified rates or deprivation of liberty for a term of three to five years with debarment from holding certain positions or engaging in certain activities. Note also Article 297 which criminalizes the public incitement to violent change of the constitutional system, and Article 299 which criminalizes the instigation of national, racial, religious or inter-regional hostility.

[331] According to the data in the Court Information System, there have been no convictions under Article 882 of

In **Lithuania**, making public declarations orally, in writing or in the media, promoting or inciting an act of terrorism or other crimes relating to terrorism or expressing contempt for victims of terrorism are criminalized.[332] According to Article 2501 of the Criminal Code any person found guilty of incitement to terrorism shall be punished by a fine (ranging from 37 to 3765 Euro) or by restriction of liberty (ranging from three months to two years) or by arrest (ranging from 15 to 90 days) or by imprisonment for a term of up to three years. The possession of content involving terrorist propaganda is not criminalized in Lithuania.

In **Montenegro**, the Criminal Code, along with its amendments in 2010, aiming at implementing the European Convention on the Suppression of Terrorism, introduced various new offences including public incitement to commit terrorist acts, recruitment, and training for committing terrorist acts.[333] In **Moldova**, incitement to terrorism, i.e., distribution or other appraisal of the general public of information with the intention of abetting to commit crimes of a terrorist nature or in the awareness that this information might do so is criminalized. Furthermore, the Criminal Code also criminalizes public justification of terrorism, i.e., distribution or other appraisal of the general public of information about recognition of an ideology or practice of committing crimes of a terrorist nature as being correct, due for support or worthy of imitation.[334]

In **Norway**, public incitement to terrorism is prohibited.[335] The maximum penalty for incitement to terrorism is six years' imprisonment. Section 147c of the Penal Code is applicable to distribution of terrorist propaganda trough open websites. Furthermore, Section 147c(2) refers to statements that are suitable to reach a large number of people. This means that Section 147c is applicable regardless of propaganda actually reaching a certain number of people. In Norway there are no provisions specifically addressing the possession of terrorist propaganda. However, it can be noted that all forms of aiding and abetting terrorist actions may be punishable subject to Section 147a.

In **Poland,** Article 255 of the Penal Code criminalizes public incitement to any offence, including terrorism. Public incitement referring to innumerable audience covers also the Internet by definition as a modus operandi. Depending on the circumstances of a case, possession of content related to "terrorist propaganda" could be prosecuted as a preparatory act to an offence.[336]

In the **Russian Federation** liability is envisaged for encouraging terrorist activity, incitement to terrorist activity or public justification of terrorism without singling out the Internet as a specific platform of crime. Article 3(2) of Federal Law "On Counteracting Terrorism"[337] defines incitement to terrorism[338] and terrorist propaganda as terrorist activity.[339] The

---

the Criminal Law during the period from 1 January 2007 to 30 June 2010.

332 Article 2501 "Incitement of Terrorism" of the Criminal Code.

333 The Law on Ratification of the European Convention on Suppression of Terrorism has been published in the Official Gazette of Montenegro 5/2008 dated 7 August 2008, by means of which Montenegro ratified this Convention.

334 Article 2792 introduced by Law No. 136-XVI dated 19 June 2008, which entered into force on 8 August 2008.

335 Section 147c of the Penal Code 1902. The current legislation concerning terrorism is maintained in the Penal Code 2005 chapter 18. These rules are not yet in force.

336 See Article 16 of the Penal Code.

337 Federal Law No. 35-FZ of 6 March 2006.

338 Articles 205, 205.1, and 205.2 of the Russian Federation Criminal Code describe terrorism as "the perpetration of an explosion, arson, or any other action endangering the lives of people, causing sizable property damage, or entailing other socially dangerous consequences, if these actions have been committed

possession of content involving terrorist propaganda is not criminalized by law. Article 205.2 of the Russian Federation Criminal Code envisages that public incitement to terrorist acts or public justification of terrorism shall be punishable by a fine of up to 300,000 roubles or in the amount of the wage or salary, or any other income of the convicted person for a period of up to three years, or deprivation of liberty for a term of up to four years.

Article 110 of the Criminal Code of **Slovenia** also criminalizes incitement and public glorification of terrorist activities.[340] In **Sweden**, the Act on Criminal Responsibility for Public Provocation, Recruitment, and Training concerning Terrorist Offences and other Particularly Serious Crime came into force on 1 December 2010.[341] The new Act includes offences such as public provocation, recruitment, training, and other provisions concerning criminal responsibility. These provisions can be applicable to acts committed on the Internet provided that the website is not protected by Swedish Fundamental Law on Freedom of Expression.[342] Such protection is given to websites provided by mass media companies, or those having a valid certificate of no legal impediment to publication. However, incitement to terrorism, terrorist propaganda, and/or terrorist use of the Internet can to some extend fall under the scope of the provision on inciting rebellion, which is applicable even to constitutionally protected speech and websites.[343]

In **Turkey**, it is an offence to print or publish declarations or leaflets emanating from terrorist organisations.[344] This is punished by a term of imprisonment of one to three years. Periodicals whose content openly encourages the commission of offences within the framework of the activities of a terrorist organisation, approves of the offences committed by a terrorist organisation or its members or constitutes propaganda in favour of the terrorist organisation may be suspended for a period of fifteen days to one month as a preventive measure by the decision of a judge or, if a delay is detrimental, on an instruction from a public prosecutor.[345]

---

for the purpose of violating public security, frightening the population, or exerting influence on decision-making by governmental bodies, or international organisations, and also the threat of committing said actions for the same ends" (Article 205); of liability for assisting in terrorist activity (Art. 205.1) and for public incitement to terrorist acts or for public justification of terrorism (Art. 205.2).

339 Actions aimed at substantiating or justifying terrorism, including information or other aiding and abetting in the planning, preparation, and/or performance of a terrorist act, as well as terrorist propaganda, the distribution of materials or information inciting terrorist activity or substantiating or justifying the need to perform such activity are defined as terrorist activity (Article 3 (2 (e, f)) of Federal Law No. 35-FZ of 6 March 2006 "On Counteracting Terrorism" (hereinafter referred to as the Law "On Terrorism").

340 Article 110, Criminal Code (Official Gazette Republic of Slovenia No 55/2008): (1) Whoever incites commitment of criminal offences under Article 108 of this Penal Code and therefore propagates messages or makes them available to other persons in some other manner with the intention to promote terrorist criminal offences and thus causes danger that one or more such criminal offences would be committed, shall be sentenced to imprisonment between one and ten years. (2) Whoever directly or indirectly publicly glorifies or advocates criminal offences under Article 108 or the criminal offence referred to in the preceding paragraph by, with the purpose under preceding paragraph, propagating messages or making them available to the public and therefore causes danger that one or more such criminal offences would be committed, shall be punished in the same manner.

341 This Act contains provisions for the implementation of the Council of Europe Convention on the Prevention of Terrorism, and the EU Council Framework Decision 2008/919/JHA.

342 SFS 1991:1469. See <http://www.riksdagen.se/templates/R_Page____6316.aspx>.

343 See Chapter 5, Section 1 of the Fundamental Law on Freedom of Expression, Chapter 7, Section 4 of the Freedom of the Press Act, and Chapter 16, Section 5 of the Swedish Penal Code. The sole possession of content involving "terrorist propaganda" is not criminalized.

344 Section 6(2) of the Prevention of Terrorism Act (Law no. 3713), amended by Law no. 5532, which entered into force on 18 July 2006.

345 Section 6(5) of the Prevention of Terrorism Act (Law no. 3713), amended by Law no. 5532, which entered into force on 18 July 2006. On 3 March 2006 the former President of Turkey lodged a case with the Constitutional Court (case no. 2006/121) challenging the validity of section 6(5) of Law no. 3713. It had

Such punitive injunctions are issued with regards to several websites in Turkey under this provision.[346]

In **Turkmenistan**, the spreading of the information that provokes or justifies terrorism and extremism is prohibited.[347] In the **United Kingdom**, the Terrorism Act 2006 contains provisions to criminalize encouragement of terrorism in Section 1,[348] as well as the criminalisation of the dissemination of terrorist publications in Section 2.[349] Section 1 creates an offence of encouragement of acts of terrorism or Convention offences. The offence has been introduced to implement the requirements of Article 5 of the Council of Europe Convention on the Prevention of Terrorism. This requires State parties to have an offence of 'public provocation to commit a terrorist offence'. This new offence supplements the existing common law offence of incitement to commit an offence. Section 1 applies to a statement that is likely to be understood by some or all of the members of the public to whom it is published as a direct or indirect encouragement or other inducement to them to the commission, preparation or instigation of acts of terrorism or Convention offences. Section 1(3) provides that indirect encouragement of terrorism includes a statement that glorifies the commission or preparation of acts of terrorism or Convention offences but only if members of the public could reasonably be expected to infer that what is being glorified in the statement is being glorified as conduct that should be emulated by them in existing circumstances. Glorification is defined in Section 20(2) as including praise or celebration. Section 20(7) clarifies that references to conduct that should be emulated in existing circumstances includes references to conduct that is illustrative of a type of conduct that should be so emulated.[350]

---

been argued, inter alia, that this section had created an unconstitutional penalty. On 18 June 2009 the Constitutional Court dismissed the case (decision no. 2009/90).

346 See further Report of the OSCE Representative on Freedom of the Media *on Turkey and Internet Censorship*, January 2010, at <http://www.osce.org/documents/rfm/2010/01/42294_en.pdf>.

347 The Law of Turkmenistan "On Combating Terrorism" Paragraph 4 of Part 2 of Article 16.

348 Under s.1(3), the statements that are likely to be understood by members of the public as indirectly encouraging the commission or preparation of acts of terrorism or Convention offences include every statement which "(a) glorifies the commission or preparation (whether in the past, in the future or generally) of such acts or offences; and (b) is a statement from which those members of the public could reasonably be expected to infer that what is being glorified is being glorified as conduct that should be emulated by them in existing circumstances." A person guilty of an offence of encouragement of terrorism under s.1 shall be liable on conviction on indictment, to imprisonment for a term not exceeding seven years or to a fine, or to both; and on summary conviction in England and Wales, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum, or to both.

349 Under s.2(2), the dissemination of terrorist publications include distributing or circulating a terrorist publication; giving, selling or lending such a publication; offering such a publication for sale or loan; providing a service to others that enables them to obtain, read, listen to or look at such a publication, or to acquire it by means of a gift, sale or loan; transmitting the contents of such a publication electronically; or having such a publication in his possession with a view to its becoming the subject of conduct falling within the above mentioned activities. According to s.2(3), a publication will be regarded as a 'terrorist publication' if matter contained in it is likely "(a) to be understood, by some or all of the persons to whom it is or may become available as a consequence of that conduct, as a direct or indirect encouragement or other inducement to them to the commission, preparation or instigation of acts of terrorism; or (b) to be useful in the commission or preparation of such acts and to be understood, by some or all of those persons, as contained in the publication, or made available to them, wholly or mainly for the purpose of being so useful to them." Section 2(13) states that "publication" means an article or record of any description that contains any of the following, or any combination of them (a) matter to be read; (b) matter to be listened to; (c) matter to be looked at or watched. A person guilty of an offence under this section shall be liable, on conviction on indictment, to imprisonment for a term not exceeding seven years or to a fine, or to both; and on summary conviction in England and Wales, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum, or to both.

350 For example, if it was reasonable to expect members of the public to infer from a statement glorifying the bomb attacks on the London Underground on 7 July 2005 that what should be emulated is action causing

Section 2 of the Terrorism Act 2006 creates offences relating to the sale and other dissemination of books and other publications,[351] including material on the Internet, that encourage people to engage in terrorism, or provide information that could be useful to terrorists. Section 2(3)sets out the definition of 'terrorist publication'.

> A publication will be considered a terrorist publication if it meets one of two tests. The first test is if matter contained in it is likely to be understood by some or all of the persons to whom it is or may become available as a consequence of the conduct in subsection (2) as a direct or indirect encouragement or other inducement to the commission, preparation or instigation of acts of terrorism. The second test is if it contains any matter which is likely to be useful in the commission or preparation of such acts and it is likely to be understood by some or all of the persons to whom it is or may become available as being contained in the publication, or made available to them, wholly or mainly for the purposes of being so useful to them. The first reason for a book or other publication being a terrorist publication relates to the new offence under section 1. In either case, only a small part of a publication needs to satisfy the test for the publication to be a terrorist publication. As the whole publication will be a terrorist publication if a small part of it satisfies the test this means that the whole publication can be seized under the powers set out in section 28 and Schedule 2 (which provide for search, seizure and forfeiture of terrorist publications). However, in relation to the defence in subsection (9) of section 2, in order to establish part (a) of the defence, the defendant need only show that the part of a publication which satisfies the test did not express his views or have his endorsement.[352]

Section 5(5) provides that whether or not a publication is a terrorist publication must be determined at the time of the particular conduct in question, and having regard to the content of the publication as a whole and the circumstances in which the particular conduct occurred. This means that account can be taken of the nature of the bookseller or other disseminator of the publication.

Legal provisions criminalizing Child Pornography

Observing the rights of children, and their protection from sexual exploitation, child pornography has generally been recognized as an international problem.[353] Significant policy initiatives at the supranational, regional, and international levels have been put forward to address this issue.[354] However, harmonisation efforts to combat illegal Internet content, including the universally condemned content such as child pornography, have been protracted

---

severe disruption to London's transport network, this will be caught. See the Explanatory Notes for the Terrorism Act 2006 at <http://www.legislation.gov.uk/ukpga/2006/11/notes/division/4/1/1>.

351 Section 2(13)defines publication for the purposes of section 2 as an article or record of any description which contains matter to be read, matter to be listened to, or matter to be looked at or watched. This means that as well as covering books the section will also cover, amongst other things, films and videos (with or without sound), cassette tapes, electronic books, material contained on CD-ROMs and photographs.

352 *Ibid*.

353 Note the following instruments in relation to the need to extend particular care to children: Geneva Declaration of the Rights of the Child of 1924 and in the Declaration of the Rights of the Child adopted by the General Assembly on 20 November 1959; the Universal Declaration of Human Rights, in the International Covenant on Civil and Political Rights (in particular in articles 23 and 24), in the International Covenant on Economic, Social and Cultural Rights (in particular in article 10). See further the Convention on the Rights of the Child, adopted, and opened for signature, ratification and accession by General Assembly resolution 44/25 of 20 November 1989. The Convention entered into force on 2 September 1990, in accordance with article 49.

354 See generally Akdeniz, Y., Internet Child Pornography and the Law: National and International Responses, Ashgate, 2008 (ISBN-13 978-0-7546-2297-0).

and are ongoing[355] despite the adoption of several legal instruments, including the European Union's Framework Decision on combating the sexual exploitation of children and child pornography,[356] the Council of Europe's Cybercrime Convention 2001,[357] Council of Europe's more recent Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse,[358] 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.[359] These legal instruments require member states to criminalize production, distribution, dissemination or transmission of child pornography, supplying or making available of, and the acquisition or possession of child pornography among other child pornography related crimes. While these international agreements provide for up to ten years' imprisonment for the more serious offences of production and distribution, up to five years of imprisonment is generally envisaged for the relatively less serious offence of possession.

In terms of what constitutes "child pornography", the Council of Europe's Cybercrime Convention 2001 defines it[360] as pornographic material that visually depicts:

> (a) a minor engaged in sexually explicit conduct;
> (b) a person appearing to be a minor engaged in sexually explicit conduct;
> (c) realistic images representing a minor engaged in sexually explicit conduct.

Similarly, Council of Europe's Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse defines child pornography as "any material that visually depicts a child engaged in real or simulated sexually explicit conduct or any depiction of a child's sexual organs for primarily sexual purposes."[361]

The EU definition is provided in the Council Framework Decision which defines child pornography[362] as pornographic material that visually depicts or represents:

> (i) a real child involved or engaged in sexually explicit conduct, including lascivious exhibition of the genitals or the pubic area of a child; or
> (ii) a real person appearing to be a child involved or engaged in the conduct mentioned in (i); or

---

355 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.

356 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). For a summary of the Framework Decision see <http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_trafficking_in_human_beings/l33138_en.htm >.

357 Convention on Cybercrime, ETS No: 185, at <http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm>. Note Article 9 which includes criminal santions for child pornography.

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

359 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).

360 See Article 9(2).

361 See Article 20(2).

362 See Article 1(b).

(iii) realistic images of a non-existent child involved or engaged in the conduct mentioned in (i);

Finally, the United Nations' Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography defines child pornography as "any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes".[363]

All four legal instruments define a child as under the age of 18, and all four cover both real depictions as well as realistic and simulated representations within the definition of child pornography. Computer-generated images, as well as images of real persons above the age of 18 who appear to be a child under the age of 18, would be covered by these broad definitions. While the EU and CoE definitions refer to visual depictions and representations, the UN definition is broader as it refers to "any representation," and could also cover textual material including cartoons, and drawings.[364]

In terms of ratification at the Council of Europe level, 30 member states (as well as the United States)[365] implemented the Convention provisions into national legislation as of April 2011. Andorra, Monaco, Russia, and San Marino are the member states which have yet to sign the Convention, and 15 Council of Europe member states who signed the convention are yet to ratify the Convention. 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 enhance trust in information and communication technologies. This could result in further support for the Convention.

So far as the OSCE participating States are concerned, all of the CoE ratifying States are also members of the OSCE, while 11 OSCE participating States neither signed nor ratified the Cybercrime Convention.

---

363 See Article 2(c).

364 Written materials were deliberately left out of the EU definition as there was no support or agreement for the inclusion of textual or written material in the definition of child pornography. See the European Parliament report on Sexual exploitation of Children (A5-0206/2001), the European Parliament legislative resolution on the proposal for a Council Framework Decision on combating the sexual exploitation of children and child pornography (COM(2000) 854 — C5-0043/2001 — 2001/0025(CNS)), 2002/C 53 E/108-113, vol 45, 28 February 2002.

365 The full list of member states which ratified the Cybercrime Convention as of April 2011 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,[365] and the former Yugoslav Republic of Macedonia.

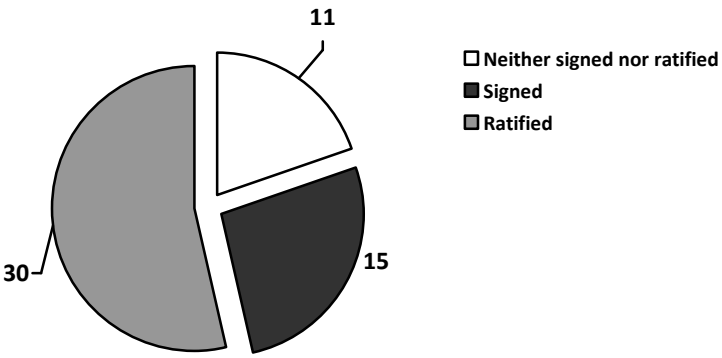


Figure 30. Status with regards to signing and ratification of the CoE Convention on Cybercrime

The Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse[366] which was opened to signature in October 2007 came into force in July 2010. So far, 42 contracting states signed the Convention but only 11 of them ratified it.[367]

It should also be noted that the EU Council Framework Decision came into force in January 2004, and the EU Member States implemented the provisions of the Framework Decision into national law by 20 January 2006. [368] In terms of the UN level ratification, 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 April 2011, 118 UN member states signed the Optional Protocol, and 142 members have ratified or acceded the Optional Protocol.[369]

The OSCE participating States were asked whether **there are specific legal provisions criminalizing child pornography** in their country **(Question 7).**[370] The overwhelming majority of the participating States (43, 76.8%) stated that they had such laws in place. Only three states (5.4%) (Azerbaijan,[371] Kyrgyzstan,[372] and Turkmenistan[373]) answered negatively. No data was obtained from ten (17.9%) of the participating States.

366 CETS No. 201.

367 Albania, Austria, Denmark, France, Greece, Malta, Montenegro, Netherlands, San Marino, Serbia, and Spain.

368 Note that the EU is consideing to amend the 2004 Council Framework Decision: 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, 2009/0049 (CNS), COM(2009)135 final, Brussels, 25.3.2009.

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

370 The participating States of the OSCE were also asked how these offences are defined by law, 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, which sanctions (criminal, administrative, civil) are envisaged by law, the maximum prison term envisaged by law for such offences, any statistical information in relation to convictions under such provisions for the reporting peri from January 2007 until 30 June 2010, and whether the law (or relevant regulations) prescribes blocking access to websites or any other types of Internet content as a sanction for these offences.

371 The legislation of the Azerbaijan Republic has no specific legal provisions criminalizing child pornography. The Azerbaijan Republic is a signatory to the Optional Protocol to the Convention on the Rights of the Child concerning the trafficking in children, child prostitution, and child pornography.

372 There are no specific child pornography laws in Kyrgyzstan.

373 There are no specific child pornography laws in Turkmenistan. Article 29 (Protection of the Child from Obscenities) of the Law of Turkmenistan "On the Guarantees of the Rights of the Child" states that the

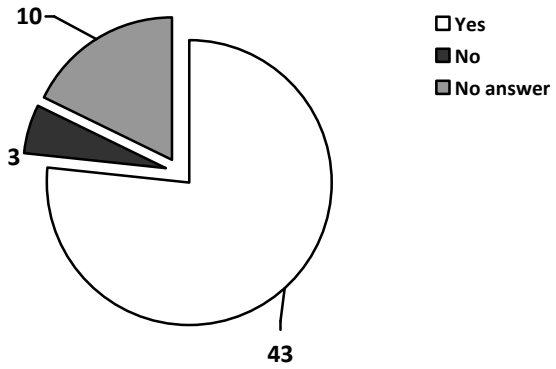


Figure 31. OSCE participatibg States' responses with regards to specific legal provisions criminalizing child pornography (Question 7)

In terms of the responses received, the recently amended **Albanian** Criminal Code[374] contains specific legal provisions related to the criminalization of child pornography and child exploitation. These provisions criminalize the production, distribution, advertising, importing, selling or publication of pornographic materials of minors, as well as the use of minors for the production of pornographic materials, and their publication or distribution through the Internet or other means of communication.[375] There are also criminal provisions on child exploitation (which potentially apply to the issue of child pornography) involving physical or psychological maltreatment of minors by their guardians.[376] The maximum prison term envisaged by law for the child pornography offences is five years, and for the exploitation offences it is 20 years.[377] The Albanian legislative framework does not have specific provisions regarding unreal characters (drawings, paintings, cartoons, artificially created images etc.) and computer-generated imagery within the concept of child pornography.

In **Austria**, Section 207a(1) of the Criminal Code criminalizes the pornographic depictions of minors.[378] The offence includes producing, as well as offering, providing, disseminating, demonstrating or otherwise making accessible pornographic depictions of minors to/for others.[379] Section 207a(2) criminalizes producing, importing, transporting or exporting pornographic depictions of minors for the purpose of distribution. Section 207a(3) criminalizes the procurement and possession of pornographic depictions of minors. Section 207a(3a) criminalizes knowingly accessing pornographic depictions of minors on the Internet. Subject to section 207a(5) production and possession of pornographic depictions of minors of age (14 to 18) are not criminalized if these are produced with the consent of the minor and for

---

production and dissemination of pornographic printed publications, films or any pornographic items shall be prohibited in Turkmenistan, and the state shall guarantee the protection of children from any sexual abuse. However, this particular law does not refer to specific crimes associated with child pornography.

374 Law No. 9859 (21.01.2008) "On some addenda and amendments to Law No. 7895 (27.01.1995) "The Criminal Code of the Republic of Albania".

375 Article 117.

376 Article 124/b.

377 Since the recent adoption of the relevant legal provisions in the Criminal Code in 2008, no convictions have been recorded.

378 An underage minor for the purposes of section 207a StGB means a person who has not yet celebrated his/her 14th birthday (section 74 para. 1 n° 1 StGB). A minor is a person who has not yet celebrated his/her 18th birthday (section 74 para. 1 n° 3 StGB). A minor of age is a person who has celebrated his/her 14th, but not yet 18th birthday.

379 Punishable with up to three years of imprisonment.

their own usage. Virtual child pornography is also covered by the Austrian provisions.[380] However, the production and possession of virtual pornography[381] of a minor is not criminalized if the perpetrator produces or possesses the depictions for his/her own usage, and if there is no danger that the depictions are distributed.[382]

In **Armenia**, forcing minors to get involved in the creation of software, video or film materials, pictures or other items of pornographic nature, as well as presenting children's pornography through computer networks is punished with a fine in the amount of 400 to 800 minimal salary, or with arrest for the term of up to three months, or with imprisonment for the term of up to three years.[383] In **Belarus**, criminal liability is provided for producing or storing for the purpose of distribution or advertisement, or distributing or advertising materials with images of a known minors or publicly demonstrating a film or video of pornographic content with such an image, using the World Wide Web, other means of public telecommunications or a dedicated telecommunications network.[384] Liability for the given acts may be up to thirteen years' deprivation of liberty with or without confiscation of property.[385] In **Bulgaria**, whoever produces, exhibits, broadcasts, offers, sells, lends or in any other way circulates works of pornographic content involving a minor, underage person, or a person with such an appearance shall be imprisoned for up to five years.[386] Furthermore, possession is also criminalized and applies to pornographic content involving "a minor, underage person, or a person with the appearance of a minor or underage person," and the possession offence is punished with a maximum imprisonment term of up to one year.[387]

In **Canada**, the Criminal Code prohibits the making, distributing, transmitting, making available, accessing, selling, advertising, exporting/importing as well as simple possession of child pornography.[388] Child pornography includes material that depicts sexual abuse of a real or imaginary child under the age of 18; written or audio material that advocates or counsels unlawful sexual activity with a child; and written or audio material that has, as its predominant characteristic, the description of prohibited sexual activity with persons under 18 years old where that description is provided for a sexual purpose. The definition also includes visual depictions, both real and fictional, of sexual activity involving persons under the age of 18.

---

380 Section 207a(4) of the Criminal Code covers realistic depictions of sexual acts of an underage minor or of an underage minor with himself/herself, with another person or with an animal, realistic depictions of acts with underage minors the observation of which considering the circumstances suggests that they are sexual acts on the underage minor, of the underage minor with himself/herself, with another person or with an animal, and the realistic depictions of (a) sexual acts in the sense of n° 1 or n° 2 with minors of age, or (b) of the genitalia or pubes of minors, if they are luridly distorted, reduced to themselves and detached from other manifestations of life which serve the sexual arousal of the observer. The purely artistically generated depictions that seem to be deceptively real as well as depictions trying to transmit a realistic impression based on manipulated depictions, fulfill the criteria of pornographic depiction.

381 See Section 207a(4)(4) of the Criminal Code.

382 There were in total 195 convictions in 2007, 205 in 2008, and 179 in 2009 involving child pornography related offences in Austria.

383 Article 263(2) of the Criminal Code of Armenia, "Illegal dissemination of pornographic materials or items".

384 Article 3431 of the Criminal Code (introduced into the Criminal Code by Law of the Republic of Belarus of 10 November 2008).

385 In 2009, one person was convicted under Article 3431 of the Criminal Code.

386 Article 159(1) and 159(3) of the Criminal Code (Amend., SG 92/02) (1) (Amend., SG 28/82; SG 10/93; SG 62/97). Nine persons were convicted in 2007, 15 in 2008, 11 in 2009, and eight in the first half of 2010 for crimes specified in article 159.

387 Article 159(5).

388 Section 163.1.

	2003/2004		2004/2005		2005/2006		2006/2007	
Article	**Total**	**Guilty**	**Total**	**Guilty**	**Total**	**Guilty**	**Total**	**Guilty**
163.1	2	1	2	1	1	1	1	1
163.1(1)	0	0	0	0	0	0	1	1
163.1(1)(a)	0	0	0	0	2	2	0	0
163.1(2)	5	3	3	2	4	2	9	8
163.1(2)(a)	4	3	5	4	2	2	2	2
163.1(2)(b)	0	0	0	0	0	0	0	0
163.1(3)	11	9	20	18	17	16	12	11
163.1(3)(a)	2	2	7	5	6	6	5	5
163.1(3)(b)	0	0	2	2	0	0	0	0
163.1(4)	96	65	111	81	141	104	144	114
163.1(4)(a)	17	13	17	11	25	21	29	22
163.1(4)(b)	6	5	7	6	8	8	3	1
163.1(4.1)	1	1	7	6	15	12	15	12
163.1(4.1)(a)	0	0	0	0	0	0	0	0
TOTAL 163.1	**144**	**102**	**181**	**136**	**221**	**174**	**221**	**177**

Table 3. Canada - Section 163.1: Total Cases and Convictions Statistics[389]

Section 163.1 provides for a two-pronged, harm-based "legitimate purpose" defence that is only available for an act that (a) has a legitimate purpose related to the administration of justice, science, medicine, education or art; and (b) does not pose an undue risk of harm to children.

In **Croatia**, the crime of abuse of children and juveniles in pornography[390] is committed by one who uses a child or a juvenile for the purpose of making photographs, audiovisual material or other objects of pornographic nature, or possesses, imports, sells, distributes or presents such material or induces such persons to take part in pornographic shows. The penalty provided for this crime is imprisonment for the term of one to eight years. Due to the increase in distribution of child and juvenile pornography on the Internet, amendments to the Criminal Code were adopted in 2004 to introduce specific provisions in line with the CoE Convention on Cybercrime. Therefore, in the newly introduced Article 197.a, a criminal offence of dissemination of child pornography[391] by means of a computer system or network was established:

> (1) Anyone who, with the help of a computer system or network, makes, offers, distributes, procures for himself or for others, or who in a computer system or in the media for storage of computer data, possesses pornographic content showing children or minors in a sexually explicit activities or focused on their sexual organs, shall be punished by a prison term of one to ten years.
> (2) Anyone who through a computer system, network or media for the storage of computer data makes available to a child photographs, audiovisual content or other items of pornographic content, shall be punished by a prison term of six months to three years.

389 Recent statistics on child pornography offences in Canada can be obtained from the Canadian Centre for Justice Statistics Profile Series, Child and Youth Victims of Police-reported Violent Crime, 2008, by Lucie Ogrodnik, available at <http://www.statcan.gc.ca/pub/85f0033m/85f0033m2010023-eng.pdf>.

390 Article 196 of the Criminal Code.

391 Croatian national laws does not contain the definition of "child pornography", since the definition is transposed from the Optional Protocol to the Convention on the Rights of the Child on the sale of Children, Child Prostitution, and Child Pornography, which Croatia signed on 8 May 2002, and ratified on 15 of May 2002.

(3) Special devices, means, software or data used or adjusted for the commission of the crime referred to in paragraphs 1a and 2 hereof shall be taken away.

In the **Czech Republic**, amendments made to the Criminal Code in 2009 resulted in the criminalization of production and handling of child pornography. Therefore, a person who possesses photographic, film, computer, electronic or other pornographic materials, which display or otherwise use a child, shall be punished with imprisonment of up to two years.[392] Furthermore, any person who produces, imports, exports, transports through, offers, makes publicly available, arranges, puts into circulation, sells or otherwise procures photographic, film, computer, electronic or other pornographic materials, which display or otherwise use a child, or whoever profits from such pornographic materials, shall be punished with imprisonment for six months to three years, a ban of activity or, additionally, with a forfeiture or loss of other assets.[393] The Czech legislation defines child pornography as "pornographic work that displays or otherwise uses a child". This definition includes not only visual art (photographs, drawings, films, sculptures), but also literary or audio materials (fantasy stories, children's voice recordings, etc.).

In **Denmark**, a person who takes or records indecent photographs, or films of a person who is under the age of 18 with the intention to sell or otherwise disseminate the material, shall be liable to a fine or imprisonment for any term not exceeding two years or, in particularly aggravating circumstances, imprisonment for any term not exceeding six years.[394] Furthermore, a person who disseminates indecent photographs or films or other indecent visual reproductions of persons under the age of 18, shall be liable to a fine or imprisonment for any term not exceeding two years, or in particularly aggravating circumstances, imprisonment for any term not exceeding six years.[395] In terms of possession, a person who possesses or in return for payment acquires access to or knowledge of indecent photographs, films or other indecent visual reproductions etc. of persons under the age of 18, shall be liable to a fine or imprisonment for any term not exceeding one year.[396] An exception has been provided by law for the possession offence and this provision does not include possession of indecent pictures of a person who has reached the age of 15, if that person has consented to possession.[397] The Danish legislation on child pornography also covers unreal characters and computer-generated imagery if these are realistic and appear in the same way as or in approximately the same way as photographs.

In **Estonia**, use of minors under the age of 18 in the production or performance of pornographic works is punishable with a pecuniary sanction or with up to five years' imprisonment.[398] Furthermore, the use of minors less than 14 years of age or less than 18 years

---

392 Act No. 40/2009 Coll. Penal Code Article 192(1).

393 Act No. 40/2009 Coll. Penal Code Article 192(2).

394 Section 230 of the Danish Criminal Code. The circumstances that are considered particularly aggravating are especially situations in which the life of a child is endangered, where gross violence is used, where the child suffers serious harm, or where the recording is of a more systematic or organized character. The Danish Ministry of Justice did not have statistical information in relation to convictions under these provisions.

395 Section 235 of the Danish Criminal Code. The circumstances that are considered particularly aggravating are situations in which the life of a child is endangered, where gross violence is used, where the child suffers serious harm, or where the dissemination is of a more systematic or organized character.

396 Section 235(2) of the Danish Criminal Code.

397 Section 235(3) of the Danish Criminal Code.

398 Article 177 of the Criminal Code. Three convictions were registered during the reporting period of 01.01.2007-30.06.2010. Seven convictions were recorded between 2006-2008, according to a report of the Special Rapporteur on trafficking in children, child prostitution and child pornography, Mission to Estonia, A/HRC/12/23/Add.2 10 July 2009.

of age but in need of assistance in the production of erotic materials is punishable by a pecuniary punishment or with up to five years' imprisonment.[399] The production of works involving child pornography or making child pornography available is also criminalized.[400] The UN Special Rapporteur on the sale of children, child prostitution and child pornography recommended that the definition of child pornography provided by the Estonian law amended in accordance with the definition provided in the Optional Protocol on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography as currently the law refers to materials "depicting a person of less than 18 years old in a pornographic situation" or "a person of less than 14 years old in an erotic situation" without further defining "pornographic situation" or "erotic situation".[401]

In **Finland**, the production, distribution, and possession of child pornography[402] are criminalized.[403] A maximum of two years' imprisonment is envisaged for the production and distribution offences, while possession is punished with a maximum of one year's imprisonment.[404] However, the law also provides for an aggravated version of these crimes, especially if the children depicted on the sexually explicit content are particularly young, the content also depicts severe violence or particularly humiliating treatment of the child, the offence is committed in a particularly methodical manner or, the offence has been committed within the framework of a criminal organisation. The offender shall be sentenced to imprisonment between for the term of four months to six years for these aggravated offences.[405]

In **France**, the Penal Code criminalizes recording or transmitting a picture or image of a minor with a view to circulating it, where that image has a pornographic character. These

---

399 Section 1771 of the Criminal Code.

400 Section 178 of the Criminal Code: A person who manufactures, stores, hands over, displays or makes available in any other manner pictures, writings or other works or reproductions of works depicting a person of less than 18 years of age in a pornographic situation, or person of less than 18 years of age in a pornographic or erotic situation, if the act does not have the necessary elements of an offence provided for in § 177 or 177.1 of this Code, also knowingly attending pornographic performances involving the participation of children, in cases where children have been recruited or coerced or influenced in any other manner, shall be punished with a pecuniary punishment or with up to three years' imprisonment. 31 convictions were recorded during the reporting period of 01.01.2007-30.06.2010. 30 convictions were recorded between 2006-2008, according to a report by the Special Rapporteur on the sale of children, child prostitution and child pornography, Mission to Estonia, A/HRC/12/23/Add.2 10 July 2009.

401 See Report of the Special Rapporteur on the sale of children, child prostitution and child pornography, Mission to Estonia, A/HRC/12/23/Add.2 10 July 2009. According to the Special Rapporteur, the consent of a person under 18 years of age to such activities (pornograph**y** or prostitution) is irrelevant. As the age of sexual consent is 14 years of age, the Special Rapporteur recommended that Estonian law clearly stipulate that a child under 18 years of age is unable to consent to any form of sexual exploitation, including child pornography and child prostitution.

402 The current status of whether unreal images can be regarded as child pornography is somewhat unclear. It is clear that for example drawings where a real child has been used as a model can be considered as child pornography. Finland is currently renewing the provisions on child pornography and this question is meant to be clarified in the process.

403 The provisions on distribution of sexually obscene content also cover production of child pornography: See sections 18 and 18a of the Criminal Code. A person under 18 years of age and a person whose age cannot be determined but who can be justifiably assumed to be under 18 years of age is regarded as a child.

404 Section 19 of the Criminal Code: A person who unlawfully has in his or her possession a photograph, video tape, film or other realistic visual recordings depicting a child referred to in section 18, subsection 4 having sexual intercourse or participating in a comparable sexual act or depicting a child in another obviously obscene manner shall be sentenced for possession of sexually obscene pictures depicting children to a fine or imprisonment for the maximum of one year. Between 2007 and 2008, a total of 35 convictions were recorded.

405 Section 18 of the Criminal Code. Between 2007 and 2008, a total of 14 convictions were recorded.

offences are punishable with five years' imprisonment and a fine of 75,000 euros.[406] The same penalties apply to the distribution of such content. The act of regularly accessing an online communications service open for the dissemination of such images or for the possession of such images is punishable with two years' imprisonment and a fine of 30,000 euros.

In **Georgia**, recent amendments to the Criminal Code aimed to bring the national legislation, including provisions criminalizing child pornography, in compliance with the international standards provided by the CoE Convention on Cybercrime.[407] Child Pornography is outlawed by Article 255(2) of the Criminal Code.[408] This section criminalizes intentional obtaining, keeping, offering, distribution, transfer, promotion or otherwise making available pornographic material containing an image of a child.[409] These crimes are punished with a fine or correctional labour for up to two years and/or with imprisonment not exceeding three years. Furthermore, intentional production or sale of pornographic material containing an image of a minor is also criminalized, and punished with a fine or deprivation of liberty ranging from three to five years.[410] For the purposes of Article 255, material containing an image of a child is any kind of visual or audio material produced in any manner, involving a child or his/her image in real, simulated or computer-generated sexual scenes. Displaying a child's genitals for the purpose of satisfying consumer's sexual needs shall be considered as pornographic production. Content created or applied for the medical, scientific, cultural or other legal purposes shall not be considered as pornographic.

In **Germany**, the distribution, acquisition and possession of child pornography[411] is criminalized.[412] Therefore, whoever disseminates, publicly displays, presents, or otherwise makes accessible; or produces, obtains, supplies, stocks, offers, announces, commends, or undertakes to import or export in order to use them or copies made from them or facilitates such use by another pornographic written materials related to sexual activities performed by, or in the presence of, children shall be liable to imprisonment ranging from three months to five years. The penalty shall be imprisonment of six months to ten years if the offender acts on a commercial basis or as a member of a gang whose purpose is the continued commission of such offences and the content (child pornography) reproduced is actual or realistic activity.[413] Moreover, whoever undertakes to obtain possession of child pornography reproducing actual or realistic activity shall be liable to imprisonment for the maximum of two years or a fine. Whosoever possesses written materials[414] containing child pornography shall incur the same penalty.[415] In 2007: 2,190; in 2008: 2,806; and in 2009: 2,433 convictions were registered for the crimes of distribution, acquisition and possession of child pornography in Germany.[416]

---

406 Article 227-23 of the Penal Code (Penalties for producing, recording, transmitting, or possessing images of minors of a pornographic character). The provisions of this article also apply to pornographic images of a person whose physical appearance is that of a minor, unless it is proved that the person was over eighteen years of age on the date the picture was taken or recorded.

407 On 24 September 2010, amendments to the Criminal Code of Georgia entered into force. The ratification process of the Convention is currently ongoing.

408 Illicit Production or Sale of Pornographic Material or other Object.

409 A child is defined as a person under the age of 18.

410 Article 255(3) of the Criminal Code.

411 A "child" is a person under fourteen years of age: Section 176(1) German Criminal Code.

412 Section 184b(1) of the German Criminal Code. Note further section 184c on the distribution, acquisition and possession of juvenile pornography.

413 Section 184b(3) of the German Criminal Code.

414 Audiovisual media, data storage media, illustrations and other depictions shall be equivalent to written material in the provisions which refer to this subsection.

415 Section 184b(4) of the German Criminal Code.

416 Section 184b of the German Criminal Code. Statistisches Bundesamt (Federal Statistics Office) (ed.),

In **Ireland**, the Child Trafficking and Pornography Act 1998 as amended by the Criminal Law (Sexual Offences) (Amendment) Act 2007, and the Criminal Law (Human Trafficking) Act 2008 deals specifically with the matter of child pornography. The 1998 Act defines child pornography[417] as

> (a) any visual representation -
> (i) that shows or, in the case of a document, relates to a person who is or is depicted as being a child and who is engaged in or is depicted as being engaged in explicit sexual activity,
> (ii) that shows or, in the case of a document, relates to a person who is or is depicted as being a child and who is or is depicted as witnessing any such activity by any person or persons, or
> (iii) whose dominant characteristic is the depiction, for a sexual purpose, of the genital or anal region of a child,
> (b) any audio representation of a person who is or is represented as being a child and who is engaged in or is represented as being engaged in explicit sexual activity,
> (c) any visual or audio representation that advocates, encourages or counsels any sexual activity with children which is an offence under any enactment, or
> (d) any visual representation or description of, or information relating to, a child that indicates or implies that the child is available to be used for the purpose of sexual exploitation within the meaning of section 3, irrespective of how or through what medium the representation, description or information has been produced, transmitted or conveyed and, without prejudice to the generality of the foregoing, includes any representation, description or information produced by or from computer-graphics or by any other electronic or mechanical means but does not include-
> (I) any book or periodical publication which has been examined by the Censorship of Publications Board and in respect of which a prohibition order under the Censorship of Publications Acts, 1929 to 1967, is not for the time being in force,
> (II) any film in respect of which a general certificate or a limited certificate under the Censorship of Films Acts, 1923 to 1992, is in force, or
> (III) any video work in respect of which a supply certificate under the Video Recordings Acts, 1989 and 1992, is in force...

Section 2 of the Child Trafficking and Pornography Act 1998 provides that the definition of child pornography shall include reference to a figure resembling a person that has been generated or modified by computer-graphics or otherwise, and in such a case, if it is a fact, that some of the principal characteristics shown are those of an adult shall be disregarded if the predominant impression conveyed is that the figure shown is a child. Section 4 of the 1998 Act criminalizes any person who, having the custody, charge or care of a child, allows the child to be used for the production of child pornography, and liability is provided on conviction on indictment to a fine not exceeding £25,000 or to imprisonment for a term not exceeding 14 years or both. Section 5 criminalizes anyone who knowingly produces, distributes,[418] prints or publishes any child pornography, knowingly imports, exports, sells or shows any child pornography, knowingly publishes or distributes any advertisement likely to be understood as conveying that the advertiser or any other person produces, distributes, prints, publishes, imports, exports, sells or shows any child pornography, encourages or knowingly causes or facilitates any activity mentioned above, or knowingly possesses any

---

special publication series (Fachserie) 10 "Administration of Justice", series 3 "Prosecution of Offences" (Conviction statistics), table 2.1. Crimes committed in connection with the Internet (cybercrimes) are not collected separately.

417 Section 2(1), Child Trafficking and Pornography Act 1998.

418 In this section "distributes", in relation to child pornography, includes parting with possession of it to, or exposing or offering it for acquisition by, another person, and the reference to "distributing" in that context shall be construed accordingly.

child pornography for the purpose of distributing, publishing, exporting, selling or showing it. Anyone guilty of these offences shall be liable on summary conviction to a fine not exceeding €1.500 or to imprisonment for a term not exceeding 12 months or both, or on conviction on indictment to a fine or to imprisonment for a term not exceeding 14 years or both. Furthermore, any person who knowingly possesses child pornography shall be guilty of an offence, and shall be liable on summary conviction to a fine not exceeding £1,500 or to imprisonment for a term not exceeding 12 months or both, or on conviction on indictment to a fine not exceeding £5,000 or to imprisonment for a term not exceeding five years or both.[419]

Child pornography offences (Ireland)	2006	2007	2008
Recorded Offences (Number)	39	81	46
Detected Offences (Number)	26	45	26
Recorded Offences with Relevant Proceedings (Number)	19	27	13
Recorded Offences with Court Proceedings Commenced (Number)	15	22	6
Recorded Offences with Convictions (Number)	8	14	0
Court Outcome: Pending incl. appeals allowed (Number)	5	8	6
Court Outcome: Non Conviction (Number)	2	0	0

Table 4. Child pornography offences (Ireland) statistics

In **Italy**, child pornography is considered illegal along with any other activity aimed at creating, distributing, and trading it through any means, including the Internet. The maximum punishment envisaged for such crimes is 14 years.[420] Virtual images are also defined and criminalized as child pornography under the Italian Criminal Code.[421]

Year	Investigated persons subject to measures limiting personal freedom	Persons reported but not arrested
98/00	43	399
2001	25	210
2002	29	552
2003	9	712
2004	21	769
2005	21	471
2006	18	370
2007	33	352

419 Section 6, Child Trafficking and Pornography Act 1998. Sections 5 and 6 concern the production, distribution and possession of child pornography shall not apply to a person who possesses child pornography in the exercise of functions under the Censorship of Films Acts, 1923 to 1992, the Censorship of Publications Acts, 1929 to 1967, or the Video Recordings Acts, 1989 and 1992, or for the purpose of the prevention, investigation or prosecution of offences under this Act. Without prejudice to subsection (2), it shall be a defence in a prosecution for an offence under section 5 (1) or subsection (1) for the accused to prove that he or she possessed the child pornography concerned for the purposes of bona fide research.

420 See generally Act 269/98 and Act 38/2006. Note also that in the Criminal Code sections 600bis (Juvenile prostitution), 600ter (Juvenile pornography), 600quater (possession of pornographic material), 600quinquies (Tourism initiatives aimed at juvenile prostitution exploitation), and 600septies (Aggravating and mitigating circumstances) - as introduced in sections 2, 3, 4, 5, 6 and 7 of Act 269/98 - provide for the crimes of minor's sexual exploitation through the Internet.

421 Section 600quater is supplemented by subsection 1 envisaging virtual pedophilia as illegal and establishes its exact definition (section 4 of Act 38/2006): section 600quater.1. (virtual pornography). The provisions under sections 600ter and 600quater shall also apply when pornographic material consists in virtual images realized by using images of minors under 18 years of age or parts thereof. In this case punishment shall be decreased by a third. Virtual images are to be intended as images realized with graphic processing techniques that are not fully or partly linked to real-life situations, whose quality of definition makes non-real situations appear as real.

2008	39	1167
2009	53	1185
2010 (as of 15 September)	104	482
Total	395	6669

Table 5. Statistics on the activities of the Italian Postal and Communications Police Service

In **Kazakhstan**, under Article 273-1 of the Criminal Code,[422] the distribution of child pornography entails criminal liability even though there is no special definition of child pornography provided by law. Subject to this criminal provision, the manufacture, storage or movement of materials or objects with pornographic images of minors across the State border of the Republic of Kazakhstan for the purposes of distribution, public demonstration or advertisement shall be punished by imprisonment for the period of three to six years, including confiscation of pornographic materials or objects, as well as facilities for their manufacture and reproduction. Furthermore, the involvement of minors in pornographic entertainment as performers by persons who had reached the age of eighteen shall be punished by imprisonment for the period of five to seven years including confiscation of pornographic materials or objects, as well as facilities for their manufacture and reproduction.[423] However, the possession of child pornography is not criminalized in Kazakhstan.[424]

In **Latvia**, a person who commits procurement or utilization of minors for the production (manufacturing) of pornographic or erotic materials is sanctioned with imprisonment for a term not exceeding six years. Furthermore, for a person who commits procurement or utilization of juveniles (under the age of 14 years) for the production (manufacturing) of pornographic or erotic materials, the applicable sentence is imprisonment for a term between five and twelve years.[425] Downloading, acquisition, importation, production, public demonstration, advertising or other distribution of such pornographic or erotic content that relates to or portrays the sexual abuse of children,[426] bestiality, necrophilia or violence of a

422 Manufacture and realization of materials or objects containing pornographic images of minors or their involvement in pornographic entertainments.

423 Note also Article 115 of the Code of the Republic of Kazakhstan on Administrative Offences entitled "Involvement of minors in the production of articles with erotic content" which can result in an administrative fine of fifty monthly calculation indices, with confiscation of the said products of erotic content.

424 The ratification of the CoE Cybercrime Convention has been considered, as well as the decision to bring the norms of the legislation of Kazakhstan in line with the norms of the Convention. Thus, the Criminal Code of the Republic of Kazakhstan was supplemented with Article 273-1 in 2010. "Production and turnover of materials or objects with pornographic images of minors or their involvement in entertainments of a pornographic nature".

425 Article 166(3) of the Criminal Law on Violation of Provisions Regarding Importation, Production and Distribution of Pornographic or Erotic Materials. According to the data in the Court Information System, a total of 11 persons have been convicted under Article 166 of the Criminal Law during the period from 1 January 2007 until 30 June 2010.

426 The definition of child pornography is provided in Article 1.2 of the Law on Pornography Restriction, and it is stated that child pornography is a material of a pornographic nature, in which a child is depicted or described, or any other material which: a) depicts or describes a child who is involved in sexual activities, a child completely or partially without clothing in a sexual pose or in clothing of an obscene nature; children's genitals or pubic region are depicted in a stimulating way, b) depicts or describes, or presents a person having the appearance of a child who is involved in the activities specified in sub-paragraph 'a' of this Article in a manner specified in sub-paragraph 'a' c) contains realistic images with an actually non-existent child who is involved in the activities specified in sub-paragraph 'a' of this Article or presented in a manner specified in sub-paragraph 'a'.

pornographic nature, or keeping of such materials is also criminalized, and subject to deprivation of liberty for a term up to three years.[427]

In **Lithuania**, the Criminal Code criminalizes child pornography.[428] Article 162 establishes that a person who involves a child in pornographic events or uses a child for the production of pornographic material or gains profit from such activities of the child shall be punished by a fine or by arrest or by imprisonment for a term of up to five years. Article 309(1) states that a person who, for the purpose of distribution, produces or acquires pornographic material or distributes such material shall be punished by community service or by a fine or by restriction of liberty or by imprisonment for a term of up to one year. Article 309(2) states that a person who produces, acquires, stores, demonstrates, advertises or distributes pornographic material displaying a child or presenting a person as a child shall be punished by a fine or by imprisonment for a term of up to two years. Article 309(3) states that a person who, for the purpose of distribution, produces or acquires or distributes a large quantity of pornographic material displaying a young child shall be punished by imprisonment for a term of up to five years.[429]

In **the former Yugoslav Republic of Macedonia**, the use of minors in pornographic content is punished with imprisonment of at least eight years.[430] Furthermore, anyone who produces child pornography with the intention to distribute it, distributes it, transmits or offers or in any other way makes accessible child pornography through computer systems, shall be punished with imprisonment of at least five years.[431] The Criminal Code also stipulates that anyone who procures child pornography for himself or for another one, or possesses child pornography shall be punished with imprisonment for the period between five and eight years.[432] If these offences are committed via a computer system or other means for public communication, the perpetrator shall be punished with imprisonment of at least eight years.[433] In **Moldova**, the Criminal Code criminalizes the producing, handing out, distributing, importing, exporting, providing, selling, exchanging, using or possessing photographs or other images of a child or several children involved in overt sexual activities, real or simulated, or photographs or other images of the sex organs of a child presented in a lewd or obscene manner, including in electronic format. These crimes are punishable by deprivation of liberty for a period of one to three years. A legal entity involved in such crimes is sanctioned with a fine in an amount of 2,000 to 4,000 conventional units with deprivation of the right to engage in certain

427 Article 166(2) of the Criminal Law.

428 See articles 157, 162, and 309. In 2007, there were 18 crimes registered under Article 157; in 2008 this number decreased to two crimes. In 2007, there were six crimes registered under Article 162; in 2008 this number decreased to two crimes. In 2007, there were five crimes registered under Article 309(2); one case was referred to the court; and in 2008 there were 25 crimes under Article 309(2), six cases were referred to the court.

429 It should be noted that in Lithuania, the Law on Fundamentals of Protection of the Rights of Child has a provision, stating that administrative or criminal liability, in accordance with the laws, shall be applied in cases of encouraging or coercing a child to take part in sexual activity, using him for prostitution or involving him in prostitution, using him for pornography, as well as in production or dissemination of pornographic publications, or other materials of a pornographic or erotic nature.

430 Article 193 of the Criminal Code. Note also Article 193-b (Luring a minor younger than 14 years into sex or other sexual activity): "Anyone who via computer-communication means by scheduling a date or in any other way lures minor younger than 14 into sex or other sexual activities or for production of children pornography or if with such an intention the offender meets the minor, shall be punished by imprisonment between one and five years."

431 Article 193-a(1) (Production and Distribution of Child Pornography via Computer System) of the Criminal Code.

432 Article 193-a(2) of the Criminal Code.

433 Article 193-a(3) of the Criminal Code.

activities.[434] In **Montenegro**, the Criminal Code provides for the offence of production,[435] procurement,[436] and possession of child pornography. A partial defence for possession is provided for when the senior juvenile depicted in content involving child pornography has given his/her consent thereof, and if the person who has the content keeps them exclusively for his/her own use.[437]

The **Netherlands** has criminal law provisions on child pornography. Amendments were made to the Criminal Code in 2002, and Article 240b[438] of the Criminal Code was introduced which criminalized virtual child pornography. This legislative change was necessitated by the circumstance that modern technology makes it possible to produce true to life child pornographic visual material without directly involving real children. The amendments made also increased the age limit to which the ban applies from 16 to 18. Finally, the possession offence was clarified with these amendments. Further changes to the Dutch law were made subsequent to the ratification of the CoE Convention on the protection of children against sexual exploitation and sexual abuse (Lanzarote Convention). The implementation of the Convention[439] has led to a tightening of the Dutch criminal law provisions on the protection of children against sexual abuse. The child pornography provisions were further tightened with the criminalisation of obtaining access, through information and communication technologies, to child pornography.[440]

In **Norway**, the Criminal Code prohibits producing, possessing and all other forms of dealing with such materials.[441] The provision applies to offences committed on the Internet. The penalty for violation is a fine or up to three years' imprisonment. The maximum penalty for a negligent breach of section 204a of the Criminal Code is imprisonment for a term not exceeding six months. The offender may also be liable to pay damages.

---

434 Article 2081 (Child pornography) of the Criminal Code.

435 Article 211(2) of the Criminal Code: Anyone who uses a minor to produce pictures, audio-visual or other objects of pornographic content or for a pornographic show, shall be punished by an imprisonment sentence for a term of six months to five years.

