FREEDOM OF EXPRESSION AND THE INTERNET

"Everyone has the right to freedom of expression."
Article 10, European Convention on Human Rights

Wolfgang **Benedek**
and Matthias C. **Kettemann**

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Freedom of expression and the Internet

by Wolfgang Benedek and Matthias C. Kettemann

Council of Europe Publishing

Cover photo: Shutterstock

Cover design: Documents and Publications Production Department (SPDP), Council of Europe

Layout: Jouve, Paris

Council of Europe Publishing
F-67075 Strasbourg Cedex
http://book.coe.int

ISBN 978-92-871-7702-5

Printed at the Council of Europe

Contents

List of abbreviations

A2K	Access to Knowledge
ACHPR	African Commission on Human and Peoples' Rights
ACPO	Association of Chief Police Officers
ACTA	Anti-Counterfeiting Trade Agreement
AFP	Agence France Press
APC	Association for Progressive Communications
Art.	Article
ccTLD	country code Top-Level Domain
CDMC	Committee on the Media and New Communication Services
CJEU	Court of Justice of the European Union
CMPF	Centre for Media Pluralism and Media Freedom
CNIL	Commission Nationale de l'Informatique et des Libertés
CPT	European Committee on the Prevention of Torture
DDoS	Distributed Denial-of-Service
DNS	Domain Name System
ECHR	European Convention on Human Rights
ECPA	Electronic Communications Privacy Act
ECPT	European Convention for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment
ECRI	European Commission against Racism and Intolerance
ECSR	European Committee on Social Rights
EDRi	European Digital Rights
ESC	European Social Charter
ETS	European Treaty Series
EU	European Union
EuroDIG	European Dialogue on Internet Governance
FCNM	Framework Convention for the Protection of National Minorities (FCNM)
FoE	Freedom of Expression
FTC	Federal Trade Commission
GAC	Governmental Advisory Committee
GC	Grand Chamber
GNI	Global Network Initiative
gTLD	generic Top-Level Domains
HRC	Human Rights Council
IBR	Internet Bill of Rights
ICANN	Internet Corporation for Assigned Names and Numbers

ICCPR	International Covenant on Civil and Political Rights
ICESCR	International Covenant on Economic, Social and Cultural Rights
ICT	Information and Communication Technology
IFEX	International Freedom of Expression Exchange
IGF	Internet Governance Forum
INHOPE	International Association of Internet Hotlines
IP	Internet Protocol
ISP	Internet Service Provider
IT	Information Technology
ITU	International Telecommunication Union
IWF	Internet Watch Foundation
NGOs	Non-Governmental Organisations
NTD	Notice and Take Down
OAS	Organization of American States
ODIHR	Office for Democratic Institutions and Human Rights
OHCHR	Office of the High Commissioner for Human Rights
OSCE	Organization for Security and Co-operation in Europe
PDHRE	People's Movement for Human Rights Education
PIPA	Protect IP ACT
Rec.	Recommendation
RevESC	Revised European Social Charter
RFoM	Special Representative for the Freedom of the Media
RWB	Reporters without Borders
SEC	US Securities and Exchange Commission
SOPA	Stop Online Piracy Act
TİB	Telekomünikasyon İletişim Başkanlığı (Turkish Telecommunications Directorate)
TLD	Top-Level Domain
TMG	German Telemediengesetz (Telemedia Act)
UDHR	Universal Declaration of Human Rights
UN	United Nations
UNESCO	United Nations Educational, Scientific and Cultural Organization
URL	Uniform Resource Locator
US	United States
VPNs	Virtual Private Networks
WSIS	World Summit on the Information Society
www	World Wide Web

Table of cases

European Court of Human Rights

Anheuser-Busch Inc. v. Portugal (11 October 2005), application No. 73049/01

Appleby v. United Kingdom (6 May 2003), application No. 44306/98

B.H; M.W; H.P; G.K. v. Austria (12 October 1989), application No. 12774/87

Bergens Tidende and Others v. Norway (2 May 2000), application No. 26132/95

Casado Coca v. Spain (24 February 1994), application No. 15450/89

Communist Party of Germany v. the Federal Republic of Germany (20 July 1957), application No. 250/57

Delfi AS v. Estonia (communication of 11 February 2011), application No. 64569/09

Dink v. Turkey (14 September 2010), application Nos. 2668/07, 6102/08, 30079/08, 7072/09 and 7124/09

Heinisch v. Germany (21 July 2011), application No. 28274/08

Editorial Board of Pravoye Delo and Shtekel v. Ukraine (5 May 2011), application No. 33014/05

Erbakan v. Turkey (6 July 2006), application No. 59405/00

Faruk Temel v. Turkey (1 February 2011), application No. 16853/05

Fatullayev v. Azerbaijan (22 April 2010), application No. 40984/07

Féret v. Belgium (16 July 2009), application No. 15615/07

Garaudy v. France (24 June 2003), application No. 65831/01

Handyside v. the United Kingdom (7 December 1976), application No. 5493/72

Honsik v. Austria (18 October 1995), application No. 25062/94

Jankovskis v. Lithuania (communicated on 27 September 2010), application No. 21575/08

Jersild v. Denmark (23 September 1994), application No. 15890/89

K.U. v. Finland (2 December 2008), application No. 2872/02

Karakó v. Hungary (28 April 2009), application No. 39311/05

Karatas v. Turkey (8 July 1999), application No. 23168/94

Krone Verlag GmbH & Co KG v. Austria No. 3 (11 December 2003), application No. 39069/97

Leroy v. France (2 October 2008), application No. 36109/03

Lingens v. Austria (8 July 1986), application No. 9815/82

Mosley v. the United Kingdom (10 May 2011), application No. 48009/08

Mouvement Raëlien Suisse v. Switzerland (13 July 2012), application No. 16354/06

Neij and Sunde Kolmisoppi v. Sweden (13 March 2013), application No. 40397/12

Norwood v. the United Kingdom (16 November 2004), application No. 23131/03

The Observer and Guardian v. United Kingdom (26 November 1991), application No. 13585/88

Otegi Mondragon v. Spain (15 March 2011), application No. 2034/07

Paeffgen GmbH v. Germany (18 September 2007), application Nos. 25379/04, 21688/05, 21722/05, 21770/05

Pavel Ivanov v. Russia (20 February 2007), application No. 35222/04, admissibility decision

Perrin v. the United Kingdom (18 October 2005), application No. 5446/03

Pfeifer v. Austria (15 November 2007), application No. 12556/03

Polanco Torres and Movilla Polanco v. Spain (21 September 2010), application No. 34147/06

Refah Partisi (The Welfare Party) and Others v. Turkey (13 February 2003), application Nos. 41340/98, 41342/98, 41343/98 and 41344/98

Renaud v. France (25 February 2010), application No. 13290/07

Stoll v. Switzerland (10 December 2012), application No. 69698/01

Sürek v. Turkey (8 July 1999), application No. 26682/95

Times Newspapers Limited v. the United Kingdom (10 March 2009, 10 June 2009), application Nos. 1 and 2, Nos. 3002/03 and 23676/03

