Media Freedom on the Internet: An OSCE Guidebook

Do read this book, it contains important information related to the Internet. > Do remember that the Internet is not confined to your own country. > Do ensure citizens' access to the Internet. > Do acknowledge that freedom of expression extends not only to ideas and information generally regarded as inoffensive but even to those that might offend, shock or disturb. > Do ensure that the principle of network neutrality is respected by Internet access providers. > Do participate in the development of national legal frameworks in order to ensure the protection of the right to freedom of expression, access to the Internet and the right to privacy. > Do remember that user-generated content on the Internet provides an unprecedented platform for the exercise of freedom of expression. > Do rely on blocking only within a strict legal framework with regards to content identified as illegal by the courts of law. > Do recall that blocking is not an effective method to address problems associated with Internet content and could have serious side effects including over blocking. > Don't develop laws or policies to block access to social media platforms. > Don't forget that the State should not stand between the speaker and his or her audience. > Don't allow Internet access providers to restrict users' right to receive and impart information by means of blocking, slowing down, degrading or discriminating Internet traffic associated with particular content, services, applications or devices. > Don't impose general content monitoring requirements for the intermediaries. > Do clarify liability issues surrounding the intermediaries based on a knowledge and control test.

OSCE
The Representative on Freedom of the Media

6 Wallnerstrasse
A-1010 Vienna Austria
Phone: +43-1-51436-6800
Fax: +43-1-51436-6802
e-mail: pm-fom@osce.org

Media Freedom on the Internet: An OSCE Guidebook

Written by Professor Yaman Akdeniz, commissioned by the Office of the OSCE Representative on Freedom of the Media

March 2016

OSCE
The Representative on Freedom of the Media

CONTENTS

Foreword

by Dunja Mijatović, OSCE Representative on Freedom of the Media

Dear Readers,

I am pleased to present my Office's latest publication, "Media Freedom on the Internet: An OSCE Guidebook". This study, commissioned by my Office and carried out by Professor Yaman Akdeniz of Istanbul Bilgi University in Turkey, illustrates the importance of the protection of our fundamental freedoms online.

Keeping the Internet free, open and safe for all has never been more important, but defending freedom on the Internet is an ongoing struggle that encompasses a wide range of issues, including regulation, technical infrastructure, privacy, security, access and content.

The objective of this guidebook is to give a comprehensive overview of the major issues with and developments on freedom of expression on the Internet in the OSCE region. It also details the complexities of the issues of the free flow of information and media pluralism online, including new media, such as social media platforms.

At its very core, the argument for Internet freedom is plain and simple. Basic human rights, including freedom of expression and freedom of the media, should apply as much to the online as to the offline world.

The relationship between the OSCE and the Internet goes back to the early days of the Internet and the birth of the OSCE as an international body in 1975. It is remarkable that Article 19 of the Declaration of Human Rights, Article 19 of the International Covenant on Political and Civil Rights and the Helsinki Final Act, were written in such a way as to be applicable to today's advanced technology and digitalization, protecting freedom of expression on the Internet.

Article 19 of the Universal Declaration of Human Rights states as follows:

> *"Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."*

Indeed, this declaration, adopted back in 1948, has withstood the test of time; providing a framework for as much protection of expression on the internet as for print media or free speech.

In 2012, with the adoption of the landmark Resolution 20/8 "The promotion, protection and enjoyment of human rights on the Internet", the UN Human Rights Council confirmed that Article 19 of the Universal Declaration of Human Rights applies online in exactly the same way as it does offline.

The human rights framework on free expression on the Internet is clear; however, freedom on the Internet is constantly being challenged in a number of OSCE participating States. On a daily basis, websites are blocked, filtered and shut down in many of the 57 OSCE countries that my Office monitors.

We must also not forget the rapidly growing world of social media, which is transforming the media landscape as we know it. Social media platforms have become instrumental for the exercise of the right to media freedom and free expression. Yet, numerous restrictive measures of varying magnitude have been taken to hinder free expression on the Internet via websites, blogs and social media platforms, with the overarching goal of suppressing and limiting freedom of expression and free media online.

Governments have a crucial role to play when it comes to regulating the Internet and guaranteeing its freedom. This responsibility extends to the protection of minors and minorities from harmful content, combatting racism and content inciting hatred or violence, and even fighting cybercrime. Governments must also ensure that all stakeholders, including civil society, are consulted and continuously involved in these efforts. Most importantly, these obligations can only be successfully met if governments also ensure that any regulation designed to ensure the safety of the Internet also prioritizes and safeguards freedom of expression.

There are, of course, aspects of the Internet that require regulation, but just as important are those aspects that must remain out of the reach of government control. The challenge is to identify, on the one hand, areas that benefit from no regulation or self-regulation, and, on the other hand, effective approaches for addressing facets of the Internet where regulation is needed, all the while preserving freedom of expression and media freedom.

This publication is part of my office's Open Journalism project, to assist the OSCE states in safeguarding freedom of expression and media freedom online. I hope that it will prove useful not only for representatives of governments, but also for members of civil society, academia, non-governmental organizations striving to improve online freedom of expression, and, of course, for journalists. I trust that it will also serve to bring us a step closer to the more comprehensive and sustainable protection of free expression on the Internet.

My thanks go to the governments of Sweden and Czech Republic for their kind contribution to the Open Journalism project, without which this publication would not have been possible.

Dunja Mijatović
March 2016

Do's and Don'ts for the Policy Makers

- Do read this book, it contains important information related to the Internet.
- Do remember that the Internet is not confined to your own country.
- Do ensure citizens' access to the Internet.
- Do ensure that the principle of network neutrality is respected by Internet access providers. Do safeguard it in the development of national legal frameworks in order to ensure the protection of the right to freedom of expression, access to information and the right to privacy.
- Do remember that user-generated content on the Internet provides an unprecedented platform for the exercise of freedom of expression.
- Do acknowledge that freedom of expression extends not only to ideas and information generally regarded as inoffensive but even to those that might offend, shock, or disturb.
- Do rely on blocking only within a strict legal framework with regards to content identified as illegal by the courts of law.
- Do recall that blocking is not an effective method to address problems associated with Internet content and could have serious side effects including over blocking.
- Do remember that protection of children from harmful content policies should not be limited to filtering content from home computers and schools.
- Do clarify liability issues surrounding the intermediaries based on a knowledge and control test.
- Do read the European Court of Human Rights decisions in *Ahmet Yıldırım v. Turkey* and *Cengiz and Others v. Turkey* in relation to the Court's consideration of access blocking policies from a freedom of expression perspective.

- Do read the decision of the European Court of Human Rights in *Delfi AS v. Estonia* involving liability principles with regards to third-party comments with caution. Do read *Delfi AS v. Estonia* in the light of *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary* decision.

- Do note also the right to be forgotten decision of the Court of Justice of the European Union while addressing issues surrounding the competing rights of freedom of expression and right to privacy.

- Do read the communiqué of the OSCE Representative on Freedom of the Media on the "right to be forgotten" decision of the Court of Justice of the European Union and its possible implications for investigative journalism and media freedom. [1]

- Don't allow Internet access providers to restrict users' right to receive and impart information by means of blocking, slowing down, degrading or discriminating Internet traffic associated with particular content, services, applications or devices.

- Don't forget that the State should not stand between the speaker and his or her audience.

- Don't develop laws or policies to block access to social media platforms.

- Don't forget that, while their protection is needed, children also have a right to receive and impart information regardless of frontiers.

- Don't impose general content monitoring requirements for the intermediaries.

1 Communiqué by OSCE Representative on Freedom of the Media on ruling of the European Union Court of Justice, issued on 16 May 2014: http://www.osce.org/fom/118632

Glossary

Blocking – is an activity which is used to prevent access to Internet content or websites including social media platforms. Various methods can be used to prevent access completely from within one country or through a single Internet service provider.

Circumvention techniques – refers to various processes used by Internet users to bypass the technical aspects of Internet blocking or filtering and gain access to otherwise inaccessible content. Examples of such techniques include use of proxy tools, VPN services and anonymous browsers such as TOR.

Filtering tools – have been developed to prevent primarily children from deliberately or accidentally accessing illegal and harmful content from home computers or by schools or libraries. Such tools could be software based, or used at server level by Internet service providers.

Internet governance – is the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet.

Intermediaries – is a reference to primarily, for-profit companies including Internet service or access providers, hosting companies, social media platforms, and search engines providers. Within the European context, they are referred to as 'information society service providers'.

Net neutrality – is the principle that Internet service providers should enable access to all content, services and applications equally, regardless of the source, without favouring or blocking particular online services or websites.

Web 2.0 – is the current and second generation of the world wide web characterized by greater user driven content, collaboration and interactivity.

Introduction

> *"The new communications and information technologies have loosened the state's exclusiveness of control of its territory, reducing its capacities for cultural control and homogenisation. It is a commonplace that digitalised communications, satellites, fax machines, and computer networks have rendered the state licensing and control of information media all but impossible, not merely, undermining ideological dictatorships but also all attempts to preserve cultural homogeneity by state force."*[2]
>
> *Hirst P., & Thompson, G.,*
> *"Globalization and the Future of the Nation State"*

New communication technologies, including the Internet, undoubtedly are a boon to freedom of expression and media freedom. Currently, the Internet provides an unprecedented means of access to information and possibility to engage in dialogue and interact through the increasingly popular social media platforms to anyone across the globe. Citizens of the world are much more empowered as a result of the advancement in communication technologies.

However, as the Internet does not recognise boundaries and resist individual state attempts to suppress or censor any kind of information, individual governments find it difficult to govern and control the free flow of information inside and outside their borders. In fact, it is not surprising that through out history, communication systems from printing press through the advent of radio, television and satellite transmissions reaching out finally the Internet has been faced with scepticism and suspicion, including by governmental authorities, as they spark fear of potential detrimental effects on society, security and political power structures. As "too much information for the regular citizen" meant empowerment, communication tools and systems have been always subject to excessive regulation through out history. Therefore, prior to the 1990s, it could be said that 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

2 Hirst P., & Thompson, G., "Globalization and the Future of the Nation State," (1995) *Economy and Society*, 24(3), 408 - 442, at 419.

media content made available and the discussions it triggered remained confined within territorially defined areas.

However, along with television, other communications technologies such as satellites, fax machines, and mobile phones together with computers and modems played an important role in the globalisation of information systems "rendering national boundaries invisible."[3] Several recent historical events are directly linked to the free flow of information and the power of modern communications media.[4] Undoubtedly, "telecommunications played as much of a role as pickaxes and shovels in bringing down the Berlin Wall and the barbed wire of the Iron Curtain."[5]

During the 1990s, attention turned to the Internet, the largest and most complex communication network in the world often referred to as the "network of networks". What was so different about the Internet was that nobody owned the Internet and there was no single entity, no single government governing it. It was and it remains completely decentralized, a truly borderless medium for communications. During this decade users witnessed the launch of platforms and search engines such as Yahoo, MSN and Google. As access to this borderless new communications 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'[6] shared by many states and governments, certain civil-society organizations and concerned citizens.

As one of the foundations of state power is the control of information,[7] this was challenged by the borderless nature of the Internet and by the free flow of information across borders around the globe without respecting national laws. That is why in a sense the moral "panics are no longer about social control but rather about the fear of being out of control"[8] as the circulation of information does not only create problems in totalitarian regimes such as in China but also in

3 See Hudson, H.E, *Global Connections: International Telecommunications Infrastructure and Policy*, New York: Van Nostrand Reinhold, 1997, chapter 1.

4 Martin, W.J., *The Global Information Society*, Aslib Gower, Guildford: 1995, 9-10. See also Sparks, C., *Communism, Capitalism and the Mass Media*, London: Sage, 1997.

5 McGowan, W., 'The part as Prologue: The Impact of International Telecommunications,' in Hugh Chaloner ed., *Telecom 91 Global Review*, London: Kline Publishing, 1991, 56.

6 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.

7 See for example Couch, C.J., "Mass communications and state structures," (1990) *The Social Science Journal* 27 (2) 111-128.

8 McRobbie, A., *Postmodernism and Popular Culture,* London: Routledge, 1994, at 199.

democratic societies in Western Europe. Basically, with the Internet, the States could no longer control the widespread availability of certain types of content deemed either "illegal" or "harmful" as the Internet did not necessarily respect national rules or territorial boundaries. This dissolution of the "sovereignty" of content control, coupled with the globalization of information, came along with an increased multilingualism observable in many countries.

During this period it was understood that the old concepts of regulation, reliant as they are upon tangibility in time and space, may not be easily applicable or enforceable to the Internet. That is why considerations for the wider concept of Internet governance with responsibility for rule-making distributed to a variety of players at both public and private levels of governance were initially considered. Kofi Annan, famously said "clearly, there is need for governance, but that does not necessarily mean that it has to be done in the traditional way, for something that is so very different."[9] According to the Working Group on Internet Governance (WGIG),[10] which was set up by the Secretary-General of the United Nations in accordance with the mandate given to him by the first phase of the World Summit on the Information Society (WSIS), held in Geneva in December 2003, "governance is a part of many different processes related to the Internet, including the development of technical standards and the management of core resources, as well as regulation of the misuse and abuse of the Internet".[11]

In the 2000s, while the debate on how to regulate or govern the borderless medium continued, the Internet itself evolved and has shifted from being a mostly one sided information transmission tool into a user-driven interactive communication network with the introduction of Web 2.0 applications and services such as Friendster, MySpace, YouTube, Facebook and Twitter. The increasing popularity of these user-driven interactive platforms seemed to eliminate virtual Internet borders even further by creating a seamless global public sphere. More importantly, these platforms are not only used for pure entertainment and social purposes but more importantly they have become a boon for political speech and political and social activism. In fact, the significance of the social media platforms has been recognised at the European Court of

9 Kofi Annan, Global Forum on Internet Governance, 24 March 2004 (*Internet Governance: A Grand Collaboration*, March 2004).

10 See generally www.wgig.org/.

11 The WGIG Background Report, June 2005, at www.wgig.org/docs/BackgroundReport.doc, para. 31. See further the WGIG Report, June 2005, at www.wgig.org/docs/WGIGREPORT.doc, and Drake, W. J., ed., *Reforming Internet Governance: Perspectives from the Working Group on Internet Governance (WGIG)*, United Nations ICT Task Force, 2005, at www.wgig.org/docs/book/WGIG_book.pdf.

Human Rights level with the Court stating that "user-generated expressive activity on the Internet provides an unprecedented platform for the exercise of freedom of expression".[12] That, according to the Court is undisputed and has been recognised by the Court on several occasions.[13] More recently, the Court also noted that political information ignored by the mainstream media have often been disclosed through the YouTube platform which allowed the emergence of citizen journalism.[14]

Therefore, this global, borderless and user-driven version of the Internet heavily reliant on the social media platforms had a considerable impact on the political upheaval in the Middle East and North Africa during the Arab Spring. Although the jury is still out on the true impact of the social media platforms on the Arab Spring, the platforms certainly played a crucial role in terms of spreading up-to-date and instant news and raise awareness about ongoing events and protests from the region not only locally but globally. The platforms were also used to organize demonstrations and protests.

So, on the one hand the Internet provides essential tools for participation and deliberation in political and other activities of public interest [15] and "had now become one of the principal means of exercising the right to freedom of expression and information,"[16] on the other hand, it has become a major challenge for some governments in terms of their efforts to control and in some cases even prohibit certain types of information as well as conduct. These two conflicting realities have been subject of legal dispute[17] as will be explored in this book. However, it must be said at the outset that 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.

12 *Delfi AS v. Estonia*, GC, no. 64569/09, 16 June, 2015, para 110.

13 See *Ahmet Yıldırım v. Turkey*, no. 3111/10, § 48, ECHR 2012, and *Times Newspapers Ltd (nos. 1 and 2) v. the United Kingdom*, nos. 3002/03 and 23676/03, § 27, ECHR 2009.

14 *Cengiz and Others v. Turkey*, nos. 48226/10 and 14027/11, 01.12.2015.

15 Recommendation CM/Rec(2011)8 of the Committee of Ministers to member states on the protection and promotion of the universality, integrity and openness of the Internet, adopted by the Committee of Ministers on 21 September 2011 at the 1121st meeting of the Ministers' Deputies (para 3).

16 *Ahmet Yildirim v. Turkey*, Application No. 3111/10, judgment of 18 December 2012, 18.03.2013 (final).

17 *Delfi AS v. Estonia*, GC, no. 64569/09, 16 June, 2015

"With technologies that increasingly destroy distance, the challenge of seizing the opportunities of the new age is not merely national, but global in nature. The new technologies are truly creating an arena independent of jurisdictions and boundaries. With this new reality comes an ever more pressing need to align national strategies with the world wide movement toward a global information society."[18]

Today, many OSCE participating States feel the need to react to the development of the Internet as a major media and communication platform. Governments believe it is, on the one hand, the critical infrastructure that requires protective measures and, on the other hand, content available through the Internet 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 undesirable) content. Governments are particularly concerned about the availability of terrorist propaganda,[19] racist content,[20] hate speech, sexually explicit content, including child pornography,[21] as well as state secrets and content critical to certain governments or business practices on the Internet.

In addition to these, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression cites defamation (to protect the rights and reputation of others against unwarranted attacks), direct and public incitement to commit genocide (to protect the rights of others) and advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence (to protect the rights of others, such as the right to life) among the types of content that may be subject to governmental restrictions.[22] However, the governance of illegal as well as harmful (which falls short of illegal) Internet content may differ from one country to another and variations are evident within

18 See Preparing Canada for a Digital World: Final Report of the Information Highway Advisory Council, September 1997.

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

20 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.

21 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.