436 Article 211(3) of the Criminal Code: Anyone who procures, sells, shows, attends the displaying of, publicly exhibits or in electronic or some other manner makes available pictures, audio-visual or other objects of pornographic content resulting from the commission of acts referred to in paragraph 2 of this Article, or who owns such objects, shall be punished by an imprisonment sentence not exceeding two years.

437 Article 211(6) of the Criminal Code.

438 Article 240b of the Dutch Penal Code currently reads as follows: 1. The person who distributes, offers, openly displays, produces, imports, forwards, exports, acquires, has in his possession or gains access by means of an automated work or by making use of a communication service, an image – or a data carrier containing an image – of a sexual act, in which someone who evidently has not reached the age of eighteen is involved or appears to be involved, will be punished with a term of imprisonment of maximum of four years or a fine of the fifth category (EUR 76.000). 2. Those who make a profession or habit of the commission of one of the criminal offences described in the first paragraph, will be punished with a term of imprisonment of at most eight years or a fine of the fifth category.

439 Dutch law changed as from 1 January 2010.

440 Technological developments have made it possible to gain access via IT-technology to remote files containing child pornography, encrypted or otherwise protected. It is therefore possible to have this material at one's disposal and to view the material if so desired, without storing the material on one's own computer. The criminalisation of obtaining access offers a wider scope and forms a useful and desirable safety net concerning those cases that might not fall under the criminal offence of 'possession'. It is irrelevant whether the child pornography was in the possession of the person concerned. Prosecution may be successful in case a person frequently logs in to a website with illegal content or uses his credit card to pay for using a particular website.

441 Section 204a of the Norwegian Penal Code 1902.

In **Poland**, whoever produces, records or imports to disseminate, keeps or holds or distributes or publicly presents pornographic content in which a minor participates, shall be subject to the penalty of the depravation of liberty for a term between six months and eight years.[442] It follows that whoever records pornographic content in which a minor under 15 years of age participates, shall be subject to the penalty of the deprivation of liberty for a term of between one to 10 years.[443] Whoever imports, keeps or holds such content shall be subject to the penalty of the deprivation of liberty for a term of between three months to five years.[444] Whoever produces, distributes, presents, stores or holds pornographic content presenting any produced or reproduced image of a minor participating in a sexual act shall be subject to the penalty of a fine, restriction of liberty or the deprivation of liberty of up to two years.[445]

Convicted persons (1st instance court)	2007	2008	2009	30 June 2010
Art. 202	114	254	269	135

Table 6. Convictions under the Polish law for the reporting period of 1 January 2007 – 30 June 2010

In **Romania**, child pornography is regulated by two special laws. Child pornography in general is regulated by Law 678/2001 on prevention and combating of trafficking in persons. At the same time child pornography committed through computer systems is regulated by Law 161/2003.[446] Under Article 18 of Law 678/2001, the deed of exposing, selling or spreading, renting, distributing, manufacturing or producing in any other way, of transmitting, offering, supplying or holding in view of spreading of objects, films, pictures, slides, emblems or other visual content that represent sexual positions or acts of a pornographic nature presenting or involving minors under the age of 18, shall be the offence of infantile pornography and shall be punished with imprisonment for the term of three to ten years. Furthermore, subject to Article 51 of Law 161/2003, producing for the purpose of distribution, offering or making available, distributing or transmitting, procuring for oneself or another of any child pornography material, or illegal possession of child pornography materials within a computer system or computer data storing device is considered a criminal offence and is punished with imprisonment for the period of three to 12 years.

In the **Russian Federation**, there are no specific legal provisions criminalizing child pornography on the Internet. Liability is envisaged for making and circulating materials or items with pornographic images of minors, without singling out the Internet as a specific medium of crime. For example, Article 242.1 of the Criminal Code envisages liability for the distribution of child pornography, and the making, keeping or moving across the state border of the Russian Federation for the purpose of dissemination, public showing or advertising, or dissemination, public showing or advertising, of materials or articles with pornographic images of known minors, as well as drawing known minors as performers to entertainment events of pornographic nature by a person who has reached the age of 18 years. These offences are punishable by deprivation of liberty for a term of two to eight years with restraint of liberty for a term of up to one year, or without it.[447] According to Article 242 of the

442 Article 202(3) of the Penal Code.
443 Article 202(4) of the Penal Code.
444 Article 202(4a) of the Penal Code.
445 Article 202(4b) of the Penal Code.
446 Other relevant provisions with regard to the sexual exploitation of minors, including for pornographic purposes are to be found in the Criminal Code and Law 196/2003.
447 The same deeds committed by a parent or other person who is obligated under the law to bring up the minor, as well as by a pedagogue or other employee working for an educational, pedagogical, medical or other institution who is obligated to exercise supervision over the minor; committed against a person

Criminal Code, unreal characters (drawings, paintings, cartoons, artificially created images etc.) may be recognized as pornographic material, the distribution of which is criminally punishable. At present, the necessary measures are being taken to prepare the Russian Federation for performing the obligations of becoming a party to the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, and the CoE Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse.

In **Serbia**, whoever uses a child to produce photographs, audio-visual or other items of pornographic content or for a pornographic show, shall be punished with imprisonment from six months to five years.[448] In **Slovenia**, whoever abuses a minor in order to produce pictures or audiovisual or other items of a pornographic or other sexual nature, or uses them in a pornographic or other sexual performance or is knowingly present at such performance, [449] or produces, distributes, sells, imports or exports pornographic or other sexual material depicting minors or their realistic images, supplies it in any other way, or possesses such materials, or discloses the identity of a minor in such materials[450] shall be given a prison sentence of between six months and five years. In **Sweden**, according to a recent amendment that came into force in January 2011, it is no longer relevant for criminal liability whether the age of the person depicted is apparent from the picture and its attendant circumstances. If the actual age is known to the portrayer this person can be held liable under Section 10 A of the Swedish Penal Code.[451] This provision criminalizes depicting children in a pornographic picture, distributing, transferring, showing, putting such a picture of a child at another person's disposal or in another way making such a picture available for another person, acquiring or offering such a picture of a child for sale, procuring contacts between buyers and sellers of such picture of children or taking another similar measure with the view to promoting trafficking in such pictures, or having such a picture of children in possession[452] is convicted of the crime of child pornography and sentenced to imprisonment for not more than two years or, if it is a petty crime, is fined or sentenced to imprisonment for no more than six months.[453]

In **Turkey**, the Penal Code criminalizes child pornography. A person who uses children in the production of obscene writings or audio-visual materials shall be sentenced to a penalty of

---

known to be under 14 years old; by a group of persons in a preliminary conspiracy or by an organized group, or with deriving a large income shall be punishable by deprivation of liberty for a term of three to ten years along with deprivation of the right to hold specified offices or engage in specified activities for a term of up to fifteen years, or without it, and with restraint of liberty for a period of up to two years, or without it.

448 Article 185 of the Criminal Code. Terms such as "unreal characters" or "computer-generated imagery" are not included specifically in the legal definition of child pornography.

449 Article 176(2) (Presentation, Production, Possession and Distribution of Pornographic Material) of the Criminal Code (Official Gazette Republic of Slovenia No 55/2008).

450 Article 176(3) of the Criminal Code.

451 The number of persons found guilty of child pornography crimes were in 2007: 74, in 2008: 78, in 2009: 84.

452 The prohibitions of depiction and possession do not concern the person who draws, paints or in another similar craftsman like way makes such a picture referred to in the first paragraph, if the picture is not meant to be distributed, transferred, shown or in another way put at other persons disposal. Also in another cases an act shall not constitute a crime if special circumstances make the act obviously justified.

453 If a person has committed a crime, that is considered to be serious, he shall be convicted of a serious child pornography crime and sentenced to imprisonment for a minimum of six months and not more than four years. When judging whether a crime is serious it is to be especially taken into consideration if it has been committed professionally or for the purpose of making profits, has formed part of criminal activities that have been carried on methodically or to a great extent, has concerned an especially large number of pictures or has concerned pictures where children are subjected to especially ruthless treatment.

imprisonment for a term of five to ten years and a judicial fine of up to five thousand days. Any person who brings such materials into the country, who copies or offers for sale such materials, or who sells, transports, stores, exports, retains possession of such materials, or offers such materials for the use of others shall be sentenced to a penalty of imprisonment for a term of two to five years and a judicial fine of up to five thousand days.[454]

In **Ukraine**, the use of juveniles in activities concerned with producing and circulating of sexual or erotic products, pornographic materials; the distribution of sexual, erotic, or pornographic materials, use of images of children in any form in the products of sexual or erotic nature, manufacturing (production), storage, advertising, distribution, purchase of products containing child pornography, importing, exporting and transit through Ukraine of such content, are prohibited.[455] In the **United Kingdom**, the Protection of Children Act 1978, prohibits the taking, making, distribution, showing and possession with a view to distribution of any indecent photograph or pseudo-photograph[456] of a child under the age of 18, and such offences carry a maximum sentence of ten years' imprisonment. Section 160 of the Criminal Justice Act 1988 also makes the simple possession of indecent photographs or pseudo-photographs of children an offence and carries a maximum sentence of five years' imprisonment. The Criminal Justice and Immigration Act 2008 extended the meaning of a photograph to include derivatives of photographs such as tracings (made by hand or electronically) and data stored on computer disc or by other electronic means.[457] Furthermore, under Section 62 of the Coroners and Justice Act 2009 (which extends to England, Wales and Northern Ireland), it is an offence to possess prohibited images of children.[458] The offence excludes certain images and is subject to certain defences. This includes non-photographic visual depictions of child sexual abuse, including computer-generated images of child abuse which are regulated by the above mentioned provisions.[459] The offence carries a three year maximum prison sentence.

---

454 Article 226(3) of the Turkish Penal Code. Furthermore, subject to Article 226(5), any person who broadcasts or publishes the materials described in sections three and four, or who acts as an intermediary for this purpose or who ensures that children see, hear or read such materials shall be sentenced to a penalty of imprisonment for a term of six to ten years and a judicial fine of up to five thousand days.

455 Article 7 of the Law of Ukraine "On protection of public morals". Note further Article 301 of the Criminal Code of Ukraine which states that forcing minors to participate in the creation of work, image or film and video production, pornographic computer software is punishable with imprisonment from three to seven years.

456 A pseudo-photograph is an image, whether made by computer-graphics or otherwise which appears to be a photograph.

457 Section 69 of the Criminal Justice and Immigration Act 2008.

458 Section 62 (Possession of prohibited images of children) subsections (2) to (8) set out the definition of a "prohibited image of a child". Under subsection (2), in order to be a prohibited image, an image must be pornographic, fall within subsection (6) and be grossly offensive, disgusting or otherwise of an obscene character. The definition of "pornographic" is set out in subsection (3). An image must be of such a nature that it must reasonably be assumed to have been produced solely or mainly for the purpose of sexual arousal. Whether this threshold has been met will be an issue for a jury to determine. Subsection (4) makes it clear that where (as found in a person's possession) an individual image forms part of a series of images, the question of whether it is pornographic must be determined by reference both to the image itself and the context in which it appears in the series of images. Subsection (6) and (7) provide that a prohibited image for the purposes of the offence is one which focuses solely or principally on a child's genitals or anal region or portrays any of a list of acts set out in subsection (7).

459 There are also a number of offences which relate to involving children in pornography (defined as the recording of an indecent image) through causing or inciting their involvement, controlling involvement and arranging or facilitating child pornography: see ss. 47 to 50 of the Sexual Offences Act 2003, which extend to England and Wales and Northern Ireland.

Statute	2007	2008	2009
Protection of Children Act 1978 S.1 as amended by Criminal Justice & Public Order Act 1994 S.84	782	958	1,024
Criminal Justice Act 1988 S.160 as amended by the Criminal Justice & Court Services Act 2000	185	229	222
TOTAL	967	1,187	1,246

Table 7. Conviction statistics in relation to child pornography related offences in England and Wales

As can be seen from the above statistics, a total of 3400 convictions were registered for child pornography related crimes between 2007 and 2009 in England and Wales.

Legal provisions outlawing obscene and sexually explicit (pornographic) content

Legislation on obscene publications and sexually explicit content exists in many states. However, approaches differ, and definitional variations do exist. The OSCE participating States were asked whether **there are specific legal provisions outlawing obscene and sexually explicit (pornographic) content** in their countries **(Question 8)**.[460] 41 (73.2%) of the OSCE participating States stated that they have such laws in place. In only five (8.9%) countries (Bosnia and Herzegovina, Croatia,[461] Hungary, Liechtenstein, and Moldova) no such provisions exist. No data was obtained from 10 (17.9%) of the participating States.

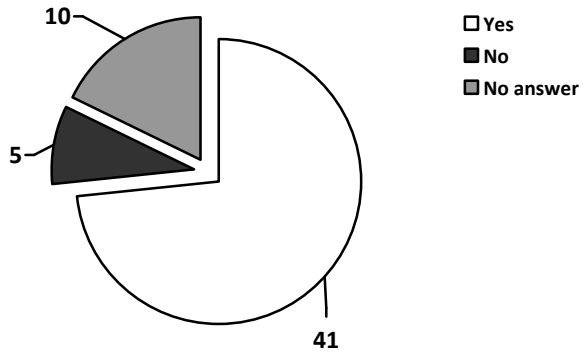


Figure 32. OSCE participating States' responses with regards to specific legal provisions outlawing obscene and sexually explicit (pornographic) (Question 8)

In terms of the responses received most legal provisions outlaw making available or showing obscene and sexually explicit (pornographic) content to children.[462] In some States, the

460 The participating States of the OSCE were also asked how these offences are defined by law, which sanctions (criminal, administrative, civil) are envisaged by law, what is the maximum prison term envisaged by law for such offences. They were also requested to provide any statistical information about convictions under these provisions for the reporting period between 1 January 2007 and 30 June 2010, and whether the law (or relevant regulations) prescribes blocking access to websites or any other types of Internet content as a sanction for these offences.

461 Obscene and sexually explicit (pornographic) content, except for content constituting child pornography, is not sanctioned by law in Croatia.

462 For example this is the case in Albania and in Germany (Section 184 German Criminal Code: 333 convictions in 2007, 264 in 2008, and 214 in 2009). In Lithuania, Article 4(3) of the Law on the Protection of Minors against the Detrimental Effect of Public Information states that except for the cases provided for in Article 7 of this Law, making available to the public or dissemination of public information that may be detrimental to physical, intellectual or moral development of minors, especially the portrayal of pornography and/or gratuitous violence shall be prohibited. Note also Article 186 of the Spanish Criminal

production, manufacture, dissemination, storing for the purpose of distribution or advertisement of pornographic materials or items are criminalized per se.[463] Sanctions vary from administrative fines[464] to criminal sanctions. Possession of such content is generally not criminalized.

For example, in **Austria**, the Pornography Act (Pornographiegesetz) contains provisions on criminal acts, and on the procedure concerning pornographic content.[465] The criminal act is to be punished with a prison sentence of up to one year. In addition to the prison term, a fine of up to 360 daily rates is also a possible sanction.[466]

In **Denmark**, according to Section 234 of the Criminal Code a person who sells indecent pictures or objects to a person under the age of 16 shall be liable to a fine. In **France** since 1994, gross indecency is criminalized only if the pornographic content reaches minors.[467] In **the former Yugoslav Republic of Macedonia**, a person who sells, shows or by public presentation in some other way makes available pictures, audio-visual or other objects with a pornographic content to a minor younger than 14 years of age, or shows him a pornographic performance, shall be punished with imprisonment between six months and three years.[468]

Code, and Article 226 of the Turkish Penal Code with regards to the provision of sexually explicit content to children.

463 For example see Article 263 of the Armenian Criminal Code, Article 242 of the Criminal Code of Azerbaijan, and Article 343 of the Criminal Code (introduced into the Criminal Code by Law of the Republic of Belarus on 10 November 2008). During the period from 2007 through 2009, 176 people were convicted under this article of the Criminal Code in the Republic of Belarus. Note also Article 159 of the Bulgarian Penal Code, Article 255(1) (Illicit Production or Sale of a Pornographic Piece or Other Object) of the Georgian Criminal Code. The maximum term of imprisonment for acts envisaged by Article 255(1) is two years. In Kazakhstan, Article 273 (Illegal Distribution of Pornographic Materials or Objects) of the Criminal Code states that illegal manufacture for the purposes of distribution or advertisement, or distribution and advertisement of pornographic materials or objects, as well as illegal trade in publications, cinema or video materials, pictures, or other objects of pornographic nature, shall be punishable by a fine in the amount from 500 to 1,000 monthly calculation indices, or in the amount of the salary or other income of the convicted person for a period of five months to one year, or by correctional work for up to two years, or by deprivation of liberty for a term of up to two years with confiscation of the pornographic materials or objects, as well as the means of their production or reproduction. Note also Article 262 of the Criminal Code of the Kyrgyz Republic, and Article 164 (The Production or Dissemination of Pornographic Items) of the Criminal Code of Turkmenistan

464 Article 1732(1) of the Latvian Administrative Violations Code provides for administrative liability in the case of violation of the requirements regarding the importation, manufacture, distribution, public demonstration or advertising of erotic and pornographic materials (essays, magazines, images, computer programs, films, video recordings and audio recordings, television and radio broadcasts). The sanctions involve issuing a warning or imposing a fine with or without a confiscation of these materials.

465 According to section 1(1) of the Pornography Act a person commits a criminal act if he/she with the intention of acquiring profit a) produces, publishes or, for the purpose of distribution, stocks lewd writings, depictions, films or other lewd objects, b) imports, transports or exports such objects, c) offers or allocates such objects to others, publicly exhibits, puts up, posts or otherwise distributes them or shows such films to others, d) in public or in front of several persons or in print media or distributed writings offers himself/herself for one of the actions mentioned in lit. a) to c); e) by ways mentioned in lit. d) informs how, by whom or through whom lewd objects can be acquired, rented or where such objects can be viewed.

466 Section 1(2) of the Pornography Act. In 2007 three persons were convicted under the Pornography Act, and in 2008 four people were convicted. There were no convictions in 2009.

467 Article 227-24 of the Penal Code states that "The manufacture, transport, distribution by whatever means and however supported, of a message bearing a pornographic or violent character or a character seriously violating human dignity is punishable by three years' imprisonment and a fine of €75,000 (€375,000 for corporations) where the message may be seen or perceived by a minor.

468 According to article 193 of the Criminal Code (showing pornographic materials to a minor), if the crime is performed through the public media, the offender shall be punished with a fine, or with imprisonment between three and five years.

In certain States, such as **Canada,** the Criminal Code does not prohibit sexually explicit content that does not qualify as obscene or as child pornography. Obscene materials are defined as any publication whose dominant characteristic is the undue exploitation of sex or of sex and violence, crime, horror, or cruelty.[469] In the **Czech Republic** not all kinds of pornographic content are regarded criminal.[470] Similarly, in **Liechtenstein** obscenity in general is not outlawed unless the content involves child pornography, sexual acts with animals, sexual acts showing violence or human excrements.[471] In **Finland**, unlawful marketing of obscene material is criminalized under Criminal Code.[472] In **Germany**, the distribution of pornography depicting violence or sodomy is criminalized under section 184a of the Criminal Code.[473] There were a total of 97 convictions under this particular provision between 2007 and 2009 in Germany.[474]

In **Ireland**, Section 18 of the Censorship of Publications Act of 1929 prohibits the sale or the keeping for sale of indecent pictures. Section 42 of the Customs Consolidation Act of 1876 gives the customs authorities power to seize any obscene or indecent articles being imported into the country. In **Italy**, the Penal Code criminalizes the publication of obscene content including writings, drawings, images, or other obscene objects of any type.[475] The "public" distribution of pornographic images on the Internet, including the websites that do not deal with obscene material, can be considered as legal provided that minors under eighteen years of age are not the subject, and when it does not take place in an indiscriminate way, and without prior notice.[476]

In **Kazakhstan**, the manufacture, possession, import, and transportation in the territory of the Republic of Kazakhstan of media products containing pornography is punishable by fining

---

469 Section 163 of the Criminal Code prohibits making, publishing, distributing, circulating or possessing for the purpose of publication, distribution or circulation, obscene materials.

470 Article 191 (Dissemination of Pornography) of the Czech Republic Penal Code states that any person who produces, imports, exports, transports, offers, makes publicly available, arranges, puts into circulation, sells or otherwise procures photographic, film, computer, electronic or other pornographic work that reflects the violence and disrespect for a man, or that describes or depicts or displays of sexual intercourse with an animal shall be punished with imprisonment for up to one year, a ban on activity or with forfeiture of the property or other asset.

471 Section 218a of the Criminal Code.

472 Section 20 (Unlawful marketing of obscene material) of the Criminal Code: A person who, for gain, markets an obscene picture, visual recording or object which is conducive to causing public offence, by (1) giving it to a person under 15 years of age, (2) putting it on public display, (3) delivering it unsolicited to another, or (4) openly offering it for sale or presenting it by advertisement, brochure or poster or by other means causing public offence, shall be sentenced for unlawful marketing of obscene material to a fine or to imprisonment for at most six months. The provision on distribution of sexually obscene pictures (Section 18, Criminal Code) also covers the distribution and production of sexually obscene pictures or visual recordings depicting violence or bestiality.

473 Whosoever 1. disseminates; 2. publicly displays, presents, or otherwise makes accessible; or 3. produces, obtains, supplies, stocks, offers, announces, commends, or undertakes to import or export, in order to use them or copies made from them within the meaning of Nos 1 or 2 above or facilitates such use by another, pornographic written materials (section 11 (3)) that have as their object acts of violence or sexual acts of persons with animals shall be liable to imprisonment of not more than three years or a fine.

474 34 convictions in 2007, 36 in 2008, and 25 in 2009. Statistisches Bundesamt (Federal Statistics Office) (ed.), special publication series (Fachserie) 10 "Administration of Justice", series 3 "Prosecution of Offences" (Conviction statistics), table 2.1.

475 Section 528 of the Criminal Code (Publications and obscene spectacles).

476 Pornographic images shall be destined to adults only and only after their conscious and voluntary access to the relevant site. Pornographic images shall be offered on sites that are clearly identifiable by third persons as sites that distribute this kind of products, without offering in anticipation manifestly obscene or pornographic images.

individuals in the amount of up to 20, officials and individual businessmen in the amount of up to 25, legal entities of small or medium business or non-profit organizations in the amount of 50 to 100, and legal entities of big business in the amount of 100 to 200 monthly calculation indices with confiscation of the media products.[477] Furthermore, under Article 273 of the Criminal Code,[478] the illegal manufacture for the purposes of distribution or advertisement, or distribution, and advertisement of pornographic materials or objects, as well as illegal trade in publications, cinema or video materials, pictures, or other objects of pornographic nature, may be punished by a fine in the amount from five hundred to one thousand monthly calculation indices, or in the amount of wages or other income of the given convict for a period from five months to one year, or by correctional labour for the period to two years, or by imprisonment for the period to two years with confiscation of pornographic materials or objects, as well as means for their manufacture or reproduction.

In **Norway**, pornography means "sexual depictions that seem offensive or are in any other way likely to have a humanly degrading or corrupting effect, including sexual depictions involving the use of corpses, animals, violence and duress."[479] Section 204a of the Penal Code 1902 refers to any person who "publishes, sells or in any other way attempts to disseminate pornography". Section 204b applies to importation of pornographic material with intent to disseminate such content, electronical distribution via the Internet or satellite transmissions are also covered. The penalty for involvement in pornography is a fine or up to three years' imprisonment. In the **Russian Federation**, there are general provisions outlawing the illegal distribution of pornographic materials.[480] In **Sweden**, pornographic content that is not considered to be child pornography is in principle legal. However, unlawful depiction of "sexual violence" is regulated by the Penal Code.[481] In Ukraine, importation into Ukraine of works, images or other pornography items for the purpose of sale or distribution or production, storage, transportation or other movement for the same purposes, or sale or distribution, and also forcing to participate in their creation is punishable for up to three years of imprisonment, with the confiscation of pornography, and their means of production and distribution.[482] In the **United Kingdom**, the Obscene Publications Act 1959 criminalizes in England and Wales the publication of obscene articles, and defines an obscene article as one which is such as to tend to deprave or corrupt those likely to read, see or hear it. The offence carries five years' maximum prison sentence.

Statute	2007	2008	2009
Obscene Publications Act 1959 S.2(1) as amended by Obscene Publications Act 1964 S.1(1) [(4)]	21	23	19
Criminal Justice and Immigration Act 2008 S.63 (1) & (7)(a)	*	*	0
Criminal Justice and Immigration Act 2008 S.63 (1) & (7)(b)	*	*	4

477 Article 344(1) (Manufacture, Possession, Import, Transportation, and Dissemination in the Territory of the Republic of Kazakhstan of Media Products and Other Products) Criminal Code of the Republic of Kazakhstan No. 167-I of 16 July 1997 (with amendments and addenda as of 6 October 2010).

478 Illegal dissemination of pornographic materials or objects.

479 Section 204 of the Penal Code 1902. The penal provision regarding pornography is maintained in the Penal Code 2005 section 317, which has not yet entered into force.

480 Articles 242, 242.1 of the Russian Federation Criminal Code. In accordance with Article 242 of the Criminal Code, illegal making for the purpose of distribution or advertising, dissemination, or advertising of pornographic materials or items, and likewise illegal trade in printed publications, cinema and video-materials, pictures, or any other pornographic items, shall be punishable by a fine in the amount of 100 000 to 300 000 roubles, or in the amount of the wage or salary, or any other income of the convicted person for a period of one to two years, or by deprivation of liberty for a term of up to two years.

481 Section 10c of the Penal Code. This provision also covers the Internet, and sanctions are criminal.

482 Article 301 of the Criminal Code of Ukraine.

Criminal Justice and Immigration Act 2008 S.63 (1) & (7)(c)	*	*	0
Criminal Justice and Immigration Act 2008 S.63 (1) & (7)(d)	*	*	12
TOTAL	21	23	35

Table 8. Convictions for obscene publications, and extreme pornography in England and Wales

More recently, the Criminal Justice and Immigration Act 2008 was introduced. Under Section 63 it is an offence to possess extreme pornographic images[483] (subject to certain defences). The offence carries a two or three year maximum prison sentence, depending on the nature of the image. The offence extends to England and Wales, and Northern Ireland.

Legal Provisions Outlawing Internet Piracy

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."[484] The industry claims that rather than purchasing copyright protected content legally, Internet users download large quantities of pirated content. The entertainment industry also claims that piracy not only includes downloading music, or movies but also TV episodes, software, books, newspapers, magazines, comics, and even pirated adult pornography. Live TV sports transmission ("stremaning piracy") is also subject to piracy through various streaming websites and platforms around the globe.

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 are described in **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 for the purpose of establishing international standards on intellectual property rights enforcement. It will also review the approaches adoped by the OSCE participating States in this area. 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, and leaked versions of the draft Agreement appeared online prior to an official draft release for discussion in April 2010.

The draft Agreement proposes notice-based liability regime for online service providers with regards 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 measures. This notice-based procedure included in the draft Agreement as a possible measure to tackle online IP infringements, as in the case of the more broad provisions of the EU E-Commerce Directive,

---

483 Section 63(6) defines what constitutes an "extreme image", and an image falls within this subsection if it portrays, in an explicit and realistic way, images involving acts which threaten or appear to threaten a person's life (section 63(7)(a)), acts which result, or is likely to result, in serious injury to a person's anus, breasts or genitals, (section 63(7)(b)), acts which involve sexual interference with a human corpse (section 63(7)(c)), a person performing an act of intercourse or oral sex with an animal (whether dead or alive) (section 63(7)(d)), and a reasonable person looking at the image would think that any such person or animal was real. Furthermore, section 63(6)(b) states that an extreme image is "grossly offensive, disgusting or otherwise of an obscene character".

484 *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.

"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."[485]

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 the 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[486] 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)."[487]

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".[488]

Despite such strong statements, certain states have developed, or started to develop legal measures which are often referred as "**three-strikes**". These measures 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 for dealing with copyright infringement as a legitimate means to addressing the problem, it is met with reservations and criticism by others who recognize access to the Internet as a fundamental right. There are also concerns that a considerable amount of copyright infringement 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, and 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."[489] According to the Irish court "in failing to

---

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

486 European Parliament Resolution of 10 March 2010 on the transparency and state of play of the ACTA negotiations, Strasbourg, P7_TA(2010)0058.

487 *Ibid*.

488 *Ibid*.

489 *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,

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."[490]

With this background the OSCE participating States were asked whether **there are specific legal provisions outlawing Internet piracy** in their country **(Question 9)**.[491] 44 (78.6%) of the participating States confirmed the existence of such legal provisions. Only **Turkmenistan** stated that it does not have any legal provisions outlawing Internet piracy. No data was obtained from 11 (19.6%) of the participating States.

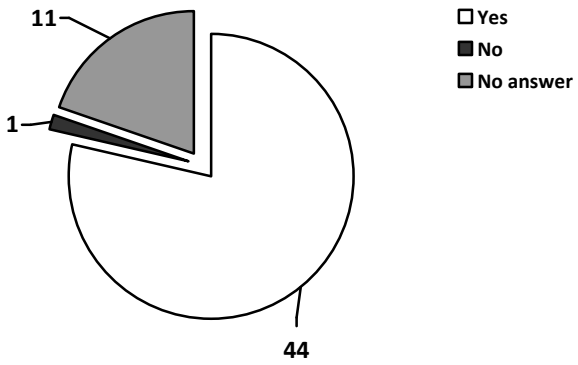


Figure 33. OSCE participating States' responses with regards to specific legal provisions outlawing Internet piracy (Question 9)

The responses received showed that almost all OSCE participating States have general intellectual property laws that may be used to combat Internet piracy. Liability and sanctions may be provided in the form of administrative, civil, and criminal liability. Graduated response mechanisms to limit users' access to the Internet for alleged copyright violations have been also developed in a few OSCE participating States, as it will be detailed below.

In **Austria**, the legal consequences of violations of copyright are regulated through the Copyright Act (Urheberrechtsgesetz – UrhG), independent from whether they are committed with through the Internet or not. Liability is also provided for ISPs but the liability provisions are based on the safe harbour provisions of the EU E-Commerce Directive as will be detailed below.

In **Azerbaijan**, there is no *corpus delicti* in the current legislation for violating copyright or related rights through the Internet. However, holders of copyright and related rights can apply to a court to defend their rights.[492] In addition to liability under civil law, piracy can lead to an administrative offence, and a fine may be imposed along with the confiscation of materials

---

2010.

490 *Ibid.*

491 The OSCE participating States were also asked how these offences are defined by law, which sanctions (criminal, administrative, civil) are envisaged by law, the maximum prison term envisaged by law for such offences, any statistical information in relation to convictions under such provisions for the reporting period of 1 January 2007 – 30 June 2010, and whether the law (or relevant regulations) prescribes blocking access to websites or any other types of Internet content as a sanction for these offences.

492 Article 45 (Methods of Defending Copyright and Related Rights) of the Law "On Copyright and Related Rights".

and equipment for manufacturing pirated content and making copies of pirated content.[493] Furthermore, criminal liability is also provided for, and depending upon the nature of the infringement, fines or imprisonment sentences up to three years may be imposed.[494] Use of the Internet for such actions does not alter the classification of the crime. In such cases, the Internet is merely the method by which the crime is committed.

The legislation of the Republic of **Belarus** does not contain any special rules prescribing criminal or administrative liability for Internet piracy. However, general rules on liability for violation of copyright, neighbouring rights, invention and patent rights exist under the Criminal Code,[495] and under the Code of Administrative Offences.[496] In **Bulgaria**, in addition to criminal liability,[497] civil liability is also provided for. In **Canada**, there are no specific legal provisions outlawing Internet piracy. Although the existing offences in Canada's Copyright Act were not drafted with the Internet in mind, it is likely that they would cover at least some forms of Internet piracy.[498] Section 42(1c) of the Copyright Act[499] includes an offence for the act of distributing an infringing copy of a work or other subject-matter in which copyright subsists either for the purpose of trade or to such an extent as to affect

---

493 Article 50 of the Code on Administrative Offences ("Violations of Copyright and Related Rights").

494 Article 165 (165.1) of the Criminal Code ("Violation of Copyright or Related Rights") stipulates that illegal use of items protected by copyright or related rights (i.e., the publication of others' scientific, artistic, or other works under one's own name or claiming authorship by other means, the illegal secondary publishing of such a work or its distribution, and forced co-authorship) is punishable by a fine of 100 to 500 manaty or 160 to 240 hours of community service if substantial harm was incurred as a result of such actions. According to article 165.2, the same actions, upon a repeat offence or, upon an offence by a group or organized group are punishable with a fine of 500 to 1,000 manats, a material compensation or imprisonment for a period of up to three years.

495 See article 201 of the Criminal Code which entails punishment of up to five years imprisonment. During the period from 2007 through 2009, there were 110 convictions under article 201 of the Criminal Code.

496 Article 9.21 of the Code of Administrative Offences entail imposition of a fine on an individual in an amount of up to fifty base units, on an individual entrepreneur – of up to one hundred base units, and on a legal entity – of up to three hundred base units. Confiscation of the subject of the administrative offence may also be applied to all those held administratively liable under the given article.

497 Article 172A of the Penal Code (Art. 172a - 173). Art. 172a. (New, SG 50/95) (1) (Amend., SG 62/97) - Who records, reproduces, circulates, broadcasts or transmit by a technical device or uses in any other way another's work of science, literature or art, without the consent of the bearer of the copyright required by the law, shall be punished by imprisonment of up to three years and a fine of one thousand to three thousand levs. (2) (Amend., SG 62/97) The punishment under para 1 shall also be imposed on those who records, reproduces, circulates, broadcasts or transmit by a technical device or uses in any other way a sound record, video record or radio programme, TV programme, software or computer programme without the necessary consent of the bearer of the copyright required by the law. (3) (Amend., SG 62/97) If the act under para 1 and 2 has been committed again or substantial harmful consequences have been caused the punishment shall be imprisonment of one to five years and a fine of three thousand levs to five thousand levs.

498 Amendments to this Act which would deal with "enablers" have recently been introduced in Parliament (see s. 42, of Bill C-32, the Copyright Modernization Act). Although one cannot predict with certainty whether these proposed amendments will actually become law, they would play a role in countering Internet piracy if passed. See <http://laws-lois.justice.gc.ca/eng/C-46/FullText.html> for the Criminal Code provisions. See <http://www2.parl.gc.ca/HousePublications/Publication.aspx?Docid=4580265&File=24> for the drafting text of the Copyright Modernization Act. It is interesting to note that that Bill C-32, known as the Copyright modernization Act, which is now at second reading stage contemplate provisions against the tampering of technological measures and rights management information used by copyright owners in association with their works or sound recordings, performers' performances fixed in sound recordings. The tampering of technological measures is an act for which an individual could be found guilty, on summary conviction, to a fine not exceeding $ 25,000 or to imprisonment for a term not exceeding six months or to both; or, on conviction of indictment, to a fine not exceeding $ 1,000 000 or to imprisonment for a term not exceeding five years, or to both.

499 R.S.C., C-42.

prejudicially the owner of the copyright. This provision has been found applicable where distribution of infringing copies took place by means of an electronic bulletin boards.[500] Similarly, in **Croatia** there is no specific crime of Internet piracy but the Criminal Code includes a provision on unauthorised use of author's work or performance of a performing artist.[501] If substantial proceeds have been gained or damage caused, and the perpetrator acted with a view of gaining such proceeds or causing such damage, the perpetrator shall be punished with a prison term of six months to five years.[502] In the **Czech Republic**, Internet piracy is sanctioned under the Criminal Code provisions.[503]

In **Denmark**, Internet piracy is outlawed through the general provisions of the consolidated Danish Copyright Act.[504] However, there are no specific provisions on Internet piracy, but the act of both uploading and downloading of protected works requires consent of the right holder, and is therefore a violation of the copyright act, if done without consent. Such violation of copyright act is punishable with fines and imprisonment.[505] In **Finland**, for the purpose of prohibiting continued violation, the author or his representative has the right to take legal action against the person who makes the allegedly copyright-infringing material available to the public. In allowing the action, the court of justice shall at the same time may order that the making available of the material to the public must cease. The court of justice may impose a conditional fine to reinforce the order.[506] The court of justice may, upon the request of the author or his representative, order the maintainer of the transmitter, server or other device or any other service provider acting as an intermediary to discontinue, on pain of fine, the making of the allegedly copyright-infringing material available to the public (injunction to discontinue), unless this can be regarded as unreasonable in view of the rights of the person making the material available to the public, the intermediary, and the author.[507] Criminal liability for infringement of copyright also exists in Finland.[508]

---

500 The sanction for this offence is, on summary conviction, a fine not exceeding twenty-five thousand dollars, or a term of imprisonment not exceeding six months or to both; or, on conviction on indictment, a fine not exceeding one million dollars, or an imprisonment for a term not exceeding five years or to both.

501 Article 230(1) of the Criminal Code: Anyone who without the approval of the author or another copyright holder, or the person authorised to give the approval, when the approval is required by law, or in contravention of their prohibition, fixes to a material sub-base, reproduces, copies, brings into circulation, leases, imports, carries over the border line, shows, performs, transmits, conveys, makes available to the public, translates, adjusts, modifies, alters or in any other way makes use of a work of an author, shall be punished by a fine or by a prison term of up to three years. Article 230(3) of the Criminal Code: The punishment referred to in paragraph 1 above shall be measured out to anyone who with the intention to enable unauthorised use of an author's work or performance of an artist performer, imports, carries over the border line, brings into circulation, leases, enables another use or utilize any type of equipment or means whose main or prevailing purpose is to make possible unauthorised removal or thwarting any technical means or software aimed at the protection of the rights of the author or artist performer from unauthorised use.

502 Article 230(5) of the Criminal Code

503 Article 270 (Infringement of copyright, rights related to copyright and database rights), Act No. 40/2009 Coll. Penal Code.

504 No. 202 of February 2010. English version is available at <http://www.kum.dk/en/english/Legislation/Copyright/>.

505 Very severe violations can result in imprisonment for up to six years subject to section 299b of the Danish Criminal Code.

506 Section 60b (law nr. 821/2005) of the Copyright Act (404/1961).

507 Section 60c (law nr. 821/2005) of the Copyright Act (404/1961).

508 Section 1 (law nr. 822/2005) Copyright offence, Criminal Code, Chapter 49. If a person who uses a computer network or computer system to violate the right of another to the objects of protection referred to in subsection 1 so that the act is conducive to causing considerable detriment or damage to the holder of the right that has been violated, shall be sentenced for a copyright offence.

In **France**, the HADOPI law (Creation and Internet law)[509] was introduced during 2009 as a means to control and regulate Internet access, and encourage compliance with copyright laws through a "graduated response" system. HADOPI[510] is the acronym of the government agency created to administer the new law. The Agency would first warn the copyright offenders who download or upload pirated content, and if the offenders do not cease their allegedly illegal activity, the Agency may then suspend the alleged offender's Internet subscription.

In terms of how the system would function, upon receipt of a complaint from a copyright holder or representative, HADOPI may initiate a "three-strike" procedure described as follows in the response received from the French delegation in their response to the OSCE RFOM questionnaire:

> (1) An email message is sent to the offending Internet access subscriber, derived from the IP address involved in the claim. The email specifies the time of the claim but neither the object of the claim nor the identity of the claimant. The ISP is then required to monitor the subject Internet connection. In addition, the Internet access subscriber is invited to install a filter on his/her Internet connection. If, within the 6 months following the first step, a repeated offence is suspected by the copyright holder, or their representative, the ISP or HADOPI, the second step of the procedure is invoked.
> (2) A certified letter is sent to the offending Internet access subscriber with similar content to the originating email message. In the event that the offender fails to comply during the year following the reception of the certified letter, and upon accusation of repeated offences by the copyright holder, a representative, the ISP or HADOPI, the third step of the procedure is invoked.
> (3) The ISP is required to suspend Internet access for the offending Internet connection, that is the subject of the claim, for a specified period lasting from two months to one year.

Therefore, following the above procedure, the Internet access subscriber would be blacklisted, and other ISPs would be prohibited from providing an Internet connection to the blacklisted subscriber. The service suspension does not, however, interrupt billing, and the offending subscriber is liable to meet any charges or costs resulting from the service termination. Appeal to a court is possible only during the third phase of the action (after the blocking of Internet access), and an appeal can result in shortening but not cancellation of the blocking. The burden of proof lies with the appellant.

In June 2009, the Constitutional Council found that the power to suspend access to the Internet as punishment for the illegal downloading of works, as voted in the context of the "HADOPI" Act could not be conferred on an independent administrative authority. On 22 October 2009, the Constitutional Council approved a revised version of HADOPI, requiring judicial review before revoking a subscriber's Internet access can be suspended, but otherwise the new version of the law resembles the original requirements.[511] The subscriber may also be required to continue paying the Internet access subscription fee, despite the access suspension punishment.[512] According to an IRIS report, "on 4 October 2010, following the rejection by the Conseil d'État on 14 September 2010 of the appeal brought by the access provider FDN against the Decree on HADOPI's sanctions procedure HADOPI sent out its first warning e-mails to people who had downloaded works from the Internet illegally."[513] According to the

---

509 Loi favorisant la diffusion et la protection de la création sur Internet: Law promoting the distribution and protection of creative works on the Internet.

510 Haute Autorité pour la Diffusion des Œuvres et la Protection des Droits sur Internet.

511 Article L. 335-2 and L. 335-3 of the CPI.

512 See further Amélie Blocman, The "HADOPI 2" Act Comes into Force, IRIS 2010-1:1/23.

513 A decree dated 13 October 2010 amended the Intellectual Property Code (Art. R. 331-37), which requires

CNIL,[514] action under the HADOPI law does not exclude separate prosecutions under the French Code of Intellectual Property, particularly with regards to its articles L331-1 or L335-2, or does not limit a claimant's other remedies such as civil law liams for intellectual property infringements.

In **Georgia**, Article 189 of the Criminal Code refers to infringement of intellectual property rights in general, and covers Internet piracy as well. Under Article 189 it is an offence to reproduce work, phonogram, visual record or database or to purchase, import, keep, sale, rent, transfer without authorization their copies and/or otherwise infringe rights of a copyright-holder, neighbouring right-holder or database author for the purposes of earning income in large amounts through violating the Law of Georgia on "the Copyright and Neighbouring Rights". Penalties foreseen for this offence are a fine or restriction of liberty up to two years' imprisonment.[515]

In **Germany**, there are no special legal provisions expressly prohibiting Internet piracy. Rather, the general provisions within the relevant special statutory regulations (civil, administrative, and criminal[516]) cover also the rights entailed by intellectual property,[517] both online and offline. In **Italy**, Law No. 248[518] includes provisions on copyright protection. The Legislative Decree No. 44 introduced some rules for audiovisual media services, regardless of platforms, techniques or transmission modalities used in the perspective of a non-discriminatory and technologically neutral regulation.[519] The Postal and Telecommunications Police deals with unauthorized dissemination of copies of works through the Internet, violation of copyright through illegal access to computers or computer networks, in particular, belonging to critical infrastructure, online sale of illegal files, and content in violation of copyright; and illegal dissemination of such content through Web 2.0-based applications and services.

Year	Received Reports	Reported persons	Arrested persons	Controls	Amount of fines	Monitored virtual spaces	Seized virtual spaces
2006	52	111	2	1325	€ 468551	5362	5
2007	62	78	-	1242	€ 546721	4229	3

ISPs to send HADOPI's warning e-mails on to their subscribers by electronic means within twenty-four hours. Non-compliance can result in a fine of EUR 1,500. See Amélie Blocman, HADOPI Sends out the First Warning E-Mails, IRIS 2010-10:1/30.

514 The Commission nationale de l'informatique et des libertés.

515 Note also Article 1571 of the Code of Administrative Violations.

516 Section 106 of the German Copyright Act: (1) Any person who, other than in a manner allowed by law and without the right holder's consent, reproduces, distributes or publicly communicates a work or an adaptation or transformation of a work, shall be liable to imprisonment for up to three (3) years or a fine. (2) The attempt to commit such an offense shall be punishable. Section 108a of the German Copyright Act: (1) Where the person committing the acts referred to in section 106 to section 108 does so on a commercial basis, the penalty shall be imprisonment for up to five (5) years or a fine. Section 109 of the German Copyright Act: Offenses under sections 106 to 108 and under section 108b shall only be prosecuted on complaint unless the prosecuting authorities deem that ex officio prosecution is justified in view of the particular public interest. The Federal Ministry of Justice does not have at hand any statistical information collected in connection with convictions for offences pursuant to sections 106 et seq. of the Copyright Act (UrhG) or, respectively, with fines levied for the period specified.

517 The German Copyright Act (Urheberrechtsgesetz, UrhG) has provided for these matters in sections 106 – 111a.

518 Dated 18 August 2000.

519 Note also Article 32-bis (concerning copyright protection) of the Legislative Decree No. 177 of 31 July 2005 as amended by Legislative Decree No. 44 of 15 March 2010.

2008	42	29	-	652	€ 67718	2699	7
2009	62	30	-	499	€ 344397	2199	2
2010 (I Sem)	N/A	30	-	66	€261104	85	0

Table 9. Statistical table on the activity of the Italian Postal and Communications Police for the period of 2006-2010

In **Kazakhstan**, the Code on Administrative Offences includes a provision on breach of copyright and related rights.[520] Subject to this provision, illegal use of objects of copyright or related rights, as well as the acquisition, possession, conveyance or making of counterfeited copies of objects of copyright and/or related rights for the purpose of sale, and illegal appropriation of authorship, or coercion to co-authorship, if such acts do not contain signs of a criminally punishable deed, shall be punishable by a fine. The Criminal Code also includes a provision on breach of copyright and related rights.[521] This provision criminalizes illegal use of objects of copyright or related rights, as well as the acquisition, possession, conveyance or making of counterfeited copies of objects of copyright and/or related rights for the purpose of sale, committed on a large scale, and these crimes may be subject to a fine, or by engagement in community service for 180 to 240 hours, or by arrest for a term of three to six months. An aggravated version of these crimes would result in deprivation of liberty for a term of two to five years. Kazakhstan also has a separate copyright law,[522] and this provides civil, administrative and criminal liability for breach of copyright and related rights. The **Kyrgyz Republic** has similar laws, and liability is provided under administrative,[523] civil[524] and criminal law,[525] as well as through specific copyright law.[526] Under the Kyrgyz copyright law, the use of a work, performance of phonogram, including making it available to the public, including posting such content on the Internet without the permission of the right holder, constitutes a violation.

In **Latvia**, Article 148 of the Criminal Law on Infringement of Copyright and Neighbouring Rights,[527] includes criminal liability for infringement of copyright,[528] and of neighbouring rights, if substantial damage is caused to interests protected by law. The provision prescribes deprivation of liberty for a term up to two years, community service, or a fine not exceeding one hundred and fifty times the minimum monthly wage.[529] This provision came into effect on 1 January 2011.

---

520 Article 129 of the Code of the Republic of Kazakhstan on Administrative Offences No. 155-II of 30 January 2001 (with amendments and addenda of 6 October 2010).

521 Article 184 of the Criminal Code of the Republic of Kazakhstan No. 167-I of 16 July 1997 (with amendments and addenda of 6 October 2010).

522 Articles 48 and 49 of the Law of the Republic of Kazakhstan No. 6-I of 10 June 1996 "On Copyright and Related Rights".

523 Article 340 of the Code of Administrative Liability of the Kyrgyz Republic provides for sanctions for violations of copyright and neighbouring rights in the course of commercial use in trade networks. However, these administrative sanctions are not applicable to violations of copyright and neighbouring rights on the Internet.

524 Article 11 of the Civil Code of the Kyrgyz Republic.

525 Article 150 of the Criminal Code of the Kyrgyz Republic. The maximum term for deprivation of liberty in accordance with article 150 is five years.

526 Law of the Kyrgyz Republic "On Copyright and Neighbouring Rights": Articles 16, 37, 38, 48 and 49.

527 The law of 21 October 2010, "Amendments to the Criminal Law" amended this particular provision.

528 Administrative penalties are also provided under Article 1558 of the LAVC.

529 Aggravated liability is envisaged for the mentioned acts, when they are performed in a group upon a prior agreement, as well as for an intentional infringement of copyright and neighbouring rights, if performed at a large scale or in an organised group, or for compelling, by means of violence, threats of violence or blackmail, the renouncing of authorship or compelling of joint authorship: the applicable sentence is

In **Lithuania**, administrative[530] and criminal sanctions exist for the copyright and related rights violations, including Internet piracy.[531] Therefore, a person who unlawfully reproduces a literary, scientific or artistic work (including computer software and databases) or an object of related rights or a part thereof for commercial purposes or distributes, transports or stores for commercial purposes illegal copies thereof, where the total value of the copies exceeds, according to the prices of legal copies or, in the absence thereof, according to the prices of originals of the reproduced works, the amount of 100 MSLs, shall be punished by community service or by a fine or by restriction of liberty or by arrest or by imprisonment for a term of up to two years.

In **Norway**, there are rules applicable to Internet piracy which are included in the Copyright Act of 1961, and the General Civil Penal Code of 1902. Illegal file sharing is prohibited pursuant to Section 2 of the Copyright Act. The term "illegal file sharing" covers the uploading and/or downloading of material protected by copyright without the intellectual property rights holder's consent. Uploading infringes the copyright holder's exclusive right to make the material available to the public. Downloading violates the exclusive right to produce permanent or temporary copies of the material. It may also be noted that Section 53a(1) of the Copyright Act prohibits unathorised access to works protected by copyright. Copyright infringement is punishable according to section 54(1) of the Copyright Act, and the penalty provided is a fine or up to three months' imprisonment.

In **Romania**, the provision of protected works without the approval of the copyright holder to the public including through the Internet is punished with a fine, or imprisonment ranging from one to four years.[532] In the **Russian Federation**, there are general criminal,[533] civil,[534] and administrative legal provisions that outlaw piracy without singling out the Internet as the place where the offence is committed. Punishment in the form of a fine in the amount of up to 200,000 roubles or in the amount of the salary or other income of the convicted person for a

---

deprivation of the right to engage in a certain activity for a term up to five years, and on probation, or without probation, for a term of up to three years.

530 Article 21410 (Copyright and Related Rights Violation) of the Code of Administrative Offences of the Republic of Lithuania.

531 Article 192(1) of the Criminal Code of the Republic of Lithuania. In 2007, 76 crimes were registered under Article 192, nine cases were referred to the court; in 2008 the number of registered crimes decreased to 57, 11 cases were referred to the court. In 2007 one crime was registered under Article 192, in 2008 this number remained the same.

532 See articles 139 8, 139 9 and 143 of Law 8/1996.

533 Article 146 (2) of the Criminal Code states that illegal use of objects of copyright or neighbouring rights, as well as the acquisition, possession or carriage of counterfeit copies of works or phonograms for the purpose of sale carried out on a large scale shall be punishable with a fine in the amount of up to 200,000 roubles or in an amount of the salary or other income of the convicted person for a period of up to 18 months, or with compulsory community service for 180 to 240 hours, or with deprivation of liberty for a term of up to two years.

534 In accordance with Article 1259 of the Russian Federation's Civil Code, objects of copyright are works of science, literature and art, regardless of the merits and designation of the work, or of the way in which it is expressed: literary works; drama and musical –drama productions, stage works; choreographic works and pantomimes; musical works with or without lyrics; audiovisual works; paintings, sculptures, graphic art, design, graphic tales, comics, and other works of visual art; works of applied and scenic art; works of architecture, urban planning, and landscaping, including drawings, blueprints, images, and mock-ups; photographs and works achieved by means similar to photography; geographic, geological, and other maps, plans, sketches, and figurative works relating to geography, topography, and to other sciences; other works. Objects of copyright also include computer programs that are protected as literary works. Objects of copyright also include derivative works, i.e. works processed from another work, composite works, i.e. works created by sorting and arranging materials.

period of up to 18 months, or compulsory community service for 180 to 240 hours, or deprivation of liberty for a term of up to two years is provided for copyright related crimes.

In Spain, civil[535] and criminal[536] measures and sanctions exist to address copyright issues. Furthermore, in February 2011, the Spanish Parliament adopted the Sustainable Economy Act.[537] The new law includes a series of measures against illegal downloading of protected works (the so-called *Ley Sinde* provisions). According to an IRIS report, "the *Ley Sinde* aims at blocking or closing down in a short space of time websites from which copyrighted content may be downloaded."[538] The *Ley Sinde* provisions target information society service providers (intermediaries, and websites that provide links to infringing content) rather than users (unlike in **France**, and **United Kingdom**) who download allegedly illegal content.[539]

In **Ukraine**, criminal, administrative, and civil law measures provide liability for infringement of copyright and related rights. The offences include "publishing", "reproduction," and "distribution". These provisions also apply to Internet piracy.[540] In terms of penalties, Article 176 of the Criminal Code provides a fine of two hundred to one thousand times the income, or correctional work up to two years or imprisonment for the same term.

In the **United Kingdom**, the Copyright, Designs and Patents Act 1988 provides criminal liability for making or dealing with infringing articles.[541] The provisions would cover commercial distributors as well as non commercial distributors.[542] Civil liability for copyright also exists. The Digital Economy Act, granted royal assent in April 2010, establishes the basis through which a graduated response mechanism could be introduced in the UK. The Act imposes an obligation on ISPs to notify subscribers that IP addresses with which they are associated are alleged to have been used in the illegal downloading of copyrighted material. The notification would come from the copyright owners. Furthermore, the Act requires that ISPs, if requested by a copyright owner, compile an anonymous list of subscribers who have received a specified number of notices. ISPs will only disclose the personal identity of subscriber to rights holders after the rights holder has obtained a court order. Government's explanatory note on the Act illustrates how the provisions might work in practice:

---

535 Note Royal Legislative Decree 1/1996 of 12 April, on Intellectual Property (RDIP); Civil Procedure Act, 7 January 1/2000; the Civil Code 1889; and Information Society Measures and Electronic Commerce (11 July 23/2002).

536 Articles 197 and 264 of the Criminal Code, 23 November,10/1995. Criminal infringement in Spain assumes bad faith or knowledge that rights may be violated, and, in specified cases, gainful intention (articles 270, 271, 272, 287 and 288 of the Criminal Code). For Criminal infringement the Criminal Code in Spain includes measures such as fines or confinements in addition to penalties of prison depending on the seriousness of the harm (articles 270, 271, 272, 287, 288 of the Criminal Code).

537 These measures amend three further acts, namely the Act on Information Society Services, the Intellectual Property Act and the Act on Administrative Jurisdiction.

538 See Pedro Letai, Parliaments Finally Approves Controversial Copyright Provision, IRIS 2011-3:1/17.

539 See Miquel Peguera, "Internet Service Providers Liability in Spain: Recent Case Law and Future Perspectives," 1 (2010) JIPITEC 151, para. 1.