Tolstoy Miloslavsky v. United Kingdom (13 July 1995), application No. 18139/91

Vejdeland and Others v. Sweden (9 February 2012), application No. 1813/07

VgT (Verein gegen Tierfabriken) v. Switzerland (28 June 2001), application No. 24699/94

X and Church of Scientology v. Sweden (5 May 1979), application No. 7805/77

Yildirim v. Turkey (18 December 2012), application No. 3111/10

Court of Justice of the European Union

SABAM v. Netlog NV (16 February 2012), ECJ C-360/10

Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) (24 November 2011), ECJ C-70/10

National courts

France

Conseil constitutionnel (France), Decision of 10 June 2009 (Decision No. 2009-580 DC), *Loi favorisant la diffusion et la protection de la création sur internet*, www.conseil-constitutionnel.fr/decision/2009/2009-580-dc/decision-n-2009-580-dc-du-10-juin-2009.42666.html

Germany

Bundesgerichtshof (Third Civil Senate) (24 January 2013), III ZR 98/12

Bundesverfassungsgericht (9 February 2010), 1 BvL 1/09

Schleswig-Holsteinisches Oberverwaltungsgericht (14 February 2013), 8 B 60/12 and 8 B 61/12

Italy

Corte d'Appello di Milano (21 December 2011), sezione prima penale, case 8611/12

Tribunale Ordinario di Milano (16 April 2010), penal section, case 1972/2010

UK

Chambers v. DPP (27 July 2012), High Court, [2012] EWHC 2157

Payam Tamiz v. Google Inc. and Google UK Limited, High Court [2012] EWHC 449 (QB),

Payam Tamiz v. Google Inc., Court of Appeal, [2013] EWCA Civ 68

USA

New Jersey Coalition Against War in the Middle East v. J.M.B. Realty Corp. (1994), 138 NJ 326, 650 A.2d 757

The Green Party of New Jersey v. Hartz Mountain Industries, Inc., 2000 WL 758410 (N.J.)

Yahoo! Inc. v. LICRA and UEJF (12 January 2006), United States Court of Appeals, Ninth Circuit, 433 F.3d 1199

UN Human Rights Commission

Laptsevich v. Belarus, Comm. No. 780/1997

Mukong v. Cameroon, Comm. No. 458/1991

Park v. Korea, Comm. No. 628/1995

Preface

Dear readers,

The Internet has changed the way we communicate, work and play. It has affected the way we live and learn, participate and protest. Freedom of expression on the Internet is key to understanding the potential of information and communication technologies for increasing the level of human rights protection around the globe.

From the Arab Spring to the global Occupy movement, the role of freedom of expression on the Internet in debating the questions that shape our future has never been greater. At the same time, an increasing number of states use the Internet to spy on journalists and citizen journalists, to prosecute and jail bloggers, and to censor online information.

With the rise of the Internet the opportunities to express oneself have grown exponentially. But so have the challenges to freedom of expression.

No wonder then that protecting freedom of expression on the Internet has become an important task for international and non-governmental organisations. Declarations and recommendations building on the universal human rights commitments to freedom of expression – namely Article 10 of the European Convention on Human Rights (ECHR), as well as Article 19 of both the International Covenant on Civil and Political Rights (ICCPR) and the Universal Declaration of Human Rights – abound. The practice, however, looks different. Violations of freedom of expression online by states, companies and individuals are a daily, and sad, reality.

This book sets out to answer key questions regarding the extent and limits of freedom of expression online. It seeks to shed light on the often obscure landscape of what we are allowed to say online and how our ideas, and the process of imparting and receiving information, are protected. It shows the large ambit of rights protected by freedom of expression, including freedom of the media and the right to access information, and confirms that all aspects of the communicative process, offline just as online, are protected by freedom of expression. The book makes an important point by making clear that freedom of expression online must be protected just like freedom of expression offline, taking into account the nature of the Internet, its asynchronicity, ubiquity and speed.

The book also wishes to highlight the importance of the standard-setting, monitoring and promotion activities of international and non-governmental organisations. Freedom of expression online touches all aspects of society

and does so in all societies. We have therefore included a chapter on relevant national practices to illustrate how different states deal with the challenge that the Internet has brought to ensuring freedom of expression for all.

The book makes another important point in showing that freedom of expression implies obligations for all actors on the Internet. States must respect, protect and ensure freedom of expression online just as much as offline; Internet companies have to respect and protect freedom of expression, implement it within their sphere and remedy violations. Civil society has an important watchdog function and the individuals it comprises must ensure that, in making use of their freedom of expression, they do not violate the rights of others.

As the authors of this book, we have been working on the protection of human rights on the Internet for more than ten years. At the Institute of International Law and International Relations of the University of Graz, Austria, we have created a Focal Point on Internet Governance and Human Rights[1] to look specifically at the principles and processes of protecting human rights online. Our team has been present and active during the most important moments of the evolution of the information society in the last decade: from the World Summit on the Information Society (WSIS) and meetings of the Internet Corporation for Assigned Names and Numbers (ICANN) to all Internet Governance Forums which have so far taken place. This gives us a unique view of the challenges that freedom of expression online faces. We are also active in dynamic coalitions, including the Internet Rights and Principles Coalition.

Our team has worked intensively with the Council of Europe, and in particular its Division on the Media and Information Society and its publication services. Wolfgang Benedek is currently an expert on the Committee on the Rights of Internet Users, which is charged with preparing a Compendium on Internet User Rights.

Over the last six years we have published several books that shed light on aspects of freedom of expression online. They inform our understanding of the challenges faced by the protection of freedom of expression online.[2]

In conclusion, the authors would like to express their thanks to the Council of Europe for inviting them to produce this publication. The Council of Europe has been *the* international organisation most consistently supportive of human

1. See Focal Point on Internet Governance and Human Rights of the University of Graz, http://voelkerrecht.uni-graz.at/en/forschen/forschungsschwerpunkte.
2. Benedek W. and Pekari C. (eds), *Menschenrechte in der Informationsgesellschaft* [Human rights in the information society], Hannover: Boorberg, 2007; Benedek W., Bauer V. and Kettemann M. (eds), *Internet governance and the information society: global perspectives and European dimensions*, Utrecht: Eleven International, 2008; Kettemann M. et al. (eds), *Menschenrechte und Internet. Zugang, Freiheit, Kontrolle* [Human rights and the Internet. access, freedom, control], Berlin: Internet&Society Co:llaboratory, 2012; and Kettemann M., *The future of individuals in international law: lessons from international Internet law*, Utrecht: Eleven International 2013.

rights online. It has also enabled important insights into the topic by inviting the authors to participate in key events for freedom of expression on the Internet. By publishing our analysis of the challenges to and the protection of freedom of expression online, the Council of Europe takes its commitment one step further.