22 The UN Human Rights Council's Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression stated the following in his report of 16 May 2011 to the Human Rights Council (A/HRC/17/27), para 25.

the OSCE participating States.[23] "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 a major problem when content hosted or distributed from outside the jurisdiction is deemed illegal in another.[24]

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 social media platform providers? Should the providers be liable in the country where the content has been uploaded, viewed, or downloaded or where the server is placed or where the responsible providers reside? Many of these questions remain unanswered and provide significant challenges to the governments across the OSCE region, and indeed across the globe. Some countries fear the Internet could undermine their judicial sovereignty; others, however, embrace the Internet and praise its global nature. Nevertheless, the Internet certainly has created challenges for governments and these challenges are particularly visible when analysing 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 book)[25] 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 some

23 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.

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

25 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).

participating States of the OSCE, 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, will be detailed in this book.

While the intention of states to combat illegal activity over the Internet and to protect their citizens from harmful content is legitimate, their impact on freedom of expression should be assessed further as sometimes such policies may have an unintended negative consequence or serious side effect creating a detrimental affect on the free flow of information over the Internet.

The OSCE Representative on Freedom of the Media has long argued that Internet freedom must be priority for policymakers and International co-operation and the inclusion of corporations and civil society along with governments are needed to keep the Internet a global open forum to exchange ideas and share information.[26]

The book aims to provide a concise overview of significant issues and developments related to freedom of expression, the free flow of information and media pluralism within the context of Internet communications including the user-driven social media platforms. As its legal framework, the guide book will refer to 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.

---

26 Note the position paper of the OSCE Representative on Freedom of the Media on Internet freedom, 11 January 2012, at http://www.osce.org/fom/86003. See further the previous publications of the Office of the OSCE Representative on Freedom of the Media related to the Internet: *Spreading the Word on the Internet: 16 Answers to 4 Questions*, 2003, at http://www.osce.org/fom/13871; *The Media Internet Freedom Cookbook*, 2004, at http://www.osce.org/fom/13836; *Governing the Internet: Freedom and Regulation in the OSCE Region*, 2007, at http://www.osce.org/fom/26169; *Freedom of Expression on the Internet: A study of the legal provisions and practices related to the freedom of expression, the free flow of information and media pluralism on the Internet in OSCE participating States*, 2011, at http://www.osce.org/fom/80723; *Countering Online Abuse of Female Journalists*, 2016, at http://www.osce.org/fom/220411.

OSCE Commitments

The Organization for Security and Co-operation in Europe is the world's largest regional security organization and comprises 57 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 1997, acknowledging the need to improve the fundamental right to freedom of expression and freedom of the media in the OSCE region, the Organization has established the Office of the OSCE Representative on Freedom of the Media. The mandate of the Representative focuses on observing relevant media developments in all participating States and, with the use of a broad range of tools, promote full compliance with OSCE principles and commitments regarding freedom of expression and free media.

These commitments date as far back as 1975, when the participating States first 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".[27]

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."[28]
This was echoed by the 1996 Lisbon Summit where the OSCE participating

27 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.

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

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."[29]

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."[30]

With the spread of new technologies and their fundamental influence on free expression and media freedom, the need to protect freedom of expression online has gained increased awareness within the OSCE participating States. The promotion of the right to free expression on the Internet, including on social media, has become one of the most important activities of the Representative's Office.

In 2004, at the Sofia Ministerial Council, the OSCE participating States declared that the freedoms of opinion and expression, which include the freedom to seek, receive and impart information, are vital to democracy and are strengthened by the Internet. They 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".[31]

OSCE Heads of State or Government at the 2010 Astana Summit have emphasized that "human rights and fundamental freedoms are inalienable, and that their protection and promotion is our first responsibility." They reaffirmed that "the commitments undertaken in the field of the human dimension are matters of direct and legitimate concern to all participating States and do not belong

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

30 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.

31 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.

exclusively to the internal affairs of the State concerned." It was also noted at the Astana Summit that the participating States "value the important role played by civil society and free media in helping us to ensure full respect for human rights, fundamental freedoms, democracy, including free and fair elections, and the rule of law."

In 2015, at the Belgrade Ministerial Council, participating States emphasized the role of the media in encouraging pluralistic debates, and noted the need to fully respect the right to freedom of opinion and expression in communication efforts, including via social media, to counter violent extremist messaging.[32] This approach also reflects the efforts of the Office of the Representative in promoting the indivisibility of security and human rights. The Office has long advocated the need to not only protect, but further strengthen freedom of expression and media freedom in the efforts to create safer societies.

32 OSCE Ministerial Declaration on preventing and countering violent extremism and radicalization that lead to terrorism, 04 December, 2015 at http://www.osce.org/cio/208216?download=true

Chapter I

Internet Access – A Fundamental Human Right

This chapter provides an overview of issues related to Internet access including policy developments related to net-neutrality

Everyone should have the right to participate in the information society and states have a responsibility to ensure that citizens' access to the Internet is guaranteed. The Internet is increasingly becoming indispensable for people to take part in cultural, social and political discourse and life. Currently, in the beginning of January 2016, the number of Internet users worldwide is estimated around 3.27 billion up from around 3.17 billion in 2015.[33] In terms of social media platform usage, the number of worldwide users is expected to reach 2.5 billion by 2018, around a third of Earth's entire population[34] up from 1.4 billion in 2012. Moreover, as of the second quarter of 2015, there were a total of roughly 1.5 billion monthly active Facebook users, accounting for almost half of Internet users worldwide.[35] Twitter, on the other hand, as of the third quarter of 2015, averaged at 307 million monthly active users.[36] It must be also mentioned that over one billion people use the YouTube platform and as of May 2013 and more than 100 hours of video content were uploaded to YouTube every minute.[37] These impressive numbers and statistics show the importance of "Internet access" without which people across the globe would be deprived of not only access to vital information but also of a network which enables participation and engagement in political issues.

Internet access is therefore fundamentally crucial and has started to become an important policy topic in the last few years. In fact, certain countries and international organizations, such as the United Nations started to recognize Internet access as inherent to the right to free expression and as such to be a fundamental and universal human right.[38] Countries such as Finland and Estonia

33 See http://www.internetlivestats.com/internet-users/

34 See http://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/

35 See http://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/

36 See http://www.statista.com/statistics/282087/number-of-monthly-active-twitter-users/

37 See http://www.statista.com/statistics/259477/hours-of-video-uploaded-to-youtube-every-minute/

38 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.

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."[39] 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."[40]

Furthermore, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression highlighted the importance of Internet access in his May 2011 report and stated that "the Internet, as a medium by which the right to freedom of expression can be exercised, can only serve its purpose if States assume their commitment to develop effective policies to attain universal access to the Internet."[41]

Legal provisions guaranteeing "net neutrality"

Related to the topic of Internet access is "network neutrality" which is a reference to the principle that all Internet data traffic should be treated equally based on an end-to-end principle. This means that network operators or Internet access providers treat all 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."[42] In practice, Internet 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,

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

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

41 The UN Human Rights Council's Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression stated the following in his report of 16 May 2011 to the Human Rights Council (A/HRC/17/27), para 60.

42 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.

should apply irrespective of the infrastructure or the network used for Internet connectivity"[43] as declared by the Council of Europe Committee of Ministers. Similarly, a 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."[44]

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

Therefore, there is "growing international interest as to whether, and to what extent, traffic management should be subject to regulation."[46] According to a discussion paper issued by Office of Communications (OFCOM) in the United Kingdom "the debate ranges widely including questions such as whether citizens have a 'fundamental right' to a neutral Internet, or whether 'net neutrality' promotes economic competitiveness and growth."[47] 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.

43 *Ibid*.

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

45 *Ibid*.

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

47 *Ibid*.

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."[48]

Subsequent to the EU developments, in May 2012, the Netherlands became the first member state of the European Union and also the first OSCE country to enact a net neutrality law.[49] Under the Dutch law, operators are required to treat all Internet traffic equally and network operators are prohibited from slowing down or blocking third-party services that allow for Internet-based communications, such as Skype. The OSCE Representative on Freedom of the Media welcomed the Netherlands' passing of a net neutrality law and stated that "this law represents an important step toward ensuring a free and open Internet by protecting Internet traffic from undue restrictions or prioritization."[50]
So far as the US developments are concerned, the American Civil Liberties Union also 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."[51] Subsequently, the US Federal Communications

48 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.

49 Act of 10 May 2012 for the amendment of the Telecommunications Act for the implementation of the revised telecommunications directives. Note further EDRI, "Netherlands: Two telcos fined for net neutrality violations," 11 February, 2015, at https://edri.org/netherlands-two-telcos-fined-for-net-neutrality-violations/

50 OSCE media freedom representative welcomes Dutch net neutrality law, 14 May 2012, http://www.osce.org/fom/90535

51 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-

Commission's ("FCC") Protecting and Promoting the Open Internet policy[52] was announced in March 2015. The FCC's Open Internet rules protect and maintain open, uninhibited access to legal online content without broadband Internet access providers being allowed to block, impair, or establish fast/slow lanes to lawful content. The FCC's Open Internet rules went into effect on 12 June, 2015 and are designed to protect free expression and innovation on the Internet and promote investment in the nation's broadband networks. FCC's Open Internet rules apply to both fixed and mobile broadband service and the Bright Line Rules designed by the FCC include the following:

- **No Blocking**: broadband providers may not block access to legal content, applications, services, or non-harmful devices.
- **No Throttling**: broadband providers may not impair or degrade lawful Internet traffic on the basis of content, applications, services, or non-harmful devices.
- **No Paid Prioritization**: broadband providers may not favour some lawful Internet traffic over other lawful traffic in exchange for consideration of any kind—in other words, no "fast lanes." This rule also bans Internet Service Providers from prioritizing content and services of their affiliates.

The FCC's Open Internet rules also establish a legal standard for other broadband provider practices to ensure that they do not unreasonably interfere with or disadvantage consumers' access to the Internet. The rules build upon existing, strong transparency requirements. They ensure that broadband providers maintain the ability to manage the technical and engineering aspects of their networks.

In terms of establishing a policy within the European Union, on 23 July 2012, the European Commission launched a public consultation, seeking answers to questions on specific aspects of transparency, traffic management and switching in an Open Internet. Finally, the European Commission published a Regulation during 2015 including provisions on "net neutrality" to protect the right of every European to access Internet content without discrimination which was adopted by the European Parliament and Council.[53] This Regulation aims to

52 Federal Communications Commission, Protecting and Promoting the Open Internet, FCC-15-24, Adopted: February 26, 2015 Released: March 12, 2015, at https://transition.fcc.gov/Daily_Releases/Daily_Business/2015/db0312/FCC-15-24A1.pdf

53 Regulation (EU) 2015/2120 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union, OJEU L 310, 26 November 2015

establish common rules to safeguard equal and non-discriminatory treatment of traffic in the provision of internet access services and related end-users' rights. Furthermore, it aims to protect end-users and simultaneously to guarantee the continued functioning of the Internet ecosystem as an engine of innovation. The measures provided for in this Regulation respect the principle of technological neutrality, that is to say they neither impose nor discriminate in favour of the use of a particular type of technology.

"End-users should have the right to access and distribute information and content, and to use and provide applications and services without discrimination, via their internet access service. The exercise of this right should be without prejudice to Union law, or national law that complies with Union law, regarding the lawfulness of content, applications or services. This Regulation does not seek to regulate the lawfulness of the content, applications or services, nor does it seek to regulate the procedures, requirements and safeguards related thereto. Those matters therefore remain subject to Union law, or national law that complies with Union law." (Para 6 of the Regulation 2015/2120)

Article 3 of the Regulation entitled "Safeguarding of open Internet access" states that providers of Internet access services shall treat all traffic equally, when providing Internet access services, without discrimination, restriction or interference, and irrespective of the sender and receiver, the content accessed or distributed, the applications or services used or provided, or the terminal equipment used. However, this will not prevent providers of Internet access services from implementing reasonable traffic management measures. In order to be deemed to be reasonable, such measures shall be transparent, non-discriminatory and proportionate, and shall not be based on commercial considerations but on objectively different technical quality of service requirements of specific categories of traffic. Such measures shall not monitor the specific content and shall not be maintained for longer than necessary.

The Council of Europe also recognized in a September 2010 Committee of Ministers Declaration on Network Neutrality that the "users' right to access and distribute information online and the development of new tools and services might be adversely affected by non-transparent traffic management, content and services' discrimination or impeding connectivity of devices."[54] The Declaration,

54 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

which underlines the importance of Internet users having the greatest possible access to Internet-based content, applications and services of their choice stated that:

"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."[55]

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."[56]

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."[57]

55 *Ibid*., para 6.

56 *Ibid*., para 8.

57 *Ibid*., para 9.

As a follow-up to the adoption of the Declaration on network neutrality in 2010, the Committee of Ministers published a Recommendation in January 2016 on protecting and promoting the right to freedom of expression and the right to private life with regard to network neutrality.[58] The Recommendation called on the member States to safeguard the principle of network neutrality in the development of national legal frameworks in order to ensure the protection of the right to freedom of expression and to access to information, and the right to privacy. With this Recommendation, the Committee of Ministers issued a set of network neutrality guidelines pointing out that Internet traffic should be treated equally, without discrimination, restriction or interference irrespective of the sender, receiver, content, application, service or device.

Acknowledging that Internet traffic management can sometimes pursue legitimate purposes, the Committee of Ministers stressed that it can also result in blocking, discrimination or prioritisation of specific types of content, applications or services. According to the Draft Recommendation, the principle of network neutrality, along the lines of EU views, underpins non-discriminatory treatment of Internet traffic and users' right to receive and impart information and to use services of their choice. It reinforces the full exercise and enjoyment of the right to freedom of expression since Article 10 of the ECHR applies not only to the content of information but also to the means of its dissemination.

The Council of Europe "Guidelines on network neutrality" state that Internet traffic management measures should only be admitted in exceptional circumstances, for example to comply with an order from a court or a regulatory authority; or when needed to preserve network integrity and security; or to prevent or address network congestion. These measures should be non-discriminatory, transparent, maintained no longer than strictly necessary, and subject to regular review by the authorities. Furthermore, the Guidelines emphasize that any traffic management practice that allows assessing the content of communications is an interference with the right to privacy and it should fully comply with article 8 of the European Convention on Human Rights and national legislation, and be reviewed by the authorities.

58 Recommendation CM/Rec(2016)1 of the Committee of Ministers to member States on protecting and promoting the right to freedom of expression and the right to private life with regard to network neutrality. Adopted by the Committee of Ministers on 13 January 2016, at the 1244th meeting of the Ministers' Deputies.

Conclusion

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. With increasing number of Internet users worldwide, the states have a responsibility to ensure citizens' access to the Internet is guaranteed. Within this context, Network neutrality is an important prerequisite for the Internet to be equally accessible and affordable to all.

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. No doubt, all Internet users have a right to freedom of expression, including the right to receive and impart information protected by international conventions, by using services, applications and devices of their choice. Therefore, the users' right to receive and impart information on the Internet should not be restricted by means of blocking, slowing down, degrading or discriminating Internet traffic associated with particular content, services, applications or devices or traffic associated with services provided on the basis of exclusive arrangements or tariffs.[59]

59 Recommendation CM/Rec (2016)1 of the Committee of Ministers to member States on protecting and promoting the right to freedom of expression and the right to private life with regard to network neutrality.

Chapter II

Internet Content Regulation and Freedom of Expression

This chapter provides an overview of issues and principles related to freedom of expression on the Internet.

The Internet as the largest communication network in the world is increasingly becoming indispensable for everyone around the world to take part in cultural, social and political discourse. The Internet "enables people to have access to information and services, to connect and to communicate, as well as to share ideas and knowledge globally. It provides essential tools for participation and deliberation in political and other activities of public interest." [60] According to the European Court of Human Rights 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."[61]

Furthermore, according to the Court "in light of its accessibility and its capacity to store and communicate vast amounts of information, the Internet plays an important role in enhancing the public's access to news and facilitating the dissemination of information generally."[62] The Court, in *Ahmet Yıldırım v. Turkey*, went further by stating that the Internet "had now become one of the principal means of exercising the right to freedom of expression and information."[63] Furthermore, in its Delfi decision, the Court states that "user-generated expressive activity on the Internet provides an unprecedented platform for the

60 Recommendation CM/Rec(2011)8 of the Committee of Ministers to member states on the protection and promotion of the universality, integrity and openness of the Internet, adopted by the Committee of Ministers on 21 September 2011 at the 1121st meeting of the Ministers' Deputies (para 3).

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

62 See *Times Newspapers Ltd (Nos. 1 and 2) v. The United Kingdom*, Applications 3002/03 and 23676/03, Judgment of 10 March 2009, Final: 10 June 2009; and *Ashby Donald and Others v. France*, no. 36769/08, § 34, 10 January 2013 –not yet final

63 *Ahmet Yıldırım v. Turkey*, Application No. 3111/10, judgment of 18 December 2012, 18.03.2013 (final).

exercise of freedom of expression."[64] However, the Court also acknowledged that "defamatory and other types of clearly unlawful speech, including hate speech and speech inciting violence, can be disseminated like never before, worldwide, in a matter of seconds, and sometimes remain persistently available online."[65]

So, it must be clearly stated that freedom of expression is a fundamental human right enshrined in the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and the European Convention on Human Rights and guaranteed by OSCE commitments. Article 19 of the International Covenant on Civil and Political Rights provides that "everyone shall have the right to hold opinions without interference" subject to the provisions in Article 19, paragraph 3, and article 20.[66] The exercise of the rights provided for in Article 19 paragraph 2 carries with it special duties and responsibilities. Freedom of expression may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary for respect of the rights or reputations of others; for the protection of national security or of public order (*ordre public*), or of public health or morals.