540 Article 50 of the Law of Ukraine "On Copyright and Related Rights" defines violations of copyright and related rights. Note further article 51-2 of the Code of Ukraine on Administrative Offences on illegal use of the objects of intellectual property rights. Note further article 432 of the Civil Code of Ukraine with regards to issues involving civil law claims for copyright.

541 Section 107, Copyright, Designs and Patents Act 1988.

542 Section 23 (Secondary infringement: possessing or dealing with infringing copy), Copyright, Designs and Patents Act 1988: distributes otherwise than in the course of a business to such an extent as to affect prejudicially the owner of the copyright.

Copyright owners identify cases of infringement and send details including IP addresses to ISPs;
The ISPs verify that the evidence received meets the required standard, and link the infringement to subscriber accounts;
The ISPs send letters to subscribers identified as apparently infringing copyright. They keep track of how often each subscriber is identified;
If asked to do so by a relevant copyright owner, ISPs supply a copyright infringement list showing, for each relevant subscriber, which of the copyright owner's reports relate to that subscriber. The list does not reveal any subscriber's identity;
Government's explanatory note on the Act illustrates how the provisions might work in practice:
Copyright owners use the list as the basis for a court order to obtain the names and addresses of some or all of those on the list. At no point are individuals' names or addresses passed from the ISP to a copyright owner without a court order;
Copyright owners send "final warning" letters directly to infringers asking them to stop online copyright infringement and giving them a clear warning of likely court action if the warning is ignored; and
Copyright owners take court action against those who ignore the final warning.

The obligations will not have effect until there is a complementary code in force that has been approved or made by OFCOM, the Independent regulator, and competition authority for the UK communications industries.[543] The government's aim is for the initial obligations to significantly reduce online infringement of copyright. However, in case the initial obligations prove not as effective as expected, section 124H of the Digital Economy Act gives the Secretary of State the power to introduce further obligations, should that prove appropriate. Section 124G of the Act provides that after one year from the time the code enters into force the Secretary of State has the power to impose further "technical obligations" on ISPs, such as limiting Internet access to subscribers who have been linked to a specified number of infringements. According to the explanatory note of the Digital Economy Act, technical measures would be likely to include bandwidth capping or shaping that would make it difficult for subscribers to continue file-sharing. If appropriate, temporary suspension of broadband connections could be considered. However this is only in the event that the complementary code in effect is proving insufficient to properly act against illegal downloading, and in the event that OFCOM has assessed that such measures are necessary. The Digital Economy Act 2010 provisions are yet to be implemented, and the provisions were subject to judicial review.[544] In April 2011 the High Court substantially rejected the arguments against the validity of the Digital Economy Act.[545] The Court provided the following explanation:

---

543 OFCOM, Online Infringement of Copyright and the Digital Economy Act 2010: Draft Initial Obligations Code, Consultation, May 2010, at <http://stakeholders.ofcom.org.uk/consultations/copyright-infringement/>.

544 Application of *British Telecommunications PLC TalkTalk Telecom Group PLC and The Secretary of State For Business, Innovation and Skills*, The High Court of Justice, CO/7354/2010: This case involves a challenge brought by two telecommunications companies to sections 3 to 18 of the Digital Economy Act 2010 which concern the online infringement of copyright.

545 [2011] EWHC 1021 (Admin).). BT and TalkTalk announced on 27 May 2011 that are seeking leave to appeal against the High Court ruling on the Digital Economy Act (DEA). BT and TalkTalk believe that the DEA measures aiming to prevent online copyright infringement are inconsistent with European law. Quite apart from the potential impact on their businesses, BT and TalkTalk believe the DEA could harm the basic rights and freedoms of ordinary citizens. The two companies have chosen to seek an appeal on four of the five grounds addressed in the initial High Court case. These relate to the EU's Technical Standards Directive, the Authorisation Directive, the E-Commerce Directive and the Privacy and Electronic Communications Directive. BT and TalkTalk believe the DEA is not consistent with these directives. The fifth area addressed in the initial High Court ruling concerned whether the Act was in accordance with EU

> "In this case Parliament has addressed a major problem of social and economic policy, where important and conflicting interests are in play. On the one hand, there is evidence to suggest that the media industry, broadly interpreted, is sustaining substantial economic damage as a result of unlawful activity on the internet; and there is concern that such damage may significantly affect creativity and productivity in an economic area of national importance where, at least historically, the UK has tended to enjoy some comparative advantage in international markets. On the other hand, the business models of ISPs are constructed on the basis that they are essentially conduits for the flow of information, and the efficiency, cost effectiveness and competitiveness of their operations depend on the minimum regulatory interference with that flow of traffic, and on the minimum responsibility and burden in respect of the actual content of the material passing through the conduit. Similarly, subscribers of the ISPs and users of the internet appreciate that the technology is the most prodigious tool for the transmission and interchange of information and other material ever designed, and, in general, they would oppose restrictions on their ability to enjoy untrammeled access to such information and material. Information is also a public good, and interference with access to, and publication of, information may adversely affect general welfare. How these competing and conflicting interests should be accommodated and balanced appears to me to be a classic legislative task, and the court should be cautious indeed before striking down as disproportionate the specific balance that Parliament has legislated."[546]

Legal provisions outlawing libel and insult (defamation) on the Internet

The terms defamation and libel are most commonly referred to in the OSCE participating States' legislation to describe true and false statements of facts, and opinions which harm the reputation of the other person and/or are insulting or offensive.[547] The multi-purpose hybrid Internet, especially with the development of the 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 ascertainable. However, this user driven activity can also lead into the publication of defamatory content on such platforms.[548]

In terms of policy issues surrounding libel on the Internet there is a persistent debate over whether the ISPs, hosting companies, or 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

---

rules on proportionality. Both companies continue to take the view that the regime represents a disproportionate interference with the rights of internet service providers, subscribers and internet users and with the concept of freedom of expression. They recognise, however, the Court's view that there is an exceptionally high threshold to show that this legislation was not a proportionate response prior to the code of practice being published and have concluded not to pursue leave to appeal on this ground. See BT Press Release, BT and TalkTalk appeal Digital Economy Act judgment, DC11-126, May 27, 2011.

546 [2011] EWHC 1021 (Admin), para 211.

547 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.

548 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

Europe. For example, the EU Directive on Electronic Commerce[549] provides a limited and notice-based liability with takedown procedures for illegal content, which will be described further down. However, by way of contrast it is important to note that US based service providers have more protection from liability for third party content regardless of their "knowledge" of the alleged defamatory content,[550] and this issue will also be addressed below in the section titled "Licensing and liability related issues."

Unlike in the US, in many states notice-based liability measures represent the liability regime for ISPs, 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 ISPs under some pressure to remove material from their servers without considering whether the alleged defamatory content is true or whether the publication 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."[551]

The OSCE participating States usually regulate defamation through civil or criminal measures, and defamation on the Internet is treated as any other type of publication by almost all the participating States. For the purpose of this study, the OSCE participating States were asked whether **they have specific legal provisions outlawing libel and insult (defamation) on the Internet** in their country **(Question 10)**.[552] 36 (64.3%) of the participating States responded that they have such laws in place. Eight states[553] (14.3%) do not have criminal law provisions outlawing libel. However, although there are no criminal law provisions outlawing libel and defamation within these states, civil law provisions that could apply to the Internet do exist in those states. No data was obtained from twelve (21.4%) of the participating States. As shown below, although few states have decriminalized defamation, the decriminalization process still continues, and several states are currently in the process of abolishing criminal libel and defamation provisions.

549 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.

550 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).

551 Law Commission (England and Wales), Defamation and the Internet: A Preliminary Investigation, (Scoping Paper: Dec 2002).

552 The participating States of the OSCE were also asked how these offences are defined by law, which sanctions (criminal, administrative, civil) are envisaged by law, and what is the maximum prison term envisaged by law for such offences. They were also requested to provide any statistical information in relation to convictions under such provisions for the reporting period of 1 January 2007 – 30 June 2010. Finally, they were asked to report whether their law (or relevant regulations) prescribes blocking access to websites or any other types of Internet content as a sanction for these offences.

553 It should be noted that eight States answered this question as "No": Bosnia and Herzegovina, Bulgaria, Canada, Croatia, France, Luxembourg, Romania and the United Kingdom.

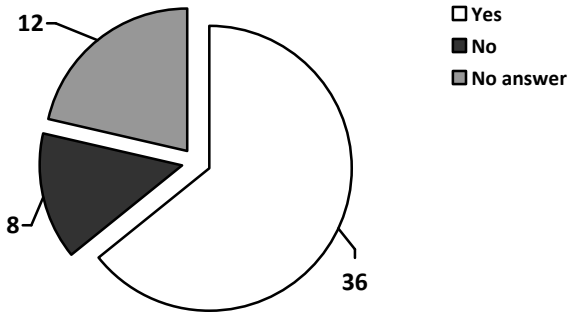


Figure 34. OSCE participating States' responses with regards to specific legal provisions outlawing libel and insult (defamation) on the Internet (Question 10)

The **Albanian** Criminal Code includes provisions governing matters relating to libel and insult (defamation), including the designation of insult against an individual or group of persons,[554] insult through computer systems based on special motivations,[555] and libel against an individual or a group of persons[556]. The law envisages sanctions of fines and imprisonment sentences for contraventions of the pertinent provisions. The maximum prison term envisaged by Article 119 is one year's imprisonment; and by Article 120 two years' imprisonment. In **Armenia**, the decriminalization of libel and insult covers the Internet as well. Currently, under the Civil Code provisions,[557] insult is deemed to be a public expression by means of speech, picture, voice, sign or by any other form of publicity with the intention of causing harm to honour, dignity and business reputation.[558] The Civil Code also contains a definition of defamation, and this is deemed to be the public statement of such facts about a person, which do not correspond to the reality, and infringe his/her honor, dignity or business reputation. In the case of insult a person can demand in court one or several of the measures including a public apology and financial compensation in the amount of up to 1000 minimum salaries.

In **Austria**, in addition to the criminal provisions under section 111ff of the Criminal Code, Section 6 of the Media Act (*Mediengesetz*) provides for a compensation in cases of defamation, slander, mockery and libel, violation of the most private area of life,[559] for revealing identities in certain cases[560] as well as violation of the presumption of innocence[561] in media. Internet websites fall under the term "media"[562] under the Austrian provisions.

In **Azerbaijan**, the dissemination of information known to be false that tarnishes the honour and dignity of an individual or undermines his reputation in a public statement, or in a work freely available to the public, or in the media is punishable by a fine in the amount of 100 to

554 See Article 119 of the Criminal Code.
555 See Article 119/b of the Criminal Code.
556 See Article 120 of the Criminal Code.
557 Article 19 of the Civil Code of Armenia "Protection of Honor, Dignity and Business Reputation", and Article 1087.1 "The Order and Terms of Compensation for Harm Caused to the Honor, Dignity and Business Reputation" of the Civil Code of Armenia.
558 Article 1087.1(2) of the Civil Code: Within the context of this Code a public expression can not be deemed as an insult in the given situation and with its content if it is based on accurate facts and is made because of an overweighing public interest.
559 Section 7 of the Media Act.
560 Section 7a of the Media Act.
561 Section 7b of the Media Act.
562 Section (1)1 no 5a lit. b of the Media Act.

500 minimum wages, or by community service for a period of up to 240 hours, or to correctional labour for a period of up to one year, or to imprisonment for a period of up to six months.[563] Similarly, consciously denigrating honour and dignity in an unseemly manner is punishable by a fine in the amount of 300 to 1,000 manats, or by community service for up to 240 hours, or by correctional labour for up to one year, or by imprisonment for up to six months.[564] According to Article 3 of the law "On the Media," the Internet is considered part of the media. Libel and insult are also criminalized, and these crimes may also be committed over the Internet.[565]

The legislation of the Republic of **Belarus** does not contain any special rules prescribing criminal or administrative liability for outlawing libel and insult on the Internet. However, general rules prescribing liability for libel and insult are envisaged within the Code of Administrative Offences with various fines.[566] Furthermore, deprivation of liberty up to three years is a sanction under the Criminal Code.[567] In **Bosnia and Herzegovina**, the High Representative decided to decriminalize defamation in 1999. The government adopted the law on the Protection against Defamation of the Federation of Bosnia and Herzegovina which has been in force in the Republica Srpska since June 2001, and in the Federation since 1 November 2002. This Law regulates civil liability for harm caused to the reputation of a natural or legal person by the making or disseminating of an expression of false facts. In **Bulgaria**, there are criminal law provisions under the Penal Code.[568] However, in 2000, a law amending the Penal Code revoked imprisonment, keeping in force only the sanctions of a fine and public reprobation.

In **Canada**, there are no specific legal provisions outlawing libel or insult "on the Internet" in the Criminal Code. However, an Ontario Superior Court dealt with a case on defamatory libel in the context of the Internet. *R. v. Barrett*,[569] is the only reported case which relates primarily

---

563 Article 147 (147.1) of the Criminal Code ("Libel").

564 Article 148 of the Criminal Code ("Insult").

565 See Articles 147 (libel) and 148 (insult) of the Criminal Code.

566 Articles 9.2 of the Code of Administrative Offences ("Libel") provides an imposition of a fine of up to and including thirty base units. Article 9.3 of the Code of Administrative Offences ("Insult") provides an imposition of a fine of up to and including twenty base units.

567 Articles 188 of the Criminal Code ("Libel") and 189 of the Criminal Code ("Insult"). During the period from 2007 through 2009, there were 13 convictions under Article 188 of the Criminal Code and 48 convictions under Article 189 of the Criminal Code.

568 Articles 146 – 148 of the Penal Code: Art. 146. (1) (Amend., SG 28/82; SG 10/93; SG 21/00) Who says or accomplishes something humiliating the honour or the dignity of another in his presence shall be punished for insult by a fine of one thousand to three thousand levs. In this case the court can also impose punishment of public reprobation. (2) If the insulted has responded immediately by an insult the court can release both of them from punishment. Art. 147. (1) (Amend., SG 28/82; SG 10/93; SG 21/00) Who divulges an ignominious circumstance regarding another or fastens a crime on him shall be punished for libel by a fine of three thousand to seven thousand levs and by public reprobation. (2) The perpetrator shall not be punished if the genuineness of the divulged circumstances or of the fastened crime is proven. Art. 148. (1) (Amend., SG 28/82; SG 10/93; SG 21/00) For insult: 1. for an insult in public; 2. circulated through a printed matter or in any other way; 3. of an official or a representative of the public during or on occasion of his duty or functions and 4. by an official or representative of the public during or on occasion of fulfillment of his duty or function the punishment shall be a fine of three thousand to ten thousand levs and public reprobation. (2) (Amend., SG 28/82, SG 21/00) For libel committed under the conditions of the preceeding para, as well as for libel as a result of which grave circumstances have occurred, the punishment shall be a fine of five thousand levs to fifteen thousand levs and public reprobation. (3) Applied in the cases under para 1, item 1 can be para 2 of art. 146. Art. 148a. (New, SG 62/97; amend., SG 21/00) Who divulges verbally, through printed matter or in any other way, data, circumstances or assertions regarding another, based on illegally acquired information from the archives of the Ministry of Interior, shall be punished by a fine of five thousand to twenty thousand levs.

569 *R. v. Barrett*, [2000] O.J. No. 2055. Michael Geist, *Internet Law in Canada*, 3rd ed., (2002) Concord,

to jurisdictional issues. In terms of general provisions, the Canadian Criminal Code contains two crimes of publishing a defamatory libel.[570] The crime of publishing a defamatory libel knowing it to be false has been held to be constitutional in Canada.[571] However, the crime of merely publishing a defamatory libel is of doubtful constitutionality. Defamatory libel is defined to include "insult" but the courts have held that it must be a serious insult. The maximum punishment for publishing a defamatory libel knowing it to be false is five years' imprisonment. The maximum punishment for the crime of publishing a defamatory libel is two years' imprisonment.[572] On the civil side, provincial legislation creates civil liability for defamation (whether in the media or otherwise) through the jurisdiction of the 10 provinces and three territories of Canada. The courts can award damages in such cases, but these damages vary depending on various factors.

In the **Czech Republic**, imprisonment for up to two years or ban of activity shall be imposed on a perpetrator who commits the act of defamation[573] in the press, film, radio, television, publicly accessible computer networks or by other similarly effective means. In **Denmark**, there exists general provisions under the Criminal Code,[574] and these may also apply to the Internet. In **Estonia**, there are no specific legal provisions outlawing libel and insult on the Internet. Nevertheless, there are certain provisions in the Penal Code that cover defamation and insult which could also be applied to the Internet. While these involve certain persons such as state officials,[575] defamation or insult of a private person is not criminalized. However, according to the Code of Civil Procedure, every person has a right of recourse to court for the protection of the person's alleged right or interest protected by law. In **Finland**, defamation is criminalized in the Criminal Code, and a person who spreads false information or a false

---

Ontario: Captus Press at 205 noted that the case settled in 2001.

570 These two crimes are presently found, respectively, in sections 301 and 300 of the Criminal Code.

571 The most important court case to date regarding the constitutionality of the crimes of defamatory libel is *R. v. Lucas*, [1998] 1 S.C.R. 439. See <http://csc.lexum.umontreal.ca/en/1998/1998scr1-439/1998scr1-439.html> for the full judgment. The Supreme Court of Canada held that section 300 of the Criminal Code, publishing a defamatory libel knowing it to be false, required both (a) an intent to defame and (b) knowledge of the falsity of the defamatory libel. The issue is whether the accused knew that the defamatory message, as it would be understood by a reasonable person, was false.

572 However, some courts have concluded that this crime is unconstitutional.

573 Act No. 40/2009 Coll. Penal Code Article 184 – Defamation: (1) Who shall issue a false statement that is capable significantly undermine the seriousness of other to his countrymen, especially harm him in his employment, disrupt his family or to cause him any serious harm/prejudice shall be punished by imprisonment up to one year.

574 Sections 267-275 of the Danish Criminal Code establish liability for defamation. Section 267: A person who defames the character of another by offensive words or deeds or by making or disseminating allegations of an act likely to disparage him in the esteem of his fellow citizens, shall be liable to a fine or imprisonment for any term not exceeding four months. Section 268: If an allegation has been maliciously made or disseminated, or if the issuer has had no reasonable ground to regard it as true, he shall be guilty of defamation and the penalty prescribed by section 267 of this Act may then be increased to imprisonment for any term not exceeding two years. Section 269.-(1): An allegation shall not be punishable if its truth is established or if the issuer of the allegation in good faith has been under an obligation to speak or acted in justified protection of an obvious public interest or his own or another's interest. Section 275.-(1) The offences described in this Part shall be subject to private prosecution.

575 Section 247 of the Penal Code states that defamation or insulting of a person enjoying international immunity or of a family member of such person is punishable by a pecuniary punishment or up to 2 years' imprisonment. If the same act is committed by a legal person, it is punishable by a pecuniary punishment. Section 275 of the Penal Code states that defaming or insulting a representative of state authority or any other person protecting public order, if committed in connection with the performance of his or her official duties by such person, is punishable by a pecuniary punishment or up to 2 years' imprisonment. Note also Section 305 of the Penal Code which includes a provision on defamation and insulting of a court or judge. 416 convictions were recorded for Section 275, and two convictions for section 305 during the reporting period for this report.

insinuation of another person so that the act is conducive to causing damage or suffering to that person, or subjecting that person to contempt, or disparages another in a manner other than referred above shall be sentenced for defamation to a fine or to imprisonment for at most six months.[576] Criticism that is directed at a person's activities in politics, business, public office, public position, science, art or in comparable public activity and that does not obviously overstep the limits of propriety does not constitute defamation.

Defamation, as well as insult and libel, are considered as delicts rather than crimes in **France**.[577] Civil law provisions do also exist in France like in almost all other OSCE participating States. Libel is defined in Article 29 of the Freedom of the Press Act 1881 as "any allegation or imputation of a fact that infringes the honour or reputation of the person or body to which the fact is imputed". In 2000, most terms of imprisonment for libel or insult were repealed. However, libel against a person or a group of persons for reasons of their origin or affiliation with a particular ethnic group, nation, race or religion may be punishable with imprisonment for a term of not more than twelve months.[578] In **Georgia**, while there are no specific legal provisions on libel and insult (defamation) on the Internet, libel and insult are regulated by the Law on Freedom of Speech and Expression which decriminalized defamation in 2004. Defamation proceedings are currently conducted exclusively through the civil courts. The new law holds people liable only for statements of substantial falsehood that damage a person's reputation.[579] Thus, the law creates a favourable environment for free discussion and debate. According to Article 1(1)(W) the term "media" is defined as printed or electronic means of mass communication, including the Internet.

In **Germany**, subject to Section 185 of the Criminal Code, an insult shall be punished with imprisonment of not more than one year or a fine and, if the insult is committed by means of an assault, with imprisonment of not more than two years or a fine.[580] Defamation is regulated by Section 186 of the Criminal Code which states that whoever asserts or disseminates a fact related to another person which may defame him or negatively affect public opinion about him, shall, unless this fact can be proven to be true, be liable to imprisonment of not more than one year or a fine. If the offence was committed publicly or through the dissemination of written materials,[581] then an imprisonment of not more than two years or a fine is provided as penalty by law.[582] As can be seen below, considerable number of prosecutions take place in Germany with regards to sections 185-187 crimes under the Criminal Code.

---

576 Section 9 (Defamation) of the Criminal Code (Chapter 24): A person who spreads false information or a false insinuation about a deceased person, so that the act is conducive to causing suffering to a person to whom the deceased was particularly close, shall be sentenced for defamation. 241 convictions were recorded in 2007, and 319 in 2008.

577 Articles R-621-2, R-624-4 and R-624-5.

578 Article 32(2) of the Law dated 29 July 1891.

579 Moreover, Article 13 distinguishes between public figures and private persons in defamation proceedings. This distinction reflects the well-established principle that public figures, because of their status in society, must tolerate a far greater degree of criticism than ordinary persons.

580 Section 185 of the German Criminal Code.

581 Section 11(3) of the German Criminal Code.

582 Section 187 of the German Criminal Code defines 'intentional defamation' as: Whoever intentionally and knowingly asserts or disseminates an untrue fact related to another person, which may defame him or negatively affect public opinion about him or endanger his trustworthiness shall be liable to imprisonment of not more than two years or a fine; and, if the act was committed publicly, in a meeting or through dissemination of written materials (section 11 (3)) to imprisonment of not more than five years or a fine.

Sections of the Criminal Code (StGB)[583]	2007	2008	2009
Section 185 (insult)	21,914	22,079	22,356
Section 186 (defamation)	231	234	253
Section 187 (intentional defamation)	216	227	238

Table 10. Convictions for sections 185-187 of the German Criminal Code[584]

In **Italy**, Section 594 of the Criminal Code criminalizes slander, and states that whoever offends the honour or dignity of another person in his or her presence is liable of imprisonment for up to six months or a fine for up to 516 EUR. The same penalty is imposed to a person who commits the offence through telegraph or telephone communications, or writings or drawings destined to the offended person. Section 595 of the Criminal Code envisages imprisonment for up to one year or a fine up to 1,032 EUR, if the offence is committed by communicating the defamatory content to more than one person. If the offence is committed against a political, administrative or judicial body, or its representative, or a collegial authority penalties are increased.

Year	Reports	Reported persons
2007	324	113
2008	304	101
2009	184	57
2010 (I Sem)	159	21

Table 11. Statistics provided by the Italy's Postal and Communications Police Service on slander through the Internet

Year	Reports	Reported persons
2008	172	75
2009	797	332
2010 (I Sem)	533	292

Table 12. Statistics drawn up by the Postal and Communications Police Service on defamation through the Internet

In **Kazakhstan**, Articles 129[585] and 130[586] of the Criminal Code envisage criminal responsibility for libel and insult, while the Code of Administrative Offences envisages administrative liability for insult.[587] Through Article 129 of the Criminal Code,[588] the

583 Source: Statistisches Bundesamt (Federal Statistics Office) (ed.), special publication series (Fachserie) 10 "Administration of Justice", series 3 "Prosecution of Offences" (Conviction statistics), table 2.1. The information refers to all persons convicted based on the above stipulations of the law. Crimes committed in connection with the Internet (cybercrimes) are not itemized separately.

584 Source: *Statistisches Bundesamt* (German Federal Statistics Office) (ed.), special publication series (*Fachserie*) 10 "Administration of Justice", series 3 "Prosecution of Offences" (Conviction statistics), table 2.1.

585 According to the Committee on Legal Statistics and Special Accounts of the General Prosecutor's Office of the Republic of Kazakhstan, 40 prosecutions were registered under Article 129 of the Criminal Code in 2008, 33 in 2009, and 20 in the first half of 2010.

586 According to the Committee on Legal Statistics and Special Accounts of the General Prosecutor's Office of the Republic of Kazakhstan, 46 prosecutions were registered under Article 130 of the Criminal Code in 2008, 48 in 2009, and 17 over the first half of 2010.

587 Articles 355, 512-1 and 529.

distribution of deliberately false information (libel) which debases the honour and dignity or another person or undermines his/her reputation is punishable by a fine in the amount of 100 to 250 monthly calculation indices, or in the amount of the salary or other income of the convicted person for up to two months, or by engagement in community service for 120 to 180 hours, or by correctional work for up to one year. Insult is defined as the debasement of the honour and dignity of another person, expressed in an obscene form, and is punishable by a fine of up to 100 monthly calculation indices, or in the amount of the salary or other income of the convicted person for up to one month, or by engagement in community service for up to 120 hours, or by correctional work for up to six months.[589] Furthermore, the Civil Code also includes a provision on the protection of honour, dignity, and business reputation.[590]

In **Kyrgyzstan**, the legislation does not consider libel on the Internet as a separate element of a crime. Libel and insult are criminalized through the Criminal Code, and libel combined with accusation of having committed a grave or especially grave crime is punishable by deprivation of liberty for a term of up to three years.[591] Insult is only punishable with a fine rather than by deprivation of liberty.[592] In **Latvia**, Article 157 of the Criminal Law on "Bringing into Disrepute" prescribes criminal liability for intentional distribution of false facts, knowing them to be untrue, and defamatory of another person (bringing into disrepute), in printed or otherwise reproduced material, if this has been committed publicly (including on the Internet). The applicable penalty, in view of the principle of proportionality, does not involve imprisonment.[593] In **Lithuania**, a person who spreads false information about another person that could arouse contempt for this person or humiliate him or undermine trust in him shall be punished by a fine or by restriction of liberty or by arrest or by imprisonment for a term of up to one year.[594] A person who libels a person accusing him of commission of a serious or grave crime or in the media or in a publication shall be punished by a fine or by arrest or by imprisonment for a term of up to two years.[595]

---

588 Criminal Code of the Republic of Kazakhstan No. 167-I of 16 July 1997 (with amendments and addenda as of 6 October 2010).

589 Article 130 of the Criminal Code of the Republic of Kazakhstan: An insult contained in a public speech, or in a publicly demonstrated work, or in the media is punishable by a fine of 100 to 400 monthly calculation indices, or in the amount of the salary or other income of the convicted person for one to four months, or by engagement in community service for up to 180 hours, or by correctional work for up to one year, or by restraint of liberty for the same period.

590 Article 143 of the Civil Code of the Republic of Kazakhstan (General Part) (adopted by the Supreme Soviet of the Republic of Kazakhstan on 27 December 1994): Through the court, an individual or a legal entity shall have the right to refute information which damages his honour, dignity or business reputation. If the information damaging the honour, dignity or business reputation of a citizen or a legal entity is distributed through the media, that information must be refuted free of charge by the same media. See further Articles 141-146 Civil Code.

591 Article 127(3) of the Criminal Code of the Kyrgyz Republic as amended by Kyrgyz Republic Law No. 309 of 17 December 2009. Amendments to the Criminal Code adopted by the Kyrgyz Parliament on 16 June 2011 decriminalized defamation but left the provisions on insult for cases related to insult of a private individual by another private individual. At the time of writing, the amendments were awaiting promulgation by the President of Kyrgyzstan.

592 Article 128 (Insult) of the Criminal Code of the Kyrgyz Republic

593 According to the data in the Court Information System, seven persons have been convicted under Article 157 of the Criminal Law during the period from 1 January 2007 until 30 June 2010.

594 Article 154(1) (Libel), Criminal Code of the Republic of Lithuania. Note further Article 155 (Insult). In 2007 there were registered 56 crimes under Article 154 and in 2008 this number increased to 59, 1 case was referred to the court.

595 Article 154(2) (Libel), Criminal Code of the Republic of Lithuania. Note further Article 2146 (Insult or Libel of the President of the Republic in the Media), Code of Administrative Offences of the Republic of Lithuania.

In **the former Yugoslav Republic of Macedonia**, while anyone who insults another person shall be punished with a fine, a person who publicly ridicules another person through a computer system because of other person's affiliation with a certain community which is different in terms of race, the colour of the skin, ethnic or national affiliation shall be fined or imprisoned for up to one year.[596] In **Moldova**, any person is entitled to be respected, and his/her honour, dignity and business reputation protected. Therefore, any person is entitled to demand refutation of information denigrating his/her honour, dignity or business reputation, provided that the disseminator of such information cannot prove that it is true. Any person in relation to whom information is distributed denigrating his/her honour, dignity and business reputation shall be entitled, in addition to refutation of such information, to claim reimbursement of losses and material and moral damages caused by distribution thereof.[597] In **Montenegro**, the legal system provides for criminal and civil responsibility for violations of honour and reputation. Just satisfaction in relation to such acts is awarded by the courts as a result of criminal or civil proceedings.[598] The Criminal Code[599] defines as a basic form of the criminal offence of defamation an act of speaking or transmitting untrue information about someone that may harm his/her honour and reputation, while a serious form of this offence is defamation through the media or other similar means or at a public gathering. This is the so called 'public defamation', where the aggravating circumstance is the manner of its commission – a large number of people is informed, thus increasing the danger of harmful consequences. An increased fine is provided for the situations where the spoken or transmitted untrue information results in serious consequences for the injured. However, if the defendant had a reason to believe in the truthfulness of what he/she spoke or transmitted, he/she will not be punished for defamation, but may be punished for insult.

In **Norway**, the penal provisions do not specifically address defamation on the Internet. However, the available provisions under the General Civil Penal Code of 1902 with regards to libel and insult also apply to the Internet.[600] Penalties also include six months' imprisonment. The amended Penal Code of 2005, however, does not any longer contain the defamation provisions.[601] In **Poland**, the offence of libel is criminalized by Article 212 of Penal Code.[602] Furthermore, Article 216 of the Penal Code penalizes the offences of insult and defamation. Fines and imprisonment sentences are provided for whoever commits offences against honour, personal inviolability, insult and defamation. However, a private prosecution is required by law. The **Romanian** criminal law does no longer incriminate libel and insult.[603]

In the **Russian Federation**, there is no specific law that outlaws libel and insult on the Internet. Liability for libel and insult is envisaged without singling out the Internet as a specific place of crime. Article 129 of the Criminal Code envisages liability for libel, and Article 130 of the Criminal Code envisages liability for insult. The term "defamation" is not

596 Article 173 (Insult) of the Criminal Code.

597 Article 16 (Protection of honour, dignity and business reputation), Criminal Code of the Republic of Moldova No. 985-XV dated 18 April 2002. [Article 16 supplemented by Law No. 262-XVI dated 28 July 2006, effective date 11 August 2006]

598 With respect to the criminal aspect of liability for violations of honour and reputation, it should be noted that these criminal offences now carry only a fine, as the principal and the only penalty.

599 On 26 June 2011 major daily newspapers in Montenegro reported that the Parliament had decriminalized libel and insult. Articles 195 (Insult) and 196 (Defamation) were reportedly removed from the Criminal Code completely. At the time of writing, the amendments were awaiting promulgation by the President.

600 See sections 246, 247, and 249 of the General Civil Penal Code 1902.

601 This regulation has not yet entered into force.

602 The Penal Code (Act of 6 June 1997), Chapter XXVII, Article 212 (Offences against Honour and Personal Inviolability).

603 Libel and insult provisions were removed from the Romanian Criminal Code by Law 278/2006.

defined under Russian law.[604] Article 129 of the Criminal Code defines libel as the spreading of deliberately falsified information that denigrates the honour and dignity of another person or undermines his reputation. Liability could result in a fine in the amount up to 80,000 roubles, or in the amount of the wage or salary, or any other income of the convicted person for a period of up to six month, or by compulsory community service for 120 to 180 hours, or by correctional work for a term of up to one year, or restraint of liberty for the same term.[605] Article 130 of the Criminal Code defines insult as the denigration of the honour and dignity of another person, expressed in indecent form. Liability could result in a fine in the amount up to 40,000 roubles, or in the amount of the wage or salary, or any other income of the convicted person for a period of up to three month, or by compulsory community work for a term of up to 120 hours, or by correctional work for a term of up to six months, or by restraint of liberty for up to one year.[606]

In **Serbia**, there are no specific legal provisions outlawing libel and insult on the Internet. All prohibitions that apply to traditional media, apply to the Internet as well. Insult and defamation are criminalized.[607] Insults, and defamation are punished solely with fines, but no imprisonment penalties exist. In **Slovenia**, the Criminal Code has provisions on insult, slander, and defamation.[608] An insult may be punished with a fine or imprisonment for not more than three months. If the offence has been committed through the press, radio, television or other means of public information or at a public assembly, the perpetrator shall be punished by a fine or sentenced to imprisonment for not more than six months.[609] In terms of defamation, whoever asserts or circulates anything false about another person, which is capable of causing damage to the honour or reputation of that person, shall be punished by a fine or sentenced to imprisonment for not more than three months.[610] If the offence is committed through the press, radio, television or other means of public information or at a public assembly, the perpetrator shall be punished by a fine or sentenced to imprisonment for not more than six months. In **Sweden**, the general provisions on defamation,[611] and insulting behaviour[612] within the Penal Code are also applicable to acts on the Internet.

In **Turkmenistan**, there are no separate provisions envisaging liability for defamation and insults over the Internet. General provisions apply indiscriminately to all media including the Internet. Slander (defamation) in a public speech, publications laid open to public or in mass

---

604 See articles 129 and 130 of the Russian Federation Criminal Code.

605 According to Article 129(2) of the Russian Federation Criminal Code, libel contained in a public speech or in a publicly performed work, as well as libel commited in media, shall be punishable by a fine in the amount of up to 120,000 roubles, or in the amount of the wage or salary, or any other income of the convicted person for a period of up to one year, or by compulsory community service for 180 to 240 hours, or by correctional work for a term of one year to two years, or by restraint of liberty for up to two years, or by arrest for a term of three to six months.

606 According to Article 130(2) of the Criminal Code, insult contained in a public speech, in a publicly performed work, or in the media shall be punishable by a fine in the amount of up to 80,000 roubles, or in the amount of the wage or salary, or any other income of the convicted person for a period of up to six months, or by compulsory community service for up to 180 hours, or by correctional work for a term of up to one year, or by restraint of liberty for up to two years.

607 Articles 170 and 171, the Criminal Code of Republic of Serbia (section 17).

608 Articles 158/2, 159/2, 160/2 and Art 161/2 of the Criminal Code (Official Gazette Republic of Slovenia No 55/2008).

609 It should be noted that Article 158(4) states that if the injured person has returned the insult, the Court may punish both parties, or one of them, or may remit the punishment.

610 Article 160 (Defamation) of the Criminal Code. Note also Article 26 of the Mass Media Act (Official Gazette of Republic of Slovenia, Nr.110/2006).

611 Chapter 5, Section 1 and 2 of the Swedish Penal Code.

612 Chapter 5, Section 3 of the Swedish Penal Code.

media may be punished with a fine established at the rate of from ten to twenty average monthly wages, or with correctional labour for the term of up to two years.[613] An insult, which is described as the deliberate humiliation of honour of dignity of the other person expressed in an indecent manner, is punished by an assignment of the responsibility to make amends for the harm caused or by a fine established at the rate of from five to ten average monthly wages. Insulting in a public speech, publications laid open to public or in mass media is punished with a fine established at the rate of from ten to twenty average monthly wages, or with correctional labour for the term of up to one year.[614] Furthermore, there are specific provisions involving insult or slander against the President of Turkmenistan which may be punished by a prison sentence of up to five years.[615]

In **Turkey**, Criminal Code provisions regulate defamation,[616] and any person who acts with the intention to harm the honor, reputation or dignity of another person through concrete performance or giving impression of intent, is sentenced to imprisonment from three months to two years or to a punitive fine. In order to punish the offense committed in absentia of the victim, the act should be committed in presence of least three persons.[617] This provision covers any audiovisual means. The punishment may be increased if the offence is committed against a public officer.

Furthermore, Article 9 of Law No. 5651 deals with private law matters and provides measures of content removal, and right to reply. Under this provision, individuals who claim their personal rights are infringed through content on the Internet may contact the content provider, or the hosting company if the content provider cannot be contacted, and ask them to remove the infringing or contested material. The individuals are also provided with a right to reply under Article 9(1), and can ask the content or hosting provider to publish their reply on the same page(s) the infringing or contested article was published, in order for it to reach the same public and with the same impact, for up to a week. Therefore, the courts can only order the removal or take-down of the infringing content from a website rather than access blocking. The content or hosting providers are required to comply with a 'removal (take down) order' within 48 hours upon receipt of a request.[618] If the request is rejected or no compliance occurs, the individual can take his case to a local Criminal Court of Peace within 15 days, and request the court to issue a take down order and enforce his right to reply as provided under Article 9(1).[619] The Judge residing at the local Criminal Court of Peace should issue its decision without trial within three days. An objection can be made against the decision of the Criminal Court of Peace according to the procedure provided under the Criminal Justice Act. If the court decides in favour of the individual applicant, the content or hosting providers are be required to comply with the decision within two days of

---

613 Article 132 (Slander) The Criminal Code of Turkmenistan. The slander that caused serious consequences, or is aggravated by the accusation of a particularly grave crime shall be punished by a prison sentence of up to three years.

614 Article 133 of the Criminal Code of Turkmenistan.

615 Article 176 (Offences against the President of Turkmenistan) of the Criminal Code of Turkmenistan. Note also Article 192 (Slandering a Judge, Assessor in the People's Court, Prosecutor, Investigation Officer or Investigator), Article 212 (Insulting Public Official), and Article 341 (Insulting Military Servant) of the Criminal Code. Note further Article 19816 (The Insult of an Official of the Customs Authority) of the Administrative Code of Turkmenistan, and Article 5 of the Law "On Print Media and Other Mass Media in the Turkmen SSR".

616 See articles 125-131 (Eight Section: Offenses Against Honor) of the Criminal Code, Law Nr. 5237 Passed On 26.09.2004 (Official Gazette No. 25611 dated 12.10.2004).

617 Article 125 of the Criminal Code.

618 Article 9(1) of Law No. 5651.

619 Article 9(2) of Law No. 5651.

notification.[620] A failure to comply may result in a criminal prosecution and the individuals who act as the content providers or individuals who run the hosting companies could face imprisonment for a period between six months and two years.[621] If the content provider or hosting provider is a legal person, the person acting as the publishing executive or director would be prosecuted. However, despite the availability of the Article 9 mechanism, civil courts of law issue substantial number of blocking orders[622] with respect to allegations of defamation by relying on the Law on Civil Procedure.[623]

In the **United Kingdom**, materials on the Internet are subject to the general civil law on defamation that exists in England and Wales. This area of law is devolved in Scotland and Northern Ireland. In order to launch a defamation complaint, the claimant must prove that the defendant has published, or is responsible for publishing, defamatory material which refers to the claimant. Material is libellous where it is communicated in a permanent form, or broadcast, or forms part of a theatrical performance. If the material is spoken or takes some other transient form, it is classified as slander. Whether the material is defamatory is a matter for the courts to determine. The law of defamation is developed under common law but certain aspects are contained in statutes in particular within the Defamation Acts of 1952 and 1996. It is open to a claimant to bring proceedings against publishers of a defamatory statement. In relation to the Internet, this means that it is possible for a claimant to bring a civil action against the person responsible for posting the defamatory material online and against the ISP responsible for hosting the defamatory content. In the event of the civil action being successful, a defendant may be required to remove the defamatory content, and may also be ordered to pay damages to the claimant. A secondary publisher, such as an ISP, has open to them the defence of innocent dissemination, under section 1 of the Defamation Act 1996. This provides that a defendant will not be liable where he or she is not the author, editor or primary publisher of the statement complained of; took reasonable care in relation to its publication, and did not know, and had no reason to believe, that what he did caused or contributed to the publication of a defamatory statement. Currently, the ISP liability provisions with regards to defamation are under review through a consultation on the Draft Defamation Bill published by the Ministry of Justice.[624]

Legal provisions outlawing the expression of views perceived to be encouraging extremism

In certain OSCE participating States legal provisions on "extremism" or "extreme speech" exist. Therefore the participating States were asked whether **there are specific legal**

620 Article 9(3).

621 Article 9(4).

622 For example Wordpress.com was blocked for approximately 8 months between August 2007 and April 2008. Google Groups ban lasted for nearly 2 months (March-May 2008). Access to Richard Dawkins' website (<http://richarddawkins.net/>) is blocked since September 2008. Dawkins, a British ethologist, evolutionary biologist, and popular science writer is well known for such books like *The Selfish Gene* and *The God Delusion*. See BiaNet, "Evolutionist Dawkins' Internet Site Banned in Turkey," 17 September, 2008 at <http://ww.bianet.org/english/kategori/english/109778/evolutionist-dawkins-internet-site-banned-in-turkey?from=rss>.

623 Akdeniz, Y., & Altiparmak, K., *Internet: Restricted Access: A Critical Assessment of Internet Content Regulation and Censorship in Turkey,* Ankara: Imaj Yayinevi (http://www.imajyayinevi.com/), November 2008. An online version is available through <http://www.cyber-rights.org.tr>. See further Akdeniz, Y., Report of the OSCE Representative on Freedom of the Media *on Turkey and Internet Censorship*, January 2010, at <http://www.osce.org/documents/rfm/2010/01/42294_en.pdf>.

624 See Ministry of Justice, Draft Defamation Bill Consultation, Consultation Paper CP3/11, CM 8020, March 2011: The growth of the Internet and the increase in the use of user generated content has raised concerns that the section 1 (Defamation Act 1996) provisions may be unclear and may not sufficiently protect secondary publishers engaging in multimedia communications.

provisions outlawing the expression of views perceived to be encouraging extremism in their country **(Question 11)**.[625] 20 (35.7%) of the participating States answered with "yes", 26 (46.4%) with "no", and no data was obtained from ten (17.9%) participating States.

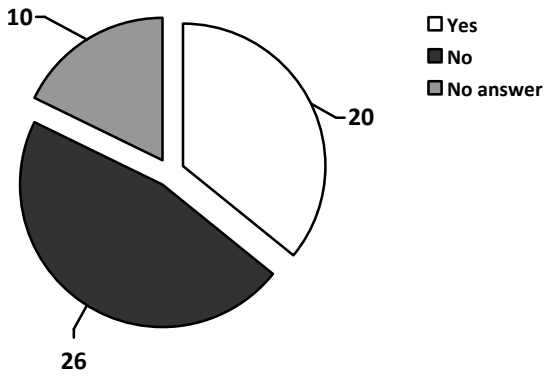


Figure 35. OSCE participating States' responses with regards to specific legal provisions outlawing the expression of views perceived to be encouraging extremism (Question 11)

In terms of the responses received, in **Albania** the regulatory framework of the Criminal Code contains legal provisions outlawing the expression of views encouraging extremism concerning the designated areas of terrorism-related matters, racism and xenophobia, as well as libel and insulting. The Criminal Code includes specific provisions on endangering public peace through calls for national hatred against other parts of the population, insulting or defaming them, or through the use of force or arbitrary actions against them.[626] Furthermore, the defamation of the Republic of Albania and her symbols is also criminalized.[627] The law envisages fines and imprisonment sanctions for breaching the pertinent provisions.[628] However, there exists no specific definition of "extremism" in the domestic legislation in force.

In **Azerbaijan**, the concept of extremism is not defined by law. Certain specific types of extremism are, however, listed in the Criminal Code. For example, Article 101 of the Criminal Code criminalizes occupational incitement to the outbreak of war. This offence is punishable by up to three years of imprisonment. Article 281 criminalizes open incitement against the government, the seizure and retention of power, or altering the constitutional order of the Azerbaijan Republic through violence or through open calls for violating its territorial integrity. The dissemination of such content is punishable by imprisonment for up to five years. The same actions performed repeatedly or by a group of persons are punishable by imprisonment for five to eight years. Internet resources are regarded as merely means by which these crimes may be committed and certain types of inflammatory content might be disseminated. Therefore, the dissemination of such content over the Internet falls under the appropriate sections of the Criminal Code.

---

625 The OSCE participating States were also asked how the law defines these offences, which sanctions (criminal, administrative, civil) are envisaged by law, and the maximum prison term the law envisages for such offences. The OSCE participating States were also asked to provide any statistical information in relation to convictions under these provisions for the reporting period from 1 January 2007 until 30 June 2010 and whether the law (or relevant regulations) prescribes blocking access to websites or any other types of Internet content as a sanction for these offences.

626 Article 266 of the Criminal Code.

627 Article 268 of the Criminal Code.

628 The maximum prison terms envisaged by law for such offences are two years (Article 268) and five years (Article 266).

In the **Czech Republic**, there is no legal definition of "extremism". Extremism is not criminalized and, consequently, cannot be used as "flexible" ground for the criminalization of speech. However, racist, ethnic, religious, national, class or other hatred related discourse with an extremist motive can materialize in "extremist" speech or conduct which may be criminalized as "hatred against race".[629] In **Estonia**, indirect reference to extremism can be found in Section 237 of the Penal Code which criminalizes the preparation of and incitement to acts of terrorism. This section states that organizations training or recruiting persons for the purpose of commissioning or preparing a criminal offence or publicly inciting to criminal offences are punishable by two to ten years' imprisonment. In **Georgia**, there is no specific law outlawing the expression of views perceived to be encouraging "extremism". However, a broad interpretation of Article 9(d) of the Law of Georgia on Freedom of Speech and Expression can include the expression of views perceived to be encouraging extremism within its scope. Namely, Article 9(d) states that freedom of speech and expression may be regulated and limited by law if it is directed towards incitement to commit crime.

German criminal law does not include any regulation that penalizes the encouragement of extremism as such. However, sections 86[630] and 86a[631] of the Criminal Code do criminalize the dissemination of propaganda material of unconstitutional organizations and the use of symbols of unconstitutional organizations. It should be emphasized that the term "propaganda material of unconstitutional organizations" is more restrictive than the term "extremism". Accordingly, the encouragement of extremism is governed by Sections 86 and 86a of the Criminal Code only if it takes the form of unconstitutional propaganda being disseminated. The maximum term of imprisonment amounts to three years for both of these offences. As

---

629 See e.g. Article 356 (Incitement to hatred against a group of persons or to restrict their freedoms and rights), or Article 403 (Establishment, support and promotion of movements aimed at suppressing human rights and freedoms) of the Penal Code.

630 Section 86 German Criminal Code (Dissemination of Means of Propaganda of Unconstitutional Organizations): (1) Whoever domestically disseminates or produces, stocks, imports or exports or makes publicly accessible through data storage media for dissemination domestically or abroad, means of propaganda: 1. of a party which has been declared to be unconstitutional by the Federal Constitutional Court or a party or organization, as to which it has been determined, no longer subject to appeal, that it is a substitute organization of such a party; 2. of an organization, which has been banned, no longer subject to appeal, because it is directed against the constitutional order or against the idea of international understanding, or as to which it has been determined, no longer subject to appeal, that it is a substitute organization of such a banned organization; 3. of a government, organization or institution outside of the territorial area of application of this law which is active in pursuing the objectives of one of the parties or organizations indicated in numbers 1 and 2; or 4. means of propaganda, the contents of which are intended to further the aims of a former National Socialist organization, shall be punished with imprisonment for not more than three years or a fine. (2) Means of propaganda within the meaning of subsection (1) shall only be those writings (Section 11 subsection (3)) the content of which is directed against the free, democratic constitutional order or the idea of international understanding. (3) Subsection (1) shall not be applicable if the means of propaganda or the act serves to further civil enlightenment, to avert unconstitutional aims, to promote art or science, research or teaching, reporting about current historical events or similar purposes. (4) If guilt is slight, the court may refrain from imposition of punishment pursuant to this provision.

631 Section 86a (Use of Symbols of Unconstitutional Organizations): (1) Whoever: 1. domestically distributes or publicly uses, in a meeting or in writings (Section 11 subsection (3)) disseminated by him, symbols of one of the parties or organizations indicated in Section 86 subsection (1), nos. 1, 2 and 4; or 2. produces, stocks, imports or exports objects which depict or contain such symbols for distribution or use domestically or abroad, in the manner indicated in number 1, shall be punished with imprisonment for not more than three years or a fine. (2) Symbols, within the meaning of subsection (1), shall be, in particular, flags, insignia, uniforms, slogans and forms of greeting. Symbols which are so similar as to be mistaken for those named in sentence 1 shall be deemed to be equivalent thereto. (3) Section 86 subsections (3) and (4), shall apply accordingly.

can be seen below a considerable number of convictions have been secured with regards to Section 86 and Section 86a crimes under the Criminal Code in Germany.

Section 86 of the Criminal Code	Total number of convictions
2007	1112
2008	1139
2009	1022
Section 86a of the Criminal Code	Total number of convictions
2007	778
2008	816
2009	801

Table 13. Sections 86 and 86a convictions under the German Criminal Code

Irish law also does not specifically criminalize the expression of views perceived to be encouraging "extremism". Article 40(6) of the Constitution guarantees citizens the rights to express freely their convictions and opinions and to form associations and unions. Prosecutions under the Prohibition of Incitement to Hatred Act 1989 are for the judge to decide on consideration of all the facts presented during a criminal trial, whether any alleged conduct was intended or likely to stir up hatred. If the Court considers that the conduct was intentional or likely to stir up hatred it can be considered a criminal offence as provided for under Section 2 of the 1989 Act.

In **Kazakhstan**, the legal and institutional framework for combating extremism in order to protect the rights and freedoms of a person and a citizen, the foundations of the constitutional system, the sovereignty of the Republic of Kazakhstan, integrity, inviolability and inalienability of its territory, and national security are all contained in the Law "On Countering Extremism" of 2005.[632] The Law defines extremism as the organization and/or commission

> by an individual and/or legal entity, a group of individuals and/or legal entities of acts on behalf of organizations duly recognized as extremist;
> by an individual and/or legal entity, a group of individuals and/or legal entities of acts directed at: a forced change in the constitutional system; violating the sovereignty of the Republic of Kazakhstan and the integrity, inviolability and inalienability of its territory; undermining national security and state defence capacity; forced seizure of power or forced holding of power; creating, supervising and participating in illegal paramilitary formations; organizing an armed revolt and participating in it, inciting social and class strife (political extremism);
> inciting racial, national, and tribal strife, specifically, if it involves violence, or calls for violence (national extremism);
> inciting religious enmity or strife, specifically, if it involves violence, or calls for violence, as well as the use of any religious practice posing a threat to the safety, life, health, morality or rights and freedoms of citizens (religious extremism).

Furthermore, Article 7 defines the responsibility of government bodies (national security and internal affairs bodies) for identifying and intercepting extremism.[633] The manufacture,

---

632 The Law of the Republic of Kazakhstan No. 31-III of 18 February 2005 "On Counteracting Extremism".

633 Article 7(2) states that "upon detection of instances of violation of the legislation of the Republic of Kazakhstan in counteracting extremism by individuals and legal entities and/or their structural divisions (branches and representative offices) or if information is available testifying to the preparation of illegal acts, as well as if extremist materials are distributed via the media which could be detrimental to human and

possession, import, transportation, and dissemination in the territory of the Republic of Kazakhstan of media products and other products involving and justifying extremism or terrorism, as well as revealing the techniques and tactics of antiterrorist operations during their implementation is criminalized by the Code on Administrative Offences.[634] This offence is punishable by a fine. Furthermore, a number of offences under the Criminal Code also contain elements of extremism.[635]

In terms of the Internet, the Law on Counteracting Extremism prohibits the use of networks and media for engaging in extremism, and publishing and distributing extremist materials.[636] If networks or the media are used for engaging in extremism, bodies carrying out special investigations according to the law of Kazakhstan shall have the authority to suspend the activity of such networks and media. Furthermore, the activity of networks and media shall be prohibited by the courts as envisaged by respective legislation. Information material distributed within Kazakhstan and containing elements of extremism shall be recognized as extremist by the courts in accordance with a statement from a public prosecutor. Its conveyance, publication and distribution shall be prohibited. The court is required to base its ruling on the material's extremist nature which has to be established by a forensic investigation.

In **Latvia**, the notion of "extremism" is not defined by law, and, hence, there are no provisions concerning liability of an individual for expressing his or her personal opinion even if the ideas expressed might be regarded as "extreme". However, this does not apply to cases where supporting "extremism" is connected with incitement to genocide,[637] justification of genocide, crimes against humanity, crimes against peace, and war crimes,[638] incitment to war of aggression,[639] inciting national, ethnic, and racial hatred,[640] inciting to forcibly overthrow the Government of the Republic of Latvia, and forcibly change the political

---

citizen rights and freedoms, as well as to the interests of legal entities, society, and the state, prosecutors shall issue acts of prosecutor's supervision on the elimination of any manifestations of extremism, the causes and conditions conducive to its commission, and on restoration of the violated rights; submit statements to court on the suspension and banning of the activity of organizations engaging in extremism; and engage in criminal prosecution as prescribed by the laws of the Republic of Kazakhstan."

634 Article 344 of the Code of the Republic of Kazakhstan on Administrative Offences No. 155-II of 30 January 2001 (with amendments and addenda as of 06 October 2010).

635 The crimes stipulated by Articles 164, 168-171, 233-3, 23, Art. 337 (2 and 3), and Art. 337-1 of the Criminal Code of the Republic of Kazakhstan No. 167-I of 16 July 1997 (with amendments and addenda as of 06 October 2010) shall be recognized as crimes containing elements of extremism: Article 164. Incitement of Social, National, Tribal, Racial, or Religious Enmity; Article 168. Forced Seizure of Power or Forced Holding of Power or Performance by Representatives of a Foreign State or a Foreign Organization of Powers Constituting the Competence of Authorized Bodies and Officials of the Republic of Kazakhstan; Article 169. Armed Mutiny; Article 170. Calls to Carry out Forced Overthrow or Change in the Constitutional Order, or Forced Violation of the Territorial Integrity of the Republic of Kazakhstan; Article 171. Sabotage; Article 233-3. Financing Extremism or Terrorist Activity; Article 236. Organization of an Illegal Paramilitary Formation; Article 337. Creation or Participation in the Activity of Illegal Public and Other Associations; Article 337-1. Organization of the Activity of a Public or Religious Association or Other Organization after the Issue of a Court Ruling Banning its Activity or its Liquidation due to its Engaging in Extremism.