Special thanks go to Manuela Ruß and Johanna Weber for their substantial support in finalising the manuscript. We would also like to thank Annick Pachod for her editorial support and Gerard M.-F. Hill for the language review.

The Internet has a catalytic function for the exercise of all human rights. Just as Gutenberg's printing press helped to spread the Reformation, the Internet can support the respect, protection and implementation of all human rights for all people everywhere. In this emancipatory quest, freedom of expression is a key enabling right, not to mention an essential human right in itself. Ensuring freedom of expression online is not without its challenges. Read on and you will see how to meet them head on.

Wolfgang Benedek and Matthias C. Kettemann
Graz, May 2013

1. Introduction: the challenges of ensuring freedom of expression on the Internet

Paul Chambers was in love. He was very much looking forward to seeing his girlfriend in Belfast, so when adverse weather conditions forced his local airport to close, he was understandably upset. "Crap! Robin Hood airport is closed", he wrote in early 2010, "you've got a week and a bit to get your shit together otherwise I'm blowing the airport sky high!!" *[sic]*. He was convicted of making statements of a menacing character and lost two jobs over the trial before the judgment was finally overturned.[3]

While this case concerns just one person and the limits between humorous and menacing speech, it illustrates neatly what fundamental questions are at stake in the information society. Every day brings new and increasingly difficult cases to the fore that challenge what we know about protecting freedom of expression.

Both the speed of the appearance of these new challenges and their number is astounding. In December 2012 alone:

- the European Court of Human Rights ruled in *Yildirim* that Turkey was not allowed to issue a blanket ban on specific Internet services;[4]
- an Austrian law student group announced its intention to go after Facebook for violations of data protection;[5]
- after threats by British authorities, the British Pirate Party stopped offering technology that allowed users to circumvent a state-wide block on the search engine The Pirate Bay, which was used by many for downloading copyrighted material;[6]

3. Bowcott O. (27 July 2012), "Twitter joke trial: Paul Chambers wins high court appeal against conviction", *The Guardian*, at www.guardian.co.uk/law/2012/jul/27/twitter-joke-trial-high-court. (All websites correct as of 1 May 2013.)
4. European Court of Human Rights, *Yildirim v. Turkey* (18 December 2012), application No. 3111/10, at www.bailii.org/eu/cases/ECHR/2012/2074.html. (Unless indicated otherwise, all cases cited in this publication are from the European Court of Human Rights.)
5. O'Brien K. J. (4 December 2012), "Law students in Austria challenge Facebook privacy policy", *New York Times*, at www.nytimes.com/2012/12/05/technology/austrian-group-plans-court-challenge-to-facebooks-privacy-policies.html?r = 0.
6. Lee D. (10 December 2012), "Pirate Party threatened with legal action over Pirate Bay proxy", BBC News, at www.bbc.co.uk/news/technology-20668699.

– the Chinese Government intensified its Internet monitoring by means of a new programme that allows them to discover and prevent connections through virtual private networks which had been used by activists to bypass national content blocks;[7]
– the regional data-protection office of the German state of Schleswig-Holstein ordered Facebook to allow pseudonyms and change its real-name policy, as required by German law.[8]

These cases offer but a glimpse of the challenges to freedom of expression in the information society. Since the emergence of the Internet, the debates on the reach of freedom of expression have taken centre stage. UN Special Rapporteur Frank La Rue described the right to freedom of opinion and expression as an essential "enabler" of other rights through the Internet: "by acting as a catalyst for individuals to exercise their right to freedom of opinion and expression, the Internet also facilitates the realisation of a range of other human rights". But the Internet also brings about new challenges to these human rights.[9]

While the Internet has brought along substantial new possibilities for exercising and protecting human rights, the possibilities for human rights violations have also grown exponentially.[10] The explosion of Internet usage has also led to a backlash in terms of governmental control. States increasingly restrict Internet access or monitor Internet use through sophisticated technologies and, fearing social and political activism, criminalise certain forms of expression.

The unique characteristics of the Internet in which its advantages are rooted, including its speed, its universal nature and the relative anonymity it offers, can also lead to challenges to human rights.[11] Do we therefore need new human rights for the Internet?

On 5 July 2012, the UN Human Rights Council (HRC) adopted by consensus a key resolution on the promotion, protection and enjoyment of human rights on the Internet.[12] Presented by Sweden, the resolution enjoyed broad international backing from more than 70 HRC member countries and non-members from all regional groups. The resolution affirms that "the same rights that

7. Osborne C. (17 December 2012), *China reinforces its 'Great Firewall' to prevent encryption,* at news.cnet.com/8301-1009_3-57559531-83/china-reinforces-its-great-firewall-to-prevent-encryption.
8. BBC News (18 December 2012), *Germany orders changes to Facebook real name policy*, at www.bbc.co.uk/news/technology-20766682.
9. See also Benedek W. (2008), "Internet governance and human rights", in Benedek W., Bauer V. and Kettemann M. C. (eds), *Internet governance and the information society: global perspectives and European dimensions*, Utrecht: Eleven International, pp. 31-49.
10. La Rue F. (16 May 2011), *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, UN Doc. A/HRC/17/27, paras. 22 and 23.
11. Ibid., paras. 20, 22 and 23.
12. Human Rights Council (5 July 2012), *The promotion, protection and enjoyment of human rights on the Internet*, 20th Session, UN Doc. A/HRC/20/8.

people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice, in accordance with Articles 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights".

We see here a clear commitment to the special role of freedom of expression in the information society and on the Internet, a commitment that is necessary in a digital age with two faces: increasing the potential to exercise freedom of expression, but also increasing the potential to restrict it.

This book takes on the challenge of presenting a nuanced approach to this central challenge by analysing the impact of new technologies and their influence on human behaviour. We will study, for instance, the role of search engines, which have made the storing of information partly redundant as any information is now available at any time. The new opportunities offered by the Internet also include online publications such as blogs, which allow the immediate sharing of often highly personal information. As we have seen in the three cases mentioned at the beginning of this chapter, bloggers have been held accountable for the content on their blogs just like journalists, which raises the issue of their protection.

These new opportunities require responsible use as they also offer human rights abusers new avenues for hate speech, child abuse and incitement to terrorism. They create new challenges for the regulation of freedom of expression and information in a human rights-consistent way.

With regard to human rights, the principle of "what applies offline should also apply online" can provide general guidance. However, the universal nature of the Internet and its decentralised management needs to be borne in mind. Consequently, the major challenge for freedom of expression on the Internet, as for human rights in general, is to maintain the offline standards while taking the online environment properly into account.

Against this background, this book will address the following key question in its many forms: what are the new challenges the Internet has brought for freedom of expression, and how must the right to freedom of expression be interpreted in order to maintain its integrity in the Internet environment?