Although there may be certain restrictions based on conditions provided in article 19(3) of the ICCPR or Article 10(2) of the ECHR, freedom of expression is applicable not only to 'information' or 'ideas' that are favourably received or regarded as inoffensive but also to those that offend, shock or disturb.[67]

Undoubtedly differences exist among approaches adopted to regulate content on the Internet. Content regarded as harmful or offensive does not always fall within the boundaries of illegality in all OSCE participating States. Usually, the difference between illegal and harmful content is that the former is criminalized by national laws, while the latter is considered offensive, objectionable, unwanted or undesirable by some but is generally not considered criminal. While child pornography could be regarded as a clear example of content criminalized in most, if not all the 57 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

64 *Delfi AS v. Estonia* [GC], Application no. 64569/09, judgment of 16 June 2015, para 110.

65 *Ibid*.

66 Article 20: 1. Any propaganda for war shall be prohibited by law. 2. Any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law. See communications Nos. 359/1989 and 385/1989, *Ballantyne, Davidson and McIntyre v. Canada*, Views adopted on 18 October 1990.

67 *Handyside v. the United Kingdom*, 7 December 1976, Series A no. 24, p. 23, § 49; *Lingens v. Austria*, 8 July 1986, Series A no. 103, p. 26, § 41; and *Jersild v. Denmark*, 23 September1994, Series A no. 298, p. 26, § 37.

drinking and gambling. Certain zealous 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", concerns remain about possible access to this type of content by children.

In line with international human rights instruments including the European Convention on Human Rights, the right to freedom of expression, amongst others, contains not only to impart but also to seek and receive information. Article 19 of the International Covenant on Civil and Political Rights includes "freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice" including audio-visual as well as electronic and Internet-based modes of expression.[68] On the other hand, Article 10 of the European Convention on Human Rights applies not only to the content of information but also to the means of transmission or reception since any restriction imposed on the means necessarily interferes with the right to receive and impart information.[69]

Furthermore, freedom to receive information is not limited to the forum state. On the contrary, as stated in Article 10 of the Convention and recognised by the European Court freedom to receive information applies "regardless of frontiers".[70] More importantly, the State must not stand between the speaker and his audience and thus defeat the purpose for which the protection of expression is realised.[71]

The UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression emphasized that due to the unique characteristics of the Internet, regulations or restrictions which may be deemed legitimate and proportionate for traditional media are often not so with regard to the Internet.[72] In terms of restrictions, there is often a strict criteria provided by the international instruments and the strict criteria as provided by the jurisprudence of the European Court of Human Rights with regards to article 10 of the European Convention on Human Rights will be provided below.

---

68 Note the new General Comment No.34 on Article 19 which was adopted during the 102nd session of the UN Human Rights Committee, Geneva, 11-29 July 2011, at <http://www2.ohchr.org/english/bodies/hrc/docs/CCPR-C-GC-34.doc>.

69 *Autronic AG v. Switzerland,* 22 May 1990, §§ 47-48, Series A no. 178; *Öztürk v. Turkey* [GC], no. 22479/93, § 49, ECHR 1999-VI.

70 *Groppera Radio Ag and Others v. Switzerland*, no. 10890/84, judgment of 28/03/1990, para. 50.

71 *Ibid*.

72 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>, para 27.

Strict Criteria under Article 10 of the European Convention on Human Rights

Policy and legal developments with regard 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 hateful 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'."[73] 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.[74] Such state-level differences undoubtedly complicate harmonization of laws and approaches at the international level.

However, the European Court of Human Rights has made clear that "freedom of political debate is at the very core of the concept of a democratic society which prevails throughout the Convention".[75] Under Article 1 of the European Convention on Human Rights, each Contracting State "shall secure to everyone within [its] jurisdiction the rights and freedoms defined in ... [the] Convention".[76]

Within the Council of Europe region, any restriction regarding Internet speech and content must therefore meet the strict criteria under Article 10 of the European Convention on Human Rights. According to the European Court of Human Rights jurisprudence, a strict three-part test is required for any content-based restriction. Similar to the requirements by Article 19 paragraph 3 of the International Covenant on Civil and Political Rights the restriction or interference must be "provided by law", these must be imposed for one of the grounds set out in subparagraphs (a) and (b) of paragraph 3 of Article 19 of ICCPR or Article 10(2) of the European Convention and they must conform to the strict tests of necessity in a democratic society and proportionality.[77]

---

73 *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.

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

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

76 *Marckx v. Belgium* 13 June 1979, § 31, Series A no. 31; see also *Young*, *James and Webster v. the United Kingdom*, 13 August 1981, § 49, Series A no. 44.

77 See communication no. 1022/2001, *Velichkin v. Belarus*, Views adopted on 20 October 2005.

Article 10 of the European 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.[78]

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. In order to comply with this important requirement, interference does not merely need 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.[79] 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.[80] 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.[81]

If the interference is in accordance with law, then 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

78 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>. See further General Comment No.34 on Article 19 which was adopted during the 102nd session of the UN Human Rights Committee, Geneva, 11-29 July 2011, at <http://www2.ohchr.org/english/bodies/hrc/docs/CCPR-C-GC-34.doc>.

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

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

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

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,[82] and the state interference should correspond to a "pressing social need".[83] The state response and the limitations provided by law should be "proportionate to the legitimate aim pursued".[84] The Contracting States have a certain margin of appreciation in assessing whether such a need exists, but it goes hand in hand with European supervision, embracing both the legislation and the decisions applying it, even those given by an independent court. The European Court of Human Rights requires the reasons given by the national authorities to be relevant and sufficient.[85]

So far as the freedom of the media is concerned, the European Court in almost all decisions emphasises the essential function the press fulfils in a democratic society. UN Human Rights Committee's General Comment No. 34 on Article 19 of the ICCPR also states that "a free, uncensored and unhindered press or other media is essential in any society to ensure freedom of opinion and expression and the enjoyment of other Covenant rights."[86] The European Court confirms that "although the press must not overstep certain bounds, particularly as regards the reputation and rights of others and the need to prevent the disclosure of confidential information, its duty is nevertheless to impart – in a manner consistent with its obligations and responsibilities – information and ideas on all matters of public interest". [87] Journalistic freedom also covers possible recourse to a degree of exaggeration, or even provocation.[88] On the other hand, the limits of permissible criticism are narrower in relation to a private citizen than in relation to politicians or governments.[89]

---

82 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.

83 See *Sürek v. Turkey* (No. 1), no. 26682/95, judgment of 8 July 1999, Reports 1999; *Sürek v. Turkey* (No. 3), no. 24735/94, judgment of 8 July 1999.

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

85 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 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.

86 See further General Comment No.34 on Article 19 which was adopted during the 102nd session of the UN Human Rights Committee, Geneva, 11-29 July 2011, at <http://www2.ohchr.org/english/bodies/hrc/docs/CCPR-C-GC-34.doc>, para 13.

87 See *Jersild v. Denmark*, 23 September 1994, § 31, Series A no. 298; *De Haes and Gijsels v. Belgium*, 24 February 1997, § 37, *Reports* 1997-I; and *Bladet Tromsø and Stensaas v. Norway* [GC], no. 21980/93, § 58, ECHR 1999-III

88 See *Prager and Oberschlick v. Austria*, no. 15974/90, 26 April 1995, § 38, Series A no. 313.

89 *Castells v. Spain*, no. 11798/85, 23 April 1992, § 46, Series A no. 236.

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.[90] 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.[91] 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.[92] 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".[93]

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.

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

There is documented evidence that racist organizations and individuals are currently using the Internet to disseminate racist content. As social media platforms and applications have grown popular, racist organizations and individuals have started to use on-demand video and file-sharing platforms such as YouTube 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. However, efforts

90 *The Observer and The Guardian v. the United Kingdo*m, no. 13585/88, judgment of 26 November 1991, Series A no. 216, pp. 29-30, § 59.

91 *Lingens v. Austria*, no. 9815/82, 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.

92 *Autronic AG v. Switzerland*, no. 12726/87, judgment of 22 May 1990, Series A No. 178, § 61.

93 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.

to harmonize laws to combat racist content on the Internet have proved to be problematic.[94] Since the finalization 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.[95] The Additional Protocol, which came into force in March 2006, requires the signatories to criminalize the dissemination[96] of racist and xenophobic material[97] through computer systems, as well as racist and xenophobic-motivated threats,[98] racist and xenophobic-motivated insults,[99] and the denial, gross minimisation, approval or justification of genocide or crimes against humanity, particularly those that occurred during the period 1940-45.[100] Although the Additional Protocol intended to harmonize substantive criminal law in the fight against racism and xenophobia on the Internet only 36 contracting states (including the external supporters Canada and South Africa) have signed the Additional Protocol since it was opened to signature in January 2003. 24 signatories have ratified the Additional Protocol as of December 2015.[101]

94 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.

95 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.

96 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.

97 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."

98 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.

99 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) 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.

100 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.

101 Albania, Armenia, Bosnia and Herzegovina, Croatia, Cyprus, Czech Republic, Denmark, Finland, France, Germany, Latvia, Lithuania, Luxembourg, Montenegro, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovenia, Spain, the former Yugoslav Republic of Macedonia and Ukraine.

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 177 ratifications by member states as of December 2015,[102] the ICERD provisions remain the most important normative basis upon which international efforts to eliminate racial discrimination could be built.[103] 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 or interpretative declarations regarding 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.[104] The 11th Ministerial Council meeting of Maastricht in December 2003 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 authorized to gather information and statistics collected by the participating States in full co-operation with, *inter alia*, the Committee on the Elimination of Racial Discrimination ("CERD"), the European Commission against Racism and Intolerance ("ECRI") and the European Monitoring Centre on Racism and Xenophobia ("EUMC"),[105] as well as with relevant non-governmental organisations. Since then the OSCE has organized a number of high-level conferences and meetings to address the problems of racism, xenophobia, discrimination, and anti-Semitism.[106] The need to combat hate crime, which can

102 See http://indicators.ohchr.org/

103 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.

104 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.

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

106 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).

be fuelled by racist, xenophobic and anti-Semitic propaganda on the Internet, was explicitly recognized by a decision of the 2003 Maastricht Ministerial Council.[107] This was reinforced by the OSCE Permanent Council Decision on Combating anti-Semitism (PC.DEC/607)[108] and its Decision on Tolerance and the Fight against Racism, Xenophobia and Discrimination (PC.DEC/621)[109] 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).[110]

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.[111] 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, as also, mentioned earlier, 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.[112]

The European Court of Human Rights also referred to "hate speech" in a number of its judgments. In the case of *Gündüz v. Turkey*[113] 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 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

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

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

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

110 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.

111 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.

112 *Ibid*. at decision No. 4.

113 *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.

are proportionate to the legitimate aim pursued".[114] According to the Court, "only statements which promote a certain level of violence qualify as hate speech",[115] 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".[116]

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[117] of the Council of Europe Cybercrime Convention's Additional Protocol Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems requires the criminalization of expressions which deny, grossly minimize, approve or justify acts constituting genocide or crimes against humanity as defined by international law and recognized 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 minimized, approved or justified in order to support these detestable theories and ideas".[118] This provision is supported by the European Court of Human Rights, which made it clear in its judgment in *Lehideux and Isorni*[119] that the denial or revision of "clearly established historical facts – such as the Holocaust (whose negation or

114 *Ibid*.

115 *Ibid*.

116 *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.

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

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

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

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,[120] the justification of a pro-Nazi policy could not be allowed to enjoy the protection afforded by Article 10".[121] The Court, and previously, the European Commission of Human Rights, has 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.[122]

Further examples of speech that is incompatible with the values proclaimed and guaranteed by the Convention is not protected by Article 10 by virtue of Article 17 of the Convention include linking all Muslims with a grave act of terrorism,[123] or portraying the Jews as the source of evil in Russia.[124]

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

The availability of glorification of violence and terrorist propaganda[125] on the Internet, and content which may encourage terrorist activities,[126] such as bomb-making instructions including the infamous *Anarchist's Cookbook* or the often cited *Encyclopaedia of the Afghan Jihad, The Al-Qaeda Manual*,[127] *The*

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

121 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>).

122 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 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.

123 *Norwood v. the United Kingdom* (dec.), no. 23131/03.

124 *Pavel Ivanov v. Russia* (dec.), no. 35222/04, 20 February 2007.

125 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.

126 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.

127 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/.

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 mobilize 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."[128] 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.[129]

The Council of Europe Convention on the Prevention of Terrorism (CETS No. 196), which entered into force in June 2007, provides for a harmonized legal basis to prevent terrorism and to counter, in particular, public provocation to commit terrorist offences,[130] recruitment[131] and training[132] 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 criminalized. While 44 member states out of 47 signed the Convention, only 34 of them ratified it as of December 2015.

128 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.

129 Within this context note the decision of the European Court of Human Rights in *Leroy v. France*, no. 36109/03, 02.10.2008. In this case, on 11 September 2001, the day of the attack on the twin towers of the World Trade Centre, the applicant, a cartoonist, submitted to the editorial team of a Basque weekly a drawing representing the attack with a caption which parodied the advertising slogan of a famous brand: "We have all dreamt of it... Hamas did it". The criminal court convicted the applicant and the publishing director of the charges and ordered them to pay a fine of EUR 1,500 each. According to the European Court, the publication of the drawing had provoked a reaction that could have stirred up violence and suggested that it may well have affected public order in the region. The Court, therefore, found no violation of Article 10.

130 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).

131 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).

132 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).

Regarding 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."[133] 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.[134] The OSCE Decision invited the "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."[135]

During the December 2012 Dublin Ministerial Conference, the OSCE published a Declaration on Strengthening Good Governance and Combating Corruption, Money-Laundering and the Financing of Terrorism.[136] In this declaration the OSCE participating States recognized that freedom of information and access to information foster openness and accountability in public policy and procurement and enable civil society, including the media, to contribute to preventing and combatting corruption, the financing of terrorism, and money-laundering and its predicate offences. This was reaffirmed at the December 2014 Basel Ministerial Council with the publication of the Decision on Prevention on Corruption.[137]

Furthermore, during the December 2015 Belgrade Ministerial Council meeting, the OSCE published a Ministerial Declaration on preventing and countering violent extremism and radicalization that lead to terrorism.[138] In this Declaration, the OSCE emphasized that international co-operation and public-private partnerships is necessary to develop practical measures to counter the use of the Internet

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

134 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).

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

136 See http://www.osce.org/cio/97968

137 See Decision No 5/14 at http://www.osce.org/cio/130411

138 See http://www.osce.org/cio/208216

and other means for the purposes of inciting violent extremism and radicalization that lead to terrorism and for recruiting foreign terrorist fighters.[139] According to the OSCE Declaration, such international co-operation and public-private partnerships could foster communication efforts, including via social media, to counter violent extremist messaging, while fully respecting the right to freedom of opinion and expression.[140]

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.[141] Significant policy initiatives at the supranational, regional, and international levels have been put forward to address this issue.[142] However, harmonisation efforts to combat illegal Internet content, including universally condemned content such as child pornography, have been protracted and are ongoing[143] despite the adoption of several legal instruments, including the European Union's Framework Decision on combating the sexual exploitation of children and child pornography,[144] Council of Europe's Cybercrime Convention 2001,[145] Council of Europe's more recent Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse,[146] and the United Nations' Optional Protocol to the Convention on the Rights of the Child on the Sale of

139 *Ibid*, para 10.

140 *Ibid*.

141 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.

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

143 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.

144 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 >.

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

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

Children, Child Prostitution and Child Pornography.[147] 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 of 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", Council of Europe's Cybercrime Convention 2001 defines it[148] 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."[149]

The EU definition is provided in the Council Framework Decision which defines child pornography[150] 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
(iii) realistic images of a non-existent child involved or engaged in the conduct mentioned in (i);

147 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).

148 See Article 9(2).

149 See Article 20(2).

150 See Article 1(b).

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".[151]

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 European Union and the Council of Europe definitions refer to visual depictions and representations, the United Nations definition is broader as it refers to "any representation," and could also cover textual material including cartoons, and drawings.[152]

In terms of ratification at the Council of Europe level, 39 member states (as well as the United States)[153] implemented the Convention provisions into national legislation as of December 2015.

Legal provisions outlawing 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.[154] While in a number of states libel and defamation are dealt only as a civil law matter, there are a considerable number of states which criminalize libel and defamation. With regards to criminal provisions, the Parliamentary Assembly of the OSCE has repeatedly called on participating States to repeal laws which provide criminal penalties for the defamation of public figures, or which penalize the defamation of the State, State organs or public officials as such. The Office of the OSCE Representative on Freedom of the Media since its establishment in

151 See Article 2(c).

152 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.

153 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, and the former Yugoslav Republic of Macedonia.

154 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.

1997, has been promoting the decriminalization of all speech offences, except for the cases of direct calls for violence.

Furthermore, the OSCE Representative on Freedom of the Media together with the UN Special Rapporteur and the OAS Special Rapporteur on Freedom of Expression since 1999 issue a joint Declaration addressing various freedom of expression issues. In their Joint Declarations of November 1999 and December 2002, they called on States to repeal their criminal defamation laws. According to their 2002 statement "criminal defamation is not a justifiable restriction on freedom of expression; all criminal defamation laws should be abolished and replaced, where necessary, with appropriate civil defamation laws."[155] Following from this, their Joint Declaration of 2010 reiterated that "laws making it a crime to defame, insult, slander or libel someone or something, represent threat to freedom of expression."[156]

With this background, going back to the Internet, it should be emphasized that Web 2.0 based technologies and social media platforms, provides any user the possibility 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 a daily turnover of publications on the Internet that are globally and statistically immeasurable. However, this user driven activity can also lead to the publication of defamatory content on such platforms.[157]

In law, defamation can be seen as a limitation on freedom of expression as the right to protection of reputation is a right which is protected by international instruments including by Article 8 of the European Convention as part of the right to respect for private life.[158] However, UN Human Rights Committee's General Comment No. 34 on Article 19 of the ICCPR states that "defamation laws must be crafted with care to ensure that they comply with paragraph 3" of Article 19 and that they do not "serve, in practice, to stifle freedom of expression." [159] Equally, in order for Article 8 of the European Convention to come into play, "an attack on a person's reputation

155 Joint Declaration of 10 December 2002, at http://www.osce.org/fom/39838

156 Tenth Anniversary Joint Declaration: Ten Key Challenges to Freedom of Expression in the Next Decade, at http://www.osce.org/fom/41439

157 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

158 See *Chauvy and Others*, cited above, § 70; *Pfeifer v. Austria*, no. 12556/03, § 35, 15 November 2007; and *Polanco Torres and Movilla Polanco v. Spain*, no. 34147/06, § 40, 21 September 2010.