636 Article 12 of the Law of the Republic of Kazakhstan No. 31-III of 18 February 2005 "On Counteracting Extremism".

637 Article 711 of the Criminal Code.

638 Article 741 of the Criminal Code.

639 Article 77 of the Criminal Code on Incitement to War of Aggression, provides that for incitement to a war of aggression or to instigation of military conflict, the applicable sentence is deprivation of liberty for a term up to eight years.

640 Article 78 of the Criminal Code.

system,[641] incitement to terrorism or terrorism threat,[642] or incitement of religious hatred,[643] all of which qualify as criminal offences.[644]

In **Moldova**, extremism is defined as "a position, doctrine of certain political trends that, on the basis of extreme theories, ideas or views, strive to impose their programme by violent or radical means."[645] An extremist organization is defined as a public or religious organization, medium or other organization in relation to which, on the grounds envisaged by the law, the court has issued a court ruling that has come into legal effect to terminate or suspend its activities in connection with performance of extremist activities. Furthermore, materials of an extremist nature are defined as documents or information recorded on any media, including anonymous ones, intended for disclosure and for incitment to performance of extremist activities, justifying or validating the need to perform such activities and justifying the practice of committing military or other crimes for the purpose of complete or partial annihilation of any ethnic, social, racial, national or religious group.[646] It is therefore prohibited for the media in Moldova to distribute materials of an extremist nature or engage in extremist activities.[647] In cases where media distribute such material or disclose facts that testify to elements of extremism in their activities, the state authority that registered the given medium or the public prosecutor shall issue a warning in writing to the founder and/or editors/Editor-in-Chief of the given medium concerning the prohibited nature of such acts or activities, indicating the specific violations committed.[648] Termination or suspension of the

---

641 Article 81 of the Criminal Code on Incitement to Forcibly Overthrow the Government of the Republic of Latvia and Forcibly Change the Political System, provides for criminal liability for a person who commits public incitement to violently overthrow the government of the Republic of Latvia as established by the Constitution, or to violently change the political system, or commits the distribution of materials containing such incitement for the same purpose. The applicable sentence is deprivation of liberty for a term up to five years or a fine not exceeding one hundred times the minimum monthly wage.

642 Article 882 of the Criminal Code.

643 Article 150 of the Criminal Code.

644 According to the data in the Court Information System, there have been no convictions under Article 77 of the Criminal Law during the period from 1 January 2007 to 30 June 2010; two persons have been convicted under Article 81 of the Criminal Law.

645 Article 1, Law of the Republic of Moldova "On Countering Extremist Activities".

646 Extremist activities are defined by law as activities of a public or religious association, medium or other organization or individual to plan, organize, prepare for or carry out acts geared to violent change of the foundations of the constitutional system and violation of the integrity of the Republic of Moldova; undermining of the security of the Republic of Moldova; seizure of state power or unauthorized assumption of the powers of an official; establishment of illegal armed formations; performance of terrorist activities; incitement to racial, ethnic or religious strife, as well as social unrest connected with violence or calls to violence; denigration of national dignity; provocation of mass disorders, performance of acts of hooliganism or vandalism for motives of ideological, political, racial, ethnic or religious hatred or enmity, as well as for motives of hatred or enmity towards a particular social group; and propaganda of exclusivity, supremacy or inferiority of citizens with respect to religion or race, nationality, ethnic origins, language, religion, sex, views, political affiliation, material status or social origins; propaganda and public demonstration of Nazi attributes or symbols, attributes or symbols identical or confusingly similar to Nazi attributes or symbols; financing or other promotion of the activities or acts indicated in clauses a) and b), specifically by providing funding, real estate, training, printing, material or technical resources, telephone, fax or other means of communications, other inventories and information services; and public incitement to perform the activities or action indicated.

647 Article 7 (Liability of the media for distributing materials of an extremist nature and engaging in extremist activities) Law of the Republic of Moldova "On Countering Extremist Activities", No. 54-XV dated 21 February 2003. Note also Article 9 (Combating distribution of materials of an extremist nature) of the same law.

648 Article 7(2). If it is possible to take steps to eliminate the violations committed, the submission/warning should also set the deadline for elimination of the violations, this being one month from the date on which the submission is made/warning is issued.

activities of the given medium for a period of up to one year is possible if extremist activities continue.[649]

In the **Russian Federation**, the expression of views on the Internet is not restricted by law. However, the Russian Ministry of Internal Affairs has drawn up a federal draft law[650] that supplements certain articles of the Russian Federation Criminal Code envisaging criminal punishment for committing extremist crimes using public information and telecommunication networks, including the Internet. Furthermore, Russian law provides for liability for the manufacture, possession or distribution of extremist materials. In accordance with Article 1 of Federal Law "On Counteraction of Extremist Activity"[651], extremist activity implies, among others, the public justification of terrorism and other terrorist activity; the incitation of racial, national or religious strife; propaganda of the exclusiveness; superiority or deficiency of individuals on the basis of their attitude to religion, social, racial, national, religious or linguistic identity; the violation of rights, liberties and lawful interests of individuals and citizens on the basis of their attitude to religion, social, racial, national, religious or linguistic identity; public appeals to perform the said acts or mass distribution of knowingly extremist materials, as well as their production or possession for the purpose of mass distribution.

Subject to Article 13, and paragraph 7 of the Regulations of the Ministry of Justice,[652] the Russian Ministry of Justice is charged with the management and publishing of the federal list of extremist materials. The Ministry publishes the list which currently contains 889 items on its website, including books, newspapers, brochures, flyers, CDs, DVDs, images, and video files, blogs, and websites.[653] Courts can order the inclusion of content deemed to be extreme.

Article 15 of the Federal Law No. 114-FZ states that for the exercise of extremist activity citizens of the Russian Federation, foreign nationals and stateless persons shall bear criminal, administrative and civil law responsibility as envisaged by the legislation of the Russian Federation. Furthermore, Article 280(1) of the Criminal Code states that public appeals to the performance of extremist activity shall be punishable by a fine in an amount of up to 300,000 roubles (ca. 7,400 euros), or in the amount of the wage or salary, or any other income of the convicted person for a period of up to two years, or by arrest for a term of four to six months, or by imprisonment of up to three years.

In **Serbia**, there is no legal definition of "extremism" provided by law. However, the Criminal Code prohibits instigating national, racial and religious hatred and intolerance.[654] In **Ukraine**,

---

649 Article 7(4).

650 The addenda to the Russian Federation Criminal Code proposed by the draft law also require making simultaneous changes to the Russian Federation Criminal Procedural Code and Federal Law No. 35-FZ of 6 March 2006 "On Counteracting Terrorism."

651 Federal Law No. 114-FZ of 25 July 2002

652 Approved by a Decree of the President of the Russian Federation on 13 October 2004, No. 1313

653 See <http://www.minjust.ru/ru/activity/nko/fedspisok/>.

654 Article 317 (Instigating National, Racial and Religious Hatred and Intolerance) of the Criminal Code: "Whoever instigates or exacerbates national, racial or religious hatred or intolerance among the peoples and ethnic communities living in Serbia, shall be punished by imprisonment of six months to five years. If the offence specified in paragraph 1 of this Article is committed by coercion, maltreatment, compromising security, exposure to derision of national, ethnic or religious symbols, damage to other persons, goods, desecration of monuments, memorials or graves, the offender shall be punished by imprisonment of one to eight years. Whoever commits the offence specified in paragraphs 1 and 2 of this Article by abuse of position or authority, or if these offences result in riots, violence or other grave consequences to co-existence of peoples, national minorities or ethnic groups living in Serbia, shall be punished for the offence specified in paragraph 1 of this Article by imprisonment of one to eight years, and for the offence specified in paragraph 2 of this Article by imprisonment of two to ten years."

the manufacture and distribution of products that incite war, national and religious hatred is prohibited.[655] In **Sweden**, the Penal Code contains a provision on inciting rebellion.[656] Subject to this provision a person who orally, before a crowd or congregation of people, or in a publication distributed or issued for distribution, or in other message to the public, urges or otherwise attempts to entice people to commit a criminal act, evade a civic duty or disobey public authority, shall be sentenced for inciting rebellion to a fine or imprisonment for up to six months.

Legal provisions outlawing the distribution of "harmful content"

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

The participating States were asked whether **they have specific legal provisions outlawing the distribution of "harmful content" (i.e. content perceived to be "harmful" by law)** in place **(Question 12)**.[657] 19 (33.9%) participating States responded that there are such laws in their jurisdiction. However, in 26 (46.5%) participating States no such legal provisions exist. No data was obtained from 11 (19.6%) participating States.

It should be noted, however, that from the responses received it is not apparent whether the below listed national legal provisions on harmful content cover or apply to the Internet in each case.

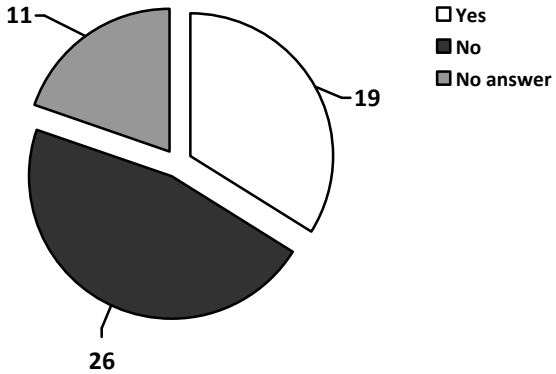


Figure 36. OSCE participating States' responses with regards to specific legal provisions outlawing the distribution of "harmful content" (Question 12)

655 Article 2 of Law of Ukraine "On protection of public morality". Note also Article 295 of the Criminal Code of Ukraine.

656 Chapter 16, Section 5 of the Swedish penal Code.

657 The participating States of the OSCE were also asked how these offences are defined by law, whether and how "harmful content" is defined by law, which sanctions (criminal, administrative, civil) are envisaged by law, the maximum prison term envisaged by law for such offences, any statistical information in relation to convictions under such provisions for the reporting period of 01 January 2007 – 30 June 2010, and whether the law (or relevant regulations) prescribes blocking access to websites or any other types of Internet content as a sanction for these offences.

In **Croatia**, the distribution of "harmful content" is prohibited by the Ordinance on the Manner and Conditions of Provision of Electronic Communications Networks and Services within the scope of Principles and General Rules for the Provision of Services.[658] According to the Ordinance, services, as well as activities for their promotion, shall be legal, and in compliance with social values, for the purpose of protection of users. Services shall not be provided nor promoted in such a manner as to offend or abuse the position and/or characteristic of individuals or group of persons, e.g. persons with special needs such as children.

In the **Czech Republic**, the provider of an audiovisual media services on-demand shall ensure that minors in the area of transmission will not normally hear or see broadcasts that may seriously affect the physical, mental or moral development of minors.[659] If the provider of an audiovisual medial service breaches this provision, an administrative fine up to 2.000.000 CZK (ca. 77,000 euros) shall be imposed. In **Georgia**, Article 3 of the "Regulations of the provision of services in the field of electronic communications and protections of consumers' rights" defines pornography, items featuring especially grave forms of hatred, violence, invasion of a person's privacy, as well as slander and insults as inadmissible production.

In **Italy**, the distribution of certain publications which may offend children's moral sense or may incite them to corruption, crime or suicide[660] is prohibited considering children's characteristic sensitivity.These provisions also apply to the Internet. The distribution of publications with shocking or gruesome content is also prohibited.[661]

In **Lithuania**, Article 17(1) of the Law on Provision of Information to the Public states that producers and/or disseminators of public information must ensure that minors are protected from public information which might have a detrimental effect on their physical, mental or moral development, in particular public information that involves pornography and/or violence or disseminates information encouraging addictions. In **Luxembourg**, the Criminal Code prohibits selling or distribution of indecent material or material which impairs the imagination of children to children under the age of 16.[662] In **the former Yugoslav Republic of Macedonia**, the Law on Broadcasting regulates the content of the programme, which may be, mutatis mutandis, applicable to the Internet. Therefore, provision of unencrypted pornography and excessive violence, which can affect children and minors is prohibited.

Legal provisions outlawing any other categories of Internet content

The survey asked whether the OSCE participating States have **specific legal provisions outlawing any other categories of Internet content (Question 13)**.[663] While in 15 (26.8%)

---

658 Article 3 Appendix 5, of the Ordinance on the Manner and Conditions of Provision of Electronic Communications Networks and Services as published in the Official Gazette 154/08.

659 Article 6(3) of Act No. 132/2010 Coll. on Audiovisual Medial Services on Demand.

660 Section 14 (Publications for Children or Teenagers), Act No. 47 of 8 February 1948 – Provisions on the Press. The same provisions shall apply to children's magazines and periodicals systematically or repeatedly depicting detective stories and adventures so as to facilitate unleashing of instincts of violence and social indiscipline.

661 Section 15 (Publications with shocking or gruesome content), Act No. 47 of 8 February 1948.

662 Article 385bis. of the Criminal Code.

663 The OSCE participating States were also asked how these offences are defined by law, which sanctions (criminal, administrative, civil) are envisaged by law, the maximum prison term envisaged by law for such offences, any statistical information in relation to convictions under such provisions for the reporting period from 1 January 2007 until 30 June 2010, and whether the law (or relevant regulations) prescribes blocking access to websites or any other types of Internet content as a sanction for these offences.

participating States such laws exist, 30 (53.6%) participating States do not have such legal provisions. No data was obtained from 11 (19.6%) participating States.

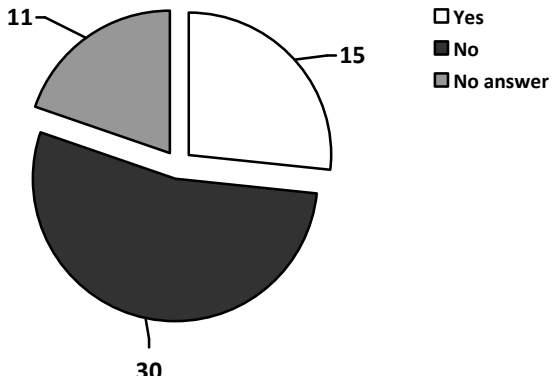


Figure 37. OSCE participating States' responses with regards to specific legal provisions outlawing any other categories of Internet content (Question 13)

In **Albania**, there are legal provisions which under specific conditions outlaw the circulation of unsolicited commercial communications, the access and storage of personal data and confidential information (privacy), the eavesdropping of telecommunications, the unauthorized access and abuse of computer data and computer systems, the training for the production and disposal of weaponry and hazardous substances, and the programming of private and public radio and television operators. The various legal provisions envisage sanctions of fines and imprisonment for contraventions of the pertinent provisions.

In **Belarus**, the law does not contain any separate rules prescribing liability for distributing information through the Internet. In the event of a violation of a legislative prohibition, the appropriate liability is imposed irrespective of the means by which the information is distributed. For example, the Criminal Code provides liability for distributing information about private lives,[664] deliberately false information damaging a competitor's business reputation,[665] false information about goods and services,[666] and malicious software.[667] In the **Czech Republic**, the unauthorized disclosure of secret information,[668] or personal data accumulated by public authority,[669] or private messages and communications[670] is prohibited whether on the Internet or elsewhere. In **Denmark**, according to Section 140 of the Criminal Code, a person who, in public, ridicules or insults the dogmas or worship of a religious community that exists lawfully in Denmark shall be liable to a fine or imprisonment not exceeding four months. In **Italy**, the training or delivery of instructions concerning manufacturing or use of explosive materials, and weapons is prohibited through electronic networks.[671] In **Kazakhstan**, the disclosure of information constituting state secret or other

664 Article 179 of the Criminal Code.
665 Article 249 of the Criminal Code.
666 Article 250 of the Criminal Code.
667 Article 354 of the Criminal Code.
668 Articles 317 and 318 of the Criminal Code.
669 Articles 317 and 318 of the Criminal Code.
670 Article 180 of the Criminal Code.
671 Section 2 bis of Act No 895 of 2 October 1967, introduced by section 8 of Act No 155 of 31 July 2005: Whoever, outside the cases allowed by legal provisions of Acts or regulations, trains someone or delivers instructions in any form, also anonymously, or through electronic transmission, relating to the manufacturing or use of explosive materials, war weapons, chemical aggressors or harmful or dangerous bacteriological substances and other lethal devices shall be punished, unless the offence is a more serious one, with imprisonment from one to six years.

secret protected by the law, propaganda and justification of extremism or terrorism, distribution of information revealing the techniques and tactics of antiterrorist operations during their implementation, promotion of drugs, psychotropic substances and their precursors, as well as the cult of cruelty, violence and pornography are prohibited.[672] In **Lithuania**, Article 8 of the Law on the Protection of Minors against the Detrimental Effect of Public Information establishes that the restrictions established for the public information assigned to public information having a detrimental effect on the development of minors shall also apply to advertising, self-promotion, announcements and trademarks. In **Moldova**, war propaganda is outlawed by the Criminal Code.[673] In the **United Kingdom**, under section 2(1) of the Suicide Act 1961,[674] it is an offence to do an act capable of encouraging or assisting the suicide or attempted suicide of another person with the intention to encourage or assist. The law applies to online actions in exactly the same way as it does offline. It applies whether or not the defendant knows or has identified the person assisted or encouraged and whether or not a suicide takes place. The maximum penalty for an offence under section 2(1) is 14 years' imprisonment.

Conclusion to Part B

Part B of this report has shown that legal provisions that criminalize racist content (or discourse), xenophobia, and hate speech, the denial, gross minimisation, approval or justification of genocide or crimes against humanity, incitement to terrorism, terrorist propaganda, child pornography, obscene and sexually explicit (pornographic) content, libel and insult (defamation), the expression of views perceived to be encouraging extremism, and the distribution of harmful content exist in many OSCE participating States. A considerable number of legal provisions have been introduced, and/or existing provisions have been amended over the last few years.

Most of the existing legal provisions criminalizing content are applicable to any medium and not specific to the Internet. Therefore, legal measures, and criminal sanctions can also be used to regulate content and conduct over the Internet. However, some OSCE participating States have developed new legal provisions specifically with regards to the Internet. As a result, this increased legislation of online content has led to challenging restrictions on the free flow of information and the right to freely impart and receive information on and through the Internet.

It is noted that definitional problems and inconsistencies exist with regards to certain speech based restrictions. Clarifications are needed to define what amounts for example to "extremism", "terrorist propaganda", "incitement to terrorism", "harmful content", "racist content", and "hate speech". As set forth in Article 10 of the European Convention on Human Rights, freedom of expression is subject to exceptions, which must, however, be construed strictly, and the need for any restrictions must be established convincingly by the States.[675]

---

672 Article 2(3) (Freedom of Speech, Receipt and Dissemination of Information) of the Law of the Republic of Kazakhstan No. 451-I of 23 July 1999 "On the Media".

673 Article 140 (War propaganda) of the 2010 Criminal Code of the Republic of Moldova No. 985-XV dated 18 April 2002 Republished in: Monitorul Oficial of the Republic of Moldova No. 72-74/195 dated 14 April 2009, Monitorul Oficial of the Republic of Moldova No. 128-129/1012 dated 13 September 2002: War propaganda, distribution of tendentious and invented information capable of inciting war or other actions for the purpose of unleashing war, carried out verbally, in writing, by radio, television, cinema or other means shall be punishable by a fine in an amount of up to 500 conventional units or imprisonment for a period of up to 6 years, with deprivation, in both cases, of the right to hold certain positions and engage in certain activities for a period of up to 5 years.

674 As amended by section 59 of the Coroners and Justice Act 2009.

675 See, among several other authorities, *Nilsen and Johnsen v. Norway* [GC], no. 23118/93, § 43, ECHR 1999-VIII, and *Fuentes Bobo v. Spain*, no. 39293/98, § 43, 29 February 2000.

Under the established principles of the European Court of Human Rights, the citizens must be able to foresee the consequences which a given action may entail,[676] and sufficient precision is needed to enable the citizens to regulate their conduct.[677] At the same time, whilst certainty in the law is highly desirable, it may bring in its train excessive rigidity as the law must be able to keep pace with changing circumstances. The level of precision required of domestic legislation[678] – which cannot in any case provide for every eventuality – depends to a considerable degree to the content in question, the field it is designed to cover and to the number and status of those to whom it is addressed.[679]

Furthermore, a considerable number of participating States are yet to decriminalize defamation. Harsh prison sentences or severe financial penalties continue to exist with regards to defamation and insult. The European Court of Human Rights recalled in a number of its judgments that while the use of criminal law sanctions in defamation cases is not in itself disproportionate,[680] the nature and severity of the penalties imposed are factors to be taken into account.[681] Within this context, it is important to remind that the Parliamentary Assembly of the Council of Europe adopted the Resolution 1577 "Towards decriminalisation of defamation", in which it urged those member States which still provide for prison sentences for defamation, even if they are not actually imposed,[682] to abolish them without delay.[683]

It is also noted that the development of so-called "three-strikes" legal measures to combat Internet piracy in a number of participating States is worrisome. These measures provide a "graduated response" resulting in restricting or cutting off the users' access to the Internet in cases where a user has attempted to download allegedly illegal copyright protected material. The third strike usually leads to the user's access to the Internet being completely cut off. This disproportionate response is incompatible with OSCE commitments on freedom to seek, receive and impart information, which are vital to democracy, and in fact are strengthened by Internet access. An interference with such a fundamental human right must be motivated by a pressing social need, whose existence must be demonstrated by the OSCE participating States and such interference must be proportionate to the legitimate aim pursued.[684] This report, in conclusion to Section A, recognized access to the neutral Internet as a fundamental human right, and therefore "graduated response" mechanisms which could restrict users' access to the Internet should be avoided by the OSCE participating States.

Finally, it should be pointed out that a considerable number of OSCE participating States which responded to the OSCE RFOM questionnaire did not provide requested data, especially

---

676 *Lindon, Otchakovsky-Laurens and July v. France* [GC], nos. 21279/02 and 36448/02, § 41, ECHR 2007-XI. See further *Kafkaris v. Cyprus* [GC], no. 21906/04, § 140, ECHR 2008.

677 *Groppera Radio AG and Others v. Switzerland*, 28 March 1990, § 68, Series A no. 173.

678 See the *Sunday Times* v. the United Kingdom (no. 1) judgment of 26 April 1979, Series A no. 30, p. 31, § 49; the Larissis and Others v. Greece judgment of 24 February 1998, *Reports* 1998-I, p. 378, § 40; *Hashman and Harrup v. the United Kingdom* [GC], no. 25594/94, § 31, ECHR 1999-VIII; and *Rotaru v. Romania* [GC], no. 28341/95, § 52, ECHR 2000-V

679 See generally in this connection, *Rekvényi v. Hungary* [GC], no. 25390/94, § 34, ECHR 1999-III.

680 See *Radio France and Others v. France*, no. 53984/00, § 40, ECHR 2004-II; *Lindon, Otchakovsky-Laurens and July v. France* [GC], nos. 21279/02 and 36448/02, § 59, ECHR 2007-XI; *Długołęcki v. Poland*, no. 23806/03, § 47, 24 February 2009; and *Saaristo and Others v. Finland*, no. 184/06, § 69 *in limine*, 12 October 2010.

681 See *Cumpănă and Mazăre v. Romania* [GC], no. 33348/96, § 111, ECHR 2004.

682 Note case of *Sabanovic v. Montenegro and Serbia*, Application no. 5995/06, Judgment of 31.05.2011.

683 See Parliamentary Assembly of the Council of Europe, Resolution 1577: Towards decriminalisation of defamation, 2007, at <http://assembly.coe.int/main.asp?Link=/documents/adoptedtext/ta07/eres1577.htm>.

684 See *Olsson v. Sweden (No. 1)*, judgment of 24 March 1988, Series A no. 130, § 67, and *Bladet Tromsø and Stensaas v. Norway* [GC], no. 21980/93, ECHR 1999-III.

with regards to statistical information in relation to convictions under relevant law(s) for the reporting period from 1 January 2007 until 30 June 2010. In the absence of reliable statistical data, or any data with regards to prosecutions and convictions involving the above mentioned content related legal provisions, it is impossible to reach conclusions on whether these content related crimes are committed over the Internet. OSCE participating States should therefore study the effectiveness of laws and other measures regulating Internet content, improve their data gathering and keeping, and make such data publically available.

C. Blocking, Filtering, and Content Removal

Despite the introduction of new laws, or amendments to existing laws, and the criminalization of the publication or distribution of certain types of content, in almost all instances extraterritoriality remains a major problem for Internet regulation. Content is often hosted or distributed from outside the jurisdiction in which it is considered illegal. As it was outlined in Part B of this report, laws are not necessarily harmonised at the OSCE level, let alone on a pan-European level. What is considered illegal in one state may be perfectly legal in another. Different rules, laws, and regulations exist based upon different cultural, moral, political, constitutional, and religious values. These differences will continue to exist and undoubtedly complicate efforts to find an appropriate balance between the right to freedom of expression and the prohibition of certain types of content deemed to be illegal by state authorities.

Based on the limited effectiveness of state laws, and lack of harmonization at international level a number of states started to block access to Internet websites and social media platforms that allegedly contain illegal content which are situated outside their legal jurisdiction. Blocking access to content seems to be faster, easier and a more convenient solution in cases where state authorities are unable to reach the perpetrators for prosecution, where mutual legal assistance agreements are not in place, or where the request for removal of such content is rejected by hosting or content providers in the countries in which the allegedly illegal content is hosted.

However, as will be seen below, blocking measures are not always provided by law, nor are they always subject to due process principles. Furthermore, blocking decisions are not necessarily taken by the courts of law, and often administrative bodies or Internet hotlines run by the private sector single handedly decide which content, website, or platform should be blocked. Blocking policies often lack transparency, and administrative bodies (including hotlines) lack accountability. Appeal procedures are either not in place, or where they are in place, they are often not efficient. Therefore, increasingly, the compatibility of blocking with the fundamental right of freedom of expression must be questioned.

Part C of this report will assess relevant policy developments within the European Union and Council of Europe and significant developments in the OSCE region with regards to blocking, filtering, and content removal policies that are adopted and implemented. For this purpose, the OSCE participating States were asked whether they have specific

- legal provisions which require closing down and/or blocking access to websites or any other types of Internet content (**Question 14**)
- legal provisions which require blocking access to web 2.0 based applications and services such as YouTube, Facebook, or Blogger (**Question 15**)
- legal provisions requiring schools, libraries, and Internet cafes to use filtering and blocking systems and software (**Question 18**)

European Union and Council of Europe policies and projects on blocking access to websites

EU perspectives on blocking access to allegedly illegal content

The development of policies to detect misuse of the Internet by extremist websites and to enhance inter-state co-operation against terrorist use of the Internet was included within the

context of the European Union's May 2006 revised Action Plan on Terrorism.[685] While it was also considered to adopt "legal measures obliging Internet service providers to remove or disable access to the dissemination of terrorist propaganda they host"[686] this policy option has been ruled out with regards to the proposal for a Council Framework Decision on combating terrorism.[687]

Speedy re-apparition of websites and inefficiency of blocking

The European Commission also 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."[688] The Commission cited as the main reason "the issue of the speedy re-apparition of websites that have been closed down" as the main reason for not recommending a blocking policy. 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.[689] The Commission also acknowledged that existing methods of filtering can be circumvented.[690] It was also noted that these systems are designed specifically for websites, and they are not capable of blocking the distribution of objectionable content through other Internet services, such as P2P networks.

The European Commission concluded that the removal or disablement of access to terrorist propaganda or terrorist expertise without the possibility to initiate an investigation and prosecute the perpetrators behind such content appears inefficient. The Commission reached the conclusion that the dissemination of such content would only be hindered rather than eliminated.[691] 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."[692]

The Commission also voiced concern with regards to 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.[693]

Blocking considered by the EU with regards to combating child pornography

The Prague declaration developed under the Czech Presidency of the European Union in 2009 set forth a series of recommendations recognizing access blocking as one very valuable

---

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

686 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.

687 Council Framework Decision on combating terrorism amending Framework Decision 2002/475/JHA.

688 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.

689 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.

690 *Ibid*., p 41.

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

692 *Ibid*., p 29.

693 *Ibid*, p 42-45.

component in the fight against child sexual abuse and exploitation.[694] The Prague declaration was followed up by the European Commission with an amended proposal for a Directive on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA.[695] The European Commission, in view of amending its policy framework, proposed to have EU wide mandatory mechanisms to block access from the Union's territory to Internet websites identified as containing or disseminating child pornography.[696] The draft provision would require Member States to take necessary measures to enable the competent judicial or police authorities - subject to adequate safeguards – to block access to Internet websites containing or disseminating child pornography. Such safeguards according to the draft provision 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."[697] In November 2010, the European Parliament doubted the effectiveness of blocking measures as an effective tool for combating child pornography during a debate of the draft Council Framework Decision.[698]

Compatibility of blocking with ECHR questioned

Furthermore, 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 right to freedom of expression, any interference would need to be prescribed by law, and be necessary in a democratic society.[699] 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."[700] 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"[701] which undoubtedly raised further concerns for proportionality.

No mandatory blocking provisions recommended by the European Parliament

On 14 February, 2011, the European Parliament's Committee on Civil Liberties, Justice and Home Affairs Committee (LIBE) adopted a text[702] in response to the European Commission's proposal on Internet blocking.[703] According to the amendments made by the Committee "child

694 Prague Declaration: A new European approach for safer Internet for children, 20 April, 2009.

695 Proposal for a Council Framework Decision on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA, COM(2010)94 final, Brussles, 29.03.2010.

696 See paragraph 12 of 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, and draft Article 18 entitled Blocking access to websites containing child pornography.

697 *Ibid*.

698 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.

699 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.

700 *Ibid*.

701 *Ibid*.

702 Committee vote on report of Roberta Angelilli (EPP, IT): 40 in favour, none against, 5 abstentions. See draft report of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (Rapporteur: Roberta Angelilli) on 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, (COM(2010)0094 – C7-0088/2010 – 2010/0064(COD)), 2010/0064(COD), 16.12.2010.

703 Article 21 and Recital 13. Committee on Civil Liberties, Justice and Home Affairs, Press Release: Delete

pornography or child abuse material on the web must be removed at source in all EU countries".[704] The Committee, therefore, did not recommend "mandatory blocking" of websites containing child pornography[705] but rather took the position that the content should be taken down entirely. However, where removal is impossible, e.g. because websites are hosted outside the EU jurisdiction, or where the state that hosts the servers in question is unwilling to co-operate, or because its procedure for removing the material from servers is particularly long, Member States "may take the necessary measures in accordance with national legislation to prevent access to such content in their territory".[706] This would mean that EU Member States may, if necessary, decide to introduce measures involving blocking. National measures preventing access "must be set by transparent procedures and provide adequate safeguards, in particular to ensure that the restriction is limited to what is necessary and proportionate, and that users are informed of the reason for the restriction".[707] Content providers and users must also be informed of the possibility to appeal, and to whom to appeal under a judicial redress procedure. It is important to mention, that according to the Committee the EU must also co-operate with third countries to secure the prompt removal of such material from servers hosted in those countries.

Negotiations between the European Parliament and European Council representatives will continue,[708] with a view to reaching a compromise preferably during 2011.[709] Once adopted, the new directive will replace current Council Framework Decision on combating the sexual exploitation of children and child pornography.[710] Member States would then have two years to transpose the new rules into their national laws.

---

child pornography web pages across the EU, says Civil Liberties Committee, 14.02.2011, at <http://www.europarl.europa.eu/en/pressroom/content/20110131IPR12841/html/Delete-child-pornography-web-pages-across-the-EU-says-Civil-Liberties-Committee>. New forms of abuse and exploitation, such as "grooming" (befriending children through the web with the intention of sexually abusing them), or making children pose sexually in front of web cameras, will also be criminalised.

704 Civil Liberties, Justice and Home Affairs Committee, Press Release, "Delete child pornography web pages across the EU, says Civil Liberties Committee," 14.02.2011, at <http://www.europarl.europa.eu/en/pressroom/content/20110131IPR12841/html/Delete-child-pornography-web-pages-across-the-EU-says-Civil-Liberties-Committee>.

705 The LIBE adopted text is as follows: Article 21(1). Member States shall take the necessary legislative measures to obtain the removal at source of Internet pages containing or disseminating child pornography or child abuse material. Internet pages containing such material shall be removed, especially when originating from an EU Member State. In addition, the EU shall cooperate with third countries in securing the prompt removal of such content from servers in their territory (2). When removal at source of Internet pages containing or disseminating child pornography or child abuse material is impossible to achieve, Member States may take the necessary measures in accordance with national legislation to prevent access to such content in their territory. These measures must be set by transparent procedures and provide adequate safeguards, in particular to ensure that the restriction is limited to what is necessary and proportionate, and that users are informed of the reason for the restriction. Content providers and users shall be informed of the possibility to whom to appeal under a judicial redress procedure. (2a). Any measure under paragraphs 1 and 2 shall respect fundamental rights and freedoms of natural persons, as guaranteed by the European Convention of the Protection of Human Rights and Fundamental Freedoms, the EU Charter of Fundamental Rights and general principles of Union law. Those measures shall provide for prior authorisation in accordance with national law, and the right to an effective and timely judicial redress. (2b). The European Commission shall submit to the European Parliament an annual report on the activities undertaken by Member States to remove child sexual abuse material from Internet pages.

706 Committee on Civil Liberties, Justice and Home Affairs, Press Release: Delete child pornography web pages across the EU, says Civil Liberties Committee, 14.02.2011.

707 *Ibid*.

708 Political agreement on final act expected at the Council level by 09.06.2011.

709 European Parliament plenary sitting: Indicative date for the meeting is 22.06.2011.

710 2004/68/JHA of 22 December, 2003.

Non-regulatory EU initiatives to block access to illegal Internet content

In addition to the amendment of the regulatory framework for combating child pornography at the European Union, and the debate on blocking as a measure to prevent access to such content from within the EU territory, there are also other initiatives of a non-regulatory nature which involves blocking access to allegedly illegal Internet content. These involve the European Union's CIRCAMP project, and the "Check the Web" project within the context of combating terrorist use of the Internet.

EU CIRCAMP Project to fight child abuse material

The Internet Related Child Abuse Material Project (CIRCAMP) is an initiative mandated by the European Police Chiefs launched in 2004. The purpose of CIRCAMP is to improve and increase co-operation between law enforcement agencies in the field of child sexual exploitation. The project tries to improve and increase co-operation by sharing more information, reducing duplication of efforts, raising quality, and saving law enforcement resources.[711] In the fall of 2006, the European Police Chief Task Force (ECPTF) accepted Action Plan II for CIRCAMP establishing a comprehensive mechanism which gives law enforcement authorities the ability to control and disrupt illegal child abuse websites. The law enforcement network included the following members:

> **Driver:** Norway **Co-driver:** UK
> **Forerunner countries:** Denmark, Belgium, France, Finland, Ireland, Italy, Malta, Poland, Sweden, the Netherlands, Spain, Germany[712]
> **Supporting units:** Europol and Interpol

The Action Plan was based on the Organized Crime Threat Assessment Report (OCTA) for Europe in which child abuse material was linked to organized crime via commercial illegal websites.[713] Primary goals of CIRCAMP are

- To detect, disrupt and dismantle networks, organizations or structures used for the production and/or distribution of child abusive files and to detect offenders, identify children and stop abuse,

---

711 Action Plan II Executive summary and outcomes 2006-2010. Action Plan II ran from 2006 until 2010. CIRCAMP was partially sponsored by the European Union Safer Internet Program between 2008 and 2010. During the period of funding one of the main objectives was to promote the CIRCAMP strategy and to provide a possible solution to the issue of commercial child abuse websites that is particularly effective if law enforcement and other stakeholders work together. Throughout Action Plan II, every forerunner country has established a standardized mechanism which would allow the disruption of commercial child abuse material within their country.

712 Forerunner countries, in addition to various other countries, have worked on the first two phases. CIRCAMP has not restricted its collaboration to forerunner countries but has welcomed the participation of law enforcement authorities in any country that is willing to take part in the fight against commercial child abuse material. During Action Plan II, **Italy**, **Finland, Norway, Sweden, Denmark and Malta** used or started using the Child Sexual Abuse Anti Distribution Filter (CSAADF). CIRCAMP also works with New Zealand and **Switzerland** in relation to their CSAADF.

713 "In recent years a considerable transnational action has been directed against the production and distribution of child abuse material on the Internet. However the circulation of such material is not decreasing. Organised criminal gangs are engaged in the production of new illegal images and movies, or they utilise the same material on different websites where they sell it through sophisticated electronic payment systems. Growing demand implies an increasing number of children being sexually abused to fulfill it. Child abuse content is also distributed through networks of child sex offenders that are not motivated by financial gain. Rather, they exchange this material because of their common sexual interest in children. Among the latter it has been noted that a large amount of illegal material is being produced and distributed by travelling sex offenders." See Europol, OCTA: EU Organised Crime Threat Assessment 2009, p 21.

- Through cooperation to create a common understanding on global policing of the Internet,
- To reduce harm to society by obstructing the distribution of child abuse material at the European level, and to disrupt the methods used by organized crime groups responsible for the illegal pay-per-view sites.

CIRCAMP is mandated to co-operate with law enforcement authorities in any country in the world, in order to assist in setting up and maintaining the so-called 'disruption system'. The CIRCAMP Action Plan II had a three-phase approach. In terms of **Phase I**, the project intended to introduce blocking technology or other technical means aimed at stopping the distribution of child abuse images and material. This system is called 'Child Sexual Abuse Anti Distribution Filter' (CSAADF). In term of the status of phase I, the CSAADF system was implemented in several countries, while other countries continued developing their systems, and then started to use it when appropriate authorization is received.[714] During **Phase I**, the competent law enforcement authorities confirm the illegality of each website containing child abuse material,[715] and report its address to the ISPs. The ISPs then implement the CSAADF blocking system in their networks, utilizing existing technology, personnel and equipment. The CSAADF principally blocks at domain level.[716] When a hosting company, such as a photo hosting service, has been taken advantage of, CIRCAMP members will inform the owner/administrator of the domain in question that child sexual abuse material is being hosted on their system.[717] The countries that have CSAADF in place share all information about illegal sites and assess content of such sites according to their national legislation. If a website is deemed to be illegal, it will be added to the national list.

Although all the information about illegal websites is shared among the participant states, erroneous blocking cannot be excluded. Furthermore, the blocking list generated by law enforcement authorities in each country will differ depending on that particular country's laws and regulations.

In order to address erroneous blocking, a project called "Funnel Web"[718] deals with requests coming from the registrants of websites that are wrongly blacklisted by the CIRCAMP filter in the countries mentioned above. Europol, in partnership with CIRCAMP, has set up a reporting mechanism for owners of blocked domains. This system aims to centralize the

---

714 By disrupting traffic to websites depicting and distributing child sexual abusive material CIRCAMP claims that it prevented the re-victimization of children, prevented the illegal distribution of files, prevented the illegal display of abuse material and reduce harm sustained by the general population, and prevented access to commercial child abuse material and shrink the market, reducing the need for new production.

715 CIRCAMP members have also developed a tool to assess reported sites. This tool was developed at the request of CIRCAMP and the development was carried out by Denmark with the approval of the Danish Police Commissioner, with Danish resources, time and money. The CIRCAMP assessment tool represents a standardized way of assessing a reported website and sharing the assessment with ISPs. CIRCAMP, in co-operation with CEPOL, has provided training for Member States in how to use the assessment tool. The tool is available within CIRCAMP.

716 CIRCAMP and Europol have established a complaint system for domain owners/administrators related to the access blocking. CIRCAMP has only received two complaints from domain owners during the year since the complaint system became available. For more information please refer to http://www.europol.europa.eu/index.asp?page=FunnelIntro In terms of the users, when an Internet user types in an address in his/her browser or clicks a link to a domain that has been found to contain child exploitation material, CIRCAMP has promoted 'best practice', meaning that the ISP redirects the browser to a specific page instead – the so-called 'stop page'. This usually contains information about what kind of content the user's browser tried to access, links to national legislation, information about where to complain about the blocking, and contact information.

717 For more information please refer to http://circamp.eu

718 See Europol, General Report on Europol's activities 2010, 10244/11, Brussels, 20 May 2011.

complaints and requests for revision of domain statuses in order to guarantee that the requests can be processed in all countries where the domain is blacklisted. Europol facilitates contacts between the owners of domains and competent law enforcement agencies. However, it is at the discretion of the Member States to decide upon possible judicial consequences induced by revision requests.

Phase II of the project intended to analyze sites and identify legal elements in the business side, for example targeting 'payment systems', and aim to disrupt the capacity to make a profit from abusive content. In term of the status of phase II, CIRCAMP (with analytical support from Europol) monitored reported sites in order to detect what financial mechanisms were being utilized by the criminal organizations.

Phase III of the project aimed to investigate the people that benefit financially from the commercial distribution of child abuse material. This has lead to the launching of a large scale investigation into a 'payment system' that was linked to a criminal organization responsible for a significant number of illegal websites.

Furthermore, information gathered for this report show that CIRCAMP has also agreed on a new Action Plan III which takes a holistic approach, and assess all aspects of the problem of child abuse and exploitation where online technology is involved targeting not only commercial but also non commercial distribution through P2P sites and other services.[719] While it was understood that information sharing within the CIRCAMP group was important, there was a need to allow other states to take part in the project. CIRCAMP has therefore launched a project to enable the ISP industry and law enforcement authorities worldwide to disrupt the distribution of child abuse material within their countries. In order to do so, CIRCAMP initiated a resolution at the Interpol's 78th General Assembly in Singapore, which was passed unanimously.[720]

CIRCAMP has seen a significant decrease in the number of commercial child abuse websites throughout Action Plan II as the criminals responsible for these websites have had their activities disrupted by various governmental and non-governmental initiatives.[721] While a decrease in commercial illegal websites is noted, there is still a need to continue disruption activities, utilizing all technical means to ensure there is a constant deterrent. CIRCAMP has therefore changed its focus, but will continue to devote a small 'dedicated resource' to pursue crimes against children on the Internet. CIRCAMP Action Plan III has a proactive focus mandating the forerunner counties to conduct a feasibility study on new problems and to take further action.

---

719 During recent years access and spread of the Internet has grown. Moreover, technological advances have made it easier for individuals to produce and distribute child abuse material in many different ways, for instance on photo sharing sites, peer to peer networks and forums. None of these areas yield monetary proceeds, and they and can therefore easily go undetected. Furthermore, Commercial distribution of child abuse material represented a worldwide challenge.

720 CIRCAMP also contributed a dedicated law enforcement officer to the Interpol General secretariat. This officer has been seconded from the Norwegian Police Directorate for 18 months. The objective was to develop a system, evaluate illegal content and make the information available to all 188 Interpol member countries. This is referred to as the 'Worst of list'. This project is still running.

721 Including efforts by the United States financial coalition, the European financial coalition, the International Association of Internet Hotlines (INHOPE), the European Commission's 'Safer Internet programme,' and CIRCAMP.

European Union "Check the Web" Project to prevent terrorist use of the Interent

In addition to the CIRCAMP project, the EU "Check the Web" (monitoring) Project should also be noted. This separate EU project was launched in May 2006 under 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 the Internet. The project is carried out by Europol and monitors websites advocating terrorism (mainly Islamist extremist terrorism).[722] 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."[723] 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"[724] in the fight against terrorist use of the Internet. The Commission has started a dialogue between law enforcement authorities and service providers to reduce the dissemination of illegal terrorism-related content on the Internet. A European Agreement Model to facilitate public/private cooperation on the issue is under development.[725]

AG's Opinion in the Court of Justice Case C-70/10 *Scarlet Extended v Sabam*

It is also worth noting that Advocate General Cruz Villalón of the Court of Justice of the European Union published his opinion with regards to a case from Belgium in April 2011.[726] The European Court of Justice case is important as it involves the use of filtering and blocking systems at the ISP level in Belgium. The outcome of the court decision may have EU wide implications.[727] According to Advocate General Cruz Villalón, a measure ordering an ISP to install a system for filtering and blocking electronic communications in order to

---

722 The Check the Web portal is more and more recognized within the EU Member State Counter Terrorism community as a point of reference for listing Islamist extremist Websites and providing information on Islamist extremist propaganda material found on the Internet. The number of user accounts has also increased from five accounts per EU Member State to 200 accounts per EU Member State. A fourth version of this portal is in preparation. See further EU Counter-Terrorism Coordinator (CTC), EU Action Plan on combating terrorism, 15893/1/10 REV 1, Brussels, 17 January 2011.

723 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

724 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.

725 See EU Counter-Terrorism Coordinator (CTC), EU Action Plan on combating terrorism, 15893/1/10 REV 1, Brussels, 17 January 2011. Furthermore, the Commission has contracted two studies, one on non-legislative measures to prevent the distribution of violent radical content on the Internet, including co-operation between NGOs and law enforcement authorities, another on methodologies and adapted technological tools to efficiently detect violent radical content on the Internet. The results are expected in 2011.

726 The Advocate General's Opinion is not binding on the Court of Justice. It is the role of the Advocates General to propose to the Court, in complete independence, a legal solution to the cases for which they are responsible.

727 A reference for a preliminary ruling allows the courts and tribunals of the Member States, in disputes which have been brought before them, to refer questions to the Court of Justice about the interpretation of European Union law or the validity of a European Union act. The Court of Justice does not decide the dispute itself. It is for the national court or tribunal to dispose of the case in accordance with the Court's decision, which is similarly binding on other national courts or tribunals before which a similar issue is raised.

protect intellectual property rights in principle infringes fundamental human rights.[728] Villalón opined that:

> "In order to be permissible, such a measure must comply with the conditions laid down in the Charter of Fundamental Rights to govern restrictions on the exercise of rights. It must therefore be adopted, inter alia, on a legal basis that meets the requirements concerning 'the quality of the law' at issue."[729]

Advocate General Cruz Villalón considered that the installation of the filtering and blocking system is a restriction on the right to respect for the privacy of communications and the right to protection of personal data, both of which are rights protected under the Charter of Fundamental Rights. By the same token, the deployment of such a system would restrict freedom of information, which is also protected by the Charter of Fundamental Rights. The Advocate General pointed out, however, that the Charter of Fundamental Rights accepts that the exercise of the rights and freedoms which it guarantees may be restricted, on condition, *inter alia*, that any such restriction is 'in accordance with the law'. Applying the case-law developed in this field by the European Court of Human Rights, the Advocate General considered that the legal basis for any restriction on the exercise of the rights and freedoms guaranteed by the Charter of Fundamental Rights must meet requirements concerning 'the quality of the law' at issue. Thus, in his view, a restriction on the rights and freedoms of Internet users such as that at issue would be permissible only if it were adopted on a national legal basis which was accessible, clear and predictable.

CoE Perspectives on Blocking Access to Allegedly Illegal Content

As it has been highlighted in section B of this report a number of Council of Europe conventions include content related provisions. These are offences related to child pornography,[730] the dissemination of racist and xenophobic material through computer systems,[731] and public provocation to commit a terrorist offence.[732] None of these legal measures cover blocking provisions, and instead – as in any offline environment – cover the criminal activity of dissemination, and publication (and possession in the case of child pornography).

Access and hosting providers are protected under the provisions of these CoE Conventions.[733] Without the required intent under domestic law service providers would not be held criminally liabile for serving as a conduit or for hosting a website or newsroom containing above mentioned material.[734] Moreover, and important to stress, as provided by the EU E-

---

728 Court of Justice of the European Union, Press Release: Advocate General's Opinion in Case C-70/10 Scarlet Extended v Société belge des auteurs compositeurs et éditeurs (Sabam), No 37/11, Luxembourg, 14 April 2011.

729 *Ibid*.

730 Article 9 of the CoE Cybercrime Convention and Article 20 of the CoE Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse.

731 Article 3 of the Additional Protocol of the Cybercrime Convention.

732 Article 5 of the CoE Convention on the Prevention of Terrorism.

733 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.

734 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>.

Commerce Directive, a service provider is not required to monitor conduct to avoid criminal liability under the CoE provisions.

With regards to 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.[735] More importantly, a CoE Committee of Ministers Recommendation of 2007[736] 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 offline) means of content delivery.[737]

In March 2008, the Committee of Ministers in Recommendation (2008)6[738] recalled the Declaration of the Committee of Ministers on Freedom of Communication on the Internet of 28 May, 2003[739] which also 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.[740] 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."[741]

Legal provisions which require closing down and/or blocking access to websites and access to Web 2.0 based services

Question 14 of the survey concerns **specific legal provisions which require closing down and/or blocking access to websites or any other types of Internet content**. In 28 (50%) of the participating States no such legal provisions exisit while 17 (30.4%) of the participating States do have laws in place which could be used to block access to websites. No data was obtained from eleven (19.6%) of the participating States.

735 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.

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

737 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.

738 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.

739 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.

740 *Ibid*, Principle 3: Provided that the safeguards of Article 10, paragraph 2, of the Convention for the Protection of Human Rights and Fundamental Freedoms are respected, measures may be taken to enforce the removal of clearly identifiable Internet content or, alternatively, the blockage of access to it, if the competent national authorities have taken a provisional or final decision on its illegality.

741 *Ibid*.

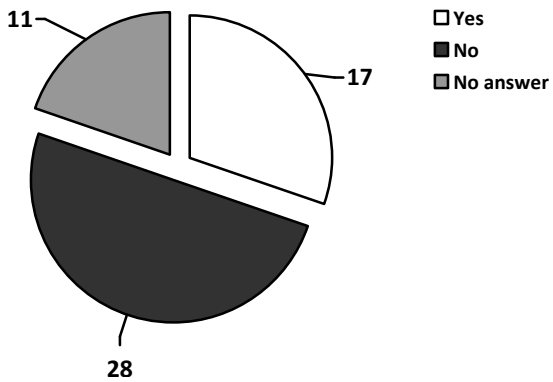


Figure 38. OSCE participating States' responses with regards to specific legal provisions which require closing down and/or blocking access to websites or any other types of Internet content (Q14)

In addition to the question on legal provisions which require closing down and/or blocking access to websites, the participating States were also asked whether they have **specific legal provisions which require blocking access to web 2.0 based applications and services such as YouTube, Facebook, or Blogger** in place **(Question 15)**. Only **Italy** responded positively to this question. 44 (78.6%) countries responded negatively and **Albania**, **Azerbaijan**, **Belarus**, **Kazakhstan**, **Kyrgyzstan**, **Latvia**, **Lithuania**, **Norway**, and **Poland** explicitly stated that there are no specific provisions which require blocking access to web 2.0 based applications and services. No data was obtained from 11 (19.6%) of the participating States.

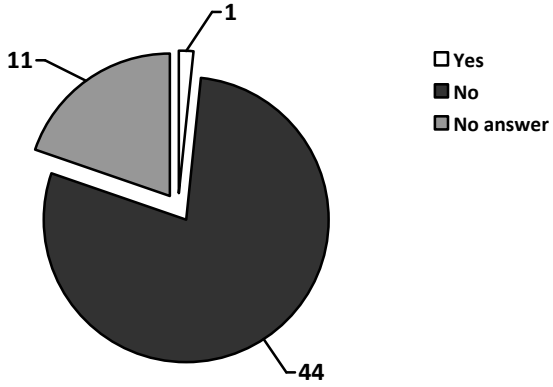


Figure 39. OSCE participating States' responses with regards to specific legal provisions which require blocking access to web 2.0 based applications (Question 15)

Question 14 of the OSCE RFOM study referred to legal provisions which require closing down and/or blocking access to websites or any other types of Internet content. As will be seen below different policies are adopted by different OSCE participating States. Based on the responses received, there were no general legal provisions involving blocking in 10 participating States of the OSCE. These are **Austria**, **the Czech Republic**, **Germany**, **Luxembourg**, **the former Yugoslav Republic of Macedonia**, **Moldova**, **Montenegro**, **Poland**, **Serbia**, and **Slovakia**. However, there may be some removal provisions or other sanctions provided for in those countries.

Furthermore, table 14 below shows the list of OSCE participating States that report having **specific legal provisions** in the absence of **general legal provisions** which require closing down and/or blocking access to websites with regards to individuals questions (Questions 4-13) covered in this study.

Question	Existent legal provisions prescribing blocking based on	No of OSCE States	List of OSCE States
4G	Racist content, xenophobia, and hate speech	**2**	Latvia Russian Federation
5G	Denial, gross minimisation, approval or justification of genocide or crimes against humanity	**1**	Latvia
6G	Incitement to terrorism, terrorist propaganda and/or terrorist use of the Internet?	**1**	Estonia
7G	Child pornography	**6**	Bulgaria Estonia Finland Latvia Netherlands United Kingdom
8F	Obscene and sexually explicit (pornographic) content	**3**	Estonia Latvia Russian Federation
9F	Internet piracy	**4**	Estonia Hungary Latvia Russian Federation
10F	Libel and insult (defamation) on the Internet	**2**	Estonia Latvia
11G	Expression of views perceived to be encouraging "extremism"	**3**	Estonia Latvia Russian Federation
12G	Distribution of "harmful content"	**1**	Estonia
13F	Any other categories of Internet content	**1**	Cyprus

Table 14. OSCE participating States that report having specific legal provisions which require closing down and/or blocking access to websites, in the absence of general legal provisions requiring closing down and/or blocking access to websites.

Additionally, table 15 below shows OSCE participating States that report having neither **general legal provisions**, nor **specific legal provision** which directly require closing down and/or blocking access to websites with regards to individuals questions (Qs 4-13) covered in this study. The absence of these legal provisions does not exclude that blocking or take-down of content and websites might occur in those states, subject to court orders or voluntary measures.