Other key questions we address include: how has the European Court of Human Rights reacted to the new challenges and what has been the response of other European and global human rights institutions? In particular, has the Internet enlarged the scope of freedom of expression and information and has this led to a new balance of rights and corresponding responsibilities, which may necessitate stronger interference by regulatory bodies and the state? What kind of new regulations might be considered legitimate, if not necessary, in response to the challenges to the reputation and rights of children in the Internet? What are the limitations of state or international regulation of the Internet in order not to violate freedom of expression and other related

human rights? Is there a need for additional protection of freedom of expression on the Internet in response to due restrictions in practice? What has been the role of the Council of Europe and other international organisations in this respect? What principles and general guidance can be derived from the emerging case law of the European Court of Human Rights in this respect?

In Chapter 2 we present freedom of expression and its many dimensions as key human rights on the Internet. Based on Article 10 of the European Convention on Human Rights (ECHR), we differentiate between the different aspects of freedom of expression on the Internet, including freedom of opinion, freedom of information, freedom of the press and the media, freedom of international communication, artistic freedom and access to the Internet as a right. We also discuss the importance of corollary rights, including association, education, access to knowledge and broadband access.

Freedom of expression is not an unlimited right. Chapter 3 presents possible restrictions of this right, emphasising that any such restrictions need to be provided for by law, in the pursuit of a legitimate aim, and they must be necessary and proportional to the aim pursued. We also contextualise the current case law of the European Court of Human Rights and analyse the applicability of pre-Internet rulings on modern information and communication technologies, as well as the changes in social mores they engender.

In Chapter 4 we evaluate the standard-setting activity of the Council of Europe in the field of freedom of expression and the Internet, and give an overview of the guidelines and recommendations the Council has developed. We also analyse their impact in practice and present standard-setting activities by non-state actors. These include, to name just two, the Internet Rights and Principles Coalition, with their Charter on Human Rights and Principles for the Internet, and the Global Network Initiative.

In Chapter 5 we break down the universe of freedom of expression into a number of galaxies. We consider, *inter alia*, the need for content regulation, the right to Internet access as a precondition for freedom of expression, and the important principles of technological neutrality of human rights norms along with network neutrality, which together increase the protection of freedom of expression online. We then turn to some elementary characteristics of protected and unprotected speech online before focusing on the fight against hate speech and the balance to be struck between the right to reputation and freedom of expression.

Importantly, we also show why children and young people need special protection on the Internet. The diversity of the challenges associated with protecting freedom of expression online can be seen in our analysis of the role of domain names as instruments to express one's opinion. Internet Service Providers have become important actors both because they can regulate content and because states increasingly use them to police expressions. We therefore

devote a case study to the role of Internet intermediaries as gatekeepers of Internet-based information flows and communication networks. We conclude Chapter 5 with a look into the future, querying whether privately owned communicative spaces are becoming public forums.

Chapter 6 allows a close look at best practices on the national level with regard to, *inter alia*, the right to Internet access, filtering, blocking and the regulation of Internet Service Providers.

In Chapter 7 we analyse European monitoring mechanisms for violations of freedom of expression that aim to fulfil the main objective of the Council of Europe's Internet Governance Strategy, maximising the rights of, and freedoms for, Internet users.[13] We also consider the role of civil society watchdogs and hotlines for the protection of freedom of expression online.

In Chapter 8 we study how international organisations promote freedom of expression in the context of their activities. The Council of Europe, the EU, the OSCE, UNESCO and other international organisations have made important contributions and commitments to implementing a human rights-based approach to the Internet within the ambit of their work.

The concluding Chapter 9 offers our key insights and lessons regarding freedom of expression. We assess the standards that have been developed, analyse their effectiveness and create strategies to increase their positive impact on freedom of expression.

Finally, the executive summary contains our study's key points.

Paul Chambers, the unhappy passenger we mentioned at the beginning, was lucky. In the end, the Lord Chief Justice quashed the lower court's conviction and ruled, *inter alia*, that users "are free to speak not what they ought to say, but what they feel".[14] This is, of course, not the last word on the subject. After a number of prosecutions related to Twitter, the director of the UK Crown Prosecution Service, the agency responsible for deciding whether to try social media users, admitted that:

> [s]ocial media is a new and emerging phenomenon raising difficult issues of principle, which have to be confronted not only by prosecutors but also by others including the police, the courts and service providers. The fact that offensive remarks may not warrant a full criminal prosecution does not necessarily mean that no action should be taken. In my view, the time has come for an informed debate about the boundaries of free speech in an age of social media.[15]

13. Committee of Ministers (15 March 2012), *Internet governance: Council of Europe strategy 2012-2015*, CM(2011) 175 final, para. 5.
14. *Paul Chambers v. DPP* (27 July 2012), [2012] EWHC 2157.
15. Keir Starmer QC (20 September 2009), Director of Public Prosecutions, Crown Prosecution Service, *DPP statement on Tom Daley case and social media prosecutions*, at www.blog.cps.gov.uk/2012/09/dpp-statement-on-tom-daley-case-and-social-media-prosecutions.html.

Safeguarding freedom of expression is intrinsically difficult and raises a number of legal and ethical questions, as well as social and political challenges, and opens up cultural and economic dimensions that have to be taken into account. The ambiguities have been aptly illustrated by the WikiLeaks case. While the US has a much more open approach to whistle-blowing in general than does Europe, its reaction to WikiLeaks was framed primarily in national security terms. Similarly, the US has identified cyber attacks and hacking as key challenges to national security, but it supports civil society (which often includes hackers) in other countries as part of its Internet freedom policy.

It is the goal of this book to provide the background necessary for an informed debate on freedom of expression in the age of the Internet, to show its importance, extent and limits, and to develop strategies for how best to safeguard this enabling right in a human rights-based information society for all.

A note to readers: we have endeavoured to include online sources so as to ensure maximum information value. Yet the Internet's very nature is dynamic – and so are, very often, website addresses. All websites in this book were last accessed on 1 May 2013.

2. The content of freedom of expression online

Freedom of expression and information is the key human right of the information society.[16] This chapter presents Article 10 of the European Convention on Human Rights (ECHR) in its role of ensuring freedom of expression online; the next chapter analyses how that right can be legitimately restricted. Article 10 paragraph 1 of the ECHR reads:

> 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.

In a similar way, Article 19 of the 1948 Universal Declaration of Human Rights (UDHR) of the United Nations states that:

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

Accordingly, freedom of expression as a human right consists of several elements: freedom of opinion, freedom to express one's opinion – also called "freedom of expression" – and freedom of information. From these rights together the "freedom of the press" and the "freedom of the media" can be derived, whereas a proposed freedom of international communication has not found general support.