159 See further General Comment No.34 on Article 19 which was adopted during the 102nd session of the UN Human Rights Committee, Geneva, 11-29 July 2011, at <http://www2.ohchr.org/english/bodies/hrc/docs/CCPR-C-GC-34.doc>, para 47.

must attain a certain level of seriousness and be made in a manner causing prejudice to personal enjoyment of the right to respect for private life".[160]

If, however, the two rights compete and on the one hand the right to private life and protection of reputation is at stake, and on the other hand freedom of the media or freedom of expression is at stake, then the European Court states that as a matter of principle these rights deserve equal respect and consideration. In *Axel Springer AG*,[161] the European Court has established six criteria to be assessed in weighing the right to freedom of expression against the right to respect for private life: contribution to a debate of general interest; how well known the person concerned is and what is the subject of the report; the prior conduct of the person concerned; the method of obtaining the information and its veracity; the content, form and consequences of the publication; and the severity of the sanction imposed.

In any case, when political speech is in issue, interference with this kind of speech "requires clear and cogent justification"[162] as the limits of acceptable criticism are accordingly wider as regards a politician as such than as regards a private individual.[163] This is because politicians lay themselves open to close public scrutiny in relation to their political activities. Therefore, they are required to display a greater degree of tolerance. Therefore, these principles established at the European Court level including the balancing criteria should be taken into account at state level with regards to processing of defamation claims through the courts.

On the other hand, concerning policy issues surrounding libel on the Internet, there is a persistent debate over whether Internet access providers, hosting companies, or Web 2.0 based social media platform operators are primary publishers or only distributors of third party content. Such providers may become targets of defamation claims as secondary parties for publishing or republishing defamatory statements. This is particularly crucial considering that many defamatory statements on the Internet come from "anonymous sources". Concerning service or platform provider liability, in most instances liability will only be imposed upon providers if there is "knowledge and control" over the information which

160 See *A. v. Norway*, no. 28070/06, § 64, 9 April 2009, and *Axel Springer AG v. Germany* [GC], no. 39954/08, § 83, 7 February 2012.

161 *Axel Springer AG v. Germany* [GC], no. 39954/08, §§ 89-95) and *Von Hannover (no. 2)* (*Von Hannover v. Germany (no. 2)* [GC], nos. 40660/08 and 60641/08, §§ 108-113.

162 See *Tim Yeo v. Times Newspaper Ltd*., High Court of Justice (England & Wales), [2015] EWHC 3375 (QB), 25/11/2015, para 137.

163 See *Lingens v. Austria*, 8 July 1986, § 42, Series A no. 103.

is transmitted or stored by a provider. Based on the "knowledge and control" principle, notice-based takedown procedures have been developed in Europe. For example, the EU Directive on Electronic Commerce[164] provides a limited and notice-based liability with takedown procedures for illegal content, which will be described later in this book. 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.[165]

Unlike in the US, in many states notice-based liability measures represent a liability regime for ISPs, hosting companies, and 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 of public interest. Therefore, this may lead to 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."166

Conclusion

Almost all legal provisions criminalizing content mentioned in this chapter are applicable to any medium including to the Internet. However, content regulation developed for traditional media cannot and should not simply be applied to the Internet. Recognizing this, some 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.

It is noted that definitional problems and inconsistencies exist regarding certain speech-based restrictions. Clarifications are needed to define further for example "extremism", "terrorist propaganda", "incitement to terrorism", "harmful content",

164 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.

165 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).

166 Law Commission (England and Wales), Defamation and the Internet: A Preliminary Investigation, (Scoping Paper: Dec 2002).

"racist content", and "hate speech". As set forth in Article 19(3) of the ICCPR and in article 10(2) of the European Convention on Human Rights, freedom of expression is subject to exceptions. However, these must be construed strictly and the need for any restrictions must be established convincingly by the states.[167] 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[168] and sufficient precision is needed to enable the citizens to regulate their conduct.[169] 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[170] – 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.[171]

Furthermore, a considerable number of participating States are yet to decriminalize defamation and criminal defamation cases continue to present a serious threat to and a chilling effect for media freedom in the OSCE region. Harsh prison sentences or severe financial penalties continue to exist for defamation and insult.[172] 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,[173] the nature and severity of the penalties imposed are factors to be taken into account.[174] In fact, with regards to the straightforward defamation cases, the Court went as far as saying that the mere fact that a sanction is of a criminal nature creates a disproportionate chilling

167 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.

168 *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.

169 *Groppera Radio AG and Others v. Switzerland*, no. 10890/84, 28 March 1990, § 68, Series A no. 173.

170 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

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

172 For a recent study see International Press Institute, Out of Balance: Defamation law in the EU: A comparative overview for journalists, civil society and policymakers, January 2015, at http://www.freemedia.at/ecpm/defamation-law-report.html.

173 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.

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

effect.[175] 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 the Parliamentary Assembly urged those member States which still provide for prison sentences for defamation, even if they are not actually imposed,[176] to abolish them without delay.[177]

175 *Ibid*. See further CoE "Study on the alignment of laws and practices concerning defamation with the relevant case-law of the European Court of Human Rights on freedom of expression, particularly with regard to the principle of proportionality," CDMSI(2012)Misc11Rev2.

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

177 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>.

Chapter III

Legal and Policy Issues Surrounding Blocking and Filtering Measures

This chapter provides an overview and assessment of blocking and filtering policies restricting content and speech on the Internet.

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 highlighted previously in this book, laws are not necessarily harmonized at the OSCE level, let alone on a global level. What is considered illegal in one state may be perfectly legal in another and 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 deploy access blocking policies and measures to block access to Internet content including 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 seems to be a more convenient solution in cases where state authorities are unable to "remove content" and 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.

There are four different methods which can be deployed by Internet access providers to block access to websites and Internet content. These different blocking methods are described clearly in a recent High Court decision from England & Wales in the case of *Cartier International*

AG & Ors v British Sky Broadcasting Ltd & Ors.[178] Four such methods are as follows:

"i) **DNS name blocking**. The Domain Name System (DNS) is the system that associates a domain name (such as www.cartierloveonline.com) with the Internet Protocol (IP) address (such as 23.238.175.169) that the ISPs use to route traffic to the web server that is hosting the website in question. The ISPs operate DNS servers that their customers' computers automatically call upon to look up IP addresses corresponding to DNS names. The customers' computers request these lookups so that they can address their communications to the website in question using its IP address, which is the necessary form of address for their communications to be delivered. DNS name blocking involves an ISP removing or modifying its records of the IP address(es) for a particular DNS name, so that when the ISP's DNS server is asked by a customer's computer for the IP address corresponding to the DNS name, the ISP's system either returns no IP address or points the customer to an IP address defined by the ISP that in actuality does not correspond to the DNS name.

ii) **IP address blocking using routers**. This is implemented in network devices which the ISPs operate known as border gateway (edge) routers that send customer communications to their destinations based on the destination IP addresses of the communications. An ISP can configure its routers to discard communications destined for the IP address of the website in question or route them to an IP address defined by the ISP that is different from the actual IP address of the website. This method thus blocks a customer's communications to a website even if the customer's computer uses the correct IP address for the website.

iii) **DPI-based URL blocking**. This method involves monitoring traffic by means of Deep Packet Inspection (DPI) and blocking requests for specific Uniform Resource Locators (URLs). A URL is a web address, which usually consists of the access protocol (e.g. http), the domain name (e.g. www.example.com) and the specific resource (i.e. the page e.g. main-page), separated by a colon and slashes. This method does not involve detailed, invasive analysis of the contents of the packets in the traffic (and for that reason it is sometimes referred to Shallow Packet Inspection rather than Deep Packet Inspection). It is typically implemented using proxy servers. It can also be used to implement IP address blocking as an alternative to the router method described above.

178 [2014] EWHC 3354 (Ch) (17 October 2014).

iv) **Two-stage systems**. Some ISPs operate two-stage systems. Typically this involves a first stage of IP-address re-routing and a second stage of DPI-based URL blocking. The first stage detects whether a customer's web request relates to an IP address on which some blocked content is hosted. If there is a match, the request is re-directed to the second stage; otherwise it is passed on normally. In the second stage traffic that relates to a blocked URL (or IP address) is stopped. The second stage is typically implemented using proxy servers."[179]

It should also be added that users often rely on counter circumvention techniques and tools which are used to bypass these blocking methods and techniques deployed by the Internet service providers.

Although there remain serious question marks about the utility and effectiveness of these blocking methods, they are used to block access to websites and Internet content in various jurisdictions. By way of example, with regards to intellectual property infringements, the Danish Supreme Court upheld an injunction against a Danish Internet service provider to block access to the Pirate Bay website in May 2010.[180] The injunction was first issued by the bailiff's court in 2008 and upheld by the high court later the same year.[181] The Supreme Court concurred with the High Court that Pirate Bay contributed to serious copyright infringement and that the access provider Sonofon contributed to this infringement by providing its subscribers with access to the Pirate Bay website.

In Russia, 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.[182]

179 *Ibid*, para 25.

180 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

181 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.

182 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>.

Turkey blocked access to the YouTube platform from Turkey between May 2008 and October 2010 and to the Google Sites platform between 2009-2015 and blocked access to both the Twitter and YouTube platforms during 2014.

Access to the LiveJournal platform was also blocked from Kazakhstan in May 2009 subject to a court order blocking access to www.geo.kz.[183] In early May 2015, access to SoundCloud, an international platform for sharing music and podcasts, was blocked from Kazakhstan because allegedly the platform hosted extremist materials by the Hizb-ut-Tahrir Islamist group.[184]

In Italy, the Autonomous Administration of State Monopolies (AAMS) complies a blacklist of international or unlicensed gambling sites to be blocked as since 2006 online gambling has been permitted only via state-licensed websites.[185]

In the UK, since 1996 the Internet Watch Foundation compiles a list of known child pornography websites. Furthermore, in May 2012, the High Court ordered the blocking of the Pirate Bay website from within the UK through the servers of six ISPs including British Sky Broadcasting Limited, British Telecommunications PLC, Everything Everywhere Limited, Talktalk Telecom Group PLC, Telefónica UK Limited and Virgin Media Limited. [186] The Court also ruled that IP address blocking in addition to DNS blocking was appropriate in this case as the Pirate Bay website IP address is not a shared IP address.

In Belarus, the government authorities blocked access to the leading independent news and information websites Charter97.org, Gazetaby.com, Belaruspartisan.org, UDF.by, 21.by, Zautra.by, Belapan.by and Naviny.by during December 2014 after its currency was dragged down by Russian ruble slide to limit the dissemination of non-state information about the financial crisis.[187] The OSCE Representative on Freedom of the Media criticized the blocking and stated that these blockings threaten free speech on Internet in Belarus.[188]

183 See Ekspress-K newspaper, No. 337 (16723) of 26 May 2009.

184 See Freedom House, Freedom on the Net 2015: Privatizing Censorship, Eroding Privacy, December 2015, at https://freedomhouse.org/report/freedom-net/freedom-net-2015, p 487.

185 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>.

186 *Dramatico Entertainment Ltd & Ors v British Sky Broadcasting Ltd & Ors* [2012] EWHC 1152 (Ch) (02 May 2012).

187 The Guardian, "Belarus blocks online sites and closes shops to stem currency panic," 21 December, 2014.

188 See http://www.osce.org/fom/132866

Furthermore, according to a report published by the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, "States' use of blocking or filtering technologies is frequently in violation of their obligation to guarantee the right to freedom of expression."[189] The Special Rapporteur was also concerned by the

"emerging trend of timed (or "just-in-time") blocking to prevent users from accessing or disseminating information at key political moments, such as elections, times of social unrest, or anniversaries of politically or historically significant events. During such times, websites of opposition parties, independent media, and social networking platforms such as Twitter and Facebook are blocked, as witnessed in the context of recent protests across the Middle East and North African region."[190]

These examples are endless. However, 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. Therefore, often, blocking policies 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.

The utility and effectiveness of blocking methods to counter illegal content has been the subject of review and deliberations at both the Council of Europe and European Union levels. These will be assessed below.

Council of Europe Perspectives on Blocking Access to Allegedly Illegal Content

Council of Europe's Convention on Cybercrime and the Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse

189 See the 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, para 30.

190 *Ibid*.

and the Convention on the Prevention of Terrorism include a number of content related provisions.[191] These are offences related to child pornography,[192] the dissemination of racist and xenophobic material through computer systems,[193] and public provocation to commit a terrorist offence.[194] None of these legal measures cover blocking provisions and instead – as in any offline environment – cover the criminal activity of dissemination and publication, as well as possession in the case of child pornography.

Access and hosting providers are protected under the provisions of these CoE Conventions. Without the required intent under domestic law service providers would not be held criminally liable for serving as a conduit or for hosting a website or newsroom containing above mentioned material.[195] Moreover and important to stress, as provided by the EU E-Commerce Directive, a service provider is not required to monitor conduct to avoid criminal liability under the CoE provisions.

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.[196] More importantly, a CoE Committee of Ministers Recommendation of 2007[197] 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.[198]

---

191 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.

192 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.

193 Article 3 of the Additional Protocol of the Cybercrime Convention.

194 Article 5 of the CoE Convention on the Prevention of Terrorism.

195 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>.

196 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.

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

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

In March 2008, the Committee of Ministers in Recommendation (2008)6[199] recalled the Declaration of the Committee of Ministers on Freedom of Communication on the Internet of 28 May 2003[200] 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.[201] 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."[202] In 2014, the Committee of Ministers prepared a new Recommendation on a Guide to Human Rights for Internet Users.[203] The Guide stated that ""measures taken to block specific Internet content must not be arbitrarily used as a means of general blocking of information on the Internet" and they must not have "collateral effect in rendering large quantities of information inaccessible, thereby substantially restricting the rights of Internet users."[204] According to the Guide, "there should be strict control of the scope of blocking and effective judicial review to prevent any abuse of power."[205] A more recent Recommendation of the Committee of Ministers on the free, transboundary flow of information on the Internet was published in April 2015.[206] The Recommendation stated that States are obliged to ensure that the blocking of content or services deemed illegal is in compliance with Articles 8, 10 and 11 of the ECHR. In particular, measures adopted by State authorities in order to combat illegal content or activities on the Internet should not result in an unnecessary and disproportionate impact beyond that State's borders.[207]

---

199 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.

200 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.

201 *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.

202 *Ibid*.

203 See Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a Guide to human rights for Internet users. Adopted by the Committee of Ministers on 16 April 2014 at the 1197th meeting of the Ministers' Deputies.

204 *Ibid*, para 50.

205 *Ibid*.

206 Recommendation CM/Rec(2015)6 of the Committee of Ministers to member States on the free, transboundary flow of information on the Internet. Adopted by the Committee of Ministers on 1 April 2015, at the 1224th meeting of the Ministers' Deputies.

207 *Ibid*.

European Court of Human Rights Decisions Involving Blocking Access to Websites and Internet Content

In its first access blocking related decision, in *Ahmet Yıldırım v. Turkey*,[208] the European Court of Human Rights assessed whether the blocking provisions of an Internet law from Turkey[209] met the requirements of quality of law (foreseeability, accessibility, clarity and precision) as developed by the European Court. Furthermore, the Court assessed further whether there were any safeguards for the protection of freedom of expression within the Turkish law. The European Court of Human Rights, finding a violation of article 10 of the European Convention on Human Rights, held that a restriction on access to a source of information is only compatible with the Convention if a strict legal framework is in place regulating the scope of a ban and affording the guarantee of judicial review to prevent possible abuses.

Ahmet Yıldırım v. Turkey involved a court decision to block access to Google Sites platform, which hosted an Internet site whose "unknown owner" was investigated for insulting the memory of Atatürk. A criminal court in Denizli issued its blocking decision subject to article 8(1)(b) of Law No. 5651. The Court's blocking decision caused collateral damage and as a result of the blocking decision, access to all other sites hosted by the Google Sites platform was also blocked including the applicant's academic website hosted on Google Sites. The Telecommunications Communication Presidency made it technically impossible to access any content on Google Sites in order to implement the measure ordered by the local court. The measure in question therefore amounted to interference by the public authorities with the applicant's right to freedom of expression. The European Court concluded that article 8 of Law No. 5651, which is the basis of the interference (the blocking measure), did not satisfy the requirements under the Convention and the case law of the Court in terms of the 'quality of a law' prescribing such interference. More importantly, the Court stated that the blocking of all access to Google Sites affected the applicant, who owned another website hosted on the same platform. The Court was of the opinion that such a measure substantially restricted the rights of Internet users and had a significant collateral effect, which should have been taken into consideration by the Turkish Court issuing the blocking decision. On this issue, the European Court stated that domestic courts "should have taken into consideration, among other elements, the fact that such a measure, by rendering large quantities of information

208 *Ahmet Yıldırım v. Turkey*, Application No. 3111/10, judgment of 18 December 2012, 18.03.2013 (final).