Question	Existent legal provisions prescribing blocking based on	No of OSCE States	List of OSCE States	
4G	Racist content, xenophobia, and hate speech	**21**	Armenia Austria Bulgaria Croatia Czech Republic Estonia Finland Germany Greece Kyrgyzstan	the former Yugoslav Republic of Macedonia Moldova Montenegro Netherlands Poland Serbia Slovakia

			Luxembourg	Sweden Turkmenistan United Kingdom
5G	Denial, gross minimisation, approval or justification of genocide or crimes against humanity	**23**	Armenia Austria Bulgaria Croatia Cyprus Czech Republic Estonia Finland Germany Greece Hungary Kyrgyzstan Luxembourg	the former Yugoslav Republic of Macedonia Moldova Montenegro Netherlands Poland Russian Federation Serbia Slovakia Turkmenistan United Kingdom
6G	Incitement to terrorism, terrorist propaganda and/or terrorist use of the Internet	**19**	Armenia Austria Bulgaria Croatia Czech Republic Finland Germany Greece Luxembourg the former Yugoslav Republic of Macedonia	Moldova Montenegro Netherlands Poland Russian Federation Serbia Slovakia Sweden Turkmenistan
7G	Child pornography	**19**	Austria Croatia Cyprus Czech Republic Germany Greece Hungary Ireland Kyrgyzstan Luxembourg	the former Yugoslav Republic of Macedonia Moldova Montenegro Poland Russian Federation Serbia Slovakia Sweden Turkmenistan
8F	Obscene and sexually explicit (pornographic) content	**21**	Armenia Austria Bulgaria Cyprus	the former Yugoslav Republic of Macedonia

			Czech Republic Finland Germany Greece Hungary Kyrgyzstan Luxembourg	Moldova Montenegro Netherlands Poland Serbia Slovakia Sweden Turkmenistan United Kingdom
9F	Internet piracy	**21**	Armenia Austria Bulgaria Croatia Cyprus Czech Republic Finland Germany Kyrgyzstan Luxembourg	the former Yugoslav Republic of Macedonia Moldova Montenegro Netherlands Poland Serbia Slovakia Spain Sweden Turkmenistan United Kingdom
10F	Libel and insult (defamation) on the Internet	**20**	Armenia Austria Bulgaria Cyprus Czech Republic Finland Germany Hungary Luxembourg	the former Yugoslav Republic of Macedonia Moldova Montenegro Netherlands Poland Russian Federation Serbia Slovakia Sweden Turkmenistan United Kingdom
11G	Expression of views perceived to be encouraging “extremism”	**21**	Armenia Austria Bulgaria Cyprus Czech Republic Finland Germany Hungary Kyrgyzstan Luxembourg	the former Yugoslav Republic of Macedonia Moldova Montenegro Netherlands Poland Serbia Slovakia Spain Sweden Turkmenistan

				United Kingdom
12G	Distribution of "harmful content"	**23**	Armenia Austria Bulgaria Cyprus Czech Republic Finland Germany Hungary Kyrgyzstan Latvia Luxembourg	the former Yugoslav Republic of Macedonia Moldova Montenegro Netherlands Poland Russian Federation Serbia Slovakia Spain Sweden Turkmenistan United Kingdom
13F	Any other categories of Internet content	**21**	Armenia Austria Czech Republic Estonia Finland Germany Hungary Kyrgyzstan Latvia Luxembourg	the former Yugoslav Republic of Macedonia Moldova Montenegro Netherlands Poland Serbia Slovakia Spain Sweden Turkmenistan United Kingdom

Table 15. OSCE participating States that report having neither general legal provisions, nor specific legal provision which require closing down and/or blocking access to websites.

In terms of the responses received for this OSCE RFOM study, in **Albania**, legislation in force includes provisions that are applicable for all types of media services regarding specific content which can be taken down or blocked. In **Austria**, there are no access blocking provisions as the Media Act does not provide for the blocking of Internet pages as a sanction. However, according to section 33(1) of the Austrian Media Act, the court on application has to decide on the removal of the part of the website constituting the criminal act. The removal or deletion of parts of a website can also be ordered as an interim measure of protection if proceedings are pending and the detrimental consequences of the deletion are not disproportionally more severe than the interest in protecting the law. A deletion as an interim measure is not admitted however, if the interest in the protection of the law can also be satisfied by the publication of a notice on the fact that proceedings are pending.[742] Furthermore, a deletion order concerning illicit content accessible on the Internet can be

[742] Section 36 para. 1 and 2 of the Austrian Media Act

executed[743] under the conditions of Section 26 of the Criminal Code.[744] An obligation to delete certain illicit content, among them child pornography is possible under sections 13 to 17, especially section 16 of the Austrian E-Commerce Act.[745] The execution of the deletion in this case is the duty of the service providers.

In **Azerbaijan**, according to clause 4.2(a) of the "Rules for Using Internet Services," providers can suspend Internet services without permission by their subscribers in cases that violate the rights stipulated in the law "On Telecommunications." According to Annex No. 1 "On Agreement on Internet Service Provision"[746] of the above rules, a provider can temporarily suspend delivery of Internet services in certain cases.[747] Furthermore, according to clause 3 of an order of the Azerbaijan Republic Ministry of Communications and Information Technologies, a provider can suspend delivery of Internet services in certain circumstances including in times of war, events of natural disasters and states of emergency.[748]

In **Belarus**, certain restrictions apply under clause 8 of the presidential decree "On measures to improve use of the national segment of the Internet,"[749] and subject to the resolution "On approval of the Regulations on the procedure for restricting access of Internet users to information prohibited for distribution in accordance with legislative acts".[750] Clause 8 states that Internet providers may render their services to restrict access to information geared to the performance of extremist activities; unlawful trafficking in weapons; ammunition; explosive devices; explosive, radioactive, venomous, potent, poisonous, toxic, narcotic or psychotropic substances and their precursors; promotion of illegal migration or human trafficking; distribution of pornographic materials; and propaganda of violence, cruelty and other acts prohibited by law. Services to restrict access to other information may be provided on the basis of an agreement concluded between the Internet providers and the Internet user.[751] According to a legal analysis commissioned by the OSCE Office of the RFOM, the Decree is

---

743 Compare also sections 33 and 36a of the Media Act.

744 Confiscation – "*Einziehung*".

745 E-Commerce Gesetz – ECG.

746 Clause 5.2.

747 In cases where the subscriber, to the detriment of the provider's other subscribers (private individuals or legal entities) or personnel, uploads information onto the Internet that negatively affects their authority, and in cases that run counter to the law "On Telecommunications" or other legal acts.

748 Order of 24 February 2000. The circumstances include cases that run counter to the rules established by the legislation of the Azerbaijan Republic and the law "On Telecommunications"; when war or a state of emergency is declared; in the event of a natural disaster or other catastrophe; when services are provided to third parties without the appropriate licenses; in cases where systems that are either defective or uncertified are connected to the network.

749 1 February 2010 No. 60. According to Freedom House, "Presidential Decree No. 60 was only a prelude to suspected blocking and technical hijacking of independent and opposition websites that occurred on 19 December 2010 the date of presidential elections, and the following day. For example, the sites of the news outlets Charter97 and Belarus Partisan were temporarily inaccessible during the two day period." See Freedom House, Freedom on the Net 2011: *A Global Assessment of Internet and Digital Media*, April 2011, at <http://www.freedomhouse.org/uploads/fotn/2011/FOTN2011.pdf>, p. 59.

750 Resolution "On approval of the Regulations on the procedure for restricting access of Internet users to information prohibited for distribution in accordance with legislative acts," Operational Analysis Centre under the President of the Republic of Belarus and of the Ministry of Communications and Informatisation of the Republic of Belarus ,29 June, 2010 No. 4/11.

751 Internet providers, including authorized Internet providers, provide for restriction on access to the information indicated in part one of this clause when rendering these services to state authorities and organizations (with the exception of the authorities listed in part four, clause 6 of this Decree, other state bodies and organizations determined by the Operational Analysis Centre under the President of the Republic of Belarus), educational and cultural organizations". During the given period, the relevant rules have not yet come into effect.

the first to regulate limiting access to information at the request of the Internet service user.[752] Accordingly, at the request of individual Internet users, providers must prevent access to such resources for the users who request it (but not for all other Internet users).[753] The Decree also envisages that access to illegal information shall be automatically blocked by government authorities, cultural and educational organizations (for example, universities, schools and clubs).[754]

Furthermore, Resolution No. 4/11 "On Approving the Provisions on the Procedure for Restricting Access of the Users of Internet Services to Information Prohibited from Dissemination by the Law"[755] regulates the procedure for restricting access to prohibited information. The resolution stipulates that ISPs shall limit access "on the basis of a limited access list duly compiled by the Republic of Belarus State Telecommunications Inspectorate of the Ministry of Communications and Informatisation."[756] This process is carried out on the basis of decisions of the heads of the State Regulation Committee, the Prosecutor General's Office, the Operating and Analytical Centre under the President of the Republic of Belarus (OAC), and all state administration bodies. The decisions are adopted by the heads of these bodies within the limits of their competence. Moreover, the resolution allows for a certain limited access list compiled by the ISPs independently. The procedure for compiling such a list is not specified.

In **Belgium**, the courts may, under national legislation, issue an order for any infringement of an intellectual property right to be brought to an end. In particular, the legislation provides that, where a third party uses the services of an intermediary to perpetrate an infringement of that type, the courts are authorized to issue such an order against that intermediary. The Société belge des auteurs compositeurs et éditeurs (Sabam) applied for an interim relief against Scarlet Extended SA, ISP.[757] Sabam sought first of all a declaration that the copyright in musical works contained in its repertoire had been infringed because of the unauthorized sharing, through the use of Scarlet's services, of music files – in particular, by means of peer-to-peer software. Sabam also sought an order requiring Scarlet to bring such infringements to an end, on pain of a penalty payment, by blocking or making impossible the sending or the receiving by its customers in any way of files containing a musical work, using peer-to-peer software, without the permission of the copyright holders. By a judgment of 26 November 2004, such copyright infringements were found to have taken place. After a report had been obtained from a technical expert, Scarlet was ordered, by another judgment, delivered on 29 June 2007, to bring those copyright infringements to an end by making it impossible for its customers to send or to receive in any way, by means of P2P software in particular, files

752 See a legal analysis commissioned by the Office of the OSCE RFOM, Commentary on recent documents of the Republic of Belarus regarding use of the national segment of the Internet, 2010, at <http://www.osce.org/fom/73455>. The commentary was prepared by Andrei Richter, Director of the Media Law and Policy Institute (Moscow).

753 *Ibid*, p. 16.

754 *Ibid*, p. 20.

755 Resolution of the Operations and Analysis Centre of the President of the Republic of Belarus and the Ministry of Communications and Informatization of the Republic of Belarus No. 4/11 of 29 June 2010 "On Approving the Provisions on the Procedure for Restricting Access of the Users of Internet Services to Information Prohibited from Dissemination by the Law".

756 Legal analysis commissioned by the Office of the OSCE RFOM, Commentary on recent documents of the Republic of Belarus regarding use of the national segment of the Internet, 2010, at <http://www.osce.org/fom/73455>, p. 20.

757 Court of Justice of the European Union, Press Release: Advocate General's Opinion in Case C-70/10 Scarlet Extended v Société belge des auteurs compositeurs et éditeurs (Sabam), No 37/11, Luxembourg, 14 April 2011.

containing a musical work in Sabam's repertoire, and to do so within a period of six months, on pain of a penalty payment of 2,500 euros per day should Scarlet fail to comply with the judgment. Scarlet has appealed against that judgment to the Court of Appeal in Brussels, which must decide whether to uphold the measure adopted against Scarlet. In that context, as mentioned above the Court of Appeal is seeking a ruling from the Court of Justice on whether the European Union law and, in particular, the fundamental rights guaranteed by the Charter of Fundamental Rights, permit a national court to order an ISP to install a system for filtering and blocking electronic communications.[758]

In **Bulgaria**, there are no general blocking provisions. However, websites may be closed by a Prosecutor's order or following a court decision in relation to child pornography or piracy among other types of content.[759] Pursuant to the Ministry of Interior Act officials at the General Directorate for the Fight against Organized Crime, "Computer crimes, intellectual property and gambling" section is entitled to send instructions to ISPs ordering them to cancel access to websites in which content depicting sexual violence or sexual abuse have been encountered.[760] Furthermore, during state of martial law, state of war, or state of emergency as well as in the case of an imminent threat to national security, the competent bodies of the Ministry of Interior may block, by technical means, the provision of electronic communications.[761]

In **Canada**, there are no specific legal provisions to require blocking access to websites or other types of material found on the Internet. However, provisions are in place for the removal or forfeiture of content involving hate propaganda,[762] and voluntary blocking activity as a self-regulatory measure with regard to child pornography. Since January 2007, the majority of Canada's large ISPs voluntarily participate in Project Cleanfeed Canada,[763] which aims to

---

758 Reference for a preliminary ruling from the Cour d'appel de Bruxelles (Belgium) lodged on 5 February 2010 — *Scarlet Extended SA v Société Belge des auteurs, compositeurs et éditeurs (SABAM)*, Case C-70/10, 2010/C 113/30: A reference for a preliminary ruling allows the courts and tribunals of the Member States, in disputes which have been brought before them, to refer questions to the Court of Justice about the interpretation of European Union law or the validity of a European Union act. The Court of Justice does not decide the dispute itself. It is for the national court or tribunal to dispose of the case in accordance with the Court's decision, which is similarly binding on other national courts or tribunals before which a similar issue is raised.

759 Articles 159, and 172a of the Penal Code.

760 Articles 55 and 56, Ministry of Interior Act, Promulgated, SG No. 17/24.02.2006).

761 Article 301 of the Law on Electronic Communications, Chapter Eighteen, Provision of Electronic Communications Services During Crisis, State of Martial Law, State of War or State of Emergency: (1) The undertakings providing public electronic communications networks and/or services shall ensure possibilities for the provision of electronic communications services during crises in the sense of the Law on Crisis Management, or during a state of martial law, state of war, or a state of emergency in the sense of the Law on Defence and Armed Forces of the Republic of Bulgaria. (2) To guarantee the national security, the undertakings providing public electronic communications networks and/or services shall, if necessary, provide the competent bodies with access to the network and/or the services provided, as well as a possibility to use free of charge electronic communications over the network in the case of an imminent threat to the national security. (3) For the purpose of performing the activities under Art. 91, paragraph 1, and Art. 111, paragraph 1, item 5 of the Law on the Ministry of Interior, as well as in the case of an imminent threat to the national security, the competent bodies of the Ministry of Interior may block, by technical means, the provision of electronic communications.

762 Section 320.1 of the Criminal Code authorizes a judge to order the deletion from a computer system within the jurisdiction of the court of publicly-available hate propaganda material. This provision makes it possible to eliminate hate propaganda material from the Internet in cases where the person who posted the material is unknown or outside Canadian jurisdiction.

763 Project Cleanfeed Canada is an initiative of the Canadian Coalition Against Internet Child Exploitation (CCAICE), a voluntary, multi-sector forum comprised of industry, law enforcement, governmental and non-governmental stakeholders from across the country. Project Cleanfeed Canada is administered by the

reduce access to and distribution of child pornography. Through this project, Cybertip.ca maintains a regularly updated list of specific foreign-hosted Internet addresses (URLs) associated with images of child pornography and provides that list in a secure manner to participating ISPs, who automatically deny access to the listed sites. The list of blocked sites is a blind list, meaning that participating ISPs cannot view the content of the list.

In **Croatia**, although there are no specific laws with the use of particular web applications, a criminal activity taking place on such platforms may be subject to the provisions of the Criminal Code.

In the **Czech Republic**, there exists a domain name blocking policy. CZ.NIC-CSIRT, a security team operating within the registrar of the CZ.NIC national domain is responsible for the administration of the Czech national domain. Since January 2010, CZ.NIC-CSIRT has blocked 150 domains ending with .cz. The reasons are connected with the dissemination of harmful software and phishing attacks. CZ.NIC-CSIRT was created with the aim to minimize the risks of potential threats to the national or international computer security and to help eliminate harmful content in the .cz domain space. The team is entitled to block harmful domain names for up to one month and may do so repeatedly. However, there exists no content blocking mechanisms within the Czech Republic.

In **Denmark**, closing down services, or blocking access to websites is provided by law. According to Section 75(2) of the Criminal Code the following objects (including websites) may be confiscated, where it is considered to be necessary to prevent further crime or otherwise required due to special circumstances:

1) objects used or intended to be used in a criminal act;
2) objects produced by a criminal act; and
3) objects in respect of which a criminal offence has otherwise been committed

Regarding blocking access to websites with allegedly illegal content, the Danish National Police work together with the Danish ISPs in relation to the so-called "child-pornography-blocking-filter". The police encourage the ISPs to block access to websites containing child pornography. Finally, it must be noted that in each agreement of co-operation with the ISPs, the decision whether or not to block access to the websites in question is exclusively made by the ISPs.

It is also worth noting that the Danish Supreme Court upheld an injunction against a Danish ISP to block access to the Pirate Bay website in May 2010.[764] The injunction was first issued by the bailiff's court in 2008 and upheld by the high court later the same year.[765] The Supreme Court concurred with the High Court that Pirate Bay contributed to serious copyright infringement and that the ISP Sonofon contributed to this infringement by providing its subscribers with access to the Pirate Bay website.

Canadian Centre for Child Protection (C3P), a Canadian charitable organization that also manages Cybertip.ca, Canada's national tipline for the reporting of child pornography.

764 Højesterets kendelse, afsagt torsdag den 27. maj 2010, Sag 153/2009, Telenor (tidligere DMT2 A/S og Sonofon A/S) mod IFPI Danmark (Supreme Court's decision of 27 May 2010 in case 153/2009 (Telenor v IFPI Denmark)) See http://merlin.obs.coe.int/redirect.php?id=12604

765 See Søren Sandfeld Jakobsen, Danish Supreme Court Upholds Injunction to Block the Pirate Bay, IRIS 2010-8/24: The Supreme Court also concurred that the injunction was proportionate, considering the relatively low costs and slight disadvantages for the ISP in blocking access to the website, compared to the very large number of copyright infringements being conducted via the Pirate Bay.

In **Estonia**, there are no general legal provisions which require closing down and/or blocking access to websites or any other types of Internet content. However, the public authorities have a general right to make precepts that can also stipulate that the ISPs have to block and/or close a specific website. For example, Article 146(1) of the Electronic Communications Act stipulates that the Director General of the Communications Board, or his or her deputy, and an official authorized by the Director General has the right to issue mandatory precepts for elimination of violations of the requirements provided by this Act, of legislation established on the basis of this Act, and of the regulations of the European Union, or for the performance of certain acts for the performance of the obligations provided by this Act. These provisions may also apply to web 2.0 based applications and services.

In **France**, in terms of blocking access, according to Law of 21 June 2004, the French legislature has stated that freedom of communication by electronic means may be limited to the extent required to safeguard public order. Thus, it foresees the possibility, for the judicial authority to prescribe, either by summary or ex-parte proceedings, to any person, any measure to prevent or cease damage caused by the content of an online communications service to the public. These measures, used in the battle against racism, have been recently introduced by means of Law of 5 March 2007 amending the Law of 29 July 1881 on freedom of the press. Therefore, if the acts of justification of or incitement to commit an act of terrorism result from messages or information made available to the public by an online communications service, and they constitute patently illicit unrest, the cessation of this service may be pronounced by the judge in chambers at the request of the public prosecutor and any physical person or legal entity with an interest in the matter. Furthermore, in terms of detection, or to suppress efforts to justify crimes against humanity, incitement to racial hatred, as well as child pornography, ISPs and web hosting companies must put in place, pursuant to the Law of 21 June 2004 on Confidence in the Digital Economy, an easily accessible and visible system to report such content. Failure to do so may result with one year's imprisonment and a fine of 15,000 euros. The ISPs and web hosting companies must also promptly inform the public authorities on the means utilized to fight against these illegal activities.

Furthermore, since March 2011, it is possible to require ISPs to block websites containing child pornographic content under the LOPPSI Project (Law on Guidelines and Programming for the Performance of Internal Security).[766] A blacklist of websites, not made public, is established by the administration. ISPs in turn are required to block access to these sites.[767] There is also a requirement for ISPs to filter IP addresses designated by an order of the Minister of the Interior.[768]

---

766 Loi no. 2011-267 du 14 Mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure [Internal Security Law]. LOPPSI was announced in the French Official Gazette on 15 March 2011. The Law is known as "Loppsi 2," in reference to a law with a similar name and objective that was passed in 2002. The constitutionality of the 2011 Law was reviewed prior to its promulgation by the Constitutional Council, which struck down 13 of its articles, none of them essential. (Conseil Constitutionnel, Décision no. 2011-625 DC du 10 Mars 2011.)

767 According to Article 4, the administrative authority will notify the service providers, after the approval of the judicial authority.

768 It should also be noted that the police, with the authorization of the courts, may use any means (physical or remote) to access computers and retrieve data in various cases, ranging from serious crimes (paedophilia, murder, etc.) to arms trafficking, drug trafficking, and money laundering without the consent of the owners of the computers. This provision is also applicable for the crime of "unauthorized entry, movement, and residence of a foreigner in France committed by an organized crime group".

In **Finland**, the Act on Measures to Restrict the Distribution of Child Pornography[769] entered into force on 1 January 2007. The purpose of the act is to restrict access to child pornography by reducing Internet traffic through confidential blacklists. According to the Act, the police is responsible for preparing and updating a list of Internet sites that include illegal material. The ISPs have the right to block access to the websites containing child pornography. Some ISPs, since early 2008, decided to use the police maintained blacklist to block access to websites containing child pornography. The police may use the information provided from official sources, NGOs and citizens to develop and maintain the blacklist. According to the Parliamentary Ombudsman of Finland, over 30 complaints were made, mainly in 2008, to the Ombudsman about both the Act, and its application. The Ombudsman did not consider the activities to constitute to advance censorship that is contrary to the Constitution, but found that many important questions had been left to the applying parties to resolve.[770]

In June 2011, it was reported that the Helsinki Administrative Court has ruled that domestic websites may not be placed on the secret blocking blacklist maintained by the police.[771] The administrative court action started in February 2008 when lapsiporno.info ("childporn.info") website was added to the child pornography blacklist and has remained on the list ever since. This particular website, discovered a large part of the blacklist and circulated the findings on this website.[772] The lapsiporno.info revealed that the top five Google search results for "gay porn" were all blacklisted even though there was nothing related to children on those sites. The World Wide Web Consortium's website[773] and the memorial page of a deceased Thai princess was among the blacklisted websites. The police, however, accused the website owner of distributing child pornography and eventually put the website on the secret blacklist. The website owner therefore lodged an appeal with an administrative court for his website being blacklisted without a valid legal basis. The ruling of the court suggests that domestic sites may not be placed on such a blacklist.

In **Germany**, there are no general blocking provisions. Such a general blocking policy with regards to child pornography was considered by the parliament. However, in April 2011, after almost a year of discussions, the German government decided that removal rather than access blocking will be the policy to tackle the problem of online child pornography.[774] During discussions there were concerns that merely blocking material could open the door to wider censorship on the Internet.[775] Jugendschutz.net,[776] a German hotline therefore tries to seek

---

769 Laki lapsipornografian levittämisen estotoimista, lagen om åtgärder som hindrar spridning av barnpornografi; no. 1068/2006.

770 See The Parliamentary Ombudsman of Finland, Consideration of reports submitted by States parties under Article 44 of the Convention, Fourth reports of States Parties due in 2008, Finland /CRC/C/FIN/4, 4086/8/10, 3 January 2011.

771 See EDRi-gram, Finland: Blocking of domestic websites ruled illegal, 01 June, 2011, at <http://www.edri.org/edrigram/number9.11/blocking-case-finland-court>.

772 See The Finnish Internet Censorship List at <http://lapsiporno.info/suodatuslista/english.html>.

773 www.w3.org

774 See Deutsche Welle, Deleting trumps blocking in fight against online child porn, 06.04.2011, at <http://www.dw-world.de/popups/popup_lupe/0,,14968970,00.html>. According to Deutsche Welle, a law from the previous coalition of Christian Democrats (CDU) and Social Democrats stated that Germany would fight the spread of child pornography on the Internet by blocking sites with pornographic content involving children. The current CDU-Free Democrats (FDP) coalition believes deleting the sites is a better way to solve the problem and had previously announced it would test out the policy over the course of one year.

775 See *ibid*.

776 Jugendschutz.net was founded in 1997 by the Youth Ministers of the German Federal States, in order to check content on the Internet according to its relevance to youth protection and to see to the compliance with youth protection laws. Content that is endangering to the development of children and young persons,

removal of content involving racist content and child pornography from websites or social media platforms. In Germany, providers are obliged to remove illegal content from their servers after obtaining actual knowledge (notice and take down). In terms of illegal content abroad Jugendschutz.net contacts the host provider and asks them to delete such content. Furthermore, ISPs based in North Rhine-Westphalia have been made responsible for the illegal content they host. ECRI states in its third report on Germany, that "while this measure is reported to have resulted, for the most part, in the spontaneous removal of such illegal content by the service providers, in some instances court cases are also reported to have been initiated".[777] Similarly, the Regional Administration of Düsseldorf issued orders against certain ISPs in order to block access to websites located overseas which contained Nazi propaganda. The Higher Administrative Court of Münster upheld these orders as a suitable means to guarantee the non-proliferation of Nazi propaganda in Germany.[778]

In **Georgia**,[779] Article 102 of the 'Regulations of the provision of service in the field of electronic communications and protections of the customers' rights' declares that an owner of an Internet site shall examine any link provided through that site in order to ascertain that the Internet site/page referred to by means of the link concerned does not contain any offensive or inadmissible production.[780] There will be a requirement to take down such a link if the link contravenes the requirements of this section. Under Article 103 of the Regulations access to a website may be blocked if the website contains inadmissible production. Furthermore, in case of violation of the Georgian law on "Copyright and Neighbouring Rights" through the Internet, the National Communications Commission is authorized[781] to contact ISPs, or the relevant Internet sites and domain holders to protect the copyright law of Georgia and block or remove illegal content.

In **Italy**, the competent judicial authority (or the judicial police on their own initiative) can order seizure, either to prevent an offence or to collect evidence, of a website with illegal content, or which is used to commit an offence.[782] It is understood that these provisions may also be applicable to Web 2.0 based applications and services. Since 2006, online gambling has been permitted only via state-licensed websites, and ISPs are required to block access to international or unlicensed gambling sites identified on a blacklist compiled by the

---

i.e. harmful content, should only be accessible to adults as far as possible. The aim is to achieve a comparable youth protection as in the traditional media. Since a change in the German legislation and the entry into force of the Youth Protection Interstate Treaty (JMStV) in April 2003 jugendschutz.net is organizationally connected to the KJM (Commission for Youth Protection in the Media). However, the German Federal States continue to finance jugendschutz.net.

777 ECRI Third Report on Germany, June 2004, CRI (2004) 23, para. 110.

778 Regarding access providers, the blocking of IP addresses, the modification of domain-name servers and use of proxy servers have been accepted by German administrative courts and contemplated by German administrative authorities as a suitable means. See Study on the Liability of Internet Intermediaries, Country Report: Germany, Markt/2006/09/E (Service Contract ETD/2006/IM/E2/69), November 2007, p. 3.

779 According to the Freedom House, "while the authorities do not regularly block public access to specific websites, there have been a few cases in which they interfered with internet access on a large scale. In August 2008, during a brief military conflict between Georgia and Russia, the government blocked access to all Russian addresses (those using the .ru country code) in an effort to prevent users from receiving "unofficial" information about the fighting." See Freedom House, Freedom on the Net 2011: *A Global Assessment of Internet and Digital Media*, April 2011, at <http://www.freedomhouse.org/uploads/fotn/2011/FOTN2011.pdf>, p. 143.

780 It is not clear from the response received from the Georgian authorities what "inadmissible production" means.

781 Articles 19 and 43 of the Law of Georgia on Electronic Communications.

782 Sections 253 and 321 of the Italian Code of Criminal Procedure.

Autonomous Administration of State Monopolies (AAMS).[783] As of June 2011, access to 3,156 gambling sites are blocked from Italy. The authority transparently makes the updated blocked gambling websites list available through its website.[784] A similar blacklist for known child pornography websites is maintained by the National Center for the Fight against Child Pornography on the Internet within the Postal and Communications Police Service[785] since February 2006. Subject to the obligations envisaged by law, the black list shall be monitored by all Italian ISPs.[786]

Year	Web sites monitored	Web sites certified and obscured in Italy	Reports sent to foreign bodies	Sites included in the black list
98/00	25,847	43		
2001	24,325	2	2	
2002	23,940	22	993	
2003	50,964	58	1,356	
2004	25,446	26	1,589	
2005	59,044	1	1,951	
2006	38,372	2	2,356	
2007	22,445	10	2,635	
2008	23,281	13	104	386
2009	26,872	0	40	127
2010 (as of 15.09.2010)	15,244	2	0	142
Total	**335,780**	**179**	**11,026**	**655**

Table 16. Statistical table on the activities of Italy's Postal and Communications Police service

While several thousands of websites were monitored from Italy, as of January 2011, there were 715 websites on the Italian child pornography blacklist.[787]

In **Kazakhstan**, several provisions exist which may result to blocking access to websites. For example, subject to article 15(3) of the Law No. 567-II "On Communications,"[788] special investigations agencies are authorized to suspend the activity of any network and media if these are used for criminal purposes, i.e. which are detrimental to the interests of the individuals, society, and the state. Furthermore, subject to article 21(3) of the Law No. 217-III "On Informatization,"[789] authorized government bodies, communications operators, and

783 See further Freedom House, Freedom on the Net 2011: *A Global Assessment of Internet and Digital Media*, April 2011, at <http://www.freedomhouse.org/uploads/fotn/2011/FOTN2011.pdf>.

784 See <http://www.aams.gov.it/site.php?id=2484>.

785 See <http://www.poliziadistato.it/articolo/view/10232/>. Chapter II of Act 38/2006 provides for the setting up within the Postal and Communications Police Service of the National Centre for the Fight against Child Pornography on the Internet – a body of the Ministry of the Interior – having the task to guide, monitor and fights minors' sexual exploitation on the Internet.

786 Aection 19 of act 38/2006 amending section 14 of Act 269/98.

787 See La Nuova di Venezia e Mestre, "Pedopornografia, «ripuliti» mille siti web," 08 January, 2011, at <http://nuovavenezia.gelocal.it/cronaca/2011/01/08/news/pedopornografia-ripuliti-mille-siti-web-3132641>.

788 Article 15, Cooperation between Communications Operators and Special Investigation Agencies (5 July 2004).

789 Article 21, Use of Information and Communication Networks (11 January 2007, with amendments and addenda as of 15 July 2010).

proprietors of Internet resources shall be compelled to suspend or terminate the distribution of a media product or publication if a court rules that content distributed by information and communication networks contradicts the requirements of this Law and other national legal acts. If a court rules to suspend the distribution of unlawful content over the Internet, this could result in the suspension of the website's domain name for up to three months. [790] With respect to www.geo.kz, a website having several mirror domain names, including one on LiveJournal, a court ordered in May 2009[791] to terminate the distribution of illegal information posted on these resources. As a result of this decision access to LiveJournal was also blocked from Kazakhstan.[792] The decision of the Specialized Interdistrict Economic Court of Almaty[793] stated that the Court prohibits

> "the distribution of the media products of the Kazakhstan information portal geo.kz, mirror websites www.geokz.ru, www.geokz.su, www. geokz.com, as well as the following blogs: www.geokz.livejournal.com, http://blogs.mail.ru/list/geokz/, as well as other Internet resources containing (duplicating) the content of the Kazakhstan information portal geo.kz. To make it incumbent on Kazakhstan providers to execute the decision on prohibition of the distribution of media products by the named websites and blogs."[794]

It should also be noted that article 12 of the Law No. 31-III "On Counteracting Extremism"[795] prohibits the use of networks and the media for engaging in extremism, as well as for publishing and distributing extremist materials in the Republic of Kazakhstan.[796] If networks or media are used for engaging in extremism, authorized bodies carrying out special investigations in compliance with the legislation of the Republic of Kazakhstan shall have the authority to suspend the activity of such networks and media. Their activity shall be prohibited by courts as envisaged by the laws of the Republic of Kazakhstan. In March 2009, while presenting a report entitled "On Efforts to Develop Information Technology in the Republic of Kazakhstan", the chairman of the Agency on Informatization and Communications stated that the Authority has "to either remove or close down an average of five domains a month based on decisions of the law-enforcement agencies."[797]

The laws of the **Kyrgyz Republic** does not provide for sanctions in the form of blocking access to websites or other types of Internet content or cutting off connections to the Internet. At the same time, legislation does envisage that, within the scope of consideration of a civil suit on violation of copyright, and neighbouring rights a court may impose provisional

---

790 Article 21(4), Use of Information and Communication Networks.

791 A vibrant global social media platform where users share common passions and interests.

792 See Ekspress-K newspaper, No. 337 (16723) of 26 May 2009.

793 No. 2-2009 of 17 March 2009.

794 Ekspress-K newspaper, No. 337 (16723) of 26 May 2009.

795 Dated 18 February 2005.

796 Article 12, Prohibition of the Use of Networks and the Media for Engaging in Extremism, Publishing and Distributing Extremist Materials: Information materials distributed in the Republic of Kazakhstan and containing elements of extremism shall be recognized as extremist by the court in accordance with a statement from the prosecutor at the location of the prosecutor who issued such a statement, or at the place where such information was found, with prohibition of its conveyance, publication and distribution. The court must base its ruling on the extremist nature of an information document on the conclusion of a forensic investigation.

797 Note the following decisions: The decision of the Specialised Interdistrict Economic Court of Almaty of 17 March 2009 No. 2-2009 (on a legal action filed by the Prosecutor of the Bostandyk District of Almaty in the interests of the state against the Kazakhstan information portal geo.kz for banning the distribution of a media product); decision of the Specialized Interdistrict Economic Court of Almaty of 1 July 2008 No. 2-2361/08 (on a legal action filed by the Prosecutor of the Medeu District of Almaty in the interests of the state against the Expert Centre of National Strategy Foundation for suspending the Internet publication www.posit.kz, Pozitsiya.kz).

remedies. One possible remedy is to prohibit the respondent from performing certain actions, this potentially taking the form of blocking access to websites or other types of Internet content.[798]

In **Latvia**, the Criminal Code does not provide for blocking access to websites as a basic or a supplementary punishment. In **Liechtenstein**, there are legal provisions which require closing down and/or blocking access to websites. The National Police Law for instance allows for the formulation of recommendations to block and/or close websites. The police have also the power to freeze, seize, and confiscate propaganda material.[799] In addition, the National Police of Liechtenstein have an agreement with the Swiss Coordination Unit for Cybercrime Control (CYOS). Based on this contractual agreement, ISPs agreed to follow voluntary measures to report illegal Internet content to the respective country.

In **Lithuania**, there are legal provisions which allow the courts to impose sanctions to block access to specific websites upon the request of a person whose rights are violated. Courts can only close down and/or block access to websites or any other types of Internet content with an injunction. Furthermore, the Lithuanian administrative law also includes certain removal provisions. In March 2003, the Procedure on the Control of Forbidden Information on Public Use Computer Networks and the Distribution of Restricted Public Information was approved by Order No. 290 of the Government of the Republic of Lithuania.[800] The Procedure aims to provide regulations for the control of forbidden information[801] on public use computer networks; regulations for the distribution of restricted public information on these networks; and control over the implementation of the above-mentioned regulations.[802] According to the Procedure, the police department is responsible for the operation of a special phone number and mailbox to which violations of the procedure can be reported to. The Lithuanian Criminal Police Bureau and other law enforcement institutions must carry out the investigations within their competence in the manner prescribed by law. Violations of the procedure are reported to the information and hosting service provider or to the network service provider. Where the information and hosting service provider, and/or the network service provider have been informed that illicit information[803] is stored on their servers, they must terminate access to this information, if the termination is technically possible.

Subject to Paragraph 14 of the Procedure, content should be removed from the websites hosted on the servers of information access providers and network service providers. The latter should discontinue access to the server information upon court orders, or once information and hosting service providers or network service providers become aware of the fact that the information in question is stored on their servers, and if removal is technically possible. This provision is used, for example, with regards to content involving child pornography. However, there is no law which prescribes blocking access to websites hosted by the providers registered outside the borders of the Republic of Lithuania.

---

798 Even so, the State Intellectual Property Agency of the Kyrgyz Republic does not have at its disposal any information about a court imposing such provisional remedies.

799 Verordnung vom 8. Mai 2007 □ber Identifikationsmittel und Frequenzen im Bereich der elektronischen Kommunikation (IFV), LGBl. 2007 Nr. 118, Art. 68 ff. Gesetz vom 21. Juni 1989 □ber die Landespolizei (Polizeigesetz, PolG), LGBl. 1989, Art. 48, Art. 25d Abs. 4.

800 Resolution No. 290 (Gazette, 2003, no. 24-1002).

801 The publication and/or distribution of such information is prohibited by the Laws of the Republic of Lithuania.

802 See the Country report for Lithuania, CoE CODEXTER: CyberTerrorism, September 2007, at <http://www.coe.int/t/dlapil/codexter/4_theme_files/Lithuania.pdf>.

803 Content subject to this administrative removal process may include racist, and xenophobic content among others.

It should also be noted that article 7(3) of the Law on the Protection of Minors Against the Detrimental Effect of Public Information states that persons providing services of access to public computer networks (the Internet) must ensure the installation and operation of filtering measures for harmful Internet having a detrimental effect on minors. The procedure is approved by the Information Society Development Committee. Upon the recommendation of the Committee, the Government shall establish the procedure for the use of mandatory filtering measures at access points to public computer networks.

In **Moldova**, there are no general blocking provisions. The Moldovan legislation, however, provides for a domain name seizure policy. Sanctions in the form of recall of a domain are envisaged by the Regulations on Administration of Names in the Top Level Domain .md dated 28 August 2000,[804] based on the law "On Telecommunications" No. 241-XVI dated 15 November 2007.[805] Therefore, it is prohibited for .md domain names to include information and images of an obscene or insulting nature, content which denigrates the Republic of Moldova or other states, or incites to violence, as well as their use for purposes and activities prohibited by national legislation and international treaties. If this provision is breached, the National Registrar for domain names may terminate the registration of the relevant .md domain name.[806]

In the **Netherlands**, a voluntary public-private collaboration agreement between the Dutch police and the ISPs exist with regards to the blocking of websites with content involving child pornography hosted outside the Dutch jurisdiction. However, in November 2010, Dutch ISPs sent a letter to the Dutch Minister of Justice and expressed their intention to abondon blocking as it is deemed ineffective as a measure to combat child pornography.[807]

In **Norway**, there are various legal measures which could be used to block access to websites. Subject to the Electronic Communications Act,[808] the Authority,[809] may order providers to implement restrictions on the use of electronic communications networks and services in the interest of national security or other important societal consideration. Providers shall implement necessary restrictions on Internet use in emergency situations that involve serious threats to life or health, safety or public order, or danger of sabotage against networks or services. Providers may immediately disconnect radio and terminal equipment when it is necessary in the interest of communication security or the network's integrity and given that the provider offers an alternative solution without delay. The costs of providing an alternative solution shall be borne by the provider. The Authority may issue regulations on restrictions on use and on exceptions to the requirement for permission.

---

804 Monitorul Oficial of the Republic of Moldova No. 25-26/75 dated 01 March 2001.

805 Article 8 (effective date 14 March 2008), (National Agency for Regulation in the Sphere of Telecommunications and Informatics).

806 See sections 3.8 and 5.5, Chapter III Principles and Procedures for Registration, Prolongation, Amendment, or Recall of a Subdomain of the Regulations on Administration of Names in the Top Level Domain .md.

807 The letter stated that "based on the reports of the Child Abuse Hotline we have come to the preliminary conclusion that (...) blocking websites containing child pornography by means of a blacklist can no longer serve as a reliable and effective way to contribute to fighting child pornography on the Internet." See Bits of Freedom, Dutch providers abandon "ineffective" web blocking, 07 March, 2011, at <https://www.bof.nl/2011/03/07/dutch-providers-abandon-ineffective-web-blocking/>.

808 Sections 2-5 (Permitted restrictions on use) of the Electronic Communications, 4th of July 2003.

809 The Authority includes the King, the Ministry of Transport and Communications, and the Norwegian Post and Telecommunications Authority. Section 1-4, Authority under the Act: The King may determine the allocation of functions within the Authority, and may determine that other public or non-public entities shall have authority in limited areas under the Act.

Access to websites depicting child sex abuse is blocked at ISP level since 2004 with the establishment of the Child Sexual Abuse Anti Distribution filter (CSAADF). The law enforcement agency NCIS Norway evaluates and verifies illegal sites and provides a list of domains to the ISPs based on a written agreement between NCIS Norway and the ISPs. The contract has been developed by the Internet Service Providers Association of Norway.[810] The number of websites subject to blocking varies. On average between 800–1200 websites which could be subject to blocking are up and running at any given time .

Furthermore, in case of copyright infringement, rights holders may request a court injunction pursuant to chapter 34 of the Dispute Act to stop the alleged violation.[811] With regards to Internet piracy, a Norwegian District Court ruled that there were no grounds for ordering the Norwegian ISP Telenor to block access to the popular Pirate Bay website in November 2009. The Court of Appeal rejected an appeal filed by the music and film industry in February 2010. The appeal court held that Telenor did not unlawfully contribute to the infringement of copyright by providing access to the Pirate Bay website.[812]

In **Poland**, there are no general legal provisions which require closing down and/or blocking access to websites or any other types of Internet content. However, pursuant to the Polish Criminal Law certain activities on the Internet are prohibited including the dissemination and public presentation of child pornography or pornography involving presentation of violence, and promotion of fascist or another totalitarian regime. Concerning the rules of criminal law, it should be noted that the aforementioned provisions do not explicitly provide the possibility to mandate the provider of a website to close it down, however, such a result could be achieved on the basis of general provisions. According to the Criminal Proceedings Act it is possible to impose preventive measure by way of mandate to refrain from certain activities.[813] This may in particular consist of an order to refrain from managing a particular website. Such preventive measure may be imposed by the court in the course of criminal proceedings, as well as by the public prosecutor in the course of preparatory proceedings. Furthermore, an order to close a website is provided as a preventative measure (not a penalty) as set out in Article 39(2) of the Criminal Code.[814]

In **Romania**, Article 16 of Law 365/2002 on Electronic Commerce establishes the obligation of ISPs to report alleged illegal activities to public authorities. ISPs are also required to temporarily or permanently interrupt the transmittal or hosting of information through their systems by taking down the content or by blocking its access, if these actions have been required by ANCOM,[815] the competent authority[816] ex-officio, or at the receipt of a claim or

---

810 NCIS Norway receives statistics on a daily basis from the largest ISPs in Norway. The report is based on anonymous log files where NCIS Norway is able to see the referral site, search words leading to the illegal sites, time of day, browser and operation system. NCIS Norway does not receive the IP information, a point exclusively mentioned in the contract with the ISPs.

811 Act of 17 June 2005 no. 90 relating to mediation and procedure in civil disputes (The Dispute Act).

812 Borgarting Court of Appeal, LB-2010-6542 (10-006542ASK-BORG/04), 9 February 2010. See Winsvold, L., Telenor not Obliged to Block Access to The Pirate Bay, IRIS 2010-4:1/34. See also Winsvold, L., Unsuccessful Attempt to Block the Pirate Bay, IRIS 2010-1:1/33.

813 Article 276 of the Polish Criminal Proceedings Act.

814 This legal provision constitutes a penal measure in the form of prohibition of carrying out certain economic activity.

815 The Authority for Regulation in Communications and Information Technology.

816 Article 17 of Law 365/2002: The Authority is competent to monitor and control the compliance of the service providers to the provisions of the present law and of its methodological norms, to ascertain the contraventions and to apply the sanctions provided for.

complaint from any person.[817] Access to websites containing child pornography may be subject to these provisions. Furthermore, Article 7 of the C.N.A. Decision No. 187/2006 with its further modification on the Audiovisual Code established the obligation for adult pornography websites to be password protected, and access to such websites to be subject to a payment. Breaches of Article 7 can be reported to ANCOM which upon verification can ask the ISPs to block access to the website in question.

In the **Russian Federation**, there are no laws envisaging closing down or blocking access to websites. However, access may be blocked if provisional measures are applied under civil, administrative, or criminal proceedings. Sanctions may be applied in accordance with a court decision in the event that a website contains extremist material on the grounds of Articles 1(3) and 12 of the Law "On Extremism". The Ministry of Internal Affairs, within its competence, is taking measures to terminate within the Russian territory the functioning of Internet resources containing materials banned by Russian Federation Law. For example, in 2009, the activities of 1528 websites were suspended, 45 of them in accordance with crimes envisaged by articles 280 and 282 of the Criminal Code. Furthermore, a Federal Law entitled Protection of Rights of Communication Service Users[818] regulates the responsibilities of the communication operators and limitation of service users during the search and operative research measures conducted by authorized bodies, measures aimed at ensuring the security of the Russian Federation, and other investigatory actions.[819] Such provisions may be applied by implementing provisional measures or executing a court decision. Sanctions in the form of blocking access to websites distributing pirate content are applied in accordance with a court decision if the content of such websites is recognized as a breach of copyright on the basis of Section IV of the Civil Code.

It should be noted that in accordance with a court decision, in July 2010, the local provider in Komsomolsk-on-Amur "Rosnet" was compelled to limit users' access to YouTube, as the platform hosted "Russia For Russians", an ultra-nationalist video on the Justice Ministry's federal list of banned extremist materials. The court ban extended to four other electronic libraries (Web.archives.org, Lib.rus.ec, Thelib.ru and Zhurnal.ru) after experts found extremist materials on these websites, including the text of Adolf Hitler's 'Mein Kampf', also placed on the federal list of extremist materials banned for distribution in the Russian Federation.[820]

In **Serbia**, there are no specific legal provisions which require closing down or blocking access to websites or any other types of Internet content. However, there is a reporting duty for the ISPs who must inform the competent national authority if it reasonably suspects that a client is involved in illegal activities conducted via its services. There is, however, no general monitoring obligation.[821] In **Slovenia,** subject to articles 9-11 of the Electronic Commerce Market Act,[822] it is possible to block access to specific websites or block Internet traffic by the

---

817 Subject to Article 16(3) the claim can be made by any person who considers himself (herself) prejudiced by the contents of the respective information. The claim or complaint is made in writing, showing the reasons that substantiate it and will compulsorily be dated and signed. The claim cannot be forwarded if a trial has already been initiated with the same subject and with the same parties.

818 Chapter 9 (64) "Protection of Rights of Communication Service Users" of Federal Law No. 126-FZ of 07 July 2003 "On Communications".

819 Subject to Civil Procedural Code of the Russian Federation, Arbitration Procedural Code of the Russian Federation, Criminal Procedural Code of the Russian Federation.

820 See The Guardian, "YouTube banned by Russian court," 29 July 2010, at <http://www.guardian.co.uk/world/2010/jul/29/youtube-ban-russian-regional-court>.

821 See Section 4, Article 20 of the Law on Electronic Commerce.

822 Official Gazette Republic of Slovenia No 61/2006.

order of a judge if the measure is justified by *lex specialis*. Furthermore, the Gambling Act[823] has a special provision that makes it possible for the gambling regulatory authority to issue specific Internet blocking measures, so that foreign gambling sites are made inaccessible from Slovenia. This provision is due to be changed in the direction of a general rule, which would enable the courts of law to order Internet filtering and blocking. During the reporting period of the OSCE RFOM study the national gambling regulator issued six administrative orders to block access to certain foreign Internet gambling sites through several Slovenian ISPs. Furthermore, the authority issued 234 administrative orders to block access to certain websites.[824] Most of these administrative orders are contested by the ISPs in Slovenia.

In **Sweden**, there are no proscribed sanctions involving blocking access to websites. According to the Swedish Constitution it is not possible for public institutions to block access to websites as a sanction for an offence. However, the 1998 Act on Responsibility for Electronic Bulletin Boards[825] requires the suppliers of electronic bulletin boards to supervise their systems to an extent which is reasonable considering the extent and objective of the system on offer. If a particular message posted to the forums contains racial agitation,[826] child pornography,[827] or other types of illegal content, the 1998 Act requires the suppliers of the service to remove and delete such content. A fine or imprisonment is possible for those who intentionally or through gross negligence violate Article 5. Furthermore, the ISPs, and the National Police Board provide for a voluntary blocking measure for content involving child pornography. Injunctions may also be issued with regards to copyright infringements. Such injunctions may include blocking access to websites.

In **Switzerland**, there are no laws allowing a state institution to block access to unlawful websites. Liability for Swiss providers is provided on an actual knowledge basis. However, there have been no cases involving an ISP during the reporting period for this OSCE study. In terms of websites hosted abroad, the Swiss ISPs are invited to block access to websites carrying child pornography. A list is maintained by the Swiss Coordination Unit for Cybercrime Control (SCOCI) and updated weekly. The ISPs block these websites on a "voluntary basis", and there is no law compelling the Swiss ISPs to do so. However, a non-binding agreement is reached between the ISPs and SCOCI. Furthermore, two exceptions where the Swiss law itself provides for a website or domain name to be blocked or deleted should be noted. Subject to Article 13a BWIS,[828] the Federal Act on Measures for Safeguarding National Security, propaganda material can be removed if hosted in Switzerland, or access blocked if hosted abroad. Furthermore, under certain conditions, the SWITCH foundation, which is the domain name registry for ".ch" is obliged to freeze a domain name[829] which is used for "phishing" or the spread of malicious software following a request by OFCOM, the recognized body for the fight against cybercrime.[830]

---

823 Article 107, Gambling Act (Official Gazette Republic of Slovenia No 27/1995).

824 DNS poisoning is the method employed to block access to websites from Slovenia.

825 An electronic bulletin board means a service for conveyance of electronic messages, basically Internet-based forums for discussion.

826 Section 8, Penal Code.

827 Section 10, Penal Code.

828 Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit.

829 Article 14fbis AEFV: blocking of a domain name for suspected abuse.

830 The amendment of Decree on Addressing Resources in the Telecommunications Sector (ORAT, SR 784.104), 4 November 2009, the Federal Council measures against cyber crime, came into force on 1 January 2010.

Access to a substantial number of websites have been blocked in **Turkey** since the enactment of Law No. 5651[831] in May 2007. Under Article 8(1) of Law No. 5651 websites are subject to blocking if there is 'sufficient suspicion' that certain crimes are being committed on a particular website. The Article 8 provisions do not clarify or establish what is meant by 'sufficient suspicion'. The eight specific crimes that are included in Article 8 are encouragement and incitement of suicide,[832] sexual exploitation and abuse of children,[833] facilitation of the use of drugs,[834] provision of dangerous substances for health,[835] obscenity,[836] prostitution,[837] gambling,[838] and crimes committed against Atatürk.[839] Article 8 blocking provisions were extended in January 2008, and are applicable in matters concerning football and other sports betting websites. Websites which enable users to play games of chance via the Internet and which are based outside the Turkish jurisdiction and lack valid licence or permission are also susceptible to blocking.[840] More recently, in February 2011, the blocking list was extended to include websites which sell and provide alcohol and tobacco related products to those under the age of 24. Websites that carry content subject to Article 8 could be taken down if hosted in Turkey, or blocked and filtered through Internet access and service providers if hosted abroad.

Law No. 5651 enables not only the courts of law to issue judicial blocking orders, but also an administrative body, the Telecommunications Communication Presidency ("TIB") to issue administrative blocking orders. Neither the courts nor TIB can block access to websites based on reasons outside the scope of Article 8. The directors of hosting and access providers who do not comply with the blocking orders issued through a precautionary injunction by a public prosecutor, judge, or a court, could face criminal prosecution, and could be imprisoned between six months and two years under Article 8(10). Furthermore, Article 8(11) states that access providers who do not comply with the administrative blocking orders issued by TIB could face fines between 10,000YTL (ca. 4,735 euros) and 100,000YTL (ca. 47,350 euros). If an access provider fails to comply with an administrative blocking order within twenty-four hours of being issued an administrative fine, the Telecommunications Authority can revoke the access provider's official licence (activity certificate) to act as a service provider.[841]

An OSCE report published in January 2010 stated that approximately 3,700 websites had been blocked from Turkey since the enactment of Law No. 5651.[842] The official blocking statistics are kept secret and since May 2009 have not been published.[843] However,

---

831 Law No. 5651 is entitled "Regulation of Publications on the Internet and Suppression of Crimes Committed by means of Such Publication".

832 Article 84 of the Turkish Penal Code.

833 Article 103(1) of the Turkish Penal Code.

834 Article 190 of the Turkish Penal Code.

835 Article 194 of the Turkish Penal Code.

836 Article 226 of the Turkish Penal Code.

837 Article 227 of the Turkish Penal Code.

838 Article 228 of the Turkish Penal Code.

839 Law No. 5816, dated 25/7/1951.

840 Law Amending Some Acts to Harmonise Criminal Law No 5728, Article 256. Official Gazette, 23.1.2008, No. 26781.

841 All decisions of TIB and the Authority can be challenged at administrative courts as provided under Administrative Justice Procedure Act No. 2577.

842 Akdeniz, Y., Report of the OSCE Representative on Freedom of the Media *on Turkey and Internet Censorship*, January 2010, at <http://www.osce.org/documents/rfm/2010/01/42294_en.pdf>.

843 A legal challenge under the freedom of information law has been lodged with an Ankara administrative court with regards to obtaining the blocking statistics: See Bianet, "TİB'e Erişim Engelleme İstatistiklerini Gizlemekten Dava," 13 May, 2010, at <http://bianet.org/bianet/ifade-ozgurlugu/121956-tibe-erisim-engelleme-istatistiklerini-gizlemekten-dava>.

Engelliweb, a project which collects data on blocked websites, estimates that number to be around 14,000 as of April 2011.[844] The application of Law No. 5651 resulted in blocking access to a considerable number of foreign websites including prominent sites such as YouTube, Geocities, DailyMotion, Metacafe,[845] Google Sites, Playboy, and Rapidshare. Similarly, websites in Turkish, or addressing Turkey related issues have been subjected to blocking orders under the Law No. 5651. This has particularly affected news websites such as Özgür Gündem, Azadiya Welat, Keditör, Firat News, and Günlük Gazetes that are reporting on south-eastern Turkey and Kurdish issues. Furthermore, Gabile.com and Hadigayri.com, which form the largest online gay community in Turkey with approximately 225,000 users, were also blocked during 2009. Sanalika.com, a Turkish virtual world and playground, and 5Posta.org, a popular blog containing articles about sexuality, sexual politics, and Internet censorship among other issues have been also subject to blocking decisions. With regards to the YouTube ban that lasted almost two and a half years, three separate applications have been lodged with the European Court of Human Rights between 2009 and 2011.[846] The Strasbourg Court is yet to decide whether to assess further these applications and possible violations of Article 10. However, an application made to the Strasbourg Court in January 2010 with regards to the blocking of Google Sites[847] is currently being reviewed by the Court.[848]

Further blocking provisions are provided under Supplemental Article 4 of the Law No. 5846 on intellectual property. This particular measure which was introduced in March 2004 provides a two-stage approach. Initially, the law requires the hosting companies, content providers, or access providers to take down the infringing article from their servers upon 'notice' given to them by the right holders. The providers need to take action within 72 hours. If the allegedly infringing content is not taken down or there is no response from the providers, the right holders may ask a Public Prosecutor to provide for a blocking order which would be executed within 72 hours. This legal remedy is therefore predominantly issued with regards to websites related to piracy and IP infringements. Media reports suggest that at least 3,000 websites were blocked under Law No. 5846, the majority of which are blocked indefinitely. However, these provisions were also used to block access to popular social media platforms such as Blogspot,[849] Myspace, and Last.fm. Access to Fizy.com, a popular music and video-sharing Turkish website which won an award for best music search engine at the 2010 Mashable Awards was also blocked from Turkey. An appeal to the European Court of Human Rights based on an infringement of Article 10 was lodged in 2010 with regards to the blocking of the Last.fm website from Turkey. The Strasbourg Court decided to assess further the Last.fm application,[850] and published its statement of facts on its website in February 2011.