2.1. Main elements of the right

The right to freedom of expression covers any kind of expression, whether oral or written, including journalistic freedoms, whether that journalism is in print or online, and all forms of art. We are reminded of this broad reach by Article 19 paragraph 2 of the International Covenant on Civil and Political Rights (ICCPR), which states the right to freedom of expression along the lines of Article 19 of the UDHR. In the case of the ECHR, we can look to the elaborate jurisprudence of the European Court of Human Rights. The Court has made it clear already in *Handyside* that information or ideas which "offend, shock or disturb the state or any sector of population" are covered

16. Benedek W. (2013), "Menschenrechte in der Informationsgesellschaft" [Human Rights in the Information Society] in Schüller-Zwierlein A. and Zillien N. (eds), *Informationsgerechtigkeit*, De Gruyter, pp. 69-88 and Verpeaux M. (2010), *Freedom of Expression*, Council of Europe.

by freedom of expression.[17] This is not to say that mainstream ideas deserve less protection; it is simply that they need it less.

As a result of the potential of the Internet as an interactive and global medium, freedom of expression has gained much importance. At the same time, the human rights obligations which states have entered into have gained new dimensions.[18] Although this could not be foreseen at the drafting of the Convention or of other human rights instruments, the formulation "through any media" in the Universal Declaration makes the right a dynamic one: a right that is not limited to certain technologies known at the time of drafting or adoption. It does not matter that this wording has not been included in the ECHR, as the absence of a reference to any specific media implies that no forms of media are excluded. Thus the provision applies to any media. The Court regularly refers to its interpretation of Article 10 "in the light of present-day conditions".[19] The Internet, of course, greatly influences today's "conditions" of communicating. Thus, cases related to the Internet clearly fall within the ambit of Article 10. Because of the nature of the Internet as a new medium allowing for global information and opinion exchange, specific questions emerge, in particular with regard to possible limitations of the right foreseen in Article 10 paragraph 2 ECHR and in Article 19 paragraph 3 ICCPR, respectively. These are discussed in Chapter 3.

According to the established case law of the European Court of Human Rights, "freedom of expression constitutes one of the essential foundations for a democratic society and one of the basic conditions for its progress and for each individual's self-fulfilment".[20] Consequently, freedom of expression, and especially freedom of expression exercised through new media in new democracies, has been called the "oxygen of democracy".[21] If freedom of expression is the oxygen of democracy then the Internet is the atmosphere, where people are living, breathing and exercising their freedom of expression.

The human right to freedom of expression is traditionally directed against state authorities, who might control or censor expression. It is, however, also very important by way of its horizontal effects for private authorities like media owners, intermediaries, Internet Service Providers and the like, which also need to respect, protect and ensure freedom of expression. Accordingly,

17. *Handyside v. UK* (7 December 1976), application No. 5493/72, para. 49.
18. Cuceranu D. (2008), *Aspects of regulating freedom of expression on the Internet*, Intersentia, p. 179 et seq.
19. E.g. *Stoll v. Switzerland* (10 December 2007), application No. 69698/01, para. 104 with further references.
20. Ibid., para. 101.
21. Freedom of expression and information is the oxygen of democracy – say Council of Europe leaders at meeting of Council of Europe, European Union and OSCE leaders on promoting and reinforcing freedom of expression and information at the pan-European level in Luxembourg (1 October 2002), Institute of Mass Information, http://imi.org.ua/en/node/35589.

there is a positive obligation for member states to protect individuals against restrictions of freedom of expression by private persons or institutions.[22] For this purpose, internal statutes of journalists have been created to ensure the exercise of their freedom of expression. However, problems remain due to economic interests and political interference.

According to the principle "what applies offline also applies online", these elements are also relevant in the digital environment as "digital rights". For example, the Court in its case law applies the same principles to the interpretation of Article 10 in online as in offline cases. However, this does not prevent it from carefully considering the specificities of the Internet. It can be expected to "make necessary adjustments in the application of existing principles, in order to take the particular nature of the Internet, especially in terms of ability to magnify the impact of problematic speech", into account.[23] In particular, the factors of impact, accessibility, durability and asynchronicity of information on the Internet are part of its specificity, which the Court takes into account in its case law.[24] For example, the availability of the information is not synchronous with its publication, but any time thereafter.

In *Editorial Board of Pravoye Delo and Shtekel v. Ukraine*, the Court emphasised the distinctness of the Internet from the printed media regarding its capacity to store and transmit information:

> The electronic network serving billions of users worldwide is not and potentially cannot be subject to the same regulation and control. The risk of harm posed by the content and communications on the Internet to the exercise and enjoyment of human rights and freedoms, particularly the respect for private life, is certainly higher than that posed by the press. Therefore, the policies governing reproduction of material from the printed media and the Internet may differ. The latter undeniably have to be adjusted according to the technology's specific features in order to secure the protection and promotion of the rights and freedoms concerned.[25]

Because of the relatively recent emergence of the Internet and the length of procedures in the European Court of Human Rights, only a few cases dealing with restrictions of freedom of expression online have been decided. In other cases, the Court gave attention to the specific nature of the Internet, including its amplifying effect, to which it reacted by establishing a specific balance between freedom of expression and respect for other rights like the rights of

22. *Fuentes Bobo v. Spain* (29 February 2000), application No. 39293/98, para. 38; also *Dink v. Turkey* (14 September 2010), application No. 2668/07 et al., para. 106.
23. Vajic N. and Voyatzis P., "The Internet and freedom of expression: a 'brave new world' and the European Court of Human Rights' evolving case law", in *Freedom of expression, essays in honour of Nicolas Bratza, 2012*, pp. 391-420, at p. 395.
24. Ibid., at p. 399 et seq.
25. *Editorial Board of Pravoye Delo and Shtekel v. Ukraine* (5 May 2011), application No. 33014/05, para. 63.

minors.[26] Also, a first complaint has been filed regarding the right to Internet access as an aspect of freedom of expression by a Lithuanian prisoner wishing to enrol in an online university course. A further case has been decided against Turkey, which had illegally blocked websites.[27] We can expect the number of Internet-related cases to grow significantly once they make their way through the domestic institutions and reach the Court.

An open Internet makes it nearly impossible for states concerned with their sovereignty to control what kind of content, ideas, opinions or information can be accessed or shared by citizens.[28] At the same time, new technologies based on the Internet have been developed which allow states to monitor Internet traffic in the form of connections and content. This has increased the relevance of tools securing the anonymity of the author of content, which again certain states would like to prohibit. These include Virtual Private Networks (VPNs) and anonymisers.[29] This shows that the Internet raises both old and new questions related to the freedom of expression and the right to receive and impart content regardless of frontiers.

Regarding state practice, the Chinese Government is known for its policy of limiting Chinese users' access to information available on the Internet and censoring certain content. China's very effective web of censorship has been dubbed the "Great Firewall". Countries like Iran intend to give their citizens access only to an Iranian intranet, thus blocking them from the World Wide Web. However, European governments also make numerous requests for blocking and filtering, as the biannual Google Transparency Report on removal requests shows.[30] There have also been proposals by governments that Internet users should only have one open IP address, so that all their communications on the Internet can be easily followed, which would have a "chilling effect" on their freedom of expression.