209 Article 8 of Law No. 5651 entitled "Regulation of Publications on the Internet and Suppression of Crimes Committed by Means of Such Publication" came into force in November 2007.

inaccessible, substantially restricted the rights of Internet users and had a significant collateral effect."[210] Furthermore, in *Ahmet Yıldırım v. Turkey*, the Court noted that there was no indication that the judges considering the application sought to weigh up the various interests at stake, in particular, by assessing the need to block all access to Google Sites. In the Court's view, this shortcoming was simply a consequence of the wording of article 8 of Law No. 5651 itself, which did not lay down any obligation for the domestic courts to examine whether the wholesale blocking of Google Sites was necessary, having regard to the criteria established and applied by the Court under article 10 of the Convention.[211] The Court concluded that the interference resulting from the application of section 8 of Law no. 5651 did not satisfy the foreseeability requirement under the Convention and did not afford the applicant the degree of protection to which he was entitled by the rule of law in a democratic society.

In a follow-up decision the European Court of Human Rights dealt with applications involving access blocking to the YouTube platform from Turkey between 05 May 2008 and 30 October 2010 continuously without a break by an order of the Ankara Criminal Court of First Instance. The Court order was issued because of the availability of 10 video clips on the YouTube platform allegedly involving defamatory statements and images about the founder of the Turkish Republic Mustafa Kemal Atatürk. These clips were deemed illegal under Law No. 5816 — "Crimes Against Atatürk" and access to such content can be blocked under the above mentioned Law No 5651. Subsequently a further order was imposed by the Ankara Criminal Court of First Instance on 17 June 2010 blocking access to several IP addresses associated with YouTube as well as with several other Google related services. On 30 October, 2010 the blocking order was lifted by the public prosecutor's office even though the 10 video clips were not removed by YouTube and four of them remain online as of today.

In June 2010, while the blocking orders were still in effect, two separate user based applications to overturn the blocking order were made by a lawyer and two academics. It was argued that the blocking order interfered with their right to freedom to receive or impart information and ideas. The Ankara Criminal Court of First Instance rejected their application on the ground that the blocking order had been imposed in accordance with the law and that the applicants did not have standing to challenge such decisions. It observed that the videos in question

210 *Ahmet Yıldırım v. Turkey*, Application No. 3111/10, judgment of 18 December 2012, 18.03.2013 (final), para. 66.
211 *Ibid*.

could no longer be accessed from Turkey but had not been deleted from the platform's database and could therefore still be accessed by users worldwide. Therefore, the decision of the Ankara Court was final. So, two separate applications were lodged with the European Court of Human Rights on 20 July 2010 and 27 December 2010 by the applicants.

Relying on Article 10 (freedom of expression) of the European Convention on Human Rights, the applicants complained of an infringement of their right to freedom to receive and impart information and ideas. Relying on Article 6 (right to a fair hearing), they also complained that they had not had an effective judicial remedy enabling them to have the blocking order reviewed by the courts and have possible abuse by the authorities censured. Relying on Article 46 (binding force and execution of judgments), the applicants requested the Court to indicate to the Turkish Government which general measures could be taken to put an end to the situation complained of.

The European Court of Human Rights considered it necessary to determine whether the applicants had victim status as required by the Convention. In that connection it noted that the applicants had actively used YouTube for professional purposes, particularly downloading or accessing videos used in their academic work. The Court also observed that YouTube was a single platform which enabled information of specific interest, particularly on political and social matters, to be broadcast. It was therefore an important source of communication and the blocking order precluded access to specific information which it was not possible to access by other means.

While considering the applicants' victim status, the Court recalled that the Convention does not allow an *actio popularis*, but requires for the exercise of the right of individual application that the applicants should claim plausibly to be a direct or indirect victim of a violation of the Convention resulting from an act or omission attributable to the Contracting State. For example, the Court in *Tanrıkulu and Others v. Turkey*,[212] did not recognize the victim status of the readers of a newspaper which was the subject of a distribution ban. The Court, however, accepted that in the present case YouTube had been an important means by which the applicants could exercise their right to receive and impart information or ideas and that they could legitimately claim to have been affected by the blocking order even though they had not been directly targeted by it.

212 No 40150/98, 40153/98 and 40160/98, 6 November 2001.

The European Court further observed that the Turkish Constitutional Court had also recognised that two of the applicants had victim status, in their capacity as active users, when they successfully applied to the Constitutional Court to overturn the blocking orders with regards to both Twitter[213] and YouTube.[214] So, the European Court, in line with the jurisprudence of the Constitutional Court accepted all three applicants as victims for the purpose of this application.

The Court also noted that user-generated expressive activity on the Internet provides an unprecedented platform for the exercise of freedom of expression. That is undisputed and has been recognised by the Court on previous occasions.[215] Within this context, the Court also noted that political information ignored by the mainstream media have often been disclosed through YouTube, which allowed the emergence of citizen journalism. In this regard, the Court accepted that this platform is unique given its characteristics, its level of accessibility and especially its potential impact.

The Court then regarded the blocking order as an interference by a public authority with the exercise of the rights guaranteed by article 10. The Court by reference to its previous decision of *Ahmet Yıldırım v. Turkey* stated that Law no. 5651 did not authorise the blocking of access to an entire Internet site because of some of its contents. According to the Court, under section 8(1), a blocking order could only be imposed on a specific publication where there were grounds for suspecting an offence. It therefore emerged that in the YouTube case there had been no legislative provision allowing the Ankara Criminal Court of First Instance to impose a blanket blocking order on access to YouTube. The Court, finding a violation of Article 10, concluded that the interference had not satisfied the condition of lawfulness required by the Convention and that the applicants had not enjoyed a sufficient degree of protection. As in the case of *Ahmet Yıldırım v. Turkey*, the Court stated that the public authorities as well as the courts should take particular account of the fact that such a blocking measure, which rendered inaccessible a large amount of information, could not but affect significantly the rights of Internet users and have an important side effect.

213 *Akdeniz and others* judgment, decision no 2014/3986, 02.04.2014.

214 YouTube and others judgment, decision no 2014/4705, 29.05.2014.

215 See *Ahmet Yıldırım v. Turkey*, no. 3111/10, § 48, ECHR 2012, and *Times Newspapers Ltd (nos. 1 and 2) v. the United Kingdom*, nos. 3002/03 and 23676/03, § 27, ECHR 2009.

European Union perspectives on blocking access to allegedly illegal content

The European Union considered blocking access to websites as a possible policy option to combat the availability of both terrorist propaganda as well as child pornography on the Internet. 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.[216] 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"[217] this policy option has been ruled out of the proposal for a Council Framework Decision on combating terrorism.[218]

Speedy re-apparition of websites and inefficiency of blocking

Within the discussions related to terrorist propaganda, the European 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.[219] The Commission also acknowledged that existing methods of filtering can be circumvented[220] noting 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 blocking 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.[221] Within this context, the Commission expressed that

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

217 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.

218 Council Framework Decision on combating terrorism amending Framework Decision 2002/475/JHA.

219 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.

220 *Ibid*., p 41.

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

"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."[222]

The Commission also voiced concern with regard 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.[223]

Blocking considered by the EU with regard to combating child pornography

Further consideration for blocking took place in relation to 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 component in the fight against child sexual abuse and exploitation.[224] 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.[225] 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.[226] 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."[227] In November 2010, the European Parliament doubted the

222 *Ibid*., p 29.

223 *Ibid*, p 42-45.

224 Prague Declaration: A new European approach for safer Internet for children, 20 April, 2009.

225 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, Brussels, 29.03.2010.

226 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.

227 *Ibid*.

effectiveness of blocking measures as an effective tool for combating child pornography during a debate of the draft Council Framework Decision.[228]

Within this context, 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.[229] 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."[230] However, 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"[231] 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[232] in response to the European Commission's proposal on Internet blocking.[233] According to the amendments made by the Committee "child pornography or child abuse material on the web must be removed at the source in all EU countries".[234] The

228 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.

229 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.

230 *Ibid*.

231 *Ibid*.

232 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.

233 Article 21 and Recital 13. 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, 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.

234 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>.

Committee, therefore, did not recommend "mandatory blocking" of websites containing child pornography[235] 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".[236] 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".[237] 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 continued,[238] with a view to reaching a compromise during 2011.[239] The European Parliament voted on 27 October 2011, and adopted a compromise amendment to the initial proposal. The adopted amendment corresponds to what was agreed between the three European institutions

235 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.

236 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.

237 *Ibid*.

238 Political agreement on final act expected at the Council level by 09.06.2011.

239 European Parliament plenary sitting: Indicative date for the meeting is 22.06.2011.

(Council, the European Parliament and the Commission).[240] The amended version of the blocking measure is provided below.

Article 25: Measures against websites containing or disseminating child pornography: (1) Member States shall take the necessary measures to ensure the prompt removal of webpages containing or disseminating child pornography hosted in their territory and to endeavour to obtain the removal of such pages hosted outside of their territory. (2) Member States may take measures to block access to webpages containing or disseminating child pornography towards the internet users within their territory. These measures must be set by transparent procedures and provide adequate safeguards, in particular to ensure that the restriction is limited to what is necessary and proportionate, and that users are informed of the reason for the restriction. Those safeguards shall also include the possibility of judicial redress.[241]

The new Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography replacing Council Framework Decision 2004/68/JHA was published in the *Official Journal of the European Union* on 17 December 2011.[242] Member States were required to bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by 18 December 2013. The European Commission shall, by 18 December 2015, submit a report to the European Parliament and the Council assessing the extent to which the Member States have taken the necessary measures in order to comply with this Directive, accompanied, if necessary, by a legislative proposal.[243]

Finally, it should also be mentioned that within the context of intellectual property rights protection, the EU Directive 2001/29 on the harmonisation of certain aspects of copyright and related rights in the information society[244] established special rules for the protection of copyright in the information society. In addition to various general protection measures for the rightholders, the Directive also

240 European Parliament legislative resolution of 27 October 2011 on the proposal for a directive of the European Parliament and of the Council 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)).

241 Directive of the European Parliament and of the Council on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, PE-COS 51/11, Brussels, 4 November 2011.

242 OJ L 335, 17.12.2011, p. 1.

243 The Commission report is yet to be published as of this writing.

244 See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:167:0010:0019:EN:PDF

includes a number of sanctions and remedies. Article 8(3) of the Directive 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. So, Directive 2001/29 requires that the measures which the Member States must take in order to conform to that directive are aimed not only at bringing to an end infringements of copyright and of related rights, but also at preventing them.[245]

Furthermore, the EU Directive 2004/48/EC on the enforcement of intellectual property rights also includes a provision for injunctions. Article 11 of the Directive requires Member States to ensure that, where a judicial decision is taken finding an infringement of an intellectual property right, the judicial authorities may issue against the infringer an injunction aimed at prohibiting the continuation of the infringement. The EU Directive 2004/48/EC explicitly states that Member States shall also ensure that rightholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe an intellectual property right, without prejudice to Article 8(3) of Directive 2001/29/EC. However, Article 3(1) of the Directive requires that remedies "shall not be unnecessarily complicated or costly". Both provisions were used in a number of cases by the rightholders to compel ISPs to block access to websites or content infringing intellectual property rights on the Internet.

Blocking and Filtering Related Litigation at the Court of Justice of the European Union (CJEU) Level

Blocking related policies and legal practices adopted in a number of European countries resulted with legal challenges through the courts reaching the Court of Justice of the European Union (CJEU).

In March 2014, the Court of Justice of the European Union ruled in the case of *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft mbH*[246] that an Internet service provider may be ordered to block its customers' access to a copyright-infringing website. Such an injunction and its enforcement must, however, ensure a fair balance between the fundamental rights concerned. In this case, two rightholder companies became aware that their films could be viewed or even downloaded from the website 'kino.to' without their consent. At the request of those two companies,

245 See Case C-70/10 Scarlet Extended [2011] ECR I-11959, para 31, and Case C-360/10 SABAM [2012] ECR, para 29.
246 Case C-314/12.

the Austrian courts prohibited UPC Telekabel Wien, an ISP established in Austria, from providing its customers with access to that site. UPC Telekabel considered that such an injunction cannot be addressed to it, because, at the material time, it did not have any business relationship with the operators of kino.to and it was never established that its own customers acted unlawfully. UPC Telekabel also claims that the various blocking measures which may be introduced could, in any event, be technically circumvented and that they were costly to implement.

The Oberster Gerichtshof (Supreme Court, Austria) asked the Court of Justice to interpret the EU Copyright Directive and the fundamental rights recognised by EU law.[247] The Court of Justice ruled that a person who makes protected subject-matter available to the public on a website without the agreement of the rightholder is using the services of the business which provides Internet access to persons accessing that subject-matter. Thus, an ISP, such as UPC Telekabel, which allows its customers to access protected subject-matter made available to the public on the internet by a third party is an intermediary whose services are used to infringe a copyright.

The Court noted in that regard, that the Directive, which seeks to guarantee a high level of protection of rightholders, does not require a specific relationship between the person infringing copyright and the intermediary against whom an injunction may be issued. Nor is it necessary to prove that the customers of the ISP actually access the protected subject-matter made accessible on the third party's website, because the directive requires that the measures which the Member States must take in order to conform to that Directive are aimed not only at bringing infringements of copyright and of related rights to an end, but also at preventing them.

The Court of Justice also noted that within the framework of such an injunction, copyrights and related rights primarily enter into conflict with the freedom to conduct a business, which economic agents such as ISPs enjoy and with the freedom of information of Internet users. Where several fundamental rights are at issue, Member States must ensure that they rely on an interpretation of EU law and their national law which allows a fair balance to be struck between those fundamental rights. With regard, more specifically, to the ISP's freedom to conduct a business, the Court considers that that injunction does not seem to infringe the very substance of that right, given that, first, it leaves its addressee to

247 The directive provides for the possibility for rightholders to apply for an injunction against intermediaries whose services are used by a third party to infringe their rights.

determine the specific measures to be taken in order to achieve the result sought, with the result that the ISP can choose to put in place measures which are best adapted to the resources and abilities available to it and which are compatible with the other obligations and challenges which the ISP will encounter in the exercise of his activity and that, secondly, it allows the ISP to avoid liability by proving that it has taken all reasonable measures.

The Court of Justice therefore held that the fundamental rights concerned do not preclude such an injunction, on two conditions: (i) that the measures taken by the ISP do not unnecessarily deprive users of the possibility of lawfully accessing the information available and (ii) that those measures have the effect of preventing unauthorised access to the protected subject-matter or, at least, of making it difficult to achieve and of seriously discouraging users from accessing the subject-matter that has been made available to them in breach of the intellectual property right. The Court stated that Internet users and also, indeed, the ISP must be able to assert their rights before the court. It is a matter for the national authorities and courts to check whether those conditions are satisfied.

Furthermore, in the UPC v. Constantin case,[248] an Austrian court issued a blocking decision to block access to a website which offering pirated copies of films owned by the rightholder company. The ISP opposed the blocking decision and the case was referred to the CJEU. The Court of Justice held that an ISP, by providing access to its network, is an inevitable actor in any transmission of an infringement over the Internet between one of its customers and a third party.[249] Therefore, it must be held that an ISP which allows its customers to access protected subject-matter made available to the public on the Internet by a third party is an intermediary whose services are used to infringe a copyright or related right within the meaning of Article 8(3) of Directive 2001/29. In this respect, according to the Court, the measures adopted by the ISP must be strictly targeted, in the sense that they must serve to bring an end to a third party's infringement of copyright or of a related right but without thereby affecting Internet users who are using the provider's services in order to lawfully access information. Failing that, the provider's interference in the freedom of information of those users would be unjustified in the light of the objective pursued.

248 EUECJ C-314/12 (27 March 2014).

249 See further Case C-557/07 LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten [2009] ECR I-1227, para 44.

However, it should also be noted that in both the Scarlet Extended[250] and Sabam[251] decisions, the Court of Justice classified the injunctions requiring an ISP to install a complicated, costly and permanent filtering system at its own expense in order to monitor data in its network as well as to prevent the illegal downloading of files which applies indiscriminately to all its customers as a serious infringement of the ISP's freedom to conduct its business.[252] The Court has also held that the owner of an online social network cannot be obliged to install a general filtering system, covering all its users, in order to prevent the unlawful use of musical and audio-visual work.[253]

Policies on Filtering Software and Children's Access to Harmful Content

In terms of protecting children from so called 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."[254] 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."[255] 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."[256] 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."[257]

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,

250 Case C-70/10 *Scarlet Extended* [2011] ECR I-11959.

251 Case C-360/10 *Sabam* [2012] ECR.

252 See further Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV, Case C-360/10, 16 February 2012.

253 Case C-360/10 *Sabam* [2012] ECR.

254 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>.

255 *Ibid*, p. 30.

256 *Ibid*, p. 32.

257 *Ibid*, p. 33.

promote public awareness, and create national centres for reporting illegal online content with a €55 million budget.[258]

Self-regulatory solutions are also supported at the Council of Europe level. The Declaration on Freedom of Communication on the Internet adopted by the Committee of Ministers of the Council of Europe on 28 May 2003 notably encouraged self-regulation and co-regulatory initiatives regarding Internet content.[259] With regard to protection of children from harmful content, the Council of Europe's Committee of Ministers recommended in July 2009[260] 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.[261] The Committee of Ministers also recommended that safe and secure spaces similar to walled gardens should be developed for children on the Internet. While doing so the Committee of Ministers noted that "every action to restrict access to content is potentially in conflict with the right to freedom of expression and information as enshrined in Article 10 of the European Convention on Human Rights."[262]

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"[263] as well as the development of a pan-European trustmark and labelling system[264] was encouraged, the CoE Committee did not recommend state level blocking or

258 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)).

259 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.

260 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.

261 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

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

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

264 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.

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."[265] Regarding the use of 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."[266]

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.[267] However, the Committee of Ministers stated in a 2008 Recommendation [268] 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.

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

266 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).

267 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

268 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 2008 Recommendation[269] 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.[270] 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[271] and social networking providers.[272] 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(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

269 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.

270 *Ibid*, Guideline I.

271 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.