---

844 See generally <http://engelliweb.com/>. This website's work was also mentioned in the latest edition of the Country Reports on Human Rights Practices prepared by the U.S. Department of State. See 2010 Country Reports on Human Rights Practices published in April 2011 at <http://www.state.gov/g/drl/rls/hrrpt/2010/index.htm>. The Turkey Country report is available at <http://www.state.gov/g/drl/rls/hrrpt/2010/eur/154455.htm>.

845 Metacafe has been blocked since May 2010.

846 YouTube was subjected to a total of 17 blocking orders between March 2007 and May 2008, and remained inaccessible from Turkey until October 2010. See further Akdeniz, Y., & Altiparmak, K., *Internet: Restricted Access: A Critical Assessment of Internet Content Regulation and Censorship in Turkey,* Ankara: Imaj Yayinevi, November 2008. An online version is available through <http://www.cyber-rights.org.tr>.

847 Application No. 31111/10.

848 The European Court of Human Rights published the statements of facts in February 2011, and asked the government of Turkey to respond by June 2011.

849 Blogspot was inaccessible between February-April 2011 from Turkey.

850 Application No. 20877/10.

This will be the first Internet censorship and blocking case to be reviewed jointly with the above mentioned Google Sites application by the European Court of Human Rights.

In **Ukraine**, subject to Article 39(18) of the Law "On Telecommunications" the operators and telecommunication providers must restrict access to websites that contain child pornography subject to court orders. Furthermore, subject to Article 38, telecommunications operators have the right to disconnect, pursuant to a court decision, the terminal equipment if it is used by the consumer for conducting unlawful acts. The Internet Association of Ukraine, comprised by major ISPs, informs that in practice the ISPs execute sanctions specified by the courts and at the request of law enforcement agencies.

In the **United Kingdom**, there are no legal provisions on blocking access to websites. However, there exists "voluntary blocking" mechanisms, and agreements in the UK to block access to websites containing child pornography. The British Telecom ('BT') in partnership with the Internet Watch Foundation ('IWF') developed the CleanFeed Project[851] in late 2003. This follows the decision of the IWF to assist its subscribing ISP members in filtering potentially illegal content from their client services through the use of the Child Abuse Images URL service.[852] The CleanFeed Project aims at blocking access to any images or websites that contain child pornography within the IWF database. Customers of BT (and other UK ISPs that use the system) are prevented from accessing the blocked content and websites. At present, the use of the CleanFeed system by the ISPs is voluntary, and there is no legal requirement to implement the system. However, it is estimated that ISPs who provide their services to over 90% of domestic broadband connections are currently using the system.[853] Problems with the voluntary blocking approach were highlighted in December 2008 by an incidence involving Wikipedia. The IWF, added a Wikipedia article called *Virgin Killer* to its Internet blacklist. This resulted in the entire Wikipedia website being blocked from within the United Kingdom because of a single image, which had been available on the Internet for years. The image depicted the cover of an album called *Virgin Killer* by the famous German heavy metal band Scorpions.[854] The IWF revoked its decision after five days subsequent to an appeal by the Wikipedia Foundation.[855]

In terms of blocking statistics, the IWF Annual Report 2010 revealed that online child sexual abuse content is highly dynamic and transient, as a result of which the IWF blocking list is updated twice a day. During 2010, a cumulative total of 14,602 webpages featured on the IWF webpage blocking list of live child sexual abuse content. An average of 59 webpages

---

851 IWF/BT Project CleanFeed, at <http://www.iwf.org.uk/media/news.archive-2004.39.htm>.

852 See generally Child Abuse Images URL database at <http://www.iwf.org.uk/public/page.148.htm>. See further the IWF discussion paper, *Commercialising the CAI URL Database*, June 2004, at <http://www.iwf.org.uk/corporate/page.94.176.htm>, and Addendum to the discussion paper at <http://www.iwf.org.uk/corporate/page.94.177.htm>. Note further Recommendations from the Board and FC Working Group on Commercialising the CAI Database, February 2005, at <http://www.iwf.org.uk/corporate/page.128.277.htm>, as well as the revised recommendations of May 2005, at <http://www.iwf.org.uk/corporate/page.141.304.htm>.

853 Child Abuse (Internet), House of Commons Hansard Written Answers for 15 May, 2006.

854 The Observer, "Wikipedia censorship highlights a lingering sting in the tail," 14 December, 2008, at <http://www.guardian.co.uk/technology/2008/dec/14/wikipedia-censorship-scorpions-virgin-killer>.

855 Wikimedia Foundation, "Censorship in the United Kingdom disenfranchises tens of thousands of Wikipedia editors," 07 December, 2008, at <http://wikimediafoundation.org/wiki/Press_releases/Censorship_of_WP_in_the_UK_Dec_2008>. See further Wikinews, "Wikimedia, IWF respond to block of Wikipedia over child pornography allegations," 08 December, 2008, at <http://en.wikinews.org/wiki/Wikimedia,_IWF_respond_to_block_of_Wikipedia_over_child_pornography_allegations>.

were added to the list daily reflecting the speed at which child sexual abuse content moves online location. The average number of live URLs on the list at any given time was 500 down from 1,200 in 2008.[856] According to the IWF 2010 report, over 70 ISPs, search and content providers, mobile operators and filtering companies take steps to prevent their customers from being exposed to child sexual abuse content. Furthermore, the IWF webpage blocking list is deployed across six continents and in countries including Chile, New-Zealand, the **United States**, **Ireland**, **Spain**, **Slovakia**, **Switzerland**, and **Montenegro**.

In terms of copyright infringements, Section 97A of the Copyright, Designs and Patents Act 1988[857] provides that the High Court (in Scotland, the Court of Session) shall have power to grant an injunction against a service provider,[858] where that service provider has actual knowledge of another person using their service to infringe copyright. However, the "mere (or even knowing) assistance or facilitation of the primary infringement is not enough" [859] to hold service providers liable.[860] The joint tortfeasor "must have so involved himself in the tort as to make it his own. This will be the case if he has induced, incited or persuaded the primary infringer to engage in the infringing act or if there is a common design or concerted action or agreement on a common action to secure the doing of the infringing act."[861]

Furthermore, Section 17 of the Digital Economy Act 2010 allows the Secretary of State to table regulations on court injunctions requiring service providers to block access to sites for the purpose of preventing online infringement of copyright. The regulations have to provide that a court may only grant an injunction if the Internet location is, or is likely to be, used to host or access a substantial amount of pirate content. A court should take into account the extent to which the operator of the site and the service provider have taken steps to prevent infringement of copyright on that particular website. The regulations must require the courts to consider the extent to which the copyright owner had made efforts to facilitate legal access to such content. The courts must consider the effect on legitimate uses or users of the online location, and the importance of freedom of expression. The regulations must require the service provider and operators of the location in question to be given notice of an application for an injunction. They may also provide that a court should not make a cost order against a service provider.

---

856 See generally the IWF 2010 Annual Report at <http://www.iwf.org.uk/accountability/annual-reports/2010-annual-report>.

857 This provision implements Article 8(3) of Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society which states that "Member States shall ensure that rightholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right."

858 A service provider is anyone providing an information society service. An information society service is broadly defined as any service normally provided for remuneration at a distance by means of electronic equipment for the processing (including digital compression) and storage of data and at the request of a recipient of the service (see section 97A(3) of the 1988 Act and regulation 2 of the Electronic Commerce (EC Directive) Regulations 2002 (S.I. 2002/2013)). Examples of these include Internet service providers, and providers of websites, such as Internet storage facilities.

859 See *Twentieth Century Fox Film Corp and others v Newzbin Ltd* [2010] All ER (D) 43 (Apr); [2010] EWHC 608 (Ch): The Chancery Division held that the claimants would be granted the injunction sought since the defendant's website service had infringed the claimants' copyrights. The service had authorised acts of infringement, had entered into a common design to infringe with those members and had communicated the claimants' copyright works to the public.

860 See *L'Oréal v eBay* [2009] EWHC 1094, [2009] RPC 21; *Sabaf SpA v MFI Furniture Centres Ltd* [2002] EWCA Civ 976, [2003] RPC 264; *Credit Lyonnais Bank Nederland NV v Export Credits Guarantee Dept* [1998] 1 Lloyd's Rep 19.

861 *Twentieth Century Fox Film Corp and others v Newzbin Ltd* [2010] EWHC 608 (Ch).

In June 2011, a leaked paper appeared online suggesting that the government considered proposing voluntary blocking measures to combat Internet piracy.[862] The paper was drafted by the Rightsholder Group[863] as a response to a request by the Minister for Culture to evaluate the scope to move toward a cross-industry voluntary approach to inhibiting access to websites infringing copyright. According to the document, actions of intermediaries, notably ISPs and search engines are crucial to achieving the effective prevention of infringement. Therefore, a self-regulatory "Voluntary Scheme"[864] which would require the rightsholders to identify infringing sites and ISPs to block access to such sites has been proposed. The proposal includes the development of a voluntary code and the application of judicial decisions to order blocking access to such sites.

Finally, over 2,600 domain names used for criminal activity, were seized, and taken down by the UK between December 2009 and March 2011.[865] The majority of the websites taken down were fraudulent websites, and according to the police, these concerned primarily consumer protection cases such as sale of counterfeit products, and fraud and phishing scams. Requests to seize the domain names were submitted by the Police Central eCrime Unit and the seizure activity took place through Nominet, the Internet registry for .uk domain names.

Similarly, in the **United States**, the Department of Homeland Security, and Department of Justice announced the execution of seizure warrants against ten domain names of websites engaged in the advertisement and distribution of child pornography as part of "Operation Protect Our Children", a joint operation with the U.S. Immigration and Customs Enforcement to target sites that provide child pornography. However, it was later reported that 84,000 subdomains associated with mooo.com, a shared domain operated by afraid.org were rendered inaccessible.[866] Affected websites were down for about three days, during which time visitors would encounter a notice stating that the Department of Justice and Department of Homeland Security had seized that particular domain, and that advertising, distribution, possession, transportation, and receipt of child pornography is a federal crime.[867]

---

862 The document (10 June, 2011) stated that "This note is confidential, commercially sensitive and without prejudice. In particular, the proposal made in this note is entirely without prejudice to the rights of copyright owners under UK law, including (without limitation) the claims made in the action brought by the studios represented by the MPA, directed at blocking subscriber access to the Newzbin 2 website." See Open Righrs Group, "Rights Holders' proposed voluntary website blocking scheme," 22 June, 2011, at <http://www.openrightsgroup.org/blog/2011/rights-holders-propose-voluntary-website-blocking-scheme>.

863 The Football Association Premier League Limited; the Publishers Association; BPI (British Recorded Music Industry) Limited; the Motion Picture Association; and the Producers Alliance for Cinema and Television.

864 The proposed "Voluntary Scheme" is based on and works within the parameters of existing law, notably Section 97A of the Copyright, Designs and Patents Act 1988 (S97A, CDPA) and Sections 17 and 18 of the Digital Economy Act 2010 (S17/18 DEA).

865 See O' Floinn, M., Dealing with domain names used in connection with criminal activity. Background report on views expressed, Nominet commissioned report, <http://www.nominet.org.uk/digitalAssets/48619_Report_on_Abuse_Policy_M_O_Floinn_Final_Web_amended.pdf>. See further a MET Police Department letter revealing the statistics subsequent to a freedom of information request in the UK: <http://www.met.police.uk/foi/pdfs/disclosure_2011/february/2010110005000.pdf>.

866 mooo.com is the most popular shared domain at afraid.org, which belongs to a the DNS provider FreeDNS. According to FreeDNS, mooo.com is not a domain used for child pornography; rather, it is home to some 84,000 websites primarily belonging to individuals and small businesses. See TorrentFreak, "U.S. Government Shuts Down 84,000 Websites, 'By Mistake'," 16 February, 2011, at <http://torrentfreak.com/u-s-government-shuts-down-84000-websites-by-mistake-110216/>. Note further "CE seizes 82 website domains involved in selling counterfeit goods as part of Cyber Monday crackdown, 29 November, 2010, at <zhttp://www.ice.gov/news/releases/1011/101129washington.htm>.

867 See InformationWeek, "ICE Confirms Inadvertent Web Site Seizures," 18 February, 2011, at

Policies on Filtering Software and Children's Access to Harmful Content

According to a recent OECD report, "content risks comprise three main sub-categories: i) illegal content; ii) age-inappropriate or harmful content; and iii) harmful advice. Potential consequences vary with the risk and other factors, such as the child's age and resilience."[868] The OECD study also stated that "risks vary from country to country depending on children's ability to access the Internet as well as on a range of social and cultural factors."[869] According to the OECD, "the protection of children online is a relatively recent area of public policy concern, and many countries are in the process of re-assessing existing policies and formulating new policy responses."[870] Approaches therefore vary but usually blend "legislative, self- and co-regulatory, technical, awareness, and educational measures, as well as positive content provision and child safety zones."[871]

In terms of EU policy, the European Commission's 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 euro budget.[872]

Self-regulatory solutions are also supported by the Council of Europe. 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 encourages self-regulation and co-regulatory initiatives regarding Internet content.[873] With regards to protection of children from harmful content, the Council of Europe's Committee of Ministers recommended in July 2009[874] that member states in co-operation with private sector actors and civil society shall develop and promote coherent strategies to protect children against content and behaviour carrying a risk of harm. According to a Parliamentary Assembly Recommendation of 2009 the needs and concerns of children online should be addressed without undermining the benefits and opportunities offered to them on the Internet. [875] 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

---

<http://www.informationweek.com/news/security/vulnerabilities/229218959>.

868 OECD (2011), "The Protection of Children Online: Risks Faced by Children Online and Policies to Protect Them", OECD Digital Economy Papers, No. 179, OECD Publishing, at <http://dx.doi.org/10.1787/5kgcjf71pl28-en>.

869 *Ibid*, p. 30.

870 *Ibid*, p. 32.

871 *Ibid*, p. 33.

872 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)).

873 Similar recommendations were made in Council of Europe Recommendation on self-regulation concerning cyber-content. See Council of Europe Rec(2001)8, 5 September 2001.

874 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.

875 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

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."[876]

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"[877] as well as the development of a pan-European trustmark and labelling system[878] was encouraged, the CoE Committee did not recommend state level 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."[879] 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."[880]

CoE principles therefore allow for exceptions for the protection of minors, and member states can consider the installation and use of filters in places accessible to children such as schools or libraries.[881] However, the Committee of Ministers stated in its Recommendation (2008)6[882] 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.

---

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

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

878 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.

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

880 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).

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

882 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.

The Guidelines provided within the March 2008 Recommendation[883] stated that Internet users should have the possibility to challenge the blocking decisions or filtering of content, and be able to seek clarifications and remedies.[884] 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. 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 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.

The universal and general blocking of offensive or harmful content for users who are not part of a specific vulnerable group, such as children, should be avoided according to the CoE Guidelines. This recommendation distinguishes between adults' use 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. More recently, the CoE Committee of Experts on New Media (MC-NM) developed draft guidelines for search engines[885] and social networking providers.[886] Both documents recommend that member states should guarantee that blocking and filtering, in particular nationwide general blocking or filtering measures, are only introduced if the conditions of Article 10, paragraph 2, of the European Convention on Human Rights are fulfilled. Member states should avoid general blocking of offensive or harmful content for users who are not part of the groups for which a filter has been activated to protect. The Committee believes that search engines and social network providers should be encouraged to offer adequate voluntary individual filter mechanisms which would suffice to protect vulnerable groups such as children.

Legal provisions requiring schools, libraries, and Internet cafes to use filtering and blocking systems and software

The survey asked whether **specific legal provisions requiring schools, libraries, and Internet cafes to use filtering and blocking systems and software** exist in the OSCE participating States **(Question 18)**. No such provisions are in place in 38 (67.9%) participating States while legal provisions do exist in 6 (10.7%) states.[887] No data was obtained from 12 (21.4%) of the participating States.

---

883 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.

884 *Ibid*, Guideline I.

885 See CoE Committee of Experts on New Media (MC-NM), draft Guidelines for Search Engine Providers, MC-NM(2010)009_en, Strasbourg, 5 October 2010.

886 See CoE Committee of Experts on New Media (MC-NM), Proposal for draft Guidelines for Social Networking Providers, MC-NM(2010)008_en, Strasbourg, 5 October 2010.

887 Azerbaijan, Belarus, Croatia, Lithuania, Poland, and Turkey.

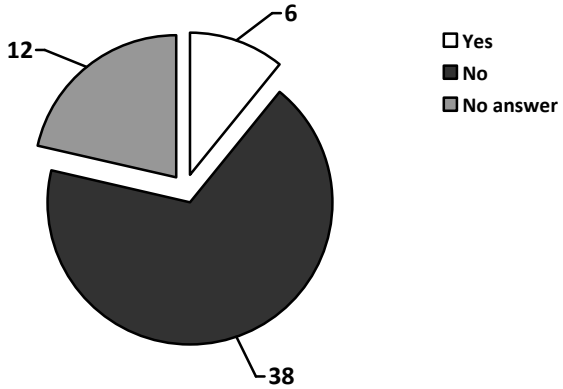


Figure 40. OSCE participating States' responses with regards to specific legal provisions requiring schools, libraries, and Internet cafes to use filtering and blocking systems and software (Question 18)

According to the International Federation of Library Associations and Institutions (IFLA) the use of filtering software in libraries has increased across the world. This is evident from the fact that 62 countries reported "yes" or "yes, to a certain degree" for the use of filtering software in libraries, compared to 50 in 2007, and 47 reported "No", compared to 60 in 2007 to a questionnaire sent by IFLA in relation to their World Report 2010.[888] According to IFLA, "by far the most common motivation for the use of filtering and blocking software is the protection of children."[889]

In **Albania**, there are no explicit legal provisions requiring schools, libraries and Internet cafes to use filtering and blocking systems or software. However, the document on the approval of the "Cross-cutting Strategy on Information Society"[890] stipulates that, in view of potential risks stemming from cyber criminality, the government shall establish necessary police structures and improve and amend the legislative and regulatory cybercrime framework. This should including the drafting of a code of conduct for ISPs and the supervision and filtering of information spread through Internet networks in the educational system. The Ministry of Education and Science is in the process of finalizing a "Plan of Integration of Information and Communication Technologies in Education 2011–2015". It focuses on online security of children, awareness raising and introduction of information and communication technologies courses in primary school curricula, as well as on the development of a digital library which includes access filters based on age groups to be used in the education system. The ministry has required ISPs to provide services to pre-university level academic institutions, adopt measures for the installation of web filters to protect children and young people from harmful websites.

In **Azerbaijan**, there are no specific legal provisions requiring the use of filtering and blocking systems or software in libraries or Internet cafes. In accordance with clause 2.4 of

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

889 According to IFLA, "A number of respondents further elaborated on the protection of children and the safeguarding of public morality and specifically mentioned the blocking of pornographic or obscene sites, sites relating to trafficking, drugs, racism, child molestation, child abuse, gambling, violence and hate speech. Some respondents also mentioned financial reasons for the use of filtering software. As in 2007 other reasons indicated for using filtering software are more technical, and include issues such as the conservation of bandwidth (preventing playing of Internet games, the downloading of large files and the use of specific programmes such as Skype) and network safety (protection against viruses, hackers and spam)." See *Ibid*, p. 21.

890 DCoM No. 59 (21.01.2009).

the "State Programme for the Informatization of the Educational System in 2008–2012,"[891] and the ministerial order "On Providing Internet Use in Academic Institutions," a "Council on Issues of Internet Use" was created under the aegis of the Ministry of Eduction. The council prepared model recommendations for Internet use in academic institutions and developed and introduced systems for classifying information unrelated to the education process in academic institutions, thereby isolating the network of academic institutions from dangerous content.

In **Belarus**, in accordance with clause 8 of Decree No. 60, ISPs are required to provide access restrictions for educational and cultural institutions on content on: extremist activities; unlawful trafficking in weapons ammunition explosive devices, explosive, radioactive, venomous, potent, poisonous, toxic, narcotic or psychotropic substances and their precursors; promotion of illegal migration or human trafficking; distribution of pornographic material; propaganda of violence, cruelty and other acts prohibited by law. The access restrictions are provided in accordance with the Regulations on the procedure for restricting access of Internet users to information prohibited for distribution.[892] Subject to clause 9 of the Regulations on the operation of computer clubs and Internet-cafés,[893] the head of a computer club or Internet-café or a person authorized thereby is required to exercise control over, and not permit use by minors of information or software subject to age restrictions.

In **Canada**,[894] the **Czech Republic**, **Hungary**, and **Norway** use of filters is voluntary, and not subject to any laws or legal provisions. Similarly, in **Kyrgyzstan**, schools, libraries and Internet cafés, at their own discretion, use filter and blocking systems and software. In **Liechtenstein**, the education authority (Schulamt) has internal provisions to filter or block certain Internet pages in order to protect pupils from illegal content. In **Belgium**, filtering software is used to some degree on local computers in libraries, mainly on terminals for children. The motivation for filtering information on library Internet terminals is to protect children and safeguard public morality.[895]

In **Croatia**, the use of the Internet in schools, libraries and Internet cafes is regulated by internal by-laws that must be in accordance with the law, and filters are used to block objectionable content. Filtering software has been implemented by ISPs, such as the Croatian Academic and Research Network (CARNET), which can prevent the display of websites that contain objectionable content on the computers in Croatian primary and secondary schools. To this end, access has been monitored for topics such as drugs, gambling, violence, hate speech and hacking, as well as websites containing nudity, profanity, pornography, school

---

891 Implemented by the Presidential Decree No. 2856 of 10 June 2008.

892 Approved by the joint resolution of the Operational Analysis Centre and the Ministry of Communications dated 29 June 2010 No. 4/11.

893 Approved by a resolution of the Council of Ministers of the Republic of Belarus dated 10 February 2007 No. 175.

894 According to IFLA, "filtering software is used to a certain degree in libraries in Canada for the protection of children and the prevention of crime. The filtering issue is a concern mainly in public libraries, and decisions regarding this are taken at local municipal level by the library and/or the library board. The Canadian Library Association (CLA) is not in favour of automatic filtering and has a policy in this regard. The association is of the opinion that the only effective filtering tool is human supervision and intervention, supported by good policy. Such a policy should clarify what type of use is acceptable and then empower staff and educate users to ensure compliance. The policy is available at http://www.cla.ca/AM/Template.cfm?Section=Position_Statements&Template=/CM/ContentDisplay.cfm&ContentID=3048." See IFLA World Report 2010, August 2010, at http://www.ifla-world-report.org

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

cheating, spam, tobacco and violence. The motivation for this approach is primarily to protect children.[896]

In **Lithuania**, article 7(3) of the Law on the Protection of Minors Against the Detrimental Effect of Public Information of the Republic of Lithuania establishes an obligation for persons providing services of access to public computer networks such as schools, libraries and Internet cafes to ensure the installation and operation of filtering measures for the harmful Internet content which has a detrimental effect on minors approved by the Information Society Development Committee under the Government of the Republic of Lithuania.

In **Poland**, subject to article 4a of the Education System Act,[897] schools and facilities providing students access to the Internet, are obligated to take measures protecting students from accessing content that may pose a threat to their normal development.

In the **Russian Federation**, although there are no such legal provisions at present, and the use of filters is voluntary, the Ministry of Education and Science of the Russian Federation is drawing up general recommendations for schools and other educational institutions on introducing content filtration and blocking systems for accessing the Internet.[898]

In **Switzerland**, there are no regulations for monitoring access to the Internet in schools and universities. However, an agreement has been agreed between SWISSCOM, Corporate Internet Connection, and the educational institutions so that SWISSCOM incorporates a filter to the network, and blocks access to a number of websites. This approach is based on a contractual basis between the different actors and not a legal requirement under Swiss law.

In **Turkey**, article 7 of Law No. 5651 regulates mass use providers, including Internet cafes. Such providers can only operate subject to an official activity certificate granted by a local authority representing the central administration. The mass use providers are required under Article 7(2) to deploy and use filtering tools approved by the Telecommunications Communication Presidency (TIB). Providers who operate without an official permission could face administrative fines between 3,000 and 15,000 Turkish lira (ca. 1,500 – 7,500 euros).[899] Under the *Regulations Governing the Mass Use Providers*,[900] providers are also required to record daily the accuracy, security, and integrity of the retained data using the software provided by TIB and to keep this information for one year.[901] The TIB is charged to determine the minimum criteria for filtering programs and the procedure that will be followed by Internet cafes to install filtering programs.[902] According to the above mentioned regulations, all mass use providers are required to use one of the filtering programs approved by the Presidency.[903] Approved programs are published on the TIB's website.[904] The TIB criteria are not made public, nor is there any official indication on what is filtered out. Some news reports claimed that a number of alternative news websites including bianet.org, alinteri.org and atilim.org, are being blocked at various Internet cafes due to certain police

---

896 This information is obtained from the IFLA World Report 2010, August 2010.

897 September 7, 1991 (Journal of Laws from 2004, No 256, item 2572 as amended).

898 A draft bill making it incumbent to use software aimed at protecting children from information that is detrimental to their health and development has been adopted in the second reading by the State Duma of the Russian Federation Federal Assembly.

899 See Article 7(3).

900 Published on 01 November 2007 on the Official Gazette, No. 26687.

901 Article 5(1)(e).

902 See Law No. 5651, article 10 (4)(ç) and (e).

903 Regulations 2, article 5(1)(c).

904 See <http://www.tib.gov.tr/onayli_filtreleme_yazilimlari.html>.

authorities compiling their own 'forbidden websites' lists and databases. It was also claimed that fines are imposed on Internet cafes that do not filter websites enumerated in these police lists.[905] More recently, news reports suggested that over one million websites are filtered through Internet cafes.[906] The filter blacklist includes apart from the so called 'harmful websites' also websites of a number of associations, NGOs', and of Turkish companies with .com.tr domain names. Further, it includes websites of model agencies , radio stations, and news portals. The Wikipedia entry for "Kurdish people" is also among the filtered pages.

Furthermore, the Turkish authorities through a decision of the Information Technologies and Communication Board (BTK)[907] decided to launch a country wide mandatory filtering system in February 2011. The BTK adopted principles and procedures for the safe use of the Internet which will force all home subscribers to choose one of four filtering profiles as of 22 August 2011. According to article 6(1) of the BTK Principles and Procedures, the ISPs will be obliged to offer four separate user profiles with different access authorizations. These four user profiles are the standard profile, children's profile, family profile and domestic Internet profile. The filtering lists for each profile including the domain names, IP addresses, port numbers and/or web proxy addresses will be provided by BTK to the ISPs. Furthermore, under article 11, the ISPs will be obliged to prevent filter circumvention methods[908] used by users for deactivating filters. ISPs will be required to periodically report the filter circumvention activities to BTK. Article 11(2) allows BTK to make further arrangements to prevent filter circumvention. The BTK decision is currently subject to a legal challenge at the Council of State which is the highest administrative court in Turkey.[909]

With the *Prevent Strategy*, the **United Kingdom** aims at responding to the "ideological challenge of terrorism and the threat from those who promote it."[910] The strategy includes tackling radicalisation on the Internet by relying on filtering technology. The Office for Security and Counter-terrorism (OSCT) engaged with the Department for Education (DfE), regional broadband consortia and the filtering software industry to explore effective filtering options in public institutions, such as schools, universities and libraries. [911] DfE and OSCT have also "secured the inclusion of language that promotes terrorism and extremism in the filtering technology 'kitemark'.[912] The kitemark covers commercial filtering software on sale to schools and families and the first accredited product is now on the market."[913] However, the government admits that it does "not yet have a filtering product which has been rolled out comprehensively across Government Departments, agencies and statutory organisations."[914] The government is "unable to determine the extent to which effective filtering is in place in schools and public libraries."[915] It also plans "to explore the potential for violent and unlawful

---

905 Bianet, "Filtrelemeci Şirkete Göre Sorumluluk Polisin," 27 June, 2007, at <http://www.bianet.org/bianet/kategori/bianet/98363/filtrelemeci-sirkete-gore-sorumluluk-polisin>.

906 Milliyet, "There is no Internet Censorship; however one-million websites are banned," 23.05.2011, at <http://privacy.cyber-rights.org.tr/?p=1466>.

907 Decision No. 2011/DK-10/91 of Bilgi Teknolojileri ve İletişim Kurumu, dated as 22 February, 2011.

908 See generally How to Bypass Internet Censorship, FLOSS Manuals, 2nd Edition, 2011, at <https://www.howtobypassinternetcensorship.org/>.

909 Council of State (10. Division), 2011/5435, commenced on 10.04.2011. The case has been initiated by IPS Communication Foundation which owns the alternative media website Bianet.

910 HM Government, *Prevent* Strategy, Cm 8092, June 2011, p. 1.

911 See *ibid*, pp 77-79.

912 The Kitemark is a UK product and service quality certification mark which is owned and operated by the British Standards Institution.

913 *Ibid*, para 10.98, p. 78.

914 *Ibid*, para 10.107, p. 79.

915 *Ibid*.

URL lists to be voluntarily incorporated into independent national blocking lists, including the list operated by the Internet Watch Foundation (IWF)."[916] The United Kingdom believes that the Home Office and police supported Counter Terrorism Internet Referral Unit "can play a significant role in developing an unlawful URL blocking list for use across the public estate."[917]

In June 2011, the Department for Education discussed how to facilitate parents' blocking of adult and age-restricted material. The *Letting Children be Children* report[918] recommended that "as a matter of urgency, the internet industry should ensure that customers must make an active choice over what sort of content they want to allow their children to access."[919] It was agreed that the Internet industry must "act decisively to develop and introduce effective parental controls, with Government regulation if voluntary action is not forthcoming within a reasonable timescale. In addition, those providing content which is age-restricted, whether by law or company policy, should seek robust means of age verification as well as making it easy for parents to block underage access."[920]

Conclusion to Part C

Complete suspension of communication services, including Internet access related services is possible in some OSCE participating States in times of war, states of emergency, as well as in the case of an imminent threat to national security. Although there is no 'Internet kill switch' in those countries, the legal provisions may allow the authorities to switch off completely all forms of communications including Internet communications in certain cases. An 'Internet kill switch' idea was considered by the **United States** where it was envisaged that the President can authorize the shutdown of critical computer systems in the event of a national cyber emergency, however, the US Senate did not act on the proposed measure.[921]

In certain countries the only remedy provided by law is removal or deletion of allegedly illegal content, while in some states, in addition to the removal measures, access blocking measures also exist. In some OSCE participating States such as in **Belarus** and the **Russian Federation** "prohibited information lists" maintained by government authorities exist. Access may be blocked if 'prohibited information' appears on the Internet. Some countries also started to develop country level domain name blocking or seizure policies (**Czech Republic, Moldova**, **Switzerland**, and **United Kingdom**).

Turkey, provides the broadest legal measures for blocking access to websites by specifying eleven different content related crimes, but does not reveal the number of websites blocked under its blocking law.

Legal provisions for blocking access to child pornography exist in **Bulgaria**, **Finland**, **Italy, Liechenstein, Romania, Turkey**, and **Ukraine**. At EU level, "mandatory blocking" of websites containing child pornography was not recommended but the member states "may take the necessary measures in accordance with national legislation to prevent access to such

916 *Ibid*, para 10.108, p. 79.
917 *Ibid*, para 10.109, p. 79.
918 Department for Education, Letting Children be Children: Report of an Independent Review of the Commercialisation and Sexualisation of Childhood by Reg Bailey, Cm 8078, June 2011.
919 *Ibid*, p. 15.
920 *Ibid*.
921 Cnet News, Internet 'kill switch' bill will return, 24 January, 2011, at <http://news.cnet.com/8301-31921_3-20029282-281.html>.

content in their territory".[922] However, in a number of countries, so-called 'voluntary blocking measures' to block access to known child pornography websites exist. **Canada**, **Denmark**, **France**, **Finland**, **Netherlands**, **Norway**, **Sweden**, **Switzerland,** and the **United Kingdom** are among the participating States where such voluntary arrangements exist. While **Canada** and the **United Kingdom** rely on the British Telecom developed Cleanfeed system for ISP-level blocking, other ISP-level blocking systems are used in other participating States where voluntary blocking measures exist. During Action Plan II of the Internet Related Child Abuse Material Project (**CIRCAMP**), **Italy**, **Finland, Norway, Sweden, Denmark** and **Malta** started using the Child Sexual Abuse Anti Distribution Filter (CSAADF) to block access to websites containing child pornography. In almost all instances, blocking lists and blocking criteria are not made public. Only in **Italy**, the blacklist for blocking access to international or unlicensed gambling websites is transparently made available.

There is concern that voluntary blocking mechanisms and agreements do not respect due process principles within the states in which they are used. In the absence of a legal basis for blocking access to websites, platforms, and Internet content, the compatibility of such agreements and systems with Article 10 of the European Convention on Human Rights is arguably problematic. Although the auhorities' good intentions to combat child pornography, and other types of illegal content is understandable, in the absence of a valid legal basis in domestic law for blocking access to websites, the authority or power given to certain organizations and institutions to block, administer, and maintain the blacklists remains problematic. Such a "voluntary interference" will be in breach of Article 10 unless the requirements of Article 10(2) are fulfilled, and the necessity for interference is convincingly established.[923] The European Court reiterated the importance of freedom of expression as one of the preconditions for a functioning democracy. Genuine, "effective" exercise of this freedom does not depend merely on the State's duty not to interfere, but may require positive measures to protect this fundamental freedom.[924] Therefore, a blocking system based exclusively on self-regulation or "voluntary agreements" risks to amount to a non-legitimate interference with fundamental rights.

It is recalled that the courts of law are the guarantors of justice which have a fundamental role to play in a state governed by the rule of law. In the absence of a valid legal basis the issuing of blocking orders and decisions by public or private institutions other than courts of law is therefore inherently problematic from a human rights perspective. Even provided that a legal basis exists for blocking access to websites, any interference must be proportionate to the legitimate objective pursued. Within this context, it is submitted that the domain-based blocking of websites and platforms carrying legal content such as YouTube, Facebook, Wordpress, and Twitter could be incompatible with Article 10 and regarded as a serious infringement on freedom of speech. Such a disproportionate measure would be too far-reaching than reasonably necessary in a democratic society.[925] The Internet started to play an essential role as a medium for mass communication, especially through the development of Web 2.0 based platforms, enabling citizens to actively participate in the political debate and discourse. These platforms provide a venue popular across the world for alternative and dissenting views. Therefore, banning access to entire social media platforms carries very strong implications for political and social expression.

---

922 Committee on Civil Liberties, Justice and Home Affairs, Press Release: Delete child pornography web pages across the EU, says Civil Liberties Committee, 14.02.2011.

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

924 See *Özgür Gündem v. Turkey*, no. 23144/93, §§ 42-46, ECHR 2000-III, and *Fuentes Bobo v. Spain*, no. 39293/98, § 38, 29 February 2000.

925 *Khurshid Mustafa and Tarzibachi v. Sweden*, App. no. 23883/06, judgment of 16 December, 2008.

State-level blocking policies undoubtedly have a very strong impact on freedom of expression, which is one of the founding principles of democracy. Blocking orders that are issued and enforced indefinitely on websites could result in "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 court.[926] This is particularly valid for the press as news is a perishable commodity and delaying its publication, even for a short period, may well deprive it of all its value and interest.[927] The same principles also apply to new media and Internet publications. It is argued that prior restraint and other bans imposed on the future publication of entire newspapers, or for that matter websites and Internet content are incompatible with the rights stipulated in the European Convention on Human Rights. The Strasbourg Court requires the consideration of less draconian measures such as the confiscation of particular issues of publications including newspapers, or restrictions on the publication of specific articles.[928] Arguably, the practice of banning access to entire websites, and the future publication of articles thereof (whose content is unknown at the time of access blocking) goes beyond "any notion of 'necessary' restraint in a democratic society and, instead, amounts to censorship". [929]

It is worth noting that litigation in **Belgium** triggered an application to the European Court of Justice with regards to ISP-level blocking and filtering of websites containing copyright infringement. Advocate General Cruz Villalón of the Court of Justice of the European Union indicated that a measure ordering an ISP to install a system for filtering and blocking electronic communications in order to protect intellectual property rights in principle infringes fundamental human rights.[930] The decision of the European Court of Justice will shed further light into blocking measures and their implications for fundamental human rights. Similarly, the European Court of Human Rights is currently considering two applications (Google Sites, and Last.fm) from **Turkey**, and both of these applications involve blocking measures. The European Court of Human Rights, therefore, may establish principles with regards to Internet and freedom of expression, and may comment on the issue of blocking access to websites. A decision surrounding these issues is expected to have broader implications within the Council of Europe region.

In terms of issues surrounding search engine providers, the CoE Committee of Experts on New Media published draft "Guidelines for Search Engine Providers" during 2010.[931] The Committee stated that "search engine providers must promote transparency about systematic nationwide blocking or filtering about certain types of content and adhere to the principle of due process when removing specific search results from their index and provide access to

---

926 *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.

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

928 *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.

929 *Cumpănă and Mazăre 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.

930 Court of Justice of the European Union, Press Release: Advocate General's Opinion in Case C-70/10 Scarlet Extended v Société belge des auteurs compositeurs et éditeurs (Sabam), No 37/11, Luxembourg, 14 April 2011.

931 See CoE Committee of Experts on New Media (MC-NM), draft Guidelines for Search Engine Providers, MC-NM(2010)009_en, Strasbourg, 5 October 2010.

redress mechanisms"[932] regardless whether the origin of removal requests is governmental, co-regulatory or private.[933]

In terms of filtering software use, such tools are mostly used in schools, libraries, and Internet cafes within the OSCE region. In most cases, there are no legal requirements for their use but in certain participating States such as **Belarus**, **Croatia**, **Lithuania**, **Poland**, and **Turkey** there are legal provisions for academic institutions, libraries, and/or Internet cafes. In other states such as **Canada**, **the Czech Republic**, **Hungary**, and **Norway** the use of filters is voluntary and not subject to any laws or legal provisions. The International Federation of Library Associations and Institutions, in conclusion to its 2010 report, warned that "such filtering could, however, very easily develop into general Internet censorship and any developments should be carefully monitored by library communities and other interested parties, so as to ensure that legitimate information needs of the general public can be satisfied. Finally, "upstream filtering" of the Internet is a matter of serious concern."[934] Here it should be noted that **Turkey** decided to introduce a country-wide mandatory filtering system that will be functional as of 22 August 2011. If realized, this will lead to the first government controlled and maintained mandatory filtering system within the OSCE region.

---

932 *Ibid*.

933 See further CoE Committee of Experts on New Media (MC-NM), Draft Recommendation on the protection of human rights with regard to search engines, MC-NM(2010)004_en, Strasbourg, 11 March 2010

934 See *Ibid*, pp. 49-50.

D. Licensing and Liability related issues, and Hotlines to report Illegal Content

The final part of this study analyzes licensing and legal liability provisions related to information society service providers including access, content, platform, and search engine providers. In terms of access providers, according to the CoE,

> "ISPs have a unique position and possibility of promoting the exercise of and respect for human rights and fundamental freedoms. In addition, the provision of Internet services is increasingly becoming a prerequisite for a comprehensive participatory democracy. ISPs also play an important role vis-à-vis states which are committed to protecting and promoting these rights and freedoms as part of their international law obligations."[935]

In terms of liability for carrying third party content, in most instances liability will only be imposed upon information society service providers (including ISPs, 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[936] provides a limited and notice-based liability with takedown procedures for illegal content. The EU Directive suggests that "it is in the interest of all parties involved in the provision of information society services to adopt and implement procedures"[937] to remove and disable access to illegal information. Section 4 of the EU Directive through articles 12-15[938] deals with liability of intermediary service providers. As far as hosting issues by information society service providers are concerned, article 14(1) of the e-Commerce Directive requires Member States to:

> "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."

Based on the above provision, the service providers based in the European Union are not immune from prosecution and liability, and they are required to act expeditiously "upon obtaining actual knowledge" of illegal activity[939] or content, and "remove or disable access to the information concerned"[940]. 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

---

935 See CoE Human rights guidelines for Internet service providers, developed by the Council of Europe in co-operation with the European Internet Services Providers Association (EuroISPA), H/Inf (2008) 9.

936 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.

937 *Ibid*.

938 Article 12: Mere conduit, article 13: Caching, article 14: Hosting, article 15: No general obligation to monitor.

939 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.

940 *Ibid*., para. 46.

this purpose at national level".[941] Under the EU Directive on Electronic Commerce, "notice" has to be specific but may be issued by an individual complainant or by a self-regulatory hotline. In some states the notice may only be issued by law-enforcement agencies or provided through court orders. However, 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". However, it was decided that the notice and takedown procedures would not be regulated in the EU Directive itself.[942] Rather, the Directive, through recital 40, and article 16, encourages self-regulatory solutions, and procedures to be developed by the Internet industry to implement and bring into action the "notice and takedown procedures".[943]

In addition to the notice-based limited liability provisions, the Directive prevents EU Member States from imposing a general monitoring obligation on service providers. Under article 5, 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".[944]

A European Commission analysis of practice on notice and take-down 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".[945] A further review was subsequently commissioned in 2007, and the study disclosed all but harmonised implementation policies because "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."[946] 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".[947] In 2010, the European Commission announced that it had found that the interpretation of the provisions on liability of intermediaries is frequently considered

---

941 *Ibid*.

942 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, section 4.7.

943 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.

944 Article 15(2). One group of member states, Belgium, Cyprus, Estonia, France, Greece, Italy, Latvia, Lithuania, Malta, and Portugal provide for a special obligation on the part of intermediaries to communicate illegal activities or information on their services. See Study on the Liability of Internet Intermediaries, Markt/2006/09/E (Service Contract ETD/2006/IM/E2/69), November 2007, p. 72.

945 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, section 4.7.

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

947 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.

necessary in order to solve problems, and subsequently launched a consultation.[948]

Furthermore, a CoE Parliamentary Assembly Recommendation on the promotion of Internet and online media services appropriate for minors[949] recommended 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,"[950] and that this work may require the drafting of a new additional protocol to the Convention on Cybercrime. However, since this call in 2009 no action has been taken at the CoE level to draft a new additional protocol to the Cybercrime Convention.

In terms of the OSCE RFOM study, the OSCE participating States were asked whether there are specific

- legal liability provisions and licensing requirements for Internet Service Providers (**Question 19**)
- legal provisions based on the "notice and take-down" principle (**Question 16**)
- legal liability provisions and licensing requirements for Internet Search Engines or Content Providers (e.g. Google, Yahoo, etc.) (**Question 20**)
- (public or private) Hotlines to report allegedly illegal content (**Question 17**)

The survey asked whether **specific legal liability provisions and licensing requirements for Internet Service Providers** are in place in the OSCE participating States. **(Question 19)** While in 19 (33.9%) states no such legislation exist, 25 (44.7%) responded positely to the question. No data was obtained from 12 (21.4%) of the participating States.

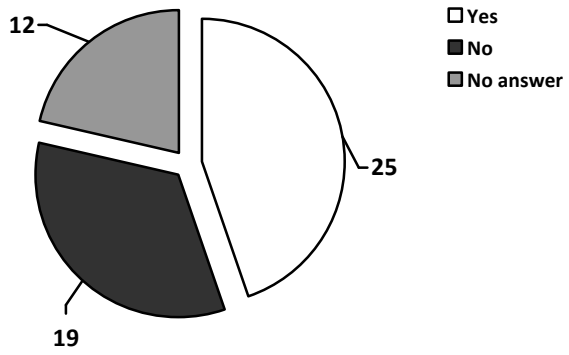


Figure 41 . OSCE participating States' responses with regards to specific legal provisions and licensing requirements for Internet Service Providers (Question 19)

Similarly, the participating States were also asked whether **there are specific legal liability provisions and licensing requirements for Internet Search Engines or Content Providers** (e.g. Google, Yahoo, etc.)**(Question 20)**. While four (7.1%) of the states responded posititely,

948 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. The result of this work will be taken into account in the Commission's deliberations with a view to the adoption in the first half of 2011 of a Communication on electronic commerce, including on the impact of the Electronic Commerce Directive .

949 1882 (2009).

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

no such legal provisions exist in 38 (67.9%) of the participating States. No data was obtained from 14 (25%) of the participating States.

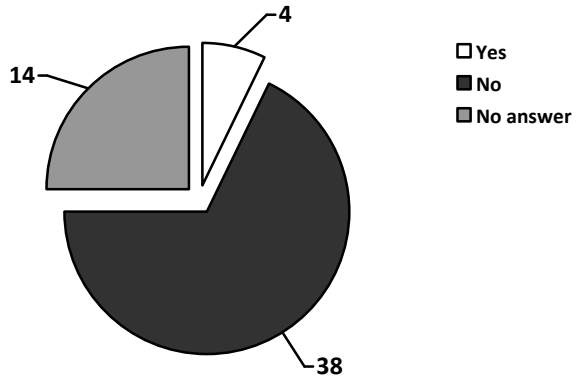


Figure 42. OSCE participating States' responses with regards to specific legal liability provisions and licensing requirements for Internet Search Engines or Content Providers (Question 20)

As can be seen above almost none of the OSCE participating States provide for any separate legal liability regime or licensing requirements for Internet search engines and content providers.

The survey also asked whether **specific legal provisions based on the "notice and take-down" principle** exist in the OSCE participating States **(Question 16)**. No such provisions are in place in 27 (48.2%) participating States while legal provisions do exist in 18 (32.2%) states. No data was obtained from 11 (19.6%) of the participating States.

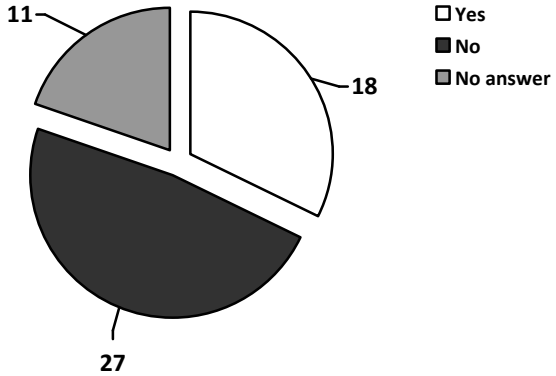


Figure 43. OSCE participating States' responses with regards to specific legal provisions based on the "notice and take-down" principle (Question 16)

Finally, the participating States were asked **whether the EU E-Commerce Directive 2000/31 has been implemented into national law in their country** (if applicable – Question 19c). In 32 (57.1%) of the participating States the EU Directive is implemented into national law.[951] 10 (17.9%) states responded negatively and no data was obtained from 14 (25%) of the participating States.

[951] It has to be noted, however, that only 27 of the 56 OSCE participating States are members of the European Union. The 32 countries that implemented the Directive include also EU candidate and potential candidate countries.

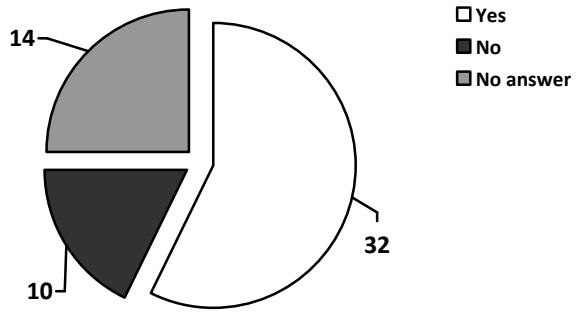


Figure 44. OSCE participating States' responses with regards to the implementation of the EU E-Commerce Directive 2000/31 (Question 19c)

The responses received for the above mentioned questions will be assessed together below as they are related to each other.

In **Albania**, the Law No. 9918 on electronic communications includes certain provisions on obligations and criteria for telecommunication operators relating to the safeguarding of fundamental rights and freedoms. The Law No. 9918 also includes provisions on technical security parameters of telecommunication networks,[952] and liability provisions for providers of public electronic communications networks and services. The provisions pertaining to service providers include data retention,[953] the safeguarding of the secrecy and confidentiality of electronic communications,[954] the provision of unsolicited commercial communications,[955] and the lawful eavesdropping of telecommunications.[956]

Similarly, Law No. 9157 on eavesdropping of telecommunications includes provisions in connection to eavesdropping capabilities of telecommunication networks[957] and obligations to cooperate with governmental authorities.[958] Law No. 9887 on the protection of personal data stipulates cases in which service providers are exempt from liability for the release of the pertinent notification regarding data processing,[959] and the measures to be taken in view of the security of personal data.[960] Furthermore, Law No. 10128 on electronic commerce includes liability provisions on unsolicited commercial communications,[961] liability exemptions for service providers acting as intermediaries,[962] and liability exemptions for temporary data storage/caching.[963] Hosting[964] and search engine[965] related liability provisions are also included. Providers may be obliged to interrupt or prevent criminal contraventions, if required by judicial or other responsible authorities designated by law.[966] Subject to article 15, service

952 Article 15 of Law No. 9918 (19.05.2008) on electronic communications.
953 Article 101 of Law No. 9918 (19.05.2008) on electronic communications.
954 Articles 121-126 of Law No. 9918 (19.05.2008) on electronic communications.
955 Article 128 of Law No. 9918 (19.05.2008) on electronic communications.
956 Article 131 of Law No. 9918 (19.05.2008) on electronic communications.
957 Article 21 of Law No. 9157 (04.12.2003) on eavesdropping of telecommunications.
958 Article 22 of Law No. 9157 (04.12.2003) on eavesdropping of telecommunications.
959 Article 21 of Law No. 9887 (10.03.2008) on the protection of personal data.
960 Article 27 of Law No. 9887 (10.03.2008) on the protection of personal data.
961 Article 9 of Law No. 10128 (11.05.2009) on electronic commerce.
962 Article 15 of Law No. 10128 (11.05.2009) on electronic commerce.
963 Article 16 of Law No. 10128 (11.05.2009) on electronic commerce.
964 Article 17 of Law No. 10128 (11.05.2009) on electronic commerce.
965 Article 18 of Law No. 10128 (11.05.2009) on electronic commerce.
966 Article 20 of Law No. 10128 (11.05.2009) on electronic commerce.

providers acting only as information intermediaries are not responsible for the information submitted by users of the services, if the provider does not initiate the transmission or modify the content and does not choose the recipient of the information. Furthermore, service providers who provide access to information to third parties are not responsible if they are unaware or cannot have knowledge of related illegal activities. However, upon becoming aware of any illegal activities or upon obtaining pertinent indications, they are obliged to remove or deactivate access to the relevant information.[967] While information society service providers have no obligation to oversee the information they transmit/store or to investigate facts or situations linked to criminal activities, they are obliged to immediately notify the responsible authorities if they have reasonable suspicion that users are carrying out illegal activities or have submitted illegal information. In these cases service providers have to submit to the responsible state authorities all necessary information that enables the identification of recipients of these services.[968] Law No. 10128 on electronic commerce is in full compliance with the requirements of the EU E-Commerce Directive 2000/31 related to legal aspects of information society services and in particular electronic commerce. While the application of EU E-Commerce Directive 2000/31 can take full effect only for EU member states, the main requirements of the Directive have been used as a model in the establishment of the regulatory framework on the domestic market for electronic commerce in Albania.

In **Armenia**, ISPs are required to obtain a license in accordance with article 43 of the Law on Licensing. In **Austria**, the E-Commerce Act transposed the EU E-Commerce Directive into national law, and certain service provider liability provisions exist under section 13. Regarding civil law, section 14 of the E-Commerce Act (ECG, BGBl. I 2001/152) provides for liability restrictions for search engines, and section 16 ECG for host providers.[969] Section 16 of the E-Commerce Act in accordance with article 14(1)(b) of the E-Commerce Directive excludes host-provider from being responsible for the information stored on behalf of a user given that the provider immediately takes action to remove illegal information or block access to it once made aware of it. Although this provision was drafted to provide for limited liability, the jurisdiction of the courts interpreted it such that the operator of an "online forum" is obliged to remove contributions if the operator becomes aware of the fact that such a forum contains illegal content.

In **Azerbaijan**, there are no specific legal provisions and licensing requirements for ISPs. However, according to the "Action Plan for Harmonizing Azerbaijan Legislation with the Legislation of the European Union,"[970] , it is planned to harmonize domestic laws with the EU E-Commerce Directive by mid-2012. A limited application of the notice and take-down system is witnessed in Azerbaijan with regards to personal data. Subject to articles 5.7, and 7.2 of the law "On Personal Data," personal data published without the consent of an individual must be removed from websites subsequent to a written demand of the individual concerned, a court, or bodies of the executive branch.

In **Belarus**, in accordance with Clause 11 of the Decree "On measures to improve use of the national segment of the Internet,"[971]

---

967 Article 18 of Law No. 10128 (11.05.2009) on electronic commerce.

968 Article 20 of Law No. 10128 (11.05.2009) on electronic commerce.

969 Host providers incur a civil law liability for the distribution of their own content just like any other direct perpetrator (desistance, removal, damages). For the distribution of alien content a claim for removal can be considered if they "conscientiously support" the distribution of illegal content.

970 As approved approved by clause 6 of the Third Protocol of the Azerbaijan Republic State Commission on Euro Integration of 23 October 2009.

971 Decree of the President of the Republic of Belarus dated 2 February 2010 No. 60.

> "in the event that gross or other violations of the requirements of this decree or other legislative acts in the sphere of use of the national segment of the Internet are identified, at the demand of agencies performing investigative activities, agencies of the public prosecutor's office and preliminary inquiry, agencies of the State Control Committee, and the tax authorities within the scope of their terms of reference, the given bodies issue, in the established manner, instructions to the legal entity or individual entrepreneur guilty of such violations to eliminate the given violations, indicating the deadline by which they must be eliminated";
>
> "in the event that gross violations , … repeat violations of other requirements of this Decree or other legislative acts in the sphere of use of the national segment of the Internet are identified within a period of six months of instructions being issued to eliminate violations identified, the Internet provider may block provision of Internet services to the legal entity or individual entrepreneur guilty of such violations at the demand of the authorities indicated in the first part of this clause";
>
> "Instructions to eliminate violations identified or a requirements to halt provision of Internet services may be appealed in a court of law in accordance with the legislation".

The licensing requirements and conditions with which a telecommunications operator must comply are determined by the Regulations on licensing of individual forms of activity, approved by Decree of the President of the Republic of Belarus dated 1 September 2010 No. 450. In accordance with Clause 149, Chapter 15 of the Regulations, the general licensing requirements and conditions to which a licensee is subject to are as follows:

- observance of the requirements and conditions established by regulatory and legal acts, including technical regulatory and legal acts regulating the licensed activity;
- at least one staff member specializing, trained and qualified in the sphere of the services rendered, as confirmed by a diploma or certificate certifying receipt of the requisite education (in accordance with the requirements of regulatory and legal acts, including technical regulatory and legal acts in the telecommunications sphere);
- a permit from the competent authority to use a radio frequency for operation of radio-electronic means, received as a result of allocation (assignment) of a radio frequency or channel for provision of public telecommunications services using the radio frequency;
- observance of the time indicated in the license to launch provision of the services.