2.1.1. Freedom of opinion

The freedom to hold opinions without interference is an essential part of freedom of expression as guaranteed by the Convention. In both the Convention and the Universal Declaration it is presented together with freedom of expression, while in Article 19 paragraph 1 of the ICCPR it is contained as a separate right. This right is a necessary precondition for freedom of expression, which is about opinions held by individuals or the media. No government may prescribe or prohibit the opinions of individuals.

26. European Court of Human Rights (2011), Research Division, Internet: Case law of the European Court of Human Rights, Council of Europe at p. 10 et seq.; see also Chapter 5.
27. *Jankovskis v. Lithuania*, application No. 21575/08, not yet decided; see also *Yildirim v. Turkey* (18 December 2012), application No. 3111/10.
28. See Mueller, Milton L. (2010), *Networks and states, the global politics of Internet governance*, MIT Press.
29. See on anonymity in the Internet *infra*, at 1.9.
30. Google, *Transparency report*, www.google.com/transparencyreport.

Article 19 ICCPR provides for the possibility of restricting freedom of expression, but not freedom of opinion. For this purpose, any reservations to freedom of opinion would be incompatible with the purpose and objective of this freedom.[31] In the case of the European Convention this separation does not exist, but it is unlikely that possible restrictions could also affect freedom of opinion, for provided that the opinions in question are not expressed, the chances of encountering problems with authorities are slim. In a similar way, the Internet as a medium does not come into play as long as opinions are not expressed. Freedom of opinion on the Internet is thus mainly of relevance as part of freedom of expression.

2.1.2. Freedom of information

The freedom to receive and impart information and ideas "regardless of frontiers" has reached its widest scope through the Internet as a truly global medium for those who have access to it. As the European Court of Human Rights interprets the Convention "in the light of present-day conditions", that interpretation has to take the specific nature of the Internet, as a "modern means of imparting information", into account.[32]

Referring to this dictum, the Court went further in *Yildirim v. Turkey* by stating that the creation and sharing of websites in a group run by Google Sites constitutes a means of exercising freedom of expression,[33] and that Article 10 guarantees freedom of expression for "everyone". These provisions do not concern only the content of the information expressed, but also the means by which it is disseminated. The Court also reiterated its position that Article 10 guarantees not only the right to communicate information, but also the right of the public to receive it.[34] As the Court held in *Mouvement Raëlien Suisse v. Switzerland*, the impact of the information is multiplied when it is displayed in public with a reference to the address of a website that is accessible to everyone through the Internet.[35]

The possible need for a licence for broadcasting, television or cinema enterprises, foreseen in Article 10 ECHR but not in Article 19 ICCPR, does not apply in online cases, although there have been efforts by states to extend these provisions to the Internet. In the case *Megadat.com SRL v. Moldova*,[36] a company which used to be the largest Internet service provider in Moldova complained about the withdrawal of its Internet and telephone service

31. Cf. Human Rights Committee (12 September 2011), General Comment No. 34, CCPR/C/GC/34, para. 5.
32. *Mouvement Raëlien Suisse v. Switzerland*, First Section (13 January 2011), application No. 16354/06, para. 54 as endorsed by the Great Chamber judgment in para. 40.
33. *Yildirim v. Turkey* (18 December 2012), application No. 3111/10, para. 49.
34. Ibid., para. 50.
35. *Mouvement Raëlien Suisse v. Switzerland*, para. 54.
36. Cf. *Megadat.com SRL v. Moldova* (8 April 2008), application No. 21151/04, para. 63.

licences, which was justified on flimsy grounds. The Court found this to be a violation of Article 1 of Protocol 1, the right to property, because the interference by the authorities was disproportionate to the goal pursued.

In *Appleby and Others v. the United Kingdom*, which related to the prohibition of setting up stalls for the distribution of leaflets in a privately owned shopping centre, the Court held that it would not exclude that "a positive obligation could arise for the state to protect the enjoyment of the Convention rights by regulating property rights", where "the bar on access to property has the effect of preventing an effective exercise of freedom of expression or it can be said that the essence of the right has been destroyed".[37] This observation may gain relevance in the context of monopoly-like Internet service providers which, according to their terms of service, are free to deny their services for any reason – or indeed for no reason, as in the case of stablish.me or Googlemail accounts, which Google may terminate at any time.[38] In such cases, the authorities could legitimately stipulate that a minimum period of access to such services has to be provided, if a clear case for the monopolistic role can be made.

Freedom of information also includes the freedom of the public to be informed,[39] which is partly assured by a free press and autonomous media, as is the dissemination of information, including reporting about hate speech.[40] In this context, the question of access to the Internet is of overarching importance for the full enjoyment of freedom of expression today, for both receiving and sharing information and ideas. Therefore, the Council of Europe, in its various resolutions, declarations and statements on standard-setting (discussed further in Chapter 4) and promotion (Chapter 8), has emphasised the importance of Internet access. Increasingly, the right to access is considered as an emerging human right in itself, because of the crucial role it plays in ensuring the enjoyment of other human rights, in particular freedom of expression, as we show at the end of this chapter and in Chapter 5.

2.1.3. Freedom of the press and the media

The freedom of the press and the media is one of the core liberal rights. A free press and autonomous media are considered cornerstones of any democratic society. A critical media is essential for furthering public discourse on the big questions a society faces, and it thus fulfils a "democracy-fostering

37. *Appleby and Others v. the United Kingdom* (6 May 2003), application No. 44306/98. On a positive obligation to protect the exercise of freedom of expression see also Reid K. (2007), *A Practitioner's Guide to the European Court of Human Rights*, Sweet & Maxwell, p. 365.
38. See Terms of Service of stablish.me at www.stablish.me/index/terms-of-reference; see also Google, Terms of Service, www.google.com/intl/en/policies/terms.
39. See *Bergens Tidende* (2 May 2000), application No. 26132/95, para. 49; and *Observer and Guardian* (26 November 1991), application No. 13585/88, para. 59.
40. *Jersild v. Denmark* (23 September 1994), application No. 15890/89, para. 35.

function".[41] In providing a forum for public discourse, and then contributing to public debate, the free press has an important monitoring and accountability function. This function presupposes that journalists have a right of access to public information.[42]

Freedom of expression includes a strong protection of journalistic activities. In the context of online journalism, the Court made clear in *Editorial Board of Pravoye Delo and Shtekel v. Ukraine* that the absence of a sufficient domestic legal framework on how to use information obtained from the Internet seriously hinders the ability of the press to exercise its vital function as a public watchdog. The exclusion of such information from the legislative guarantees of journalistic freedom was considered to constitute potential unjustified interference with press freedom under Article 10.[43] From this judgment the positive obligation to create an appropriate regulatory framework to effectively protect freedom of online expression for journalists can be derived.[44] In coming to this finding, the Court referred *in extenso* to Recommendation CM/Rec(2007)16 of the Committee of Ministers on measures to promote the public service value of the Internet,[45] according to which member states should elaborate a clear legal framework on the roles and responsibilities of all key stakeholders in new ICTs, while the private sector was encouraged to develop open and transparent self- and co-regulation, allowing key actors to be held accountable.[46]

In *Editorial Board of Pravoye Delo*, the Court also referred to the 2005 Joint Declaration of the Special Rapporteurs on freedom of expression, which stressed the need to apply international guarantees of freedom of expression to cases involving the Internet. The declaration also emphasised that "no one should be liable for content on the Internet of which they were not the author, unless they had either adopted that content as their own or refused to obey a court order to remove that content"[47] – a statement which is of particular relevance to the responsibility of Internet service providers.