272 See Recommendation CM/Rec(2012)4 of the Committee of Ministers to member States on the protection of human rights with regard to social networking services. Adopted by the Committee of Ministers on 4 April 2012 at the 1139th meeting of the Ministers' Deputies.

has been activated to protect. The Committee of Ministers believed 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.

More recently, the CoE Committee of Experts on New Media (MC-NM) developed guidelines for search engines[273] and social networking providers.[274] Both guidelines were approved by the Committee of Ministers of the Council of Europe in April 2012[275] and recommend that Member States should guarantee that 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. Within this context 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. Transparent voluntary individual filtering mechanisms are also to be encouraged. The Committee of Experts 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.

Conclusion

Despite the decisions of the European Court of Human Rights establishing important principles on the legality of blocking measures at the pan-European level there remains 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, Article 19 of the

273 See Recommendation CM/Rec(2012)3 of the Committee of Ministers to member States on the protection of human rights with regard to search engines. Adopted by the Committee of Ministers on 4 April 2012 at the 1139th meeting of the Ministers' Deputies.

274 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.

275 See Recommendation CM/Rec(2012)3 of the Committee of Ministers to member states on the protection of human rights with regard to search engines; Recommendation CM/Rec(2012)4 of the Committee of Ministers to member States on the protection of human rights with regard to social networking services, 4 April 2012.

International Covenant on Civil and Political Rights[276] and Article 10 of the European Convention on Human Rights is arguably problematic.

Although the authorities' 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' 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 of ICCPR and Article 10 of ECHR unless the necessity for interference is convincingly established.[277] 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.[278] Therefore, a blocking system based exclusively on self-regulation or 'voluntary agreements' risks being 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

276 According to the new General Comment No.34 on Article 19 "any restrictions on the operation of websites, blogs or any other internet-based, electronic or other such information dissemination system, including systems to support such communication, such as internet service providers or search engines, are only permissible to the extent that they are compatible with paragraph 3. Permissible restrictions generally should be content-specific; generic bans on the operation of certain sites and systems are not compatible with paragraph 3. It is also inconsistent with paragraph 3 to prohibit a site or an information dissemination system from publishing material solely on the basis that it may be critical of the government or the political social system espoused by the government." See General Comment No.34 on Article 19 which was adopted during the 102nd session of the UN Human Rights Committee, Geneva, 11-29 July 2011, at <http://www2.ohchr.org/english/bodies/hrc/docs/CCPR-C-GC-34.doc>.

277 See Paragraph 26 of the Final Document of the 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.

278 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.

objective pursued as it has been established by the European Court of Human Rights in the decisions involving access blocking to both the Google Sites and YouTube platforms from Turkey. Furthermore, "permissible restrictions generally should be content-specific; generic bans on the operation of certain sites and systems" should be avoided according to the UN Human Rights Committee. Within this context, it is also inconsistent with article 19(3) of the ICCPR "to prohibit a site or an information dissemination system from publishing material solely on the basis that it may be critical of the government or the political social system espoused by the government."[279]

The detrimental side effects of blocking was addressed by the European Court of Human Rights in *Ahmet Yıldırım v. Turkey*.[280] In that case and similarly in the case of *Cengiz and Others v. Turkey*[281] with regards to the blocking of access to the YouTube platform from Turkey for almost 2.5 years, the European Court was concerned about the collateral effect of such overbroad blocking decisions as a preventative measure. According to the Court, the fact that such a measure, by rendering large quantities of information inaccessible under a single website or platform, substantially restricted the rights of Internet users and had a significant collateral effect. Similarly, according to a report published by the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, "blocking measures constitute an unnecessary or disproportionate means to achieve the purported aim, as they are often not sufficiently targeted and render a wide range of content inaccessible beyond that which has been deemed illegal."[282]

Within this context, it is argued that domain-based blocking of websites and social media platforms carrying legal content such as YouTube, Twitter and Facebook would 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.[283] The reason for this is that the Internet started to play an essential role as a medium for mass communication, especially through the development of web 2.0 based

279 See General Comment No.34 on Article 19 which was adopted during the 102nd session of the UN Human Rights Committee, Geneva, 11-29 July 2011, at <http://www2.ohchr.org/english/bodies/hrc/docs/CCPR-C-GC-34.doc>.

280 *Ahmet Yıldırım v. Turkey*, Application no.3111/10, judgment of 18 December 2012, 18.03.2013 (final).

281 *Cengiz and Others v. Turkey*, nos. 48226/10 and 14027/11, 01.12.2015.

282 See the 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, para 31.

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

platforms, in particular through the social media platforms, enabling citizens to actively participate in the political debate and discourse. These platforms provide a popular venue 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 could 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 many jurisdictions including 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.[284] 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.[285] The same principles also apply to new media and Internet publications. It is therefore argued that prior restraint and other bans imposed on the future publication of entire newspapers, or for that matter websites and social media platforms are incompatible with the rights stipulated in the European Convention on Human Rights. 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". [286]

284 *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.

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

286 *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.

Chapter IV

Intermediary Liability and Content Removal Policies

This chapter provides and overview of legal and policy issues surrounding Internet service and social media platform providers and related content removal policies.

"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."[287]

Generally, intermediaries or information society service providers including ISPs, hosting companies, social media platforms, and search engines providers will only be liable for providing access to third party content if they have "**knowledge and control**" over the information which is transmitted or stored through their services. 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[288] provides a limited and notice-based liability with takedown procedures for illegal content. However, the Directive measures and its interpretation has been a subject of legal dispute reaching the Grand Chamber of the European Court of Human Rights in the case of *Delfi AS v. Estonia*.[289] The case is significantly important as it tries to formulate liability principles with regards to third-party comments published on news portals and social media platforms. This consideration will also take into account the more recent decision of the European Court (4th section) in *Magyar Tartalomszolgáltatók Egyesülete and/et Index.hu Zrt v. Hungary*.[290] Furthermore, within this context the decision of the Court of Justice of the European Union in the case of *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario*

287 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.

288 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.

289 No. 64569/09 [GC], 16 June 2015.

290 *Magyar Tartalomszolgáltatók Egyesülete and/et Index.hu Zrt v. Hungary*, no. 22947/13, 2.2.2016 [Section IV].

Costeja González[291] will also be addressed. The case raised an important debate on the right to be forgotten issue and its impact upon removal of content and freedom of expression will be discussed further in this chapter.

The European Union Policy

Rather than advocating or requiring a general blocking policy for illegal content as described in the previous chapter, the European Union favours a notice based liability system for EU based hosting companies and access providers. Therefore, the EU adopted a notice based liability system in 2000 through the European Union Directive on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce').[292] The Directive suggested that "it is in the interest of all parties involved in the provision of information society services to adopt and implement procedures,"[293] to remove and disable access to illegal information. Section 4 of the EU Directive through articles 12-15[294] 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."

This means that there is no absolute protection provided within the Directive for ISPs or other providers such as social media platform or search engine providers and they are not immune from prosecution and liability. The service providers are required to act expeditiously "upon obtaining actual knowledge" of illegal activity

291 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, (the "right to be forgotten") Case C-131/12, 13 May 2014 (decision of the Court of Justice of the European Union).

292 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, v. 43, OJ L 178 17 July, 2000 p.1. Note also Common Position (EC) No 22/2000 of 28 February 2000 adopted by the Council, acting in accordance with the procedure referred to in Article 251 of the Treaty establishing the European Community, with a view to adopting a Directive on electronic commerce, Official Journal C 128, 08/05/2000 p. 0032–0050.

293 *Ibid*.

294 Article 12: Mere conduit, article 13: Caching, article 14: Hosting, article 15: No general obligation to monitor.

or content "to remove or to disable access to the information concerned."[295] 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"[296] according to the Directive.

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.[297] 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".[298]

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".[299]

Overall, the E-Commerce Directive provides limited and notice based liability with take down procedures for illegal content and requires

295 *Ibid*, para. 46.

296 *Ibid*.

297 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.

298 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.

299 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.

Member States and the Commission to encourage the development of codes of conduct.[300]

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".[301] 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."[302] 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".[303] 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.[304]

A CoE Parliamentary Assembly Recommendation on the promotion of Internet and online media services appropriate for minors[305] 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,"[306] 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.

300 Ibid, para. 49.

301 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.

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

303 Nas, S., (Bits of Freedom), The Multatuli Project: ISP Notice & take-down, 2004, at www.bof.nl/docs/research-paperSANE.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.

304 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 .

305 1882 (2009).

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

The Case of Delfi AS v. Estonia

Within this context it is important to note that an application from Estonia has been made to the European Court of Human Rights. In Estonia, 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 the EU principles into the Information Society Services Act.[307] Similar to other EU 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,[308] limited liability for temporary storage of information in cache memory,[309] and limited liability upon provision of information storage service.[310] Furthermore, the providers are not obliged to monitor their servers.[311]

307 Infoühiskonna teenuse seadus, 14 April 2004 (Riigi Teataja 2004, 29, 191).

308 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.

309 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 recognized 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.

310 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.

311 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.

An application with the European Court of Human Rights against Estonia was lodged in December 2009 by Delfi AS, one of the largest Internet news portals in the country which publishes up to 330 news articles a day. The case involved the posting of third party comments on the Delfi portal with regards to an article published on the website during 2006.

In January 2006, Delfi published an article on its webpage about a ferry company. It discussed the company's decision to change the route its ferries took to certain islands. This had caused ice to break where ice roads could have been made in the near future. As a result, the opening of these roads – a cheaper and faster connection to the islands compared to the ferry services – was postponed for several weeks. Below the article, readers were able to access the comments of other users of the site. Many readers had written highly offensive or threatening posts about the ferry operator and its owner.

Delfi received a complaint and subsequently removed the allegedly defamatory comments according to the notice-and-take-down obligation. Despite this, the owner of the ferry company mentioned in the article sued Delfi in April 2006 and successfully obtained a judgment against it in June 2008. The Estonian court found that the comments were defamatory, and that Delfi was responsible for them. The owner of the ferry company was awarded 5,000 kroons in damages (around 320 euros). However, Delfi refused to pay damages claimed. In June 2009, the Supreme Court of Estonia ruled that both Delfi and the authors of the comments were to be considered publishers of the comments rejecting the news portal's appeal that it should be considered as an information society service provider or storage host and that its role was merely technical, passive and neutral subject to the provisions of the EU Electronic Commerce Directive 2000/31/EC. In this context, the Court also referred to the economic interest of an Internet portal administrator, defining the publisher as an entrepreneur, similar to a publisher of printed media.

Relying on Article 10 of the European Convention on Human Rights, Delfi complained to the European Court of Human Rights that the Estonian civil courts found it liable for comments written by its readers. Therefore, the European Court of Human Rights considered[312] 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

312 The statement of facts was published by the Strasbourg court on 11 February 2011.

Human Rights. It should be noted that this was the first case in which the Court had been called upon to examine a complaint about liability for user-generated comments on an Internet news portal. However, the Delfi case did not concern other similar forums on the Internet through which third-party comments could be disseminated such as social media platforms.

In its Chamber judgment of 10 October 2013, the European Court held, unanimously, that there had been no violation of Article 10. The Court found that the finding of liability by the Estonian courts had been a justified and proportionate restriction on the portal's right to freedom of expression, in particular, because the comments were highly offensive; the portal had failed to prevent them from becoming public, profited from their existence, but allowed their authors to remain anonymous and the fine imposed by the Estonian courts had not been excessive.

On 9 January 2014 Delfi asked for the case to be referred to the Grand Chamber in accordance with Article 43 of the Convention. On 17 February 2014 the Grand Chamber Panel accepted Delfi's request. A hearing was held on the case in Strasbourg on 9 July 2014. On 16 June 2015, the Grand Chamber of the European Court announced its decision (application no. 64569/09) agreeing with the Chamber decision and finding no violation of Article 10.

The question before the Grand Chamber was not whether the freedom of expression of the authors of the comments had been breached but whether holding Delfi liable for comments posted by third parties had been in breach of its freedom to impart information. The Grand Chamber found that the Estonian courts' finding of liability against Delfi had been a justified and proportionate restriction on the portal's freedom of expression because the comments in question had been extreme and had been posted in reaction to an article published by Delfi on its professionally managed news portal run on a commercial basis; the steps taken by Delfi to remove the offensive comments without delay after their publication had been insufficient and the 320 euro fine had by no means been excessive for Delfi, one of the largest Internet portals in Estonia.

The Grand Chamber noted the Supreme Court's characterisation of the comments posted on Delfi's portal as unlawful. This assessment was based on the fact that the comments were tantamount to hate speech and incitement to violence against the owner of the ferry company. The Grand Chamber thus considered that the remarks, established as manifestly unlawful, did not require

any linguistic or legal analysis. Therefore, the case concerned the duties and responsibilities of Internet news portals, under Article 10(2) of the Convention, which provided on a commercial basis a platform for user- generated comments on previously published content and some users – whether identified or anonymous – engaged in clearly unlawful speech, which infringed the personality rights of others and amounted to hate speech and incitement to violence against them.

With regards to the Information Society Services Act transposing the EU Directive on Electronic Commerce into Estonian law, the Grand Chamber found that it was for national courts to resolve issues of interpretation and application of domestic law. Thus it did not address the issue under EU law and limited itself to the question of whether the Supreme Court's application of the domestic law to Delfi's situation had been foreseeable. The Grand Chamber considered that Delfi had been in a position to assess the risks related to its activities and that it had to have been able to foresee, to a reasonable degree, the consequences which those activities could entail.

The Grand Chamber considered that the offensive comments posted on Delfi's news portal, amounting to hate speech or incitement to violence, did not enjoy the protection of Article 10 and thus the freedom of expression of the authors of the comments was not at issue. The question before the Grand Chamber was rather whether the national courts' decisions, holding Delfi liable for comments posted by third parties, were in breach of its freedom to impart information as guaranteed by Article 10 of the Convention.

The Grand Chamber agreed with the Chamber's assessment of the question which had identified four key aspects: the context of the comments; the liability of the actual authors of the comments as an alternative to Delfi being held liable; the steps taken by Delfi to prevent or remove the defamatory comments; and the consequences of the proceedings before the national courts for Delfi.

Firstly, as regards the context, the Grand Chamber attached particular weight to the extreme nature of the comments and the fact that Delfi was a professionally managed Internet news portal run on a commercial basis which sought to attract a large number of comments on news articles published by it. Moreover, as the Supreme Court had pointed out, Delfi had an economic interest in the posting of the comments. The actual authors of the comments could not modify or delete their comments once they were posted, only Delfi had the technical means to do

this. The Grand Chamber therefore agreed with the Chamber and the Supreme Court that, although Delfi had not been the actual writer of the comments, that did not mean that it had no control over the comment environment and its involvement in making the comments on its news article public had gone beyond that of a passive, purely technical service provider.

Secondly, Delfi had not ensured a realistic prospect of the authors of the comments being held liable. The owner of the ferry company could have attempted to sue the specific authors of the offensive comments as well as Delfi itself. However, Delfi allowed readers to make comments without registering their names, and the measures to establish the identity of the authors were uncertain. Nor had Delfi put in place any instruments to identify the authors of the comments making it possible for a victim of hate speech to bring a claim.

Thirdly, the steps taken by Delfi to prevent or remove without delay the defamatory comments once published had been insufficient. Delfi did have certain mechanisms for filtering hate speech or speech inciting violence, namely a disclaimer (stating that authors of comments were liable for their content, and that threatening or insulting comments were not allowed), an automatic system of deletion of comments containing a series of vulgar words and a notice-and-take-down system (whereby users could tell the portal's administrators about offensive comments by clicking a single button). Nevertheless, both the automatic word-based filter and the notice-and-take-down system had failed to filter out the manifest expressions of hatred and blatant threats to the owner of the ferry company by Delfi's readers and the portal's ability to remove offending comments in good time had therefore been limited. As a consequence, the comments had remained online for six weeks. The Grand Chamber considered that it was not disproportionate for Delfi to have been obliged to remove from its website, without delay, clearly unlawful comments, even without notice from the alleged victims or from third parties whose ability to monitor the Internet was obviously more limited than that of a large commercial Internet news portal such as Delfi. Finally, the Grand Chamber agreed with the Chamber that the consequences of Delfi having been held liable were small. The 320 euro fine was by no means excessive for Delfi, one of the largest Internet portals in Estonia, and the portal's popularity with those posting comments had not been affected in any way – the number of comments posted had in fact increased. Registered comments are now a possibility but anonymous comments are still predominant, with Delfi even having set up a team of moderators for their follow-up. Furthermore, the tangible result for Internet operators in post-Delfi cases before the national courts has

been that they have taken down offending comments but have not been ordered to pay compensation.

Based on the concrete assessment of the above aspects and taking into account the reasoning of the Supreme Court in the present case, the Grand Chamber found that the Estonian courts' finding of liability against Delfi had been a justified and proportionate restriction on the portal's freedom of expression.