If the licensee violates the licensing legislation, requirements or conditions, the procedure for suspending, terminating or cancelling the license is determined by Chapter 7 of the Regulations. In addition, licensees may be held liable in accordance with the general provisions of the civil law. Furthermore, subject to Clause 12 of Decree No. 60. providers, in particular, hosting providers, Internet providers, and Web 2.0 based service providers, are required to fulfill a lawful demand made by a criminal investigation agency, an authority conducting administrative proceedings, or a court ruling within the scope of preventing a specific unlawful act. The requirements of the Decree apply only to the national segment of the Internet , to which, for example, international search engines and service providers such as YouTube, Facebook, Google, Yahoo, and Bing do not belong to.

In **Bulgaria**, according to the Law on Electronic Communications, public electronic communications are carried out after submitting a notification to the Communications Regulation Commission (CRC). The networks and/or services, through which public electronic communications are provided, are indicated in a list, adopted by the CRC. The services for access to Internet can be carried out after submission of a notification to CRC and

respecting the general requirements when carrying out public electronic communications.[972] In terms of liability of service providers, article 13(1) of the Law on Electronic Commerce[973] states that upon providing access to or transmission through electronic communication networks the service provider shall not be liable for the content of the information transmitted and for the activities of the recipient of the service, if the provider:

1. does not initiate the transmission of the information;
2. does not select the receiver of the information transmitted, and
3. does not select or modify the transmitted information.

Providing access to or transmission through electronic communication networks referred to in article 13(1) also covers an automatic, intermediate and transient storage of the transmitted information, as this shall take place for the sole purpose of carrying out the transmission trough the electronic communication network and the information shall not be stored for any period longer than the one that is reasonably necessary for the transmission. In Bulgaria, as provided by the EU E-Commerce Directive, the service providers are not obligated either to monitor the information that they store, transmit or make accessible when providing services for the information society or to be in search of facts and circumstances that indicate unlawful activities.[974]

In **Croatia**, the requirements which are to be met by the operators including the ISPs are prescribed by the Electronic Communications Act.[975] Article 31 of the Electronic Communications Act provides general authorization for installing, using and making available any electronic communications network and providing electronic communications services on the territory of the Republic of Croatia. Article 32 states that commercial operators of public electronic communications networks and publicly available electronic communications services should notify HAKOM (the Croatian Post and Electronic Communications Agency) in writing at least fifteen days in advance about the beginning, changes and the termination of the provision of electronic communications networks and services. Within eight days following the receipt of a complete prior notification, HAKOM shall issue to the operator a certificate confirming the submission of the prior notification. Additionally, the Online Trade Act 2003 regulates the provision of information society services, the liability of the provider of information society services, and rules related to the conclusion of contracts online.

In **Canada**, there are no licensing requirements. In terms of liability issues, section 164.1 of the Criminal Code authorizes a court to order deletion of online data that constitutes child pornography or a voyeuristic recording when they are stored on a server which is within the

---

[972] The list currently relevant was promulgated in SG issue 24 of 04.03.2008.

[973] Article 13. (1) (Amended, SG No. 41/2007) Liability upon providing services for access and transmission, Law on Electronic Commerce, Chapter four: Liability incurred by the Providers of the Service for the Information Society. Furthermore, article 14 deals with liability upon providing services for automated search of information, article 15 deals with liability upon intermediate storage (caching), and article 16 with liability for storage of somebody else's information (hosting) and for electronic references to somebody else's information (linking). According to article 18, the provisions of articles 13 - 17 shall apply also to providers of information society services that are provided free of charge. In Bulgaria, the Law on Electronic Commerce has been in force since 2006 (prom. SG. 51/23 Jun 2006, amend. SG. 105/22 Dec 2006, amend. SG. 41/22 May 2007, amend. SG. 82/16 Oct 2009) The law transposes in the Bulgarian legislation Directive 2000/31/EC, known as the E-commerce Directive related to some legal aspects of the information society services and in particular to the e-commerce applied to the domestic market as well Directive 98/48 and Directive 98/34 of the European parliament and the Council of the EU.

[974] See article 17: Absence of a general obligation to monitor the information.

[975] Official Gazette 73/08.

court's jurisdiction. More specifically, the court may order the custodian of the computer system (through which the material is being made available) to: (a) give an electronic copy of the material to the court; (b) ensure that the material is no longer stored on, and made available through the computer system; and (c) provide the information necessary to identify and locate the person who posted the material. However, this *in rem* procedure allows the removal of the material regardless of where the owner of the material is located or whether he/she can be identified.[976] Similarly, section 319(4) of the Criminal Code also authorizes a court to order forfeiture of anything by means of or in relation to which an offence under section 318 (advocating genocide) or section 319 (public incitement of hatred) was committed. Furthermore, section 320.1 of the Criminal Code allows a court to order the deletion of hate propaganda that is stored on and made available to the public on a computer system.[977]

In the **Czech Republic**, the responsibility of ISPs is stipulated in Act N. 480/2004 Coll. On Certain Services of the Information Society which transposed the E-commerce Directive into national law.[978] Under the law, ISPs are responsible for content posted by third parties if they have actual knowledge of the allegedly illegal nature of the content. In such cases, ISPs may be required to take-down the content. Furthermore, the law makes hosting providers responsible for failing to block or remove illegal content it was made aware of.[979] Notification of illegal content is usually provided by NGOs working in the field of child protection and the fight against child pornography.

In **Denmark**, the provision of electronic communication services is not subject to prior authorization or licensing. The general provisions of Executive Order 714 of 26 June 2008 on the Provision of Electronic Communications Services and Networks apply to the provision of electronic communications services including ISPs. According to section 15b of the Danish Act on Competitive Conditions and Consumer Interests in the Telecommunications Market,[980] providers of electronic communications services including ISPs must register their service at the National Police (Rigspolitiet). The purpose of this registration is to ensure that ISPs provide assistance when required by law with regards to criminal investigations.

---

976 Section 164.2 of the Criminal Code authorizes a court to order forfeiture of all instruments (other than real property) that were used in the commission of a child pornography offence (section 163.1) or an Internet luring of a child offence (section 172.1) and belong to the person convicted of the offence. Section 164.3 of the Criminal Code provides a procedure whereby innocent third parties can have their rights on the instruments considered for forfeiture recognized.

977 See <http://laws-lois.justice.gc.ca/eng/C-46/FullText.html> for the Criminal Code provisions.

978 Article 12(1) of the Directive corresponds to article 3(1), Act No. 480/2004 Coll., on Certain Information Society Services; article 12(2) of the Directive corresponds to article 3(2); article 13(1) of the Directive corresponds to article 4 (1) Act No. 480/2004 Coll., on Certain Information Society Services; article 14(1) of the Directive corresponds to article 5(1) Act No. 480/2004 Coll., on Certain Information Society Services; and article 14(2) of the Directive corresponds to article 5(2) Act No. 480/2004 Coll., on Certain Information Society Services.

979 Article 5 - Responsibility of the service provider on storage of content information provided by the service user: (1) The provider, of service which consists of storing information provided by the user is to be held responsible for the content of the information stored on the user'' request, only a) if aware, due to the scope of its activities and the nature and circumstances of the case that the content of the stored information or the person's conduct are illegal, or b) if informed of the tortuous nature of the content of information stored or illegitimate conduct of the user the provider failed to take all steps and measures required to remove or disallow such information. (2) The service provider referred to in paragraph 1 is always to be held responsible for the content of information stored, if the provider directly or indirectly exercises a decisive influence on the user's activities.

980 cf. Consolidated Act No. 780 of 28 June 2007.

In **Estonia**, ISPs must register according to article 3 of the Electronic Communications Act. The Act requires the service providers to inform the Technical Surveillance Authority of the provision of communications services in accordance with the provisions of article 4 of this Act. Although there are no specific legal provisions based on the notice and take-down principle, the application of this principle is possible under the Law of Obligations which regulates disputes arising from defamation, libel and indemnity.

The provisions on liability limitation in case of mere conduit and caching services have been harmonized with the EU E-Commerce Directive 2000/31/EC. Estonia has transposed these principles into the Information Society Services Act (*Infoühiskonna teenuse seadus*).[981] Similar to other states that implemented the EU E-Commerce Directive, the Estonian law includes limited liability for mere transmission of information and provision of access to public data communications network,[982] limited liability for temporary storage of information in cache memory,[983] and limited liability upon provision of information storage service,[984] Furthermore, the providers are not obliged to monitor their servers.[985] An application with the European Court of Human Rights against Estonia was launched in December 2009 by Delfi

981 14 April 2004 (Riigi Teataja 2004, 29, 191).

982 Section 8(1): Where a service is provided that consists of the mere transmission in a public data communication network of information provided by a recipient of the service, or the provision of access to a public data communication network, the service provider is not liable for the information transmitted, on condition that the provider: 1) does not initiate the transmission; 2) does not select the receiver of the transmission; 3) does not select or modify the information contained in the transmission. (2) The acts of transmission and of provision of access in the meaning of paragraph 1 of this section include the automatic, intermediate and transient storage of the information transmitted, in so far as this takes place for the sole purpose of carrying out the transmission in the public data communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission.

983 Section 9(1): Where a service is provided that consists of the transmission in a public data communication network of information provided by a recipient of the service, the service provider is not liable for the automatic, intermediate and temporary storage of that information, if the method of transmission concerned requires caching for technical reasons and the caching is performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service at their request, on condition that: 1) the provider does not modify the information; 2) the provider complies with conditions on access to the information; 3) the provider complies with rules regarding the updating of the information, specified in a manner widely recognised and used in the industry; 4) the provider does not interfere with the lawful use of technology, widely recognised and used by the industry, to obtain data on the use of the information; 5) the provider acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court, the police or a state supervisory authority has ordered such removal.

984 Section 10(1): Where a service is provided that consists of the storage of information provided by a recipient of the service, the service provider is not liable for the information stored at the request of a recipient of the service, on condition that: 1) the provider does not have actual knowledge of the contents of the information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; 2) the provider, upon obtaining knowledge or awareness of the facts specified in subparagraph 1 of this paragraph, acts expeditiously to remove or to disable access to the information. (2) Paragraph 1 of this section shall not apply when the recipient of the service is acting under the authority or the control of the provider.

985 Section 11(1): A service provider specified in sections 8 to 10 of this Act is not obliged to monitor information upon the mere transmission thereof or provision of access thereto, temporary storage thereof in cache memory or storage thereof at the request of the recipient of the service, nor is the service provider obliged to actively seek information or circumstances indicating illegal activity. (2) The provisions of paragraph 1 of this section do not restrict the right of an official exercising supervision to request the disclosure of such information by a service provider. (3) Service providers are required to promptly inform the competent supervisory authorities of alleged illegal activities undertaken or information provided by recipients of their services specified in sections 8 to 10 of this Act, and to communicate to the competent authorities information enabling the identification of recipients of their service with whom they have storage agreements.

AS, an Internet news portal that publishes up to 330 news articles a day. The statement of facts was published by the Strasbourg court on 11 February 2011. The case involves the posting of third party comments on the Delfi portal with regards to an article. Delfi received a complaint and subsequently removed the allegedly defamatory comments according to the notice-and-take-down obligation. However, Delfi refused to pay damages claimed. In June 2009, the Supreme Court ruled that both Delfi and the authors of the comments were to be considered publishers of the comments. In this context, the Court also referred to the economic interest of an Internet portal administrator, defining the publisher as an entrepreneur, similarly to a publisher of printed media. The European Court of Human Rights will consider whether there has been a violation of the applicant company's right to freedom of expression, in particular its right to impart information and ideas as guaranteed by Article 10 of the European Convention on Human Rights. The case is significantly important as it will lay down liability principles with regards to third party comments published on news portals and social media platforms. The Court will also have the opportunity to scrutinize the "notice-based liability" measures of the E-Commerce Directive.

There are no specific liability limitation provisions for search engines or content providers in Estonia. The Ministry of Economic Affairs and Communications conducted a public consultation on this matter at the end of 2008. The results showed that such provisions were not deemed to be urgently needed at the time by the business community or other stakeholders. In theory, such provisions could be enacted based on existing liability limitation models on caching or hosting services.

In **Finland,** ISP liability provisions exist. These are in line with the EU E-Commerce Directive requirements. The Directive was transposed into national law with the Act on Provision of Information Society Services (458/2002). Chapter 4 of the Act exempts service providers, acting as intermediaries, from liability.[986] The service provider's exemption from liability shall have no effect on its obligation, under any other law, to take necessary action to implement an order or a decision by a court or by any other competent authority. The Act also contains provisions on notice and take-down. However, the notice and take-down provisions are applicable only to the hosting of services.[987]

In **Georgia**, the rights and obligations of ISPs in the field of electronic communications are defined by the Georgian Law on Electronic Communications as well as by the Regulations of the provision of service in the field of electronic communications and protections of the customers rights. According to the former, activities in the field of electronic communications (including Internet service provision) are subject to authorization by the GNCC (Georgian National Communications Commission). The law defines the general rights and obligations of persons authorized to provide Internet services in Georgia. In terms of liability, article 102 of the above mentioned Regulations declares that the owner of an Internet site shall examine any link allocated on an Internet site in order to ascertain that the linked Internet website or web

986 Section 13: Exemption from liability in data transmission services and communication network services, Section 14: Exemption from liability when caching the information, Section 16: An order to disable access to information, section 17: Competent court, section 18: Legal safeguards of the content producer, section 19: Obligation by the service provider to take action to implement a decision by the authorities.

987 Section 20 (Prevention of access to material infringing copyright or neighbouring right): A holder of copyright or his/her representative may request the service provider referred to in section 15 to prevent access to material infringing copyright as prescribed in this section and in sections 22-24. The same applies to a holder of neighbouring right and his/her representative if it concerns material infringing this right. A request must be presented to the content producer whose material the request concerns. If the content producer cannot be identified or if he/she does not remove the material or prevent access to it expeditiously, the request may be submitted to the service provider by notification prescribed in section 22.

page does not contain any offensive or inadmissible production. If such a link is found, the owner shall take appropriate measures to eliminate it. Furthermore, according to article 103 of the Regulations, issuer of an Internet domain shall periodically examine the content of the Internet sites registered by the company in order to prevent the allocation of inadmissible production on such sites. On finding such production, the issuer of an Internet domain name must immediately warn the the domain name holder, identify the time limit for the removal of inadmissible production, and block the Internet site in case if the warning is ignored.

In **Germany**, legal provisions regarding the liability of ISPs have been included in the Telemedia Act (Telemediengesetz, TMG). This Act represents the implementation of the EU E-Commerce Directive. By including sections 12-15 of the EU Directive, this Act provides for general principles of responsibility,[988] rules regarding the transmission of information,[989] the interim storage of information to enable its accelerated transmission,[990] and the storage of information.[991] In addition, claims to remedy under civil law may be enforced against the ISPs subject to the Civil Code[992]. Furthermore, there are no specific legal provisions with regards to the liability of search engine providers. Pursuant to section 7(1) of the Telemedia Act (TMG), content providers are responsible and liable for the content they create and publish on the Internet.

---

988 Section 7 (General Principles) of the Telemedia Act (Telemediengesetz, TMG): (1) Service providers shall be responsible for their own information which they keep ready for use, in accordance with general legislation. (2) Service providers within the meaning of sections 8 to 10 are not required to monitor the information transmitted or stored by them or to search for circumstances indicating an illegal activity. This shall be without prejudice to obligations to remove or disable access to information under general legislation, even where the service provider does not bear responsibility pursuant to sections 8 to 10. Privacy of telecommunications pursuant to section 88 of the Telecommunications Act must be maintained.

989 Section 8 (Acting as a conduit of information) of the Telemedia Act (Telemediengesetz, TMG): 1) Service providers shall not be responsible for the information of third parties which they transmit in a communication network or to which they give access, as long as they 1. have not initiated the transmission, 2. have not selected the addressee of the transmitted information, and 3. have not selected or modified the transmitted information. Sentence 1 shall not apply when the service provider deliberately works together with a recipient of his service to commit illegal acts. (2) The transmission of information pursuant to Sub-section 1 and the provision of access to it includes the automatic, intermediate and transient storage of this information, in so far as this takes place for the sole purpose of carrying out the transmission in the communication network and the information is not stored for any period longer than is reasonably necessary for the transmission.

990 Section 9 (Temporary storage for the accelerated transmission of information) of the Telemedia Act (Telemediengesetz, TMG): Service providers shall not be responsible for automatic, intermediate and temporary storage which serves the sole purpose of making more efficient the information's onward transmission to other recipients on their request, as long as they 1. do not modify the information, 2. comply with conditions on access to the information, 3. comply with rules regarding the updating of the information, specified in a manner widely recognised and used by industry, 4. do not interfere with the lawful use of technology, stipulated in widely recognised and used industrial standards, to obtain data on the use of the information, and 5. act expeditiously to remove or to disable access to the information they have stored within the meaning of this provision upon obtaining knowledge of the fact that the information at the initial source of the transmission has been removed from the network or that access to it has been disabled, or that a court or administrative authority has ordered such removal or disablement. Section 8 (1) sentence 2 applies mutatis mutandis.

991 Section 10 (Storing of information) of the Telemedia Act (Telemediengesetz, TMG): Service providers shall not be responsible for the information of third parties which they store for a recipient of a service, as long as 1. they have no knowledge of the illegal activity or the information and, as regards claims for damages, are not aware of any facts or circumstances from which the illegal activity or the information is apparent, or 2. upon obtaining such knowledge, have acted expeditiously to remove the information or to disable access to it. Sentence 1 shall not apply when the recipient of the service is acting under the authority or control of the service provider.

992 Subject to section 1004 of the Civil Code (Bürgerliches Gesetzbuch, BGB) analogously in conjunction with section 823 of the BGB.

In **Hungary**, subject to Act C of 2003 on Electronic Communications, ISPs have to register with a regulatory authority before starting to offer their services. Hungary approved in 2001 Act No. CVIII on certain aspects of electronic commerce and information society services (Act on E-Commerce).[993] The Act contains a set of rules that are necessary to implement Directive 2000/31/EC into national law. It introduced limitation of liability concerning providers of intermediary services and extends liability to the operators of search engines. According to an IRIS report, "while the limitation on liability of intermediaries shall be applied horizontally to all kinds of infringements committed via the Internet, the scope of the notice and take-down procedure is restricted only to cases of copyright infringement."[994]

An authorization procedure also exists in **Italy** with the Ministry for Economic Development, Department for Communications as envisaged by Legislative Decree N. 259[995] under section 25 of the E-communications Code. The Legislative Decree[996] on certain legal aspects of information society services, in particular electronic commerce, in the internal market" applies to all forms of information society services including search engines. However, like in almost all EU Member States, there is a lack of general obligation to monitor for the information service providers under this legislative decree.[997] However, ISPs have an obligation to inform the competent authorities (judicial or administrative) once they become aware of an allegedly illicit activity or information concerning the user of a given service provider. In such cases, ISPs have to immediately communicate, upon request of the competent authorities, the data they possess which could enable the identification of a service user in order to identify and prevent illicit activities. Furthermore, liability is provided for non-compliance with removal or blocking requests by the competent authorities.[998] Article 14 of the Law on "Exploitation of child prostitution, child pornography and child sex tourism as new forms of slavery"[999] stipulates a legal obligation to report child pornographic materials to the "National Centre for the Fight Against Child Pornography on the Internet". ISPs are also obliged to retain such content for at least 45 days.[1000]

---

993 The Act on E-commerce entered into force on 23 January 2002.

994 Article 13(1) of the Act on E-Commerce (Notice on an unlawful information society service) states that "Holders of a right protected by the Copyright Act, established on any copyrighted work, performance, recording, audiovisual work or database, or of an exclusive right arising from trademark protection under the Act on the Protection of Trademarks and Geographical Indications of Origin (hereinafter: "rightholders") which has been infringed by the information made accessible by the service provider – excluding the standardised address of the access to the information – may request the removal of the information infringing his right by way of sending a notice in the form of a private document with full probative force or a notarised deed to the service provider defined in articles 9 to 11."See further Lengyel, M., "Act on E-Commerce," IRIS, 2001-10:Extra.

995 1 August 2003.

996 9 April 2003 No 70 on the "transposition of the Directive 2000/31/EC.

997 Section 17(1) (Lack of the general obligation to surveillance): In providing the services under sections 14, 15 and 16, the provider shall have no general obligation to surveillance on the information which transmits or stores as well as no general obligation to actively detect facts or circumstances which suggest the existence of illegal activities.

998 Section 17(3): Providers are liable for the content of the services concerned if, should the judicial and administrative monitoring authorities request them to immediately block the entry to the content in question, they fail to do so or if they do not inform the competent authorities about the illicit nature of a service they allow access to, or in case said content is detrimental to a third party.

999 03 August 3, 1998, No. 269.

1000 See Study on the Liability of Internet Intermediaries, Markt/2006/09/E (Service Contract ETD/2006/IM/E2/69), November 2007, p. 73.

In **Kazakhstan**, communications operators shall have responsibility to maintain data on their subscribers.[1001] A licensing scheme also exists under Law No. 214-III of 11 January 2007 "On Licensing". Subject to article 22,[1002] a license must be held to provide communication services including Internet services. A detailed licensing regime is provided by Resolution No. 513 of 14 April 2009 "On Approving the Rules of Licensing Activity to Provide Communications Services, the Rules of Holding Contests to Obtain Licenses for Engaging in Communications Activity and Qualification Requirements When Applying for a License to Provide Communications Services".[1003]

In **Kyrgyzstan**, under article 9 of the Law "On Licensing," activities of ISPs are classed as licensable "data transmission" activities, but the country's legislation does not provide for any specific liability and licensing requirements exclusively for ISPs. In the Kyrgyz Republic, licences are issued by the State Communications Agency of the Kyrgyz Republic. During the period from 1 January 2007 through 30 June 2010, the State Communications Agency imposed seven fines on ISPs for violating the requirements governing the procedure for operating communications facilities and rendering communications services. Such violations can lead to monetary fines.[1004]

In **Latvia**, the Law on Electronic Communications sets the general authorization regime for electronic communications service providers, including ISPs regulated by the Public Utilities Commission, the Latvian national regulatory authority. Subject to article 32 of the law, the regulatory authority shall draft a list of electronic communications networks and services. Companies that intend to provide any of these listed services need to submit a registration notification to the regulator. [1005] The list shall be published in Latvijas Vestnes, the Latvian official gazette. If the general authorization regulations are violated repeatedly, the regulatory authority may suspend rendering of activities of the electronic communications providers in the provision of services or networks for a time period up to five years, nullifying the right for such providers to provide services and networks during that time. The regulatory authority consequently would remove the respective provider from the list of electronic communications providers.[1006] The EU E-Commerce Directive 2000/31/EC has also been transposed into the national legislation.

Liechtenstein has implemented the EU E-Commerce Directive 2000/31/EC into the national law in 2003. In **Lithuania**, article 29(1) of the Law on Electronic Communications of the Republic of Lithuania provides that companies shall have the right to engage in electronic communications activities without prior permission by state institutions. Article 5 of the Law

---

1001 Article 40. Responsibility of Operators and Users of Communications Services, Law of the Republic of Kazakhstan No. 567-II of 5 July 2004 "On Communications".

1002 Licensing of Activity in Informatization and Communications.

1003 With amendments and addenda as of 18 May 2010. Note also that article 357-1 "Violation of Rules and Norms of Licensing" of the Code of the Republic of Kazakhstan on Administrative Offences provides for violation of rules and norms of licensing.

1004 The fines were imposed based on article 269 of the Administrative Code of the Kyrgyz Republic.

1005 The regulatory authority shall review the aforementioned list once a year. A provider has the right to launch an electronic communications network or commence providing the electronic communications services included in the list if he or she has submitted the registration notification to the regulatory authority according to the procedures specified in regulatory enactments. The regulatory authority shall keep record of registered providers and shall ensure the public accessibility thereof.

1006 Detailed regulations in this respect have been issued by the Public Utilities Commission (PUC). For example, see PUC Board Decision No 425 of 12 November 2008 "Regulations on electronic communications merchant's registration and on list of electronic communications networks and services" and PUC Board Decision Nr.599 of 12 December 2007 "Regulations on general authorization".

on Information Society Services allows service providers to pursue their activity without a separate authorization from a public administration institution, The EU Directive on E-Commerce has been implemented into national law by the Law on Information Society Services.[1007] Articles 12-15 of the law cover liability for all service providers, including ISPs. The law is based on the notice-based liability provisions of the E-Commerce Directive.[1008] The "notice and take-down" principle obliges access providers to take-down banned material whenever they become aware of it.[1009] This provision applies to information access and network service providers.[1010] The notice based liability system, for example, allows copyright owners or other persons whose rights were violated or their representatives, to notify the service providers and ask them to remove the allegedly infringing content from their servers. The service provider may contact the owner of the content complained of, but if no plausible explanation is provided, the provider needs to remove the complained content. The service provider is not to be held liable if the content in question is removed.[1011] In **Luxembourg**, the provisions of the Law on E-Commerce apply to hosting, access, transport and caching providers. However, they do not apply to content providers.[1012]

In **Montenegro**, the EU E-Commerce Directive 2000/31 was implemented by the amended Law on Electronic Commerce. In the **Netherlands**, the EU E-Commerce Directive was implemented by an Act of 13 May 2004 amending the Civil Code, the Code of Civil Procedure, the Penal Code and the Law on Economic Crimes. In this regard, reference can be made to the Electronic Communications Act which provides that the provider is not liable if it expeditiously takes all necessary measures for the removal of reported content. In the Netherlands, a "simple notification like a message by anybody is insufficient, whereas a court order always meets the requirements of a notice."[1013] The Dutch interpretation of article 14 of the E-Commerce Directive ensures that hosting providers are not liable if they do not know of the illegal nature of an activity or information, or can not reasonably be expected to know.[1014] Furthermore, in 2008, the government and business community developed and published a 'Notice-and-Take-Down Code of Conduct' (NTD).[1015] The code establishes a procedure for intermediaries to deal with reports of unlawful content on the Internet, and is developed for intermediaries that provide a public (telecommunications) service on the Internet in the Netherlands.[1016] The code is not applicable to situations in which other statutory obligations or

---

1007 Entry into force on 1 July 2006.

1008 Article 15(1) states that service providers shall immediately inform the Information society development committee about suspected illegal activity.

1009 The notice and take-down principles are laid out in paragraph 14 of the "Procedure of the Control of Information", approved by Order No. 290 of the Government of the Republic of Lithuania of 5 March 2003.

1010 Paragraph 4 of the "Procedure of the Control of Information" defines information access service provider as "a person, who actually provides website hosting services in computer networks of public use" and network service provider as "a person registered in the Republic of Lithuania, who provides information transmitting via computer networks of public use or access to such networks services".

1011 Article 14 of the Law on Information Society Services, and Government 2007-08-22 decree No. 881.

1012 See articles 60-63 of the E-Commerce Law, 14 August 2000.

1013 See Study on the Liability of Internet Intermediaries, Markt/2006/09/E (Service Contract ETD/2006/IM/E2/69), November 2007.

1014 *Ibid*.

1015 See <http://www.samentegencybercrime.nl/NTD/NTD_English?p=content><

1016 The objective of the NTD code is to ensure that a report is always dealt with. This does not mean that the content must always be removed. It may well be that a report is made with respect to a site that eventually is found not to be in conflict with the law. If the content is found to be in conflict with the law, an intermediary must facilitate or assist in the removal of the unacceptable content, or in bringing the notifier into contact with the content provider.

liabilities apply for intermediaries on the basis of legislation and jurisprudence. Based on this code, the intermediaries developed their own notice and take-down procedures and policies.

In **Norway**, there exists only a duty to register the service activity with the Norwegian Post and Telecom Authority.[1017] The E-Commerce Act, of 23 May 2003 implemented the EU E-Commerce Directive into national law. In **Poland**, the relevant laws regarding specific legal liability provisions and licensing requirements for ISPs are set out in the Telecommunications Law of 16 July 2004.[1018] The Telecommunications Law defines a wide range of obligations and liability provisions with regard to telecommunications undertakings,[1019] in particular provisions concerning telecommunications confidentiality[1020] or obligations related to national defense, security and public safety.[1021] Furthermore, article 14 of the Electronic Commerce Act of 18 July 2002[1022] envisages that a host provider, who receives an official notice or 'reliable message'[1023] about the illegal character of the hosted data and prevents access to such data, is not liable for damages incurred by the service recipient as a result of preventing access to such data.

In **Portugal**, there is a licensing regime subject to articles 19 and 21 of the Electronic Communications Law. In **Romania**, there are no specific laws or regulations which establish conditions for licensing of ISPs. However, in Romania, in order to provide Internet access services, a notification has to be sent to the national regulatory authority, ANCOM, stating that the ISP intends to provide such services subject to the general authorization regime.[1024] In the Romanian Law, the EU E-commerce Directive was implemented by Law no. 365/2002 on Electronic Commerce. Article 16 of Law 365/2002 establishes the obligation of the ISPs to report to public authorities alleged illegal activities. The ISPs are also required to temporarily or permanently interrupt the transmittal or hosting of information through their systems by taking down the information or by blocking its access, if this has been required by ANCOM.[1025]

In the **Russian Federation**, there are general liability provisions and licensing requirements regarding activity in providing communication services. The licensing provisions are provided under the Government Resolution No. 87 of 18 February 2005 "On Approving the List of Communication Services Included in the Licenses and Lists of Licensing Conditions," section

---

1017 Electronic Communications Act from 4th of July 2003, section 2-1.

1018 Journal of Laws of 2004, No 171, item 1800, as amended.

1019 According to article 2(27) of the Telecommunications Law Act, telecommunications undertaking is any undertaking or entity authorized to pursue business activities under separate provisions and which conducts business activities consisting in the provision of telecommunications networks, associated facilities or in the provision of telecommunications services, whereby the telecommunications undertaking authorized to provide telecommunications services, and public telecommunications networks or associated facilities.

1020 Articles 159-175 of the Telecommunications Law Act.

1021 Articles 176-182 of the Telecommunications Law Act.

1022 Journal of Laws, 2002, No 144, item 1204 as amended.

1023 In Poland, currently alterations to the Electronic Commerce Act with regard to the 'notice and take-down procedure' are being discussed, but they are still in the 'pre–draft phase'. Above all, there is a need for a definition of the term 'reliable message' and designation of formal requirements that 'reliable message' shall fulfill. Revision of the Electronic Commerce Act shall further precise liability principles for the entities involved in the 'notice and take-down procedure'. A draft act on the revision of the Electronic Commerce Act has not been prepared yet.

1024 The relevant regulation is ANCOM President's Decision no. 338/2010 on the general authorization regime for providing electronic communications networks and services.

1025 The Authority for Regulation in Communications and Information Technology, the competent authority under article 17 of Law 365/2002.

XVI. In accordance with article 29 (1) of the Federal Law "On Communications,"[1026] legal entities intending to provide paid communication services are required to obtain a license. The list of communication services included in the licenses and the corresponding lists of licensing conditions are determined by the Russian Federation Government and annually updated. In the Russian Federation, there are no legal provisions based on the "notice and take-down" principle. However, clause 5.9.3 of the latest version of the "Regulations for Registering Domain Names in the .ru Domain",[1027] the registration agency has the right to suspend a domain immediately without sending a notification to the administrator if false information is provided during the registration process.

In **Serbia**, the licensing conditions for ISPs have changed with the adoption of the Law on Electronic Communications. The law currently provides for a general authorization regime under which every company can provide electronic communications services.[1028] Companies are only obliged to inform the Ministry of Telecommunication on the start of the activity. Serbia also implemented the EU E-Commerce Directive into national law through the Law on Electronic Commerce. The **Slovak Republic** transposed the EU Directive 2000/31/EC into national law with the Electronic Commerce Law No. 22/2004.[1029] In **Slovenia**, there are no specific legal liability provisions or licensing requirements for ISPs. Under the general authorization regime only a notification to the national regulatory authority is requested.[1030] The rules on the liability of providers of information society services, which are formulated in the E-Commerce Directive, are implemented in the Slovenian legislation with articles 8-11 of the Electronic Commerce Market Act.[1031]

In **Spain**, the legal regime applicable to ISPs is established with the Law No. 34/2002 on the Information Society which is a transposition of the EU E-Commerce Directive (LSSICE).[1032] The system of liability limitations is laid down in articles 13 to 17 of LSSICE.[1033] So far as the "actual knowledge" issue is concerned, Spain considers only notifications by competent

---

1026 No. 126-FZ of 7 July 2003.

1027 Approved on 17 June, 2009 by the Decision No. 2009-08/53 of the Coordinating Centre of the National Domain of the Internet.

1028 The Law on Electronic Communications, section 6, article 37.

1029 Entry into force in February 2004. The Electronic Commerce Law was amended by Law No. 160/2005 of the Collection of Laws, entry into force 1 May 2005.

1030 Electronic Communications Act (Official Gazette Republic of Slovenia No. 43/2004), article 4 (provision of electronic communications networks and services) and article 5 (notification).

1031 EU E-Commerce Directive 2000/31 has been implemented into national law by the Electronic Commerce Market Act (Official Gazette Republic of Slovenia No 61/2006). See article 8 (the general rules on the responsibilities of service providers), article 9 (responsibility of sole transmission provider), article 10 (responsibility of the caching service provider), and article 11 (responsibility of hosting service provider).

1032 Specifically, articles 6, 7, 8, 10, 11, 13, 14, 15, 16 and 17, explain the specific legal liability provisions and licensing requirements. See generally Peguera, M., "Internet Service Providers' Liability in Spain: Recent Case Law and Future Perspectives," 1 (2010) JIPITEC 151, para. 1.

1033 According to the official response received from the Spanish delegation for the OSCE FoM questionnaire, in Spain, there is no notice and takedown system imposed by law. The response stated that voluntary arrangements exist between the Security Forces and ISPs for the removal of certain types of content.

authorities as sufficient to assume actual knowledge.[1034] The law also includes specific requirements for Internet search engines[1035] and for content providers.[1036]

In **Sweden**, the 1998 Act on Responsibility for Electronic Bulletin Boards contains provisions on the obligation of a supplier of an electronic bulletin board to have supervision of the service. This in practice works in accordance with the notice and take-down principle. The E-Commerce Directive was incorporated into Swedish law by a number of Acts. The limitations of liability are regulated in the 2002 Act on Electronic Commerce and Information Society Services. In **Switzerland**, there is no licensing requirement for ISPs, but a notification requirement exists.[1037]

In **Turkey**, a notification requirement exists for both hosting service providers and ISPs. Article 5 of Law No. 5651 of 2007 introduced a notice-based liability system for hosting providers. This provision states that there is no general obligation to monitor the information which the hosting companies store, nor do they have a general obligation to actively seek facts or circumstances indicating illegal activity. This provision is consistent with article 15 of the EU E-Commerce Directive. However, article 5(2) obliges the hosting companies to take-down illegal or infringing content once served with a notice issued by the Telecommunications Communication Presidency (TIB), or subject to a court order with regards to article 8 of Law No. 5651. In May 2011 Turkey had 1,594 commercial hosting companies and 544 companies which provide hosting services.[1038] These hosting companies may be prosecuted under article 5(2) if they do not remove reported content consistent with the terms of the EU E-Commerce Directive.[1039]

Access and Internet Service Providers are regulated by article 6 of Law No. 5651, and as of May 2011, 135 ISPs notified the TIB that they provide Internet access related services.[1040] This provision is similar to that of hosting companies and is in line with the EU E-Commerce Directive provisions. Under article 6(1)(a), access providers are required to take-down any illegal content published by any of their customers once made aware of the availability of the content in question through TIB, or subject to a court order. Article 6(2) provides that access providers do not need to monitor the information passing their networks, nor do they have a general obligation to actively seek facts or circumstances indicating illegal activity with regards to the transmitted data. Article 7 of Law No. 5651 regulates the mass use providers, including Internet cafes. The mass use providers can only operate subject to being granted an official activity certificate obtained from a local authority representing the central administration. Mass use providers are required under article 7(2) to deploy and use filtering

---

1034 According to article 16.1.II "it will be understood that the service provider has the actual knowledge referred to in … when a competent body has declared that the data are unlaeful, or has ordered their removal or the disablement of access to them, or the existence of the damage has been declared, and the provider knew of this decision, without prejudice to the procedures of detection and removal of content that providers may apply by virtue of voluntary agreements, and without prejudice to other means of actual knowledge that might be established." See Peguera, M., "Internet Service Providers' Liability in Spain: Recent Case Law and Future Perspectives," 1 (2010) JIPITEC 151, para. 1.

1035 Article 17 of the Law 34/2002 on Information Society.

1036 Article 16 of the Law 34/2002 on Information Society.

1037 The relevant provision is article 4 of the Telecommunications Act (SR 784.10): Anyone providing a telecommunications service must notify the Federal Office of Communications (the Office) of this. The Office registers telecommunications service providers who have notified.

1038 For a list of these companies see < http://www.tib.gov.tr/dokuman/YS_listesi.html>.

1039 See further article 7 of Regulations Governing the Publications on the Internet.

1040 For a list of these ISPs see < http://www.tib.gov.tr/dokuman/ES_listesi.html>. Applications can be made through <http://faaliyet.tib.gov.tr/yetbel/>.

tools approved by the Telecommunications Communication Presidency to block access to illegal Internet content. Providers who operate without an official permission would face administrative fines between 3,000 (ca. 1,500 euros) and 15,000 Turkish lira (ca. 7,500 euros).[1041] Under related regulations, they are also required to record daily the accuracy, security, and integrity of the retained data using the software provided by TIB, and to retain this information for one year.[1042]

In terms of notice based liability provisions, article 9 of Law No. 5651 contains removal of content, and right-to-reply provisions with regards to civil law claims. Under this article, individuals who claim their personal rights are infringed by online content may contact the content provider or the hosting company if the content provider cannot be contacted, and ask the infringing or contested material to be removed. Users are also provided with a right to reply under article 9(1), and can ask the content or hosting provider to publish for up to a week their reply on the same page(s) on which the infringing or contested article was published. This should ensure that the reply reaches the same audience with the same impact. The content or hosting providers are required to comply with a 'removal (take-down) order' within 48 hours of receipt of request.[1043] If the request is rejected or no compliance occurs, the individual has 15 days to take its case to a local Criminal Court of Peace and request the court to issue a take-down order and enforce the right to reply as provided under article 9(1).[1044] The responsible judge shall issue its decision without trial within three days. An objection can be made against the decision of the court according to the procedures provided under the Criminal Justice Act. If the court decides in favour of the individual applicant, the content or hosting providers would be required to comply with the decision within two days of notification.[1045] No compliance could result in a criminal prosecution, and the individuals who act as the content providers or run the hosting companies could face imprisonment between six months and two years.[1046] If the content provider or hosting provider is a legal person, the person acting as the publishing executive or director would be prosecuted. Law No. 5651[1047] has removed the possibility for blocking access to websites with regards to disputes on personal rights. However, civil courts continue to issue permanent injunctions to block websites with regards to personal disputes such as defamation.[1048] Platforms including Wordpress,[1049] Google Groups,[1050] and websites of writers and authors[1051] have been blocked from Turkey by way of such injunctions.

In **Turkmenistan**, the Ministry of Communications is responsible for licensing communications activities in accordance with laws of Turkmenistan. Subject to the Law on

---

1041 See article 7(3).
1042 Article 5(1)(e).
1043 Article 9(1).
1044 Article 9(2).
1045 Article 9(3).
1046 Article 9(4).
1047 Article 9 of Law No. 5651.
1048 See further Akdeniz, Y., Report of the OSCE Representative on Freedom of the Media *on Turkey and Internet Censorship*, January 2010, at <http://www.osce.org/documents/rfm/2010/01/42294_en.pdf>.
1049 Blocking access to Wordpress.com lasted approximately 8 months between August 2007 and April 2008.
1050 Google Groups ban lasted for nearly 2 months (March-May 2008).
1051 For example, access to Richard Dawkins' website (<http://richarddawkins.net/>) is blocked since September 2008. Dawkins, a British ethologist, evolutionary biologist, and popular science writer is well known for his books *The Selfish Gene* and *The God Delusion*. Dawkins' website was accused of containing insults against Adnan Oktar, an Islamic creationist known for his book entitled *Atlas of Creation*. See BiaNet, "Evolutionist Dawkins' Internet Site Banned in Turkey," 17 September, 2008 at <http://ww.bianet.org/english/kategori/english/109778/evolutionist-dawkins-internet-site-banned-in-turkey?from=rss>.

Communications, all communications facilities, including terminal equipment of telecommunications networks in Turkmenistan shall be certified in conformance with state standards, technical specifications, and other norms established in accordance with the laws of Turkmenistan.[1052]

In **Ukraine**, there is a registration requirement for access providers. Entities and persons providing Internet access need to register with the registry of the operators and providers of telecommunications. The EU E-Commerce Directive provisions will be implemented into national law within the next few years according to clause 17.11 of the "Progressive Plan of Adaptation of Ukrainian Legislation to the legislation of the European Union of March 2010". Currently, the issue of providers' responsibility is regulated by the Law on Telecommunications. Under article 40(4), the operators, and providers of telecommunications shall not be held liable for the information transmitted through their networks. However, it should be emphasized that parliament of Ukraine, the Verkhovna Rada, is considering amending legislation to strengthen the protection of copyright and related rights.[1053] The amendments intend to introduce provisions on providers' responsibility in the case of copyright or related rights infringement on the Internet. Article 39 of the Law on Telecommunications was recently amended.[1054] Operators and telecommunication providers are not responsible for the content they provide access to including for content such as child pornography.

In the **United Kingdom** although there are no specific legal provisions on "notice and takedown" there exist provisions in various laws and regulations that are based on the principle of "notice and take-down". The Defamation Act of 1996 includes the first ever known Internet specific provisions that could be used to remove content from the Internet, albeit limited to libel and defamation. Section 1 of the Defamation Act 1996 regulates the defence of innocent dissemination. For the defence to succeed under section 1, the defendant needs to establish that (a) he was not the author, editor or publisher of the statement complained of; (b) he took reasonable care in relation to its publication; and (c) he did not know, and had no reason to believe, that what he did caused or contributed to the publication of a defamatory statement. There is no doubt that an ISP would qualify as a "publisher" under section 1(2) of the Defamation Act which defines a commercial publisher as a "person whose business is issuing material to the public, or a section of the public, who issues material containing the statement in the course of that business." However, for the purposes of section 1(3) of the 1996 Act, a person shall not be considered the author, editor or publisher of a statement if he is only involved

> (a) in printing, producing, distributing or selling printed material containing the statement;
> (c) in processing, making copies of, distributing or selling any electronic medium in or on which the statement is recorded, or in operating or providing any equipment, system or service by means of which the statement is retrieved, copied, distributed or made available in electronic form;
> (e) as the operator of or provider of access to a communications system by means of which the statement is transmitted, or made available, by a person over whom he has no effective control.

1052 See article 29 (The Licensing of Communication Activities), and article 30 (Certification of Communications Facilities) of the Law "On Communications", Chapter IV: The procedures of licensing communication activities and certification of communication facilities.

1053 See draft Law No. 6523

1054 No 1819 of 20 October 2010.

The defence has been used in several cases by service providers. Furthermore, the E-Commerce Directive was incorporated in the UK with the Electronic Commerce (EC Directive) Regulations 2002 (SI 2002/2013). Subject to Regulation 4(1) any requirement which falls within the coordinated field[1055] shall apply to the provision of an information society service by a service provider established in the UK irrespective of whether that information society service is provided in the UK or another Member State. Regulations 17 to 19 create a defence for intermediary service providers from any liability incurred from the activities of mere conduits, caching and hosting in the circumstances set out in those regulations. Regulation 20[1056] provides that regulations 17 to 19[1057] do not preclude the agreement of different contractual terms or affect the rights of any party to apply to a court for relief or the power of any administrative authority to prevent or stop the infringement of any rights. Regulation 21 makes provision in relation to the burden of proof in criminal proceedings arising out of the circumstances in regulations 17 to 19.[1058] Regulation 22[1059]

1055 Regulation 2(1) defines the coordinated field as requirements relating to the taking up and pursuit of the activity of an information society service and defines an information society service with reference to the definition in article 2(a) of the Directive.

1056 Regulation 20(1): Nothing in regulations 17, 18 and 19 shall—(a)prevent a person agreeing different contractual terms; or(b)affect the rights of any party to apply to a court for relief to prevent or stop infringement of any rights.(2) Any power of an administrative authority to prevent or stop infringement of any rights shall continue to apply notwithstanding regulations 17, 18 and 19.

1057 **Mere conduit: Regulation 17**. (1) Where an information society service is provided which consists of the transmission in a communication network of information provided by a recipient of the service or the provision of access to a communication network, the service provider (if he otherwise would) shall not be liable for damages or for any other pecuniary remedy or for any criminal sanction as a result of that transmission where the service provider—(a)did not initiate the transmission;(b)did not select the receiver of the transmission; and(c)did not select or modify the information contained in the transmission.(2) The acts of transmission and of provision of access referred to in paragraph (1) include the automatic, intermediate and transient storage of the information transmitted where:(a)this takes place for the sole purpose of carrying out the transmission in the communication network, and(b)the information is not stored for any period longer than is reasonably necessary for the transmission. **Caching: Regulation 18.** Where an information society service is provided which consists of the transmission in a communication network of information provided by a recipient of the service, the service provider (if he otherwise would) shall not be liable for damages or for any other pecuniary remedy or for any criminal sanction as a result of that transmission where—(a)the information is the subject of automatic, intermediate and temporary storage where that storage is for the sole purpose of making more efficient onward transmission of the information to other recipients of the service upon their request, and(b)the service provider—(i)does not modify the information;(ii)complies with conditions on access to the information;(iii)complies with any rules regarding the updating of the information, specified in a manner widely recognised and used by industry;(iv)does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and(v)acts expeditiously to remove or to disable access to the information he has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement. **Hosting: Regulation 19.** Where an information society service is provided which consists of the storage of information provided by a recipient of the service, the service provider (if he otherwise would) shall not be liable for damages or for any other pecuniary remedy or for any criminal sanction as a result of that storage where— (a)the service provider—(i)does not have actual knowledge of unlawful activity or information and, where a claim for damages is made, is not aware of facts or circumstances from which it would have been apparent to the service provider that the activity or information was unlawful; or (ii)upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information, and (b)the recipient of the service was not acting under the authority or the control of the service provider.

1058 Defence in Criminal Proceedings: burden of proof: regulation 21(1) This regulation applies where a service provider charged with an offence in criminal proceedings arising out of any transmission, provision of access or storage falling within regulation 17, 18 or 19 relies on a defence under any of regulations 17, 18 and 19.(2) Where evidence is adduced which is sufficient to raise an issue with respect to that defence, the court or jury shall assume that the defence is satisfied unless the prosecution proves beyond reasonable doubt that it is not.

makes provision in relation to matters which a court should have regard to when determining whether a service provider has actual knowledge for the purposes of regulations 18(b)(v) and 19(a)(i).

Furthermore, the Terrorism Act 2006 also includes notice and take-down provisions if the encouragement of terrorism or the dissemination of terrorist material takes place over the Internet. Sections 3 and 4 of the 2006 Act enable a police constable to give written notice to an organisation that a particular statement they publish electronically is unlawfully terrorism-related. The notice and take-down provisions are based upon the often disputed provisions of the Defamation Act 1996.[1060] Once a notice issued is by a constable, the relevant person (e.g. the ISP, the web hosting company, website owner, or forum operator, etc.) will have two working days to secure that the content in question is not available to the public or is modified to comply with the requirements of the 2006 Act. If no action is taken, the responsible party will be regarded as having 'endorsed' the so called 'terrorist publication' even if the publication has been posted, published, or uploaded by a third party. The responsible party served with a notice is also required to take all reasonable steps to prevent future re-publication of the same or similar statements. The Electronic Commerce Directive (Terrorism Act 2006) Regulations 2007 came into force in June 2007. It give effect to the EU Directive 2000/31/EC on electronic commerce in relation to matters within the scope of sections 1 to 4 of the Terrorism Act 2006 applicable on a country of origin basis.[1061] Regulations 5 to 7 create exceptions from liability for the offences under sections 1 and 2 of the Terrorism Act 2006 for ISPs when they provide mere conduit, caching or hosting services in the circumstances specified by articles 12 to 14 of the EU Directive.

In February 2010, the Home Office and the Association of Chief Police Officers (ACPO) have set up the Counter Terrorism Internet Referral Unit (CTIRU). The CTIRU is responsible for the co-ordination and execution of voluntary as well as section 3 (Terrorism Act 2006) take-down notices. The preferred route for removing potentially unlawful terrorist content is through informal contact between the police and the ISPs. As this approach has been allegedly successful, it has not been necessary to use the formal powers given under the Terrorism Act 2006 to seek the removal or modification of unlawful terrorist-related material from the Internet.[1062]

Finally, the Internet Watch Foundation (which will be detailed below) also operates a voluntary "notice and take-down" system for content involving child pornography. Upon receiving notification by users and citizens, the IWF informs service providers based in the UK and asks for the content to be taken-down. Simultaneously, the police are also being made aware of the availability of such content on UK servers.

1059 Notice for the purposes of actual knowledge: Regulation 22. In determining whether a service provider has actual knowledge for the purposes of regulations 18(b)(v) and 19(a)(i), a court shall take into account all matters which appear to it in the particular circumstances to be relevant and, among other things, shall have regard to—(a)whether a service provider has received a notice through a means of contact made available in accordance with regulation 6(1)(c), and(b)the extent to which any notice includes—(i)the full name and address of the sender of the notice;(ii)details of the location of the information in question; and(iii)details of the unlawful nature of the activity or information in question.

1060 Y. Akdeniz, and W.R.H. Rogers "Defamation on the Internet", in Akdeniz et al., *The Internet, Law and Society*, Addison Wesley Longman, 2000, pp.294–317.

1061 Article 3 of the EU Directive 2000/31/EC provides for the regulation of information society services (ISS) on a "country of origin" basis, and articles 12 to 14 require EEA states to limit, in specified circumstances, the liability of intermediary ISS providers when they provide mere conduit, caching or hosting services.

1062 See the House of Lords statement on Terrorism: Internet, HL Deb, 10 February 2010, c168W.

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".[1063] Section 230 was considered and tested 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".[1064] 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)[1065] which is the only US 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 online material provides a "safe harbor" for US based service providers and excludes liablitiy 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.[1066]

Hotlines to report allegedly illegal content

In addition to notice-based liability systems, hotlines to which allegedly illegal Internet content can be reported to have been developed in Europe and extended to other regions, too. The majority of the existing hotlines try to tackle the problem of child pornography, and most of the hotlines based in the European Union are co-financed by the EU Safer Internet Action

---

1063 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.

1064 *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.

1065 Digital Millenium Copyright Act (H. R. 2281) 1998.

1066 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.

Plan. An umbrella organization, INHOPE, the International Association of Internet Hotlines, was set up in 1999 with the aim of coordinating a network of Internet hotlines all over the world. It includes 39 national hotlines.[1067] 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 hotlines.[1068] The survey results seem to indicate a rather low public awareness of the existence and purpose of these hotlines.[1069]

The survey asked whether **specific (public or private) hotlines to report allegedly illegal content** to exist in the OSCE participating States **(Question 17).** Eight (14.3%) of the states replied negatively to this question. Hotlines exist in 37 (66.1%) of the participating States. No data was obtained from 11 (19.6%) the participating States.

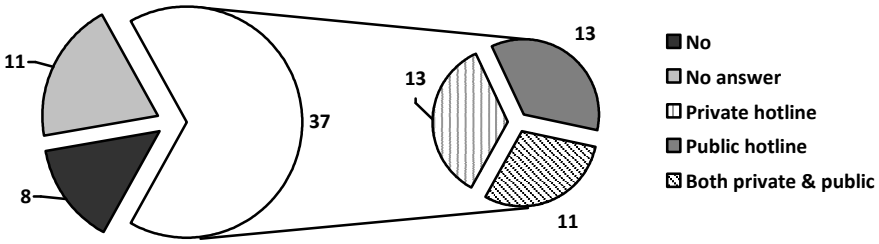


Figure 45. OSCE participating States' responses with regards to presence of specific (public or private) Hotlines to report allegedly illegal content (Question 17)

[1067] According to the INHOPE Annual Report 2010 the 39 members are: 1. **Australia** ACMA - acma.gov.au 2. **Austria** Stopline - stopline.at 3. **Belgium** Child Focus - stopchildporno.be 4. **Bosnia and Herzegovina** Emmaus - sigurnodijete.ba 5. **Bulgaria** ARC Fund - web112.net 6. **Canada** Cybertip - cybertip.ca 7. **Chinese Taipei** ECPAT Taiwan - web547.org.tw 8. **Cyprus** CNTI - cyberethics.info 9. **Czech Republic** Our Child Foundation - internethotline.cz 10. **Czech Republic** Horkalinka.cz - horka-linka.saferinternet.cz 11. **Denmark** Red Barnet - redbarnet.dk 12. **Finland** Save The Children Finland - pelastakaalapset-fi.directo.fi 13. **France** AFA - pointdecontact.net 14. **Germany** ECO - eco.de 15. **Germany** FSM - fsm.de 16. **Germany** Jugendschutz -jugendschutz.net 17. **Greece** SafeNet - safeline.gr 18. **Hungary** MATISZ - internethotline.hu 19. **Iceland** Barnaheill - barnaheill.is 20. **Ireland** ISPAI - Hotline.ie 21. **Italy** Telefono Azzurro - hot114.it 22. **Italy** STC Italy - stop-it.org 23. **Japan** Internet Association Japan - internethotline.jp 24. **Latvia** Latvian Internet Association - drossinternets.lv 25. **Lithuania** Communications Regulatory Authority - draugiskasinternetas.lt 26. **Luxembourg** LISA Stopline - lisa-stopline.lu 27. **Netherlands** Meldpunt - meldpunt-kinderporno.nl 28. **Poland -** Dyzurnet.pl 29. **Portugal** FCCN - linhaalerta.internetsegura.pt 30. **Romania** Safernet - Safernet.ro 31. **Russia** National Internet Safety Node in Russia - saferunet.ru 32. **Russia** Friendly Runet Foundation - hotline.friendlyrunet.ru 33. **Slovakia** eSlovensko - stopline.sk 34. **Slovenia** Spletno Oko - spletno-oko.si 35. **South Africa** Film Publication Board - fpbprochild.org.za 36. **South Korea** Korean Communications Standards Commission - singo.or.kr 37. **Spain** Protegeles - protegeles.com 38. **United Kingdom** Internet Watch Foundation - iwf.org.uk 39. **United States** CyberTipline - ncmec.org.

[1068] EuroBarometer Survey 2008, Summary Report, available through <http://ec.europa.eu/information_society/activities/sip/eurobarometer/index_en.htm>.