In *Times Newspapers Limited v. United Kingdom* (Nos. 1 and 2), the Court recognised the importance of the Internet for freedom of information when it held that "[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

41. Harris, O'Boyle and Warbrick (2009), *Law of the European Convention on Human Rights*, OUP, p. 465.
42. *Lingens* (8 July 1986), application No. 9815/82, para. 41.
43. *Editorial Board of Pravoye Delo and Shtekel v. Ukraine* (5 May 2011), application No. 33014/05, para. 64.
44. Cf. European Court of Human Rights (2011), Research Division, *Internet: Case law of the European Court of Human Rights*, 11.
45. Ibid., para. 29 et seq.
46. See this and other resolutions and recommendations of Council of Europe bodies in Chapter 7.
47. Cf. International Mechanisms for Promoting Freedom of Expression (21 December 2005), Joint declaration; see also 5.10 The role of Internet intermediaries in Chapter 5.

generally".[48] In view of frequent attacks on and persecution of journalists, in particular in conflict zones, this has been reconfirmed by a resolution of the UN Human Rights Council on the safety of journalists.[49] In this context, the Council refers to its past resolutions on the right to freedom of opinion and expression, in particular the July 2012 resolution on the protection and promotion of human rights on the Internet, including freedom of opinion and expression.[50] It also expresses its concern that violations of the right to freedom of opinion and expression continue and include increased attacks against and killings of journalists and media workers, which it condemns in the strongest terms. It also mentions the growing threat to the safety of journalists from non-state actors, including terrorist groups and criminal organisations. It calls on states to promote a safe and enabling environment for journalists to perform their work independently and without undue interference.[51]

In their annual joint resolution of 2012, the special rapporteurs on freedom of expression from the UN, the Organization for Security and Co-operation in Europe (OSCE), the Organization of American States (OAS) and the African Commission on Human and Peoples' Rights (ACHPR) called on governments to create a special category of "crimes against free expression". Their major concern was violence against journalists, which they called "censorship by killing", and they condemned the prevailing state of impunity for crimes against free expression.[52] The UN Special Rapporteur on the right to freedom of opinion and expression focused in his 2012 report on these challenges faced by journalists in their work when reporting on sensitive issues or in a dangerous environment, in particular via the Internet.[53] Meanwhile in 2008, the Parliamentary Assembly of the Council of Europe had adopted a resolution on the indicators for media in a democracy, which also dealt with the safety of journalists.[54] The better protection of journalists has also been the topic of a recommendation by the OSCE[55] and, in the framework of UNESCO, a UN Plan of Action on the Safety of Journalists and the Issue of Impunity has been elaborated.[56]

48. *Times Newspapers Limited v. the United Kingdom* (10 March 2009, final 10 June 2009), application Nos. 1 and 2, Nos. 3002/03 and 23676/03, para. 27.
49. Human Rights Council (27 September 2012), *Resolution on the safety of journalists*, application No. 21/12, A/HRC/21/L.6.
50. Cf. Human Rights Council Resolution 12/16 (2 October 2009), Resolution 13/24 (26 March 2010) and, in particular, Resolution 20/8 (5 July 2012).
51. Ibid.
52. Cf. IFEX (27 June 2012), *Special rapporteurs call for a "crime against freedom of expression"*, www.ifex.org/international/2012/06/27/free_expression_crime.
53. Report of UN Special Rapporteur, UN GA Doc. A/HRC/20/17 (4 June 2012); also his 2011 report (see n. 60).
54. See Council of Europe, Parliamentary Assembly (3 October 2008), Resolution 1636 (2008) on "Indicators for media in democracy" and Recommendation 1848 (2008) on the same topic to the Committee of Ministers.
55. OSCE, The Representative on Freedom of the Media (8 June 2011), *Vilnius recommendations on safety of journalists*, OSCE-doc. C10. GAL/111/11.
56. UNESCO (2012), *The international programme for the development of communication*.

Generally, journalistic freedoms cover journalistic research, protection of sources, access to public meetings and the publication of confidential information, even if it has been illegally received.[57] The Internet has also created the new phenomenon of "citizen journalists", who report from all corners of the world, in particular from zones of war and disturbances where conventional journalists have no access. They report human rights violations as they happen, often with pictures and videos, in places like Syria in 2012/13 or in situations like the riots in the United Kingdom in 2011.[58] They carry no journalist's card, are not members of press clubs and do not benefit from the protection and privileges that regular journalists can enjoy. They might be "journalists" only at the moment when they publish text, pictures or videos for public consumption. Furthermore, "bloggers" fulfil a similar function to journalists when they discuss topics of concern in their blogs, which can hardly be controlled; indeed they may be persecuted by the authorities for this very reason. This raises the question of protection of citizen journalists in their freedom of expression.

There is, however, also the problem of the quality of the news provided by persons who have no professional training. This raises the issue of extending basic principles not only of journalistic freedom but also journalistic responsibility to these "functional journalists", who, when they engage in this activity, should also follow basic ethical standards, which are mainly a matter of digital awareness and learning. Some claim that, in order to benefit from the status of journalists, these persons should announce their readiness to meet the higher due diligence standards of the profession.[59] The UN Special Rapporteur on the right to freedom of opinion and expression has emphasised the importance of this new form of journalism for a richer diversity of views and opinions, as well as its critical watchdog role in countries where freedom of expression is lacking, and he regularly intervenes on behalf of citizen journalists in his recommendations to governments. However, he also encourages these persons to respect professional and ethical standards.[60]

The resolution on the safety of journalists by the Human Rights Council does not give any definition of journalists.[61] The term thus includes citizens, journalists and bloggers. Also non-governmental organisations (NGOs) can benefit from the freedom of the press as "social watchdogs" in the more dynamic blog-based publication landscape of the Internet age.[62] With protection

57. Karpenstein, Mayer (2012), *EMRK-Kommentar*, C.H. Beck, Munich, Article 10, para. 15.
58. Benedek W. and Rao M. (2013), *Background paper,* 12th Informal ASEM Seminar on Human Rights, "Human rights and information and communication technology" in Seoul 27-29 June 2012, ASEM, Singapore, 50 et seq.; see also Quinn S., "Mobile Journalism" (2013), in Bruck P. and Rao M., *Global mobile: scenarios and strategies*, Information Today Inc., Medford NJ.
59. Cf. Kulesza J. (2012), *International Internet law*, Routledge, p. 52.
60. La Rue F. (11 August 2011), *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, UN Doc. A/65/284, para. 61 et seq.
61. Cf. *supra*, note 49.
62. *Társaság a Szabadságjogokért v. Hungary* (14 April 2009), application No. 37374/05, para. 27.