So, the outcome of the decision is that, when third-party user comments are in the form of hate speech and provide direct threats to the physical integrity of individuals, then "the rights and interests of others and of society as a whole may entitle Contracting States to impose liability on Internet news portals, without contravening Article 10 of the Convention, if they fail to take measures to remove clearly unlawful comments without delay, even without notice from the alleged victim or from third parties."[313]

However, it should be noted that the decision triggered debate on whether the Grand Chamber's assessment was right considering that Delfi immediately removed the comments in question from its website upon notification but failed to remove them prior to such notice being issued to Delfi. Both the Estonian Supreme Court and the European Court of Human Rights ruled that Delfi should have prevented the publication of comments with clearly unlawful content.[314] The Grand Chamber, considered that "a large news portal's obligation to take effective measures to limit the dissemination of hate speech and speech inciting violence – the issue in the present case – can by no means be equated to "private censorship".[315] In their joint dissenting opinion, Judges Sajó and Tsotsoria wrote that the Grand Chamber imposed a troubling "requirement of constructive knowledge on active Internet intermediaries".[316] According to the Judges, "for the sake of preventing defamation of all kinds, and perhaps all "illegal" activities, all comments will have to be monitored from the moment they are posted. As a consequence, active intermediaries and blog operators will have considerable incentives to discontinue offering a comments feature, and the fear of liability may lead to additional self-censorship by operators. This is an invitation to self-censorship at its worst."[317] Rightly so, the dissenting judges refer to the practices

313 Para 159 of the Delfi decision.

314 Para 141 of the Delfi decision.

315 Para 157 of the Delfi decision.

316 Judges Sajó and Tsotsoria's Joint Dissent Opinion, para 1.

317 Judges Sajó and Tsotsoria's Joint Dissent Opinion, para 1.

of overwhelming majority of the member States of the Council of Europe and explicitly state that the regulatory systems are based on the concept of "actual knowledge" rather than "constructive knowledge" as the majority of the Grand Chamber held.[318] Within this context, the dissenting judges also note that with the "actual knowledge" policies, a safe harbour is provided by the rule of "notice and take down". However, the Grand Chamber endorsed the standard of removal of comments "without delay" after publication and "not upon notice or on other grounds linked to actual knowledge. Active intermediaries are therefore invited to exercise prior restraint."[319] The dissenting judges, therefore, argued that the European Court should not have developed "rights restrictions which go against the prevailing standards of the member States, except in a few cases where a narrow majority found that deeply held moral traditions justified such exceptionalism."[320]

Whether you agree with the Grand Chamber or alternatively, whether you agree with the dissenting judges views or not, a "troubling uncertainty persists here."[321] It certainly remains to be seen how the member States or local judges within the member States will interpret and apply Delfi. Some answers to these important questions may be provided by a February 2016 decision of the European Court (4th section) itself in *Magyar Tartalomszolgáltatók Egyesülete and/et Index.hu Zrt v. Hungary*.[322]

The Case of Magyar Tartalomszolgáltatók Egyesülete and/et Index.hu Zrt v. Hungary

In this case, the first applicant was a self-regulatory body of Internet content providers and the second applicant the owner of an Internet news portal. Both applicants allowed users to comment on publications appearing on their portals. The applicants' portals contained disclaimers stating that the comments did not reflect the applicants' own opinion and a notice-and-take-down system allowed readers to request the removal of comments that caused concern. In February 2010 the first applicant published an opinion about two real-estate management websites the full text of which was subsequently also published on the second applicant's portal. The opinion attracted user comments some of which criticized the real-estate websites in derogatory terms. As a result, the company operating

318 See Judges Sajó and Tsotsoria's Joint Dissent Opinion, para 7.

319 Judges Sajó and Tsotsoria's Joint Dissent Opinion, para 8.

320 Judges Sajó and Tsotsoria's Joint Dissent Opinion, para 7.

321 Judges Sajó and Tsotsoria's Joint Dissent Opinion, para 20.

322 *Magyar Tartalomszolgáltatók Egyesülete and/et Index.hu Zrt v. Hungary*, no. 22947/13, 2.2.2016 [Section IV].

the websites brought a civil action against the applicants alleging damage to its reputation. The applicants immediately removed the offending user comments from their websites once aware of the court case. However, the Hungarian courts found them liable for the third party comments and they were ordered to pay procedural fees.

The European Court of Human Rights, assessed this application following the criteria established by the Court in the leading case of *Delfi AS v. Estonia*[323] including the context of the comments, the measures applied by the applicant company in order to prevent or remove defamatory comments, the liability of the actual authors of the comments as an alternative to the intermediary's liability, and the consequences of the domestic proceedings for the applicant company.[324] Each evaluation of the Court in the *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary* decision is provided below:[325]

(a) **Context in which the comments were posted** – The article under which the comments were posted concerned the allegedly unethical and misleading business practice of two real estate websites which had already prompted various proceedings against the company operating them before consumer protection bodies. The comments triggered by the article could therefore be regarded as a matter of public interest. The article was not devoid of a factual basis or liable to provoke gratuitously offensive comments. For their part, the domestic courts appeared to have paid no attention to the role, if any, played by the applicants in generating the comments.

(b) **Content of the comments** – The domestic courts had found the comments unreasonably offensive, injurious and degrading. However, the Court observed that the use of vulgar phrases in itself was not decisive and that it was necessary to have regard to the specificities of the style of communication on certain Internet portals. The expressions used in the comments, albeit belonging to a low register of style, were common in communication on many Internet portals, so the impact that could be attributed to them was thus reduced.

(c) **Liability of the authors of the comments** – The domestic courts had found the applicants liable for "disseminating" defamatory statements without

323 [GC] 64569/09 16 June 2015.

324 See *Delfi AS*, para 142-43 and *Magyar Tartalomszolgáltatók Egyesülete and/et Index.hu Zrt v. Hungary*, para 69.

325 Application no. 22947/13, 02 February, 2016 [Section IV].

embarking on a proportionality analysis to ascertain the respective liability of the authors of the comments and of the applicants. Furthermore, even accepting the domestic courts' analysis, holding the applicants liable for third-party comments was difficult to reconcile with the Court's case-law requiring "particularly strong reasons" before envisaging the punishment of a journalist for assisting in the dissemination of statements made by a third party.

(d) **Measures taken by the applicants and conduct of the injured party** – The applicants had removed the comments in question as soon as they were notified of the initiation of civil proceedings. They also had general measures in place to prevent or remove defamatory comments on their portals, including a disclaimer, a team of moderators, and a notice-and-take-down system. Despite this, the domestic courts held them liable for allowing unfiltered comments to be posted. For the Court, that finding amounted to requiring excessive and impracticable forethought capable of undermining the freedom to impart information on the Internet. The Court further noted that the domestic courts had not taken into account the fact that the plaintiff company at no stage requested the applicants to remove the comments but went directly to court.

(e) **Consequences for the injured party and the applicants** – The Court noted that what was at stake in the instant case was the commercial reputation of a private company rather than the reputation of a natural person, which enjoyed greater protection. Moreover, the comments were hardly capable of making any additional and significant impact on the attitude of consumers as inquiries into the plaintiff company's business conduct had already started when the article was published. In any event, the domestic courts did not seem to have evaluated whether the comments reached the requisite level of seriousness and whether they were made in a manner that actually caused prejudice. As for the impact of the judgments on the applicants, although they had not been required to pay compensation for non-pecuniary damage, it could not be excluded that the finding against them might form the basis for further legal action resulting in such an award. In any event, the decisive issue was that objective liability for third-party comments could have foreseeable negative consequences for an Internet portal, for example by requiring it to close the commenting space altogether. This in turn could have a chilling effect on freedom of expression on the Internet, which could be particularly detrimental for a non-commercial website such as that operated by the first applicant.

In conclusion and given the absence of hate speech or direct threats to physical integrity in the user comments, the European Court found that there was no reason to hold that, if accompanied by effective procedures allowing for a rapid response, the notice-and-take-down-system could not have provided a viable avenue to protect the plaintiff company's commercial reputation in this case. So, the Court established that the Hungary case was rather different then Delfi in terms of facts and the comments involved in that case.

Therefore, it remains the case that in cases where third-party user comments take the form of hate speech and direct threats to the physical integrity of individuals, the rights and interests of others and of the society as a whole might entitle Contracting States to impose liability on Internet news portals if they failed to take measures to remove clearly unlawful comments without delay, even without notice from the alleged victim or from third parties.[326] However, in the absence hate speech and direct threats, the Court agrees that news portals which deploy a notice-and-take-down-system for third party comments can benefit from the protection offered by Article 10.

Right to be forgotten decision of the Court of Justice of the European Union

Another decision that sparked controversy in terms of intermediary liability has been issued by the Court of Justice of the European Union with regards to the issue of whether individuals can compel search engines like Google to remove and de-link information related to them on privacy grounds from a search engine's database. The Court of Justice of the European Union held in the case of *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*[327] that the operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person's name links to web pages published by third parties and containing information relating to that person. The Court of Justice decision concerns only the information available through the search engine and requires links to be removed even though the names or other personal information related to the requester is not removed from the linked publications or when the information on those publications are lawful. This decision of the Court of Justice raised an important debate on removal of information from search engine searches and its impact upon freedom of expression.

326 See *Delfi AS*, para 159 and *Magyar Tartalomszolgáltatók Egyesülete and/et Index.hu Zrt v. Hungary*, para 91.

327 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, (the "right to be forgotten") Case C-131/12, 13 May 2014 (decision of the Court of Justice of the European Union).

The case from Spain involved a complaint by an applicant to AEPD, the Spanish Data Protection Agency in relation to his request for the removal of certain personal data related to him on an article on the website of La Vanguardia Ediciones SL (the publisher of a daily newspaper with a large circulation in Spain, in particular in Catalonia) and from Google's search engine results so that the information and data related to him no longer appeared in the search results and in the links to La Vanguardia.

The AEPD rejected the complaint against La Vanguardia, taking the view that the information in question had been lawfully published by the newspaper. On the other hand, the complaint was upheld as regards Google Spain and Google Inc. The AEPD requested Google to take the necessary measures to withdraw the data from their index and to render access to the data impossible in the future through its search engine.

Google Spain and Google Inc. then brought two actions before the Audiencia Nacional (National High Court, Spain), claiming that the AEPD's decision should be annulled. It is in this context that the Spanish court referred a series of questions to the Court of Justice. First, Advocate General Jääskinen published his opinion in June 2013 and considered that search engine service providers are not responsible, on the basis of the Data Protection Directive, for personal data appearing on web pages they process.[328] According to the Advocate General, national data protection legislation is applicable to search engine providers when they set up an office in a Member State which orientates its activity towards the inhabitants of that State, so as to promote and sell advertising space, even if the technical data processing takes place elsewhere . This view was based on the fact that Google Spain acts merely as commercial representative of Google for its advertising functions. In this capacity it has taken responsibility for the processing of personal data relating to its Spanish advertising customers. Furthermore, the Advocate General stated that "a possible 'notice and take down procedure' concerning links to source web pages with illegal or inappropriate content is a matter for national civil liability law based on grounds other than data protection."[329]

The Advocate General also argued that the EU Data Protection Directive does not establish a general 'right to be forgotten'. Such a right cannot therefore be

328 Court of Justice of the European Union, Press Release No 77/13, Luxembourg, 25 June 2013.

329 *Ibid*.

"invoked against search engine service providers on the basis of the Directive, even when it is interpreted in accordance with the Charter of Fundamental Rights of the European Union."[330] The Advocate General also made the distinction between liability of the search engine service providers under national law which may include removing or blocking access to illegal content such as web pages infringing intellectual property rights or displaying libelous or criminal information and in contrast requesting search engine service providers to suppress legitimate and legal information that has entered the public domain. The latter, according to the Advocate General would entail an interference with the freedom of expression of the publisher of the web page and this would amount to censorship by a private party.[331]

However, the Court of Justice ruled that by searching automatically, constantly and systematically for information published on the Internet, the operator of a search engine 'collects' data within the meaning of the Data Protection Directive. The Court also points out that the operations referred to by the directive must be classified as processing even where they exclusively concern material that has already been published as it stands in the media. A general derogation from the application of the directive in such a case would have the consequence of largely depriving the Directive of its effect. The Court further holds that the operator of the search engine is the 'controller' in respect of that processing, within the meaning of the Directive, given that it is the operator which determines the purposes and means of the processing. Therefore, search engine operators must ensure, within the framework of its responsibilities, powers and capabilities, that its activity complies with the Directive's requirements.

Furthermore, on the issue of territorial scope, the Court observed that Google Spain is a subsidiary of Google Inc. on Spanish territory and, therefore, an 'establishment' within the meaning of the directive. On the more important issue of the responsibility of the search engine operators, the Court held that the operator is, in certain circumstances, obliged to remove links to web pages that are published by third parties and contain information relating to a person from the list of results displayed following a search made on the basis of that person's name. As mentioned above, that also extends to scenarios in which the same information is not removed from the source website because it is lawful. Basically, the Court's decision purely concentrates on the responsibility of the search engine

330 *Ibid*.

331 *Ibid*.

providers and is not concerned with whether the original information publishes, rather than the link to that information, is removed or not.

In terms of the "right to be forgotten" issue, the Court held that a person (data subject) may, in the light of his fundamental rights under Articles 7 and 8 of the Charter, request that the information in question no longer be made available to the general public on account of its inclusion in such a list of results, those rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the data subject's name. However, the Court did not extend that right to those who hold public office and stated that in that case the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of its inclusion in the list of results, access to the information in question.

Subsequent to the decision, the OSCE Representative on Freedom of the Media warned that the decision of the Court of Justice of the European Union "might negatively affect access to information and create content and liability regimes that differ among different areas of the world, thus fragmenting the Internet and damaging its universality."[332] According to the OSCE Representative on Freedom of the Media, "information and personal data related to public figures and matters of public interest should always be accessible by the media and no restrictions or liability should be imposed on websites or intermediaries such as search engines. If excessive burdens and restrictions are imposed on intermediaries and content providers the risk of soft or self-censorship immediately appears."[333]

As of this writing, Google revealed that it has received a total of 374.210 privacy requests for search removals and the company has evaluated a total of 1,323,336 URLs for removal. Google has removed 477.106 URLs, approximately 42.4% while it declined to remove the majority of 684.401 URLs, approximately 57.6%.[334] According to the Google statistics, most privacy removal requests came from France with 79.422 requests involving 264.895 URLs. Google removed 109.278 URLs amounting to 48.4%. France is followed by Germany, with 64.737 requests involving 235.611 URLs. Google removed 98.631 URLs amounting to 48.4%. France and Germany is followed in third place by the

332 See Communiqué by OSCE Representative on Freedom of the Media on ruling of the European Union Court of Justice, issued on 16 May 2014: http://www.osce.org/fom/118632

333 *Ibid*.

334 See generally https://www.google.com/transparencyreport/removals/europeprivacy/?hl=en

United Kingdom with 45.963 requests involving 173.555 URLs. Google removed 55.753 URLs, amounting to 38.5%. According to Google, websites that are most affected by these removal requests are Facebook (with 11416 URLs removed), Profile Engine (with 8546 URLs removed), Google Groups (with 7203 URLs removed) and YouTube (with 5759 URLs removed). 4263 tweets were also de-linked from the search engine results.

In an interesting case, the UK's Information Commissioner's Office ordered Google to remove nine links to current news stories about older reports which themselves were removed from search results under the 'right to be forgotten' ruling.[335] In this case,[336] Google had previously complied with a request to remove links related to a 10 year-old criminal offence by an individual from the UK. However, subsequent to Google's removal of those links, there were further news coverage of the removal action detailing the claimant's name. However, Google refused to remove links to these later news stories arguing that they were recent and were in the public interest. Despite Google's argument the Information Commissioner's Office issued an enforcement notice ordering Google to remove nine search results linking to information about a person that was no longer relevant. The ruling recognized that journalistic content relating to decisions to delist search results may be newsworthy and in the public interest. But it confirms that this does not justify including links to that content when a Google search is made by entering the affected individual's name, as this has an unwarranted and negative impact on the individual's privacy and is a breach of the Data Protection Act.

Moreover, it is not just Google which has been affected by the removal requests. In the name of transparency, in June 2005 the BBC started to detail all the links removed to published BBC articles.[337] The Telegraph also published details of link removals affecting its website.[338] Furthermore, in France, the Commission Nationale de l'Informatique et des Libertés (CNIL) ordered in May 2015 Google to apply right to be forgotten removal orders not only to Google's European domains such as google.co.uk or google.fr, but to the search engine's global domain

335 The Guardian, "Google ordered to remove links to 'right to be forgotten' removal stories," 20 August, 2015, at http://www.theguardian.com/technology/2015/aug/20/google-ordered-to-remove-links-to-stories-about-right-to-be-forgotten-removals

336 See for the decision https://ico.org.uk/media/action-weve-taken/enforcement-notices/1560072/google-inc-enforcement-notice-102015.pdf

337 See generally http://www.bbc.co.uk/blogs/internet/entries/f4b01ccf-9128-45d8-8cac-23c1cf3455c1

338 See http://www.telegraph.co.uk/technology/google/11036257/Telegraph-stories-affected-by-EU-right-to-be-forgotten.html

google.com.[339] Although Google appealed against the decision arguing that this was a form of censorship and "risks serious chilling effects on the web",[340] CNIL rejected the appeal in December 2015 stating that once a removal request has been accepted, it must be applied across all extensions of the search engine and that not doing so allows the ruling to easily be circumvented. The decision of CNIL is final and Google will face fines if it does not follow the requirements of the ruling. Google then may appeal against the financial sanctions to Conseil d'Etat, the highest French administrative court.

Going back to the broader issues of "notice and take down" policies and practices, it must be mentioned that almost all social media platforms started to regularly publish transparency report revealing the number of removal requests including court orders and other request from government agencies, percentage or number of content removed or accounts closed. For example, looking into Facebook's removal policy, Facebook states that when the company receives such a request, the request is then scrutinized to determine if the specified content does indeed violate local laws. If Facebook determines that it does violate local laws, then the company makes that particular content unavailable in the relevant country or territory. Its report and statistics include removed content that governments have identified as illegal, as well as instances that may have been brought to our attention by non-government entities, such as NGOs, charities, and members of the Facebook community.[341] Within this context, when Facebook's January-June 2015 transparency report is assessed,[342] out of the 5198 "content restrictions" imposed by Facebook, majority of the removals with 4496 were from Turkey within the OSCE participating States. Turkey is followed by France with 295 removals and Germany with 188 on the top three.

Twitter on the other hand deploys a "country withheld content" policy[343] and if Twitter receives a valid and properly scoped request from an authorized entity, then the company reactively withholds access to certain content in a particular country from time to time. So that, the content complained and withheld is no longer visible from the country complained of but remains accessible anywhere else around the globe. Since Twitter started to publish its transparency reports,

339 The Guardian, "French data regulator rejects Google's right-to-be-forgotten appeal," 21 September, 2015, at http://www.theguardian.com/technology/2015/sep/21/french-google-right-to-be-forgotten-appeal.