[1069] 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.

Public hotlines exist in 13 OSCE participating States. Equally, 13 participating States have private hotlines and 11 have both public and private hotlines to which illegal Internet content can be reported to.

In **Albania**, while there exist no specific public or private hotlines to report allegedly illegal Internet content to, the General Directorate of the State Police at the Ministry of Interior handles cases of harmful and illegal content, legal charges and different complaints related to electronic communications. In **Austria**, both public and private hotlines exist. In terms of public hotlines, while the Criminal Intelligence Service is responsible for child pornography, the Federal Agency for State Protection and Counter Terrorism is responsible for national socialist offences.[1070] In terms of private hotlines, there exists Stopline which can also be contacted to report child pornography offences as well as 'national socialist offences'. After reports are submitted to Stopline, the hotline operators check whether the material is actually illegal according to Austrian legislation. If the reported content is deemed illegal, Stopline immediately contacts the responsible public authority, the affected Austrian ISP, and, where applicable, foreign partner hotlines within the INHOPE network.[1071]

In **Azerbaijan**, a hotline service is operated by the Ministry of Communications and Information Technologies. The Ministry of Education's Bureau for the Informatization of the Education System also operates a hotline to uncover illegal and dangerous content, and provide appropriate training sessions and monitoring. Information arriving via both hotlines is assessed and the measures are taken to eliminate the existing problems. In **Bulgaria**, the Ministry of Interior runs a hotline to report allegedly illegal content.[1072] There is also a non-governmental organization, the ARC Fund, operating the Bulgarian Safer Internet Hotline established in 2006. The hotline is co-financed by the Safer Internet Programme of the European Commission. It co-operates with the Ministry of Interior[1073] based on an official framework agreement of 2006. Child pornography, adult pornography accessible to minors, extreme violence, grooming, child trafficking, cyber-bullying, racism and xenophobia, terrorism, propaganda of drugs, pro-bulimia, pro-anorexia, pro-self-harm and websites encouraging suicide may be reported to this hotline.[1074]

In **Canada**, a private charitable organization[1075] runs Cybertip.ca, a national tipline for the public to report suspected cases of online sexual exploitation of children, in particular child pornography, online luring, children exploited through prostitution, travelling sex offenders, and child trafficking.[1076] If the incident relates to potentially illegal material, it is sent to the

---

1070 Both organizations also offer online report offices on the Internet which deal with these particular topics: <http://www.bmi.gv.at/cms/BK/meldestellen/kinder/start.aspx http://www.bmi.gv.at/cms/bmi_verfassungsschutz/meldestelle/>.

1071 See further <http://www.stopline.at/index.php?id=3&L=1>. The Stopline has been incorporated within the ISPA (the Internet Service Providers Austria, the umbrella organisation of the Internet economy) as an institution of voluntary self-control of the Austrian ISPs, and it is subject to the Code of Conduct of the ISPA members.

1072 See <http://www.cybercrime.bg>.

1073 Co-operation with the Ministry's General Directorate for Combating Organized Crime, Cybercrime Department.

1074 Statistics for the reporting period of 01 January 2007 - 30 June 2010 – Total reports received: 3,029; Actionable reports: 189; Actions taken: 866 – among them transmitted to police: 69; to other hotlines: 104; responses to queries: 108.

1075 The Cybertip.ca tipline is managed by the Canadian Centre for Child Protection (C3P), a Canadian charitable organization dedicated to the personal safety of all children. The Centre is run by a volunteer board from a diverse variety of backgrounds; it is diversely funded through sponsorships, government contributions, sales, donations and grants.

1076 Anyone coming across information or possible evidence of child sexual abuse can report the matter online

appropriate law enforcement jurisdiction and/or to the INHOPE international partner hotline. Reports that involve a child in possible need of protection are also forwarded to child welfare agencies in Canada. Cybertip.ca provides a valuable function for police across Canada by triaging reports and forwarding only relevant leads to the appropriate law enforcement agency. Reports of material that is not deemed to be illegal are responded to with educational information. Furthermore, mandatory reporting legislation in relation to child pornography is in place in the four Canadian provinces Alberta,[1077] Manitoba,[1078] Nova Scotia,[1079] and Ontario.[1080] The provincial statutes have been enacted under the provinces' civil jurisdiction over child welfare – adding to existing reporting obligations in relation to child abuse and neglect – and require everyone to report all forms of child pornography to a designated agency such as Cybertip.ca or to the police. On average, Cybertip.ca receives 800,000 hits to its website per month and triages over 700 reports. From September 2002 until August 2010, Cybertip.ca processed over 41,000 tips from the public. Approximately 45% of the reports are forwarded to law enforcement agencies.[1081] As of June 2009, cybertip.ca had triaged over 33,000 reports since becoming Canada's national tip line in 2002. Over this period, more than 90% of the reports received by cybertip.ca were related to child pornography.[1082]

In May 2010, the federal government introduced proposed criminal law reforms[1083] which, if adopted, would require those who provide Internet services to the public (i.e., those who provide Internet access, Internet content hosting or electronic mail) to report online child pornography. More specifically, providers would be required to report to a designated agency tips that they might receive regarding websites where child pornography may be available to the public. Furthermore, providers would be required to notify the police and safeguard evidence if they believe that a child pornography offence has been committed using their Internet service. Failure to comply with the duties under this proposed legislation would constitute an offence punishable by summary conviction with a graduated penalty scheme. Importantly, nothing in the proposed legislation would require or authorize a person to seek out child pornography.

In **Cyprus**, there exists the private 'Safer Internet Hotline' Any person can lodge a complaint about illegal or disturbing content including racism, libel and child pornography. In the **Czech Republic**, there are currently two hotlines to which illegal content can be reported. Both co-operate with the police, and are members of the international INHOPE network. The privately funded Internet Hotline[1084] was launched in 2007 and operated by the Foundation 'Naše dítě' (Our Child Foundation). The hotline Horká linka[1085] has been in operation since 2009 and was

---

through www.cybertip.ca or by phone (1-866-658-9022). Reports can be submitted anonymously. The Cybertip.ca web server receives the information in a secure fashion. Analysts prioritize reports involving a child victim or suspect and others according to the order in which they were received. Each incident is assigned a secondary classification based upon the Criminal Code. Analysts validate the reported incident and supplement the information through Internet searches and technology tools. All aspects of the incident are described.

1077 Bill 2020 – Mandatory Reporting of Child Pornography Act, S.A. 2010, c. M-3.3, awaiting proclamation.

1078 Bill 7 – The Child and Family Services Amendment Act (Child Pornography Reporting), S.M. 2008, c. 9, proclaimed into force on April 15, 2009.

1079 Bill 187 – Child Pornography Reporting Act, S.N.S. 2008, c. 35, proclaimed into force on April 13, 2010.

1080 Bill 37 – Child Pornography Reporting Act, 2008, S.O. 2008, c. 21, awaiting proclamation.

1081 See <http://www.childprotectionpartnership.org/cpp-latest/2010/12/06/public-safety-shares-canadas-national-strategy-protect-kids-online-cpp-event>.

1082 See House of Commons Debates, 40th Parliament, 3rd Session, 1Hansard, No. 096, 5 Novemberi 2010.

1083 Bill C-22, An Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service.

1084 See <www.internethotline.cz>.

1085 See <www.horkalinka.cz>.

established by the CZI company within a project co-financed by the Safer Internet programme. This hotline is part of the 'National Safer Internet Centre'[1086] which also organizes a number of educational activities. The Centre has initiated the signing of an agreement with mobile operators regarding the procedure for handling complaints and reports of illegal online content. The hotlines receive reports of illegal and inappropriate Internet content, such as child pornography, child prostitution, child trafficking, paedophilia, other unlawful sexual practices, racism, xenophobia, self-harm, call for hatred and violence, and drug distribution.

In **Denmark**, any person can report a suspicion regarding child pornography to the Danish Police website[1087]. Furthermore, since 2005, the Danish National Police has co-operated with the majority of Danish ISPs and the Danish division of Save the Children in order to prevent Internet access to material with child pornographic content. Save the Children in Denmark provides a hotline service where citizens can report content containing sexual assaults committed against children. Save the Children passes this information on to the Danish National Police.

In **Germany**, with the support of the European Commission's "Safer Internet" Programme, two hotlines have been set up. These are "jugendschutz.net", a governmental initiative and a project launched by the private sector[1088] to institute an Internet complaints centre. The German hotlines have been combined with the awareness node 'Klick Safe' and the Helpline "Nummer gegen Kummer" to form a centre for a safer Internet in Germany.[1089] "Jugendschutz.net" is based on a treaty on youth media protection agreed between the federal states of Germany. The Internet complaints centre is self-regulated. Illegal content, or content that is liable to corrupt youth or to impair their development can be reported to the "jugendschutz.net" hotline [1090] or to the Internet complaints centre.[1091]

In **Ireland**, Hotline.ie was established in 2000 following the recommendations of a government working party. It was set up by the ISP industry as part of a self-regulatory model and is supported by the government and overseen – on behalf of the government – by the Office for Internet Safety, an Executive Office of the Department of Justice and Law Reform. Reports can be made by telephone, in writing or via the Internet through the Hotline's website.[1092] Reports on illegal content (mainly child pornography, child grooming and child trafficking) are verified and forwarded depending on hosting (source) location:[1093]

1086 See <www.saferinternet.cz>.

1087 See <www.politi.dk>. The website is run by the Department of National Forensic Investigation Division (NITEC) of the Danish National Police.

1088 This is an joint initiative by the Internet association "Eco" and the voluntary monitoring association of multi-media companies, the Freiwillige Selbstkontrolle Multimedia e.V.

1089 See for details <http://ec.europa.eu/information_society/apps/projects/factsheet/index.cfm?project_ref=SIP-2007-CNH-143709>.

1090 See <http://www.jugendschutz.net/hotline/index.html>. The 2009 annual report of the "jugendschutz.net" hotline is available for download (in German) at <http://www.jugendschutz.net/pdf/bericht2009.pdf>.

1091 See <http://www.internet-beschwerdestelle.de/>. The Internet complaints centre has published a report for the period from March of 2007 until February of 2008 (<http://www.internet-beschwerdestelle.de/ibsde-gb-0708.pdf>); since March of 2008, the hotline has been operated as part of the "Safer Internet" centre.

1092 See <http://www.hotline.ie/>.

1093 Hotline.ie reports covering the periods 2009, 2008 and 2007 can be found at the following links: <http://www.hotline.ie/report2010/index.html> - covers the period 1st January through to 31st December 2009. <http://www.hotline.ie/annualreport/index.html> - covers the period 1st January through to 31st December 2008. <http://www.hotline.ie/5threport/documents/Hotline5thRep.pdf> - covers the period 1st January through to 31st December 2007.

- If located in Ireland: forwarded to the specific national police unit and to the ISP (to preserve evidence and to remove from public access)
- If located in a country with INHOPE hotline: forwarded to that country's INHOPE affiliated Hotline.
- If located in a country without an INHOPE hotline: forwarded to the Irish Garda Síochána (Police) contact for transmission to Interpol.

The Garda Síochána, Ireland's National Police Service, deals with all reports of breaches of the criminal law made to them through Hotline.ie.

In **Italy**, the National Police have reacted to the increased use of the Internet by setting up the "police station online",[1094] a web portal where users can find information, receive advice, general suggestions and forms. The website also offers the opportunity of submitting reports on illegal content. As far as child pornography online is concerned, the Postal and Communications Police Service plays a crucial role for the reports made every day by the NGOs.

In **Kazakhstan**, in late 2009, the Agency for Informatization and Communications formed a Computer Emergency Response Team Service (CERT). The Service's immediate objective is to prevent various types of threats relating to the use of information and communications technology. With respect to the national segment of the Internet, this primarily means assisting users, proprietors and owners of public information resources (Internet resources) with dealing with threats that they may encounter. CERT also assists in raising the reliability and security of the information technology. The Service is responsible for receiving and carrying out analysis of reports from the Kaznet users who have found viruses or other malicious codes and programs used for creating botnets. Users can also report content that clearly violates the requirements of legislation on terrorist propaganda, pornography, and breach of copyright. Within the boundaries of its competence, CERT acts as the focal point for all citizens interested in keeping the national segment of the Internet 'clean and safe'. The Service does not block Internet resources and only notifies the content owner who is to take the final decision regarding the content. The Service is also responsible for providing technical consultative support to law-enforcement bodies.[1095]

In **Latvia**, the "Latvian Safer Internet Centre", a non-governmental organization, has been established.[1096] The Centre aims at informing and educating children, adolescents, teachers and parents on the safety of Internet content, potential threats they might be exposed to on the Internet, including incitement to hatred, racism, child pornography and paedophilia, emotional online harassment, and identity theft and data abuse. This project allows the general public to

---

1094 See <www.commissariatodips.it>.

1095 Note the following official government statements: Response of the Chairman of the Republic of Kazakhstan Agency for Informatization and Communications of 3 March 2010 to a question of 1 March 2010 No. 33343 (e.gov.kz): "A Computer Emergency Response Team Service (CERT) has been formed at AIC." Response of the Minister of Communications and Information of the Republic of Kazakhstan of 9 June 2010 to a question of 2 March 2010 No. 33434 (e.gov.kz): "The activity of the Computer Emergency Response Team Service (CERT) does not envisage blocking access to any Internet resources." Response of the Minister of Communications and Information of the Republic of Kazakhstan of 19 April 2010 to a question of 29 March 2010 No. 35655 (e.gov.kz): "The activity of the newly formed Computer Emergency Response Team Service (CERT) does not envisage restricting access to any Internet resources."

1096 The "Latvian Safer Internet Centre" was established by the Latvian Internet Association in co-operation with the State Inspectorate for Protection of Children's Rights and with the support of the European Commission's Safer Internet Programme.

electronically report crimes detected on the Internet.[1097] Reports are processed and, if appropriate, sent for assessment to the Cybercrime Prevention Department of the State Police. The project also includes a helpline[1098] operated by the State Inspectorate for Protection of Children's Rights. Pornography accessible to children, violence, hate speech, racism, child sexual abuse materials, and financial fraud can be reported to the hotline.

Liechtenstein does not have any public or private hotlines to which allegedly illegal content could be reported to. However, since Liechtenstein has an agreement with **Switzerland**, content perceived as problematic can be reported to the Swiss Co-ordination Unit for Cybercrime Control (CYCOS). After an initial examination, reports are forwarded to the respective national or foreign law enforcement agencies. CYCOS is available to the public, authorities and ISPs for any legal and technical question in the field of cybercrime. As the national co-ordination unit, CYCOS is also the point of contact for foreign bodies fulfilling analogous functions. According to CYCOS, the system is efficient as it does lead to the identification of unlawful Internet content such as hardcore pornography, depiction of violence, extremism, racism, unauthorized access to IT-systems, spread of computer viruses, destruction of data, credit card misuse, violation of copyright, and illegal arms trade.

In **Lithuania**, under the "Safer Internet Plus Programme", the Communications Regulatory Authority (RRT) and the Ministry of Education and Science signed an agreement with the European Commission to implement the project "Lithuanian Awareness and Hotline Actions for Safer Internet" ("Safer Internet LT"). The Safer Internet LT runs a national safer Internet awareness node in Lithuania, which also includes a hotline.[1099] The project was extended in February 2009 to promote safer use of the Internet and new online technologies for children and youth. It aims to help children, parents and educators to avoid the dangers associated with illegal and harmful content on the Internet by teaching Internet safety in schools.[1100]

The **Netherlands** attaches great value to the Internet Discrimination Hotline, MDI. The hotline is financially supported by the Dutch government, and its main task is to review reports of online discrimination and ensure that illegal material is removed from websites. The MDI receives an average of 1,200 reports of online discrimination annually. In cases where the material is judged to be potentially criminal, MDI sends a request for removal to the site administrator. The annual removal rate fluctuates around 90%.[1101] Besides handling reports of discrimination, MDI also provides information, organizes courses, training and workshops for users and moderators of interactive websites, enabling them to recognise discriminatory material on their site more easily and ensure it is removed quickly. According

---

1097 See <www.drossinternets.lv>.

1098 Helpline 116111.

1099 An electronic report form on the project website http://www.draugiskasinternetas.lt/lt/misc/report_form is the main tool for reporting about illegal and harmful content (child sexual abuse material, including child pornography, pornography, racism, xenophobia, incitement of racial hatred, violence, etc.) on the Internet. Reports can also be delivered both by sending an e-mail or calling a hotline. The hotline is member of INHOPE since May 2008.

1100 The first agreement was signed in April 2007 with the EU. The project was succeeded by Safer Internet LT AN-HL in February 2009.
During the 3 years of operation (April 2007 – April 2010), 1366 reports on illegal or harmful content were investigated by the hotline. And the following actions were taken: 22 reports were forwarded to the Police Department; 59 reports were sent to the Office of the Inspector of Journalist Ethics; 30 reports were forwarded to the hotlines of other countries, members of INHOPE; 40 reports were forwarded to the hosting information access service providers and (or) network service providers; 1215 reports were not being processed further because the reported content was not illegal or was located in countries where it is considered to be not illegal.

1101 86% in 2009, 91% in 2008 and 90% in 2007.

to MDI, the moderation of websites is also improving. In 2009, the content reported to the hotline had already been removed by the websites, or social network operators in 9% of cases, as opposed to 7% in 2008. The vast majority of reports of discriminatory online expression concerned social networking or video sites (e.g. YouTube or Hyves, the biggest Dutch social network site). All these platforms are co-operating with the hotline, and in almost each case, MDI succeeded in securing the removal of the discriminatory material. If a site refuses to delete or remove a discriminatory utterance, MDI can lodge a criminal complaint.

Furthermore, there also exists the private "Child Pornography Hotline", subsidised by the Ministry of Justice, which plays an important role in the prevention and combating of child pornography. This hotline offers a law-threshold opportunity for reporting sexual exploitation of children. It enjoys good relations with the Dutch police and with foreign hotlines. Since 2006, the police also operate a hotline for reporting cybercrimes. Incidences of child pornography can also be reported to this hotline.

In **Norway**, the National Criminal Investigation Service (NCIS Norway) run the only hotline receiving tip offs from the general public. It was transferred from Save the Children in 2004, when they realized that the tip offs contained evidence of crimes against children. NCIS Norway receives reports in relation to illegal content, illegal behavior, sexual abuse, trafficking in human beings and hate crimes. On average NCIS Norway receive 3,000 reports annually, 50% of which are related to crimes against children.

In **Poland**, there are hotlines to report allegedly illegal content to. Their functioning is based on the co-operation between public organizations and the private sector. The Dyżurnet hotline[1102] was created by the Research and Academic Computer Network (NASK) in agreement with the European Commission[1103]. The "Helpline for Children and Youth"[1104] was created by the Office of Electronic Communications and the Ministry of Internal Affairs. Helpline.org.pl, a joint project of the Nobody's Children and the Orange Foundation is co-financed by the European Commission under the Safer Internet Action Plan. Child pornography, hardcore pornography, xenophobia, racism and other illegal content can be reported to all above mentioned hotlines.

In **Romania**, hotlines with regard to illegal content were rather recently established. The privately run "Focus Internet Hotline" has been developed under the sigur.info programme which started in 2007 under the Safernet Programme co-financed by the European Commission. The hotline receives not only complaints regarding illegal content but also regarding content perceived as harmful. The hotline forwards the complaints to INHOPE and/or to the Romanian Police if the content is located abroad or to the competent Romania authorities if the content is located in Romania. Complaints received so far relate to child pornography, adult pornography, cyber bullying, grooming and even SPAM.

In the **Russian Federation**, some hotlines receive reports from Internet users on allegedly illegal content on full or partial anonymous terms. One such hotline, the "Safer Internet Centre Russia", has been a member of the INHOPE network since 2009. It was established by public organizations (ROTSIT and the "Resistance" Human Rights Movement), and functions under the patronage of the Civic Chamber of the Russian Federation. The hotline of the "Internet Development Promotion Fund" called "Friendly Runet," was set up as a non-

[1102] www.dyzurnet.pl
[1103] Created under the framework of the EU's Safer Internet Action Plan.
[1104] Telefon Zaufania dla Dzieci i Młodzieży. See <http://www.116111.pl>.

member, non-profit organization on the basis of voluntary contributions but is also supported by the Russian Ministry of Internal Affairs. Any Internet user with information about resources that distribute 'negative content', primarily pornographic images involving minors, can use this hotline. It should be noted that there are no legal provisions in the Russian Federation that regulate hotlines. Hotlines receive anonymous reports through special web forms,[1105] and the initial verification of the information is done by hotline analysts. The hotlines take measures when there is enough reason to believe that the reported content corresponds to the definition of illegal content.[1106] Its circulation is terminated in co-operation with law enforcement bodies, hosting and content providers in compliance with reached agreements.

The Safer Internet Centre Russia receives reports on the following types of illegal content:

> sexual exploitation of children, child pornography, inducement of children by paedophiles on the Internet, racism, nationalism, other forms of xenophobia, propaganda of sectarians, cyber denigration, insult and persecution on the Internet, propaganda and public justification of terrorism, propaganda of violence and crimes on the Internet, propaganda and sale of drugs on the Internet, fraud on the Internet and information about harmful viruses, other types of illegal content.

The Centre's hotline is operating since August 2008. As of 30 June 2010, a total of 13,235 reports were received on illegal content, the break down of which is provided below:

- Sexual exploitation of children, child pornography 5991
- Inducement of children by pedophiles on the Internet 156
- Racism, nationalism, other forms of xenophobia, propaganda of sectarians 1509
- Cyber denigration, insult and persecution on the Internet 1617
- Propaganda and public justification of terrorism 380
- Propaganda of violence and crimes on the Internet 2603
- Propaganda and sale of drugs on the Internet 311
- Fraud on the Internet and information about harmful viruses 473
- Other types of illegal content 195

As a consequence, the operation of 7,114 resources and web pages has been terminated.[1107]

In the **Slovak Republic**, there are several private hotlines to which illegal and harmful content can be reported to. Two of them are run by the mobile operators Orange and T-mobile. Furthermore, in February 2010, the national centre for reporting of illegal content, "stopline.sk" was established. One of stopline.sk's official partners is the Ministry of Interior.

[1105] Specialized web forums function under special projects of the "NeDopusti" ["Do not Allow"] Centre, "No to Hooligans [Khuliganam.net]", "No to Drug Addicts [Narkomanam.net]" for posting on specific categories relating to the topic of the special project.

[1106] The Safer Internet Centre – Russia hotline also has a group of experts who examine content that the hotline analysts are unsure about. These experts are leading specialists in their sphere of knowledge, who work at leading scientific-research centres (providing consultation to hotlines is a way of expressing their civil position).

[1107] There are also other Russian hotlines which can be used to report "harmful content" such as sexual exploitation and kidnapping of children (www.detivrunete.ru, www.nedopusti.ru); cyber denigration and psychological violence on the Internet (www.huliganamnet.ru); helping authors and the owners of intellectual property on the Internet (www.stopcontrafact.ru).

Stopline.sk focuses on the protection of children and youth, and suspicious content reported to the hotline is submitted to the police.[1108]

In **Slovenia**, "Spletno oko" (Web Eye), established through self-regulation, operates within the consortium composed of two public and one non-profit organization. Child pornography as well as hate speech can be reported to the Slovenian hotline, that started operating on 1 March 2007.[1109] If a report concerns a server located in Slovenia, the information is forwarded to the Slovenian police who further investigate it. Once the police confirm the illegality of the reported content, it informs the hotline and gives it the permission to notify the relevant ISP. Each report to an ISP or hosting company is solely informative. The providers have to decide how to react to the notification. If a report involves a server located outside Slovenia, the hotline sends the notification to the Slovenian police but also to INHOPE, which assures that the report is processed by the hotline in the country where the suspected illegal content is hosted. The INHOPE partner hotline then commences their own procedures in accordance with their legislation and reporting procedures. Between March 2007 and August 2010, Spletno oko received 2,612 reports of allegedly illegal content on the Internet, with an average of 62 reports per month. In the 30 months of the project duration 7,26 reports were handed over to the police and 433 reports were forwarded to other INHOPE members.[1110]

In **Sweden**, the Swedish Police runs a special email address for their special unit for sexual abuse against children.[1111] There is also a private initiative, the ECPAT hotline.[1112] ECPAT, however, does not investigate reported content, it only forwards it to the Swedish police. In **Switzerland**, the Swiss Co-ordination Unit for Cybercrime Control (CYCO) has no legal basis governing the establishment of a hotline.[1113] However, as a center of expertise, it provides a form of public announcement on its website[1114] that allows users to disclose offences committed online. Any kind of crime can be reported through this channel. Reports are forwarded to the appropriate law enforcement authorities at home and abroad. CYCOS is also mandated to seek actively illicit content on the Internet.[1115]

In **Turkey**, article 10(4)(d) of the Law No. 5651 required the Telecommunications Communication Presidency (TIB) to establish a hotline to report potentially illegal content and activity subject to article 8(1). The hotline was established by the Presidency in 2007. Any allegation to the effect that the Law is violated can be brought to the attention of the hotline via e-mail, telephone, sms, or through an online form provided on the website of the hotline.[1116] According to the 2010 Annual Report of the TIB, the hotline received a total of

---

1108 Content potentially violating copyright can also be reported to collecting societies.

1109 In the reporting period 1 March 2007 – 30 June 2010 hotline Spletno oko received 2343 reports (1118 child pornography reports and 901 hate speech reports). Out of all received reports, 613 reports (494 reports of child pornography and 111 reports of hate speech) were estimated as allegedly illegal and sent to the police.

1110 See generally Spletno oko Annual report September 2008 - August 2010, at <http://www.spletno-oko.si/uploadi/editor/1298550689SIP-SI_Final_Report September 2008 - Avgust 2010.pdf>.

1111 childabuse@rkp.police.se

1112 www.ecpathotline.se

1113 The legal basis for CYCOS is an administrative agreement between the Confederation and the cantons, which signed the end of 2001 and subsequently by all the District Director was ratified changes. In this agreement, the federal government is authorized to take information and coordination tasks in the area of Internet crime.

1114 www.scoci.ch

1115 For statistics see the annual reports: Annual Report 2007 in French: <http://www.cybercrime.ch/report/Rechenschaftsbericht_2007_f.pdf>, Annual Report 2008 in French: <http://www.cybercrime.ch/report/Rechenschaftsbericht_2008_f.pdf>, Annual Report 2009 in French: <http://www.cybercrime.ch/report/Rechenschaftsbericht_2009_FR.pdf>.

1116 See <http://www.ihbarweb.org.tr/index.html>.

57,956 reports with regards to Law No. 5651 catalogue crimes. 59% of these reports involved adult pornography. As mentioned previously in this report, subsequent to the assessment of the reports received by the hotline, the Presidency may block access to such sites, or issue notifications for the removal of content through service and hosting providers if these are situated in Turkey.[1117]

In **Ukraine**, since December 2008 there exists the "Save spirituality" hotline. It was created by the National Commission for the protection of public morality.[1118] The hotline accepts reports on content violating the law on protection of public morals.

In the **United Kingdom**, the Internet Watch Foundation (IWF) was established in 1996 by the Internet industry to provide the UK with a hotline for the public and IT professionals to report allegedly criminal Internet content in a secure and confidential way. The IWF works in partnership with the online industry, law enforcement, government, and international partners to minimize the availability of illegal content. The IWF predominantly deals with child sexual abuse images hosted anywhere in the world, but the hotline also deals with criminally obscene adult content, incitement to racial hatred content, and non-photographic child sexual abuse images hosted in the UK. The hotline is funded by the EU and the wider online industry, including ISPs, mobile operators and manufacturers, content service providers, filtering companies, search providers, trade associations, and the financial sector. The IWF co-operates with the INHOPE network and other relevant organizations to encourage wider adoption of good practice in combating child sexual abuse images on the Internet. As such images are primarily hosted outside the UK jurisdiction, the IWF tries to protect users from inadvertent exposure to this type of content by blocking access through the provision of a dynamic list of child sexual abuse web pages.[1119] The hotline provides a child sexual abuse URL list to ISPs, mobile operators, search engines and content providers to help disrupt access to child sexual abuse content. In addition to blocking access, the IWF operates a 'notice and take-down' system to swiftly remove content at source, and it provides a targeted assessment and monitoring system to remove content in newsgroups. Furthermore, the hotline also works with domain name registries to deregister domain names dedicated to the distribution of child sexual abuse content.

Furthermore, in early 2010, the police, in association with the Home Office, launched a Counter Terrorism Internet Referral Unit (CTIRU). This new formation acts as "a dedicated police unit intended to assess and investigate Internet-based content which may be illegal under UK law and to take appropriate action against it, either through the criminal justice

---

1117 The TIB Annual Report did not provide the detailed breakdown of what action has been taken on the reports received. See TIB Annual Report 2010 at <http://www.btk.gov.tr/Yayin/Raporlar/2010/tib_rapor2010.doc>.

1118 Order of 12 December 2008 № 81/1-U.

1119 In December 2008, the Internet Watch Foundation blocked access to Wikipedia from the UK because of a single image (had been available on the Internet for years) involving the cover of an album called Virgin Killer by German heavy metal band Scorpions. The IWF revoked its decision after five days subsequent to an appeal by the Wikipedia Foundation. See the Observer, "Wikipedia censorship highlights a lingering sting in the tail," 14 December, 2008, at <http://www.guardian.co.uk/technology/2008/dec/14/wikipedia-censorship-scorpions-virgin-killer>. Note further Wikimedia Foundation, "Censorship in the United Kingdom disenfranchises tens of thousands of Wikipedia editors," 07 December, 2008, at <http://wikimediafoundation.org/wiki/Press_releases/Censorship_of_WP_in_the_UK_Dec_2008>. See further Wikinews, "Wikimedia, IWF respond to block of Wikipedia over child pornography allegations," 08 December, 2008, at <http://en.wikinews.org/wiki/Wikimedia,_IWF_respond_to_block_of_Wikipedia_over_child_pornography_allegations>.

system or by making representations to Internet service providers or, where necessary, by both these means."[1120] The CITRU also acts as a hotline to which online material can be reported to through the Directgov website.[1121] The CTIRU has removed material from the Internet on 156 occasions over the last 15 months (as of June 2011), and is beginning to liaise with law enforcement agencies overseas to obtain agreement to remove websites in their jurisdiction.[1122]

In the **USA**, ISPs have a legal responsibility to report when encountering child pornography on their servers under section 42 USC 13032 (2004). The service providers in question are required to report facts or circumstances to the CyberTipLine[1123] at the National Center for Missing and Exploited Children[1124] as soon as reasonably possible. CyberTipLine will forward the report to a law enforcement agency or agencies designated by the Attorney General, including to the members of the Internet Crimes Against Children (ICAC) task force program.[1125]

A total of 565.298 reports were logged between 1998-2008. These figures include reports made by members of the public as well as the mandated reports of child pornography from ISPs. The FBI has reported success in terms of the number of child pornography websites and web hosts being shut down following reports made to the CyberTipline.

Year	Child Pornography Tips
1998	3267
1999	7736
2000	16724
2001	21611
2002	37647
2003	76204
2004	106119
2005	64250
2006	62480
2007	83959
2008	85301

Table 17 (CyberTipline Statistics)[1126]

1120 HM Government, *Prevent* Strategy, Cm 8092, June 2011, para 10.100, p. 78.

1121 See <https://reporting.direct.gov.uk/>.

1122 See further HM Government, *Prevent* Strategy, Cm 8092, June 2011, para 10.100, p. 78.

1123 Authorized by Congress, NCMEC's CyberTipline is operated in partnership with the Federal Bureau of Investigation (FBI), the Department of Homeland Security's Immigration and Customs Enforcement (ICE), the U.S. Postal Inspection Service (USPIS), the Internet Crimes Against Children Task Forces (ICACs), the U.S. Secret Service (USSS), the U.S. Department of Justice's Child Exploitation and Obscenity Section (CEOS), as well as other international, state, and local law enforcement. See generally <http://www.cybertipline.com/>. See further <http://www.cybertip.org/en_US/documents/CyberTiplineFactSheet.pdf>.

1124 "Under the Electronic Communications Privacy Act, an ISP could not turn information over to law enforcement officials without a warrant. However, this Act requires, without a warrant, ISPs to turn over whatever information they might acquire. [See 18 U.S.C. § 2702(b)(6)(B) amending ECPA to permit disclosure]." See CyberTelecom: An Open Law Project, "Reporting Child Pornography," at <http://www.cybertelecom.org/cda/cppa.htm>.

1125 ICAC involves a network of coordinated regional task forces engaged in helping state and local law enforcement agencies to develop an effective response to cyber-enticement and child pornography cases.

1126 See <http://www.missingkids.com/en_US/documents/CyberTiplineReportTotals.pdf>.

Conclusion to Part D

Part D of this study has shown that a number of participating States have general licensing requirements for the information society service providers while others require only some level of activity notification to the relevant authorities. It should also be highlighted that in certain countries there are no licensing requirements at all.

Liability provisions for service providers are not always clear, and complex notice and take-down provisions exist for content removal from the Internet within a number of OSCE participating States. Around 30 participating States have laws based on the EU E-Commerce Directive. However, the EU Directive provisions rather than aligning state level policies, created differences in interpretation during the national implementation process. These differences emerged once the provisions were applied by the national courts. Aware of such issues, the European Commission launched a consultation during 2010 on the interpretation of the intermediary liability provisions. A review report is expected during 2011.[1127] Furthermore, the European Court of Human Rights received an application from **Estonia**. The application is significantly important as the Court will have the opportunity to scrutinize the "notice based liability" measures of the E-Commerce Directive with regards to Article 10 of the European Convention on Human Rights as well as issues surrounding third party comments published on news portals and social media platforms.

In terms of the formation of public and/or private hotlines, it should be noted that although hotlines could potentially play an important role in relation to illegal Internet content, there remain significant questions on their operation. Private hotlines are often criticised as there remain serious concerns regarding the "policing" role they might play. It is argued that decisions involving illegality should remain a matter for the courts of law to ensure the due process principle, rather than left to hotlines operating outside a legal framework. This concern was recognised in the Martabit Report to the UN stating 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".[1128] The operation of private hotlines formed through self-regulatory means should be consistent with the principles underlying the European Convention on Human Rights. States may have a positive obligation to guarantee that hotlines respect due process principles, and their functions and practice do not contravene the the principles underlying the European Convention.[1129] States must furthermore provide adequate and effective safeguards against abuse. These should include procedures for effective judicial scrutiny of the decisions taken by the hotlines.[1130]

Furthermore, lack of transparency with regards to the work of hotlines often attract accusations of censorship. Leaked "child pornography" blocking blacklists maintained by hotlines from Finland,[1131] Denmark,[1132] and Italy[1133] (as well as from China,[1134] Thailand,[1135]

1127 Public consultation on the future of electronic commerce in the internal market and the implementation of the Directive on Electronic commerce (2000/31/EC).

1128 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.

1129 See *Özgür Gündem v. Turkey*, no. 23144/93, §§ 42-46, ECHR 2000-III, and *Fuentes Bobo v. Spain*, no. 39293/98, § 38, 29 February 2000.

1130 See *Lupsa v. Romania*, no. 10337/04, § 34, 8 June 2006.

1131 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>.

Australia,[1136]) that were published on the whistleblower website Wikileaks have demonstrated that most of the hotlines also block access to adult pornographic content and even political content. In the absence of openness and transparency of the work of the hotlines and by creating secrecy surrounding the blocking criteria and keeping the list of blocked websites confidential, concerns will continue to exist regarding the work of such hotlines. The hotlines can only refute such criticism if they are established within a regulatory framework that is compatible with the requirements of the European Convention on Human Rights.

1132 Wikileaks, "Denmark: 3863 sites on censorship list," February, 2008, at <http://wikileaks.org/wiki/Denmark:_3863_sites_on_censorship_list%2C_Feb_2008>.

1133 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>.

1134 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>.

1135 Wikileaks, "Thailand official MICT censorship list," 20 December, 2008, at <http://wikileaks.org/wiki/Thailand_official_MICT_censorship_list%2C_20_Dec_2008>.

1136 Wikileaks, "Leaked Australian blacklist reveals banned sites," 19 March, 2009, at <http://wikileaks.org/wiki/Leaked_Australian_blacklist_reveals_banned_sites>.

Appendix I: OSCE RFoM Questionnaire

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

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?

- 1A. Please provide the name of the law/s, and relevant sections of these laws if such laws exist.

- 1B. 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?

- 2A. 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"?

- 3A. Please provide the name of the law/s, and relevant sections of these laws if such laws exist.

- 3B. 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?

- 4A. Please provide the name of relevant law/s and regulations, and the relevant sections of such provisions.

- 4B. Please state how these offences are defined by law.

- 4C. Please state specifically whether the possession and/or distribution of such content is criminalized.

- 4D. Please state which sanctions (criminal, administrative, civil) are envisaged by law.

- 4E. Please also state (if applicable) the maximum prison term envisaged by law for such offences.

- 4F. Please provide any statistical information in relation to convictions under relevant law/s for the reporting period of 01 January 2007 – 30 June 2010.

- 4G. 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.

- 4H. 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?

- 5A. Please provide the name of relevant law/s and regulations, and the relevant sections of such provisions.

- 5B. Please state how these offences are defined by law.

- 5C. Please state specifically whether the possession of such content is criminalized

- 5D. Please state which sanctions (criminal, administrative, civil) are envisaged by law.

- 5E. Please also state (if applicable) the maximum prison term envisaged by law for such offences.

- 5F. Please provide any statistical information in relation to convictions under this law for the reporting period of 01 January 2007 – 30 June 2010.

- 5G. 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?

- 6A. Please provide the name of relevant law/s and regulations, and the relevant sections of such provisions.
- 6B. Please state how these offences are defined by law.
- 6C. Please state specifically whether the possession of content involving "terrorist propaganda" is criminalized.
- 6D. Please state which sanctions (criminal, administrative, civil) are envisaged by law.
- 6E. Please also state (if applicable) the maximum prison term envisaged by law for such offences.
- 6F. Please provide any statistical information in relation to convictions under such law for the reporting period of 01 January 2007 – 30 June 2010.
- 6G. 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.
- 6H. 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?

- 7A. Please provide the name of relevant law/s and regulations, and the relevant sections of such provisions.
- 7B. Please state how these offences are defined by law.
- 7C. Please state which sanctions (criminal, administrative, civil) are envisaged by law.
- 7D. Please also state (if applicable) the maximum prison term envisaged by law for such offences.
- 7E. Please provide any statistical information in relation to convictions under these laws for the reporting period of 01 January 2007 – 30 June 2010.
- 7F. 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.
- 7G. 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.
- 7H. 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?

- 8A. Please provide the name of relevant law/s and regulations, and the relevant sections of such provisions.
- 8B. Please state how these offences are defined by law.
- 8C. Please state which sanctions (criminal, administrative, civil) are envisaged by law.
- 8D. Please also state (if applicable) the maximum prison term envisaged by law for such offences.
- 8E. Please provide any statistical information in relation to convictions under such law for the reporting period of 01 January 2007 – 30 June 2010.
- 8F. 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?

- 9A. Please provide the name of relevant law/s and regulations, and the relevant sections of such provisions.
- 9B. Please state how these offences are defined by law.
- 9C. Please state which sanctions (criminal, administrative, civil) are envisaged by law.
- 9D. Please also state (if applicable) the maximum prison term envisaged by law for such offences.
- 9E. Please provide any statistical information in relation to convictions under such law for the reporting period of 01 January 2007 – 30 June 2010.
- 9F. 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?

- 10A. Please provide the name of relevant law/s and regulations, and the relevant sections of such provisions.
- 10B. Please state how these offences are defined by law.
- 10C. Please state which sanctions (criminal, administrative, civil) are envisaged by law.
- 10D. Please also state (if applicable) the maximum prison term envisaged by law for such offences.
- 10E. Please provide any statistical information in relation to convictions under such law (for the reporting period).

- 10F. 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"?

- 11A. Please provide the name of relevant law/s and regulations, and the relevant sections of such provisions.
- 11B. Please state how these offences are defined by law.
- 11C. If applicable please provide the legal definition of "extremism".
- 11D. Please state which sanctions (criminal, administrative, civil) are envisaged by law.
- 11E. Please also state (if applicable) the maximum prison term envisaged by law for such offences.
- 11F. Please provide any statistical information in relation to convictions under such law (for the reporting period).
- 11G. 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)?

- 12A. Please provide the name of relevant law/s and regulations, and the relevant sections of such provisions.
- 12B. Please state how these offences are defined by law.
- 12C. If applicable please provide the legal definition of "harmful content".
- 12D. Please state which sanctions (criminal, administrative, civil) are envisaged by law.
- 12E. Please also state (if applicable) the maximum prison term envisaged by law for such offences.
- 12F. Please provide any statistical information in relation to convictions under such law (for the reporting period).
- 12G. 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?

- 13A. Please specify if any other types of Internet content is outlawed.
- 13B. Please provide the name of relevant law/s and regulations, and the relevant sections of such provisions if they exist.

- 13C. If applicable please state how these offences are defined by law.
- 13D. If applicable please state which sanctions (criminal, administrative, civil) are envisaged by law.
- 13E. If applicable please also state the maximum prison term envisaged by law for such offences.
- 13F. 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?

- 14A. If the answer is Yes, then please provide the name of relevant law/s and regulations, and the relevant sections of such provisions.
- 14B. Please state how these provisions are defined by law.
- 14C. 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?

- 15A. If the answer is Yes, then please provide the name of relevant law/s and regulations, and the relevant sections of such provisions.
- 15B. Please state how these provisions are defined by law.
- 15C. 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?

- 16A. If the answer is Yes, then please provide the name of relevant applicable law/s and regulations, and relevant sections of such provisions.
- 16B. 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.).
- 16C. Please state how these provisions are defined by law.
- 16D. 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?

- 17A. If applicable please state if these hotlines are public organizations or privately run.

- 17B. If applicable please state whether they are established by law (co-regulation) or through self-regulation.

- 17C. Please also provide information on the formation/structure of such hotlines.

- 17D. Please state which types of content can be reported to these hotlines.

- 17E. 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?

- 18A. Please provide the name of relevant law/s and regulations, and the relevant sections of such provisions if such laws, or regulations exist.

- 18B. 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?

- 19A. Please provide the name of relevant law/s and regulations, and the relevant sections of such provisions.

- 19B. Please state how these provisions are defined by law.

- 19C. (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.

- 19D. 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.)?

- 20A. Please provide the name of relevant law/s and regulations, and the relevant sections of such provisions.

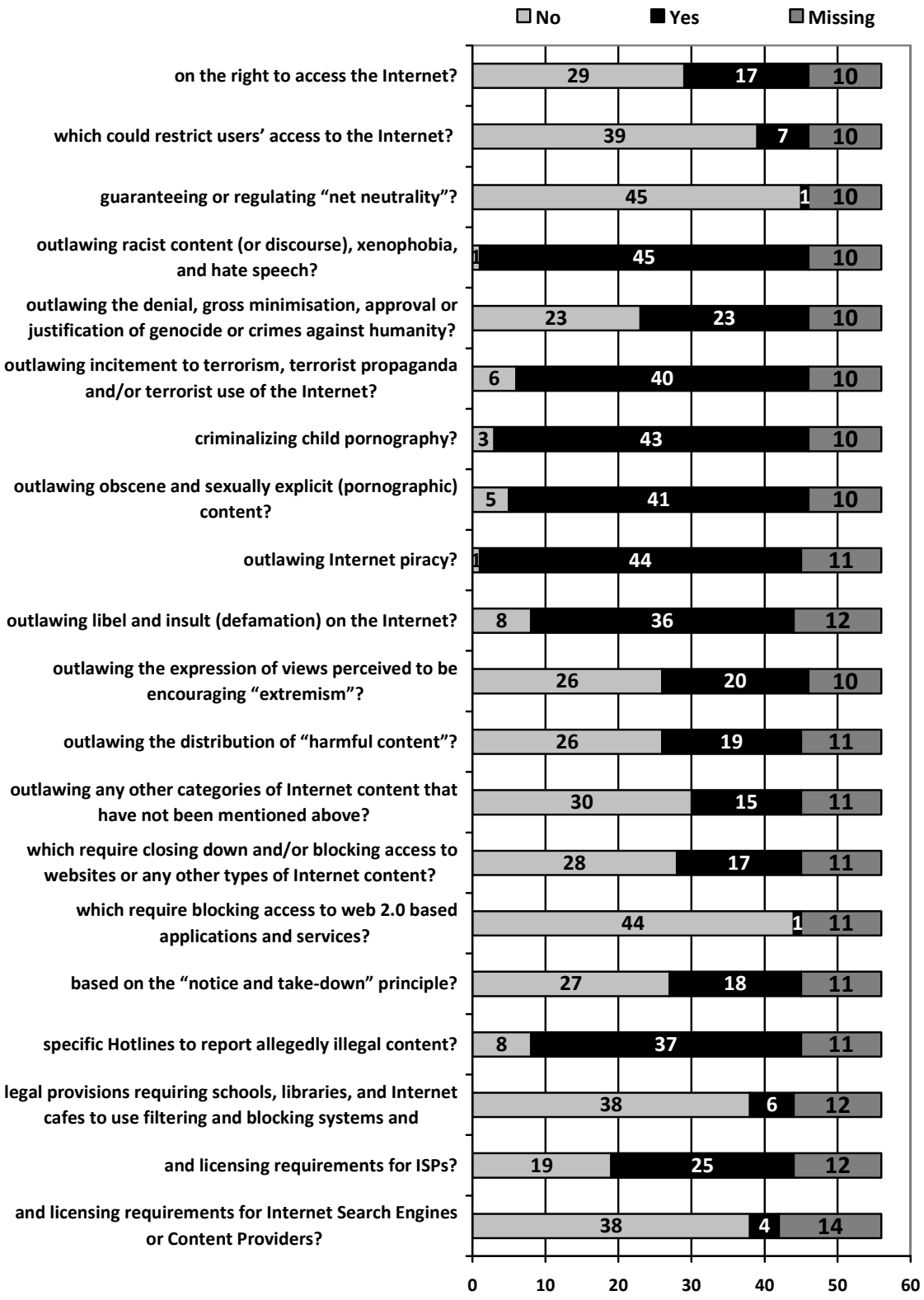
- 20B. Please state how these provisions are defined by law.

- 20C. If applicable please state any sanctions (criminal, administrative, civil) for breach of legal provisions envisaged by law.

- 20D. If applicable please also state the maximum prison term envisaged by law for any offences.

- 20E. Please provide statistical data with regards to prosecutions involving Internet Search Engines or Content Providers (for the reporting period).

Appendix II: Response Statistics



Appendix III: Response Frequencies

Specific legal provisions on the right to access the Internet

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	29	51.8	63.0	63.0
	Yes	17	30.4	37.0	100.0
	Total	46	82.1	100.0	
Missing		10	17.9		
Total		56	100.0		

Legal provisions which could restrict users' access to the Internet

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	39	69.6	84.8	84.8
	Yes	7	12.5	15.2	100.0
	Total	46	82.1	100.0	
Missing		10	17.9		
Total		56	100.0		

Specific legal provisions guaranteeing or regulating net neutrality

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	45	80.4	97.8	97.8
	Yes	1	1.8	2.2	100.0
	Total	46	82.1	100.0	
Missing		10	17.9		
Total		56	100.0		

Legal provisions outlawing racist content, xenophobia, and hate speech

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	1	1.8	2.2	2.2
	Yes	45	80.4	97.8	100.0
	Total	46	82.1	100.0	
Missing		10	17.9		
Total		56	100.0		

Racist content (or discourse), xenophobia, and hate speech: Access Blocking

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	30	53.6	75.0	75.0
	Yes	10	17.9	25.0	100.0
	Total	40	71.4	100.0	
Missing		16	28.6		
Total		56	100.0		

Legal provisions outlawing the denial, gross minimisation, approval or justification of genocide or crimes against humanity

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	23	41.1	50.0	50.0
	Yes	23	41.1	50.0	100.0
	Total	46	82.1	100.0	
Missing		10	17.9		
Total		56	100.0		

Denial, gross minimisation, approval or justification of genocide or crimes against humanity: Access Blocking

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	34	60.7	89.5	89.5
	Yes	4	7.1	10.5	100.0
	Total	38	67.9	100.0	
Missing		18	32.1		
Total		56	100.0		

Legal provisions outlawing incitement to terrorism, terrorist propaganda and/or terrorist use of the Internet

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	6	10.7	13.0	13.0
	Yes	40	71.4	87.0	100.0
	Total	46	82.1	100.0	
Missing		10	17.9		
Total		56	100.0		

Incitement to terrorism, terrorist propaganda and/or terrorist use of the Internet: Access Blocking

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	28	50.0	77.8	77.8
	Yes	8	14.3	22.2	100.0
	Total	36	64.3	100.0	
Missing		20	35.7		
Total		56	100.0		

Legal provisions criminalizing child pornography

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	3	5.4	6.5	6.5
	Yes	43	76.8	93.5	100.0
	Total	46	82.1	100.0	
Missing		10	17.9		
Total		56	100.0		

Child pornography: Access Blocking

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	29	51.8	70.7	70.7
	Yes	12	21.4	29.3	100.0
	Total	41	73.2	100.0	
Missing		15	26.8		
Total		56	100.0		

Legal provisions outlawing obscene and sexually explicit (pornographic) content

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	5	8.9	10.9	10.9
	Yes	41	73.2	89.1	100.0
	Total	46	82.1	100.0	
Missing		10	17.9		
Total		56	100.0		

Obscene and sexually explicit (pornographic) content: Access Blocking

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	32	57.1	80.0	80.0
	Yes	8	14.3	20.0	100.0
	Total	40	71.4	100.0	
Missing		16	28.6		
Total		56	100.0		

Legal provisions outlawing Internet piracy

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	1	1.8	2.2	2.2
	Yes	44	78.6	97.8	100.0
	Total	45	80.4	100.0	
Missing		11	19.6		
Total		56	100.0		

Internet piracy: Access Blocking

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	31	55.4	73.8	73.8
	Yes	11	19.6	26.2	100.0
	Total	42	75.0	100.0	
Missing	9	14	25.0		
Total		56	100.0		

Legal provisions outlawing libel and insult (defamation) on the Internet

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	8	14.3	18.2	18.2
	Yes	36	64.3	81.8	100.0
	Total	44	78.6	100.0	
Missing		12	21.4		
Total		56	100.0		

Libel and insult (defamation) on the Internet: Access Blocking

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	34	60.7	87.2	87.2
	Yes	5	8.9	12.8	100.0
	Total	39	69.6	100.0	
Missing		17	30.4		
Total		56	100.0		

Legal provisions outlawing the expression of views perceived to be encouraging extremism

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	26	46.4	56.5	56.5
	Yes	20	35.7	43.5	100.0
	Total	46	82.1	100.0	
Missing		10	17.9		
Total		56	100.0		

Expression of views perceived to be encouraging extremism: Access Blocking

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	35	62.5	87.5	87.5
	Yes	5	8.9	12.5	100.0
	Total	40	71.4	100.0	
Missing		16	28.6		
Total		56	100.0		

Legal provisions outlawing the distribution of harmful content

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	26	46.4	57.8	57.8
	Yes	19	33.9	42.2	100.0
	Total	45	80.4	100.0	
Missing		11	19.6		
Total		56	100.0		

Distribution of harmful content: Access Blocking

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	35	62.5	89.7	89.7
	Yes	4	7.1	10.3	100.0
	Total	39	69.6	100.0	
Missing		17	30.4		
Total		56	100.0		

Legal provisions outlawing any other categories of Internet content

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	30	53.6	66.7	66.7
	Yes	15	26.8	33.3	100.0
	Total	45	80.4	100.0	
Missing		11	19.6		
Total		56	100.0		

Any other categories of Internet content: Access Blocking

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	31	55.4	83.8	83.8
	Yes	6	10.7	16.2	100.0
	Total	37	66.1	100.0	
Missing		19	33.9		
Total		56	100.0		

General legal provisions which require closing down and/or blocking access to websites

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	28	50.0	62.2	62.2
	Yes	17	30.4	37.8	100.0
	Total	45	80.4	100.0	
Missing		11	19.6		
Total		56	100.0		

Legal provisions which require blocking access to web 2.0 based applications and services

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	44	78.6	97.8	97.8
	Yes	1	1.8	2.2	100.0
	Total	45	80.4	100.0	
Missing		11	19.6		
Total		56	100.0		

Legal provisions based on the notice and take-down principle

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	27	48.2	60.0	60.0
	Yes	18	32.1	40.0	100.0
	Total	45	80.4	100.0	
Missing		11	19.6		
Total		56	100.0		

Specific (public or private) Hotlines to report allegedly illegal content

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	8	14.3	17.8	17.8
	Yes	37	66.1	82.2	100.0
	Total	45	80.4	100.0	
Missing		11	19.6		
Total		56	100.0		

Legal provisions requiring schools, libraries, and Internet cafes to use filtering and blocking systems and software

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	38	67.9	86.4	86.4
	Yes	6	10.7	13.6	100.0
	Total	44	78.6	100.0	
Missing		12	21.4		
Total		56	100.0		

Legal liability provisions and licensing requirements for ISPs

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	19	33.9	43.2	43.2
	Yes	25	44.6	56.8	100.0
	Total	44	78.6	100.0	
Missing		12	21.4		
Total		56	100.0		

EU E-Commerce Directive 2000/31 has been implemented into national law

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	10	17.9	23.8	23.8
	Yes	32	57.1	76.2	100.0
	Total	42	75.0	100.0	
Missing		14	25.0		
Total		56	100.0		

Legal liability provisions and licensing requirements for Internet Search Engines or Content Providers

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	38	67.9	90.5	90.5
	Yes	4	7.1	9.5	100.0
	Total	42	75.0	100.0	
Missing		14	25.0		
Total		56	100.0		

Ratification of the Additional Protocol to the CoE Convention on Cybercrime

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Neither signed nor ratified	23	41.1	41.1	41.1
	Signed	15	26.8	26.8	67.9
	Ratified	18	32.1	32.1	100.0
	Total	56	100.0	100.0	

Ratification of the CoE Convention on the Prevention of Terrorism

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Neither signed nor ratified	13	23.2	23.2	23.2
	Signed	16	28.6	28.6	51.8
	Ratified	27	48.2	48.2	100.0
	Total	56	100.0	100.0	

Ratification of the CoE Convention on Cybercrime

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Neither signed nor ratified	11	19.6	19.6	19.6
	Signed	15	26.8	26.8	46.4
	Ratified	30	53.6	53.6	100.0
	Total	56	100.0	100.0	

Hotlines: Public or Private

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes, private hotline	13	23.2	35.1	35.1
	Yes, public hotline	13	23.2	35.1	70.3
	Both private and public hotline	11	19.6	29.7	100.0
	Total	37	66.1	100.0	
Missing		19	33.9		
Total		56	100.0		