340 See Google Europe Blog, "Implementing a European, not global, right to be forgotten," 30 July, 2015 at http://googlepolicyeurope.blogspot.be/2015/07/implementing-european-not-global-right.html

341 See generally https://govtrequests.facebook.com/about/

342 See generally https://govtrequests.facebook.com/

343 See generally https://support.twitter.com/articles/20169222?lang=en

the company used the country withheld content policy in Brazil, France, Germany, India, Japan, Netherlands, Russia, Turkey, and the United Kingdom. When Twitter's 2015 transparency report is assessed,[344] it is revealed that the company has received 928 court ordered removal requests worldwide during 2015. 858 of these requests, therefore, the majority came from Turkey, followed by 7 from France and 6 from Russia in the OSCE region. Furthermore, there were a total of 4692 other removal requests from government agencies, the police etc. during 2015. Of these, majority with 2071 requests came from Turkey, followed by 1797 requests from Russia and 179 requests from France within the OSCE region. Within the same period Twitter received requests to close down or withhold a total of 14.686 accounts. Of these, majority with 10.070 requests came from Turkey, followed by 1951 requests from Russia and 342 from France within the OSCE region. In terms of accounts withheld, Twitter withheld a total of 590 accounts during 2015. Of these, majority with 539 accounts were from Turkey, 36 from Russia and 11 from Germany within the OSCE region. Finally, in terms of number of tweets withheld, Twitter withheld a total of 4890 tweets worldwide during 2015. Of these, the majority with 4670 were from Turkey, 138 from Russia and 76 from France within the OSCE region.

Going back to Google, the company regularly receives requests from courts and government agencies around the world to remove information from Google services.[345] The most recent statistics cover 2014 during which Google received a total of 6845 removal requests involving 46.305 individual items. 3100 of these requests were court orders, and 3745 came from the governments and other governmental organisations including the police.

Conclusion

Liability provisions for intermediaries 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. However, the above mentioned 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 summary review report was

344 See generally https://transparency.twitter.com/

345 See generally https://www.google.com/transparencyreport/removals/government/?hl=en

published during 2011.[346] According to the Summary Report, "there was general consensus in favour of developing a harmonised EU 'notice-and-takedown' procedure, but much less agreement on the precise contours of these rules. Right holders and Internet Service Providers (ISPs) tended to take opposing stances, with consumer and citizen organisations often agreeing with ISPs on the basis of ethical considerations."

Furthermore, in early 2012 the Commission announced an initiative on "notice-and-action" procedures in the Communication on e-Commerce and other online services. The public consultation on "procedures for notifying and acting on illegal content hosted by online intermediaries" was held between 4 July 2012 and 12 September 2012. In total, 1060 responses were submitted. The stake-holders highlighted various problems associated with the notice and take down procedures in their submissions including problems with the meaning of "actual knowledge," requirements for notices and who issues such notices. However, as of this writing the E-Commerce Directive provisions remain in force and they should also be subject to the Delfi and *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt* interpretation of the European Court of Human Rights in the countries in which it has been transposed into national law.

In June 2011, a joint declaration on freedom of expression and the Internet was signed and published by the UN Special Rapporteur on Freedom of Opinion and Expression, OSCE Representative on Freedom of the Media, OAS Special Rapporteur on Freedom of Expression and ACHPR Special Rapporteur on Freedom of Expression and Access to Information.[347] This joint declaration included also recommendations in terms of intermediary liability:

- No one who simply provides technical Internet services such as providing access, or searching for, or transmission or caching of information, should be liable for content generated by others, which is disseminated using those services, as long as they do not specifically intervene in that content or refuse to obey a court order to remove that content, where they have the capacity to do so ('mere conduit principle').

346 Public consultation on the future of electronic commerce in the internal market and the implementation of the Directive on Electronic commerce (2000/31/EC). See the summary of the results at http://ec.europa.eu/internal_market/consultations/docs/2010/e-commerce/summary_report_en.pdf

347 Joint declaration on freedom of expression and the Internet, June 2011, at http://www.osce.org/fom/78309.

- Consideration should be given to insulating fully other intermediaries, including those mentioned in the preamble, from liability for content generated by others under the same conditions as *above*. At a minimum, intermediaries should not be required to monitor user-generated content and should not be subject to extrajudicial content takedown rules which fail to provide sufficient protection for freedom of expression (which is the case with many of the 'notice and takedown' rules currently being applied).

In March 2015, an international coalition launched the "Manila Principles for Intermediary Liability," a roadmap for the global community to protect online freedom of expression and innovation around the world. The Manila Principles[348] were developed by an open, collaborative process conducted by a broad coalition of civil society groups and experts from around the world. The framework outlines clear, fair requirements for content removal requests and details how to minimize the damage a takedown request can do with six main principles:

1. Intermediaries should be shielded by law from liability for third-party content.
2. Content must not be required to be restricted without an order by a judicial authority.
3. Requests for restrictions of content must be clear, be unambiguous, and follow due process.
4. Laws and content restriction orders and practices must comply with the tests of necessity and proportionality.
5. Laws and content restriction policies and practices must respect due process.
6. Transparency and accountability must be built in to laws and content restriction policies and practices.

In January 2016, the OSCE Representative on Freedom of the Media recommended to the participating States that[349]

- the important presence and role of intermediaries should not endanger the openness, diversity and transparency of Internet content distribution and access,

348 The principles and supporting documents can be found online at https://www.manilaprinciples.org, where other organizations and members of the public can also express their own endorsement of the principles.

349 3rd Communiqué on Open Journalism, Communiqué No.1/2016, Organization for Security and Co-operation in Europe The Representative on Freedom of the Media Dunja Mijatović, 29 January, 2016, at http://www.osce.org/fom/219391

- excessive and disproportionate provisions regarding content takedown and intermediaries' liability create a clear risk of transferring regulation and adjudication of Internet freedom rights to private actors and should be avoided. States should also discourage intermediaries from automatizing decisions with clear human rights implications,
- international documents on human rights responsibilities for non-state actors, as well as multi-stakeholder debates and initiatives such as the Manila Principles (above mentioned), should be given due consideration in this area,
- making private intermediaries more transparent and accountable is a legitimate aim to be pursued by participating States through appropriate means. However, this must not lead to excessive control by public authorities over online content,
- decisions addressed to intermediaries establishing restrictions or ordering the takedown of Internet content should be adopted according to law, by judicial or other independent adjudicatory authorities, following due process and with full respect to the principles of necessity and proportionality.

Liability debate will therefore continue for the intermediaries and for the foreseeable future they will continue to find themselves within the chain of liability in terms of the provision and transmission of allegedly illegal content. In the European region laws deriving from the E-Commerce Directive, the ruling of the Grand Chamber of the European Court of Human Rights in Delfi as well as the "right to be forgotten" decision of the Court of Justice of the European Union will complicate the matter further for the information society service providers including access providers as well as social media platform providers and search engines. So, in the foreseeable future, the intermediaries will inevitably find themselves increasingly enmeshed in policy developments targeting the availability of illegal Internet content and the subject matter of take-down and removal orders.

A *de facto* strict liability rule should be avoided at all costs for the intermediaries based on constructive knowledge principles moving away from the "actual knowledge" standards set out in the European region. That is why Delfi should be read within the strict facts of the case rather than expanding its principles into every scenario involving intermediaries within the pan European region. Otherwise, in the words of Judges Sajó and Tsotsoria, "vaguely worded, ambiguous and therefore unforeseeable laws" will have a chilling effect

on freedom of expression.[350] The European Court's subsequent *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt* decision shows that Delfi should be read strictly in relation to content involving hate speech or incitement to violence.[351]

350 Judges Sajó and Tsotsoria's Joint Dissent Opinion.

351 Within this context note Countering Online Abuse of Female Journalist, Office of the Representative on Freedom of the Media Organization for Security and Co-operation in Europe (OSCE), February 2016, at http://www.osce.org/fom/220411.

Conclusion

With the opportunities and challenges that the Internet brings, it is impossible to predict the future of this global borderless communication network. However, with certainty, the Internet will continue to keep the governments of the world "busy" in terms of how to govern this global medium which does not recognise any boundaries. This book has shown that even the development of regional or international legal instruments and conventions have a limited effect to encounter some of the common problems associated with Internet content. For example, it has taken states several years to formulate common policies even for combatting child pornography. On the other hand, definitional, legal or constitutional variations complicate finding common grounds for addressing content involving hate speech, racist or extremist content, or terrorist propaganda. So, question marks, common grounds and legal variations will continue to exist for the foreseeable future.

However, what should not be forgotten is that democracy cannot exist without freedom of expression which remains as an indispensable fundamental right for everyone, anywhere, regardless of frontiers enshrined in article 19 of the Universal Declaration of Human Rights (UDHR), article 19 of the International Covenant on Civil and Political Rights (ICCPR), article 10 of the European Convention on Human Rights and guaranteed by OSCE commitments. By reference to these important international and regional instruments, information or ideas that may be regarded as critical, controversial, shocking, offending or disturbing[352] may benefit from the protection guaranteed for freedom of expression especially within the sphere of political speech and discourse. According to the European Court, "such are the demands of that pluralism, tolerance and broadmindedness without which there is no "democratic society"."[353] Usually, according to the case-law of the European Court speech which does not contain hatred or intolerance or amount to glorification of violence or incitement or call to violence deserves protection. However, the practical and effective impact of these international and regional instruments and their application differs from one state to another.[354]

352 *Handyside v. the United Kingdom*, judgment of 7 December 1976, Series A no. 24, p. 23, para. 49, and *Observer and Guardian v. the United Kingdom*, judgment of 26 November 1991, Series A no. 216, p. 30, para. 59.

353 *Ibid*.

354 With regards to Article of the European Convention on Human Rights see Voorhoof, D., The Right to Freedom of Expression and Information under the European Human Rights System: Towards a more Transparent Democratic Society, RSCAS 2014/12, Robert Schuman Centre for Advanced Studies Centre for Media Pluralism and Media Freedom, February, 2014, at http://cadmus.eui.eu/bitstream/handle/1814/29871/RSCAS_2014_12.pdf?sequence=1

The environment where alternative views and as a result proper working democracy, can flourish, requires states to refrain from arbitrarily interfering with the rights of individuals on the one hand, while imposing some positive obligations upon them to respect those on the other. Within this context, it should be reminded that States have the primary obligation to protect and ensure the right to freedom of opinion and expression. Therefore, States must ensure that their legal systems provide adequate and effective guarantees of freedom of opinion and expression to all and that freedom of expression can be limited by law in certain, strictly defined ways and under specific circumstances by reference to the above mentioned international and regional human rights conventions and related court decisions.

The European Court of Human Rights has held that although the essential object of many provisions of the Convention is to protect the individual against arbitrary interference by public authorities, there may in addition be positive obligations inherent in effect respect of the rights concerned. A positive obligation may also arise under Article 10 with regards to freedom of expression.[355] The European Court emphasized the key importance of freedom of expression as one of the preconditions for a functioning democracy in a number of its decisions and established that genuine, effective exercise of this freedom does not depend merely on the State's duty not to interfere, but may require positive measures of protection, even in the sphere of relations between individuals.[356] These positive obligations along with negative ones guarantee the principle of pluralism. Although the level of positive obligations vary depending upon various reasons, like the kind of expression rights at stake,[357] the main aim of the Convention and the CoE can be summarised as creating an open spare for public debate. Thus, the main aim of the ECHR is not to protect sacred rulers against disturbing words but to protect the environment in which people can express themselves without fear.[358] Now it is widely accepted that those positive obligations not only protects persons against the government but also against private actors.[359]

355 See generally European Court of Human Rights (Research Division), Positive obligations on member States under Article 10 to protect journalists and prevent impunity, Research Report, December 2011.

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

357 *Özgür Gündem v. Turkey*, para. 43.

358 See generally Akdeniz, Y., & Altıparmak, K., "Silencing Effect on Dissent and Freedom of Expression in Turkey," in *Journalism at Risk: Threats, Challenges and Perspectives*, Council of Europe Publishing, 2015, 145-173.

359 See amongst other authorities, *Palomo Sánchez and Others v. Spain* [GC], 28955/06 and others, 12..9.2011, para 60; *Fuentes Bobo v. Spain*, no. 39293/98, 29.2.2000, para. 38.

In determining whether or not a positive obligation exists, regard must be had to the fair balance that has to be struck between the general interest of the community and the interests of the individual, the search for which is inherent throughout the Convention. The scope of this obligation will inevitably vary, having regard to the diversity of situations obtaining in Contracting States and the choices which must be made in terms of priorities and resources. Nor must such an obligation be interpreted in such a way as to impose an impossible or disproportionate burden on the authorities.[360]

So, the States must ensure that it is safe to speak, share opinions and receive information for everyone through all communication media including the Internet and social media platforms. This is even more crucial with regards to political and social news and events of public concern and their coverage through the press by journalists and debate on matters of public interest by anyone through the social media platforms. In the words of the European Court, "press freedom assumes even greater importance in circumstances in which State activities and decisions escape democratic or judicial scrutiny on account of their confidential or secret nature."[361] Within this context, "criminal defamation laws should be revisited as a criminal sanction with restriction of liberty is a fortiori a grave restriction of freedom of expression".[362]

As part of the on-going debate on freedom of expression on the Internet, the emergence of the concept of "citizen journalism" which is now recognised by the European Court of Human Rights[363] should not be forgotten as political information ignored by the mainstream media have often been disclosed through the social media platforms such as YouTube. Access to such social media platforms should not be the subject matter of overbroad blocking orders as established by the European Court of Human Rights. Therefore, access to such services should never be blocked, discriminated against, or slowed down.

360 See, *generally Rees v. the United Kingdom,* judgment of 17 October 1986, Series A no. 106, p. 15, § 37; *Osman v. the United Kingdom*, judgment of 28 October 1998, *Reports of Judgments and Decisions* 1998-VIII, pp. 3159-60, § 116; *Appleby and Others v. the United Kingdom,* Application no. 44306/98, judgment of 06 May 2003; *Khurshid Mustafa and Tarzibachi v. Sweden*, App. no. 23883/06, judgment of 16 December.

361 *Stoll v. Switzerland* [GC], no. 69698/01, 10 December 2007, para 110.

362 *Cumpănă and Mazăre v. Romania*, no.[GC], no 33348/96, 17 December 2004. See further CoE "Study on the alignment of laws and practices concerning defamation
with the relevant case-law of the European Court of Human Rights on freedom of expression, particularly with regard to the principle of proportionality," CDMSI(2012)Misc11Rev2, para 15.

363 *Cengiz and Others v. Turkey*, nos. 48226/10 and 14027/11, 01.12.2015.

Finally, governments and international organisations should continue to respect fundamental human rights such as freedom of expression and should encourage rather than limit citizens' access to the Internet through excessive regulation at the state level. As established in this book, responses to problems that are associated with the Internet need to be proportionate and effective. Otherwise, the Internet may end up as the most regulated medium in the history.

About the author

Professor Yaman Akdeniz, Istanbul Bilgi University

Dr. Yaman Akdeniz (LLB, MA, PhD) is a Professor of Law at the Human Rights Law Research Center, Faculty of Law and the Pro Rector for the Istanbul Bilgi University. Between 2001-2009 Akdeniz was at the School of Law, University of Leeds and has set up Cyber-Rights.Org in the mid 1990s in the UK.

Akdeniz acted as an expert to several international organizations including the United Nations High Commissioner for Human Rights (UNHCHR) Office and the Office of the OSCE Representative on Freedom of the Media with regards to human rights aspects of Internet law and policy. More recently, Akdeniz has been appointed to the Council of Europe Committee of Experts on Rights of Internet Users as an 'elected independent expert' (July 2012 - December 2013) and has been appointed to the Council of Europe Committee of experts on cross-border flow of Internet traffic and Internet freedom as an 'elected independent expert' (January 2014 - December 2015).

He has written extensively since the mid 1990s and his recent publications include *Internet Child Pornography and the Law: National and International Responses* (London: Ashgate, 2008); and *Racism on the Internet* (Council of Europe Publishing, 2010). Akdeniz also authored the 2006 Report of the United Nations High Commissioner for Human Rights Office (UNHCHR) entitled *Stocktaking on efforts to combat Racism on the Internet* (E/CN.4/2006/WG.21/BP.1, January 2006), 2010 Report of the OSCE Representative on Freedom of the Media entitled *Turkey and Internet Censorship* and 2011, and more recently the Report of the OSCE Representative on Freedom of the Media entitled *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*.

Do read this book, it contains important information related to the Internet. > Do remember that the Internet is not confined to your own country. > Do ensure citizens' access to the Internet. > Do acknowledge that freedom of expression extends not only to ideas and information generally regarded as inoffensive but even to those that might offend, shock, or disturb. > Do ensure that the principle of network neutrality is respected by Internet access providers. Do safeguard it in the development of national legal frameworks in order to ensure the protection of the right to freedom of expression, access to information and the right to privacy. > Do remember that user-generated content on the Internet provides an unprecedented platform for the exercise of freedom of expression. > Do rely on blocking only within a strict legal framework with regards to content identified as illegal by the courts of law. > Do recall that blocking is not an effective method to address problems associated with Internet content and could have serious side effects including over blocking. > Don't develop laws or policies to block access to social media platforms. > Don't forget that the State should not stand between the speaker and his or her audience. > Don't allow Internet access providers to restrict users' right to receive and impart information by means of blocking, slowing down, degrading or discriminating Internet traffic associated with particular content, services, applications or devices. > Don't impose general content monitoring requirements for the intermediaries. > Do clarify liability issues surrounding the intermediaries based on a knowledge and control test.

OSCE
The Representative on
Freedom of the Media