comes responsibility: if non-traditional journalists are to be protected like conventional journalists, they should also observe the same ethical principles and be subjected to the same legal rules.[63] In *Stoll v. Switzerland*, the Court declared that "all persons, including journalists, who exercise their freedom of expression, undertake 'duties and responsibilities', the scope of which depends on their situation and the technical means they use".[64] Accordingly, journalists enjoying the safeguard of Article 10 when reporting on issues of general interest are expected to act in good faith and "provide reliable and precise information in accordance with the ethics of journalism".[65] The importance of monitoring compliance with journalistic ethics standards will grow in "a world, in which the individual is confronted with vast quantities of information circulated via traditional and electronic media monitoring".[66]

2.1.4. Freedom of international communication

A freedom of international communication was proposed in the context of the discussion on a "new world information and communication order" in the 1970s.[67] In 2003, in preparations for the World Summit on the Information Society (WSIS), a draft declaration on the right to communicate was presented.[68] The Council of Europe subsequently adopted a Declaration on freedom of communication on the Internet.[69] The basic idea was that freedom of expression was too limited to cover all aspects of global communication, and a right to communication could have a wider focus, covering in particular interactive communication. The idea of such a right proved controversial, mainly due to the fear expressed by NGOs that it could undermine achievements in the field of freedom of expression.

It was argued that there was no real need to introduce this new right as the existing human right to freedom of expression, as contained in Article 10 ECHR or Article 19 ICCPR, already covered all aspects. Where gaps were identified – as in the communication sector's freedom from state regulation, or a right to self-regulation, which is also of potential relevance to the

63. Cf. White A. (2013), "Who should follow journalism ethical standards in the digital era?", in OSCE, The Representative on Freedom of the Media, *The online media self-regulation guidebook*, Vienna, pp. 63-9.
64. Cf. *Stoll v. Switzerland*, para. 102.
65. Ibid., para. 103.
66. Ibid., para. 104.
67. Harms L. S., Richstad J., Kie K. (eds) (1977), *The right to communicate: collected papers*, University of Hawaii Press, Honolulu; and Fisher D., Harms L. S. (eds) (1983), *The right to communicate: a new human right*, Boole Press, Dublin.
68. Cf. Hamelink C. J. (2003), *Draft declaration on the right to communicate*, Amsterdam/Geneva, www.article19.org/data/files/pdfs/analysis/hamelink-declaration-the-right-to-communicate.pdf.
69. Council of Europe (28 May 2003), Council of Ministers' Declaration on freedom of communication on the Internet.

Internet – these too could be addressed by existing human rights by way of functional interpretation of the freedom of expression.[70]

A human right to communication would provide little additional value, in particular if it had first to be recognised by states, which are anxious to protect their national sovereignty and not inclined to accept new obligations. In the end, therefore, the discussion of a human right to communicate did not result in the recognition of such a right, but it inspired dialogue on the extent to which the right to freedom of expression is covered in existing instruments.

The right to respect for one's communications, as recognised by Article 7 of the European Union's Charter of Fundamental Rights, is limited to the context of private and family life, and therefore focuses on protecting individuals' communications. Mass communications are covered by Article 11 on the freedom of expression and information, which ensures the right to hold opinions and to receive and impart information and ideas, without interference by public authority, regardless of frontiers; paragraph 2 specifies that the freedom and pluralism of the media shall be respected.

2.1.5. Freedom of artistic expression

Article 19 of the ICCPR explicitly confirms that freedom of expression "in the form of art" enjoys the same level of protection as other forms, whereas Article 10 of the ECHR remains silent on the subject. However, Article 10 is understood to include the protection of freedom of artistic expression, or "creative expression" and "cultural expression".[71]

The European Court of Human Rights considers that the creation and distribution of artistic works contributes greatly to the exchange of ideas and opinions, and as such is an essential component of any democratic society. Art can "confront the public with the major issues of the day".[72] Accordingly, artists' work is covered by the freedom of expression, as are the activities of galleries or cinemas.[73] Balancing different rights can become difficult with regard to freedom of artistic expression. For example, the European Court on Human Rights found that the freedom of expression, including artistic, can override the right of individuals to images of themselves.[74]

---

70. Jørgensen R. F. (2013), *Framing the net, the Internet and human rights*, Edward Elgar, and Schmalenbach K. (2007), "Ein Menschenrecht auf Kommunikation: Erfordernis oder Redundanz?", in Benedek and Pekari (eds), *Menschenrechte in der Informationsgesellschaft*, Boorberg, Stuttgart, pp. 183-213, at 212.
71. Grabenwarter C. and Pabel K. (2012), *Europäische Menschenrechtskonvention*, 5th edn, C. H. Beck, p. 307.
72. *Müller and others v. Switzerland*; see also *Otto-Preminger-Institut v. Austria* (20 September 1994), application No. 13470/87.
73. Cf. *Verpeaux* (2010), p. 213 and *Grabenwarter* (2012), p. 312.
74. *Müller and others v. Switzerland* (24 May 1988), application No. 10737/84.

The relevance of artistic freedom to freedom of expression on the Internet is obvious, as it can open up access to works of art, including art not supported by official networks because of its perceived lower quality or lesser renown. The Internet is a great equaliser in terms of access and thus allows access to art that is not mainstream. The restrictions explained in the next chapter, which are possible on the national level, can easily be circumvented through the global Internet.

An example is the video clip produced in the US on the Prophet Mohammed, presenting him in a way which offended the religious feelings of Muslims. The issue went global when the movie trailer appeared on YouTube, and therefore became accessible everywhere.[75] However, it can be argued that the film was not conceived as a piece of art, but rather as a mere provocation without any of the redeeming social value that characterises actual art. Some states like Pakistan asked YouTube to block users' access to the film clip, but most took no measures against it. YouTube blocked the movie trailer in some countries, but not in Pakistan. The Pakistani Prime Minister, in return, ordered YouTube to be blocked altogether until the film clip had been removed.[76] YouTube explained the ban in countries like Egypt and Libya by the fact that the trailer had led to violence there, apparently ignoring the violence which it had created in Pakistan.[77] Google, as the owner of YouTube, also rejected a request from the White House to pull the Mohammed clip. The explanations given by Google are not satisfactory and clearly show the problem of navigating between different perceptions of legitimate restrictions globally.

The emancipatory potential of the Internet notwithstanding, online resources can also fuel conflicts that would have remained localised before the digital age. When the Danish newspaper *Jyllands Posten* published cartoons showing the Prophet Mohammed, they quickly found their way to other countries, over the Internet, and through activism by Islamists, and were used for inflammatory purposes.

In such cases, which involve a conflict of human rights – in this case freedom of expression v. freedom of religion – different margins of appreciation appear to be necessary in order to avoid serious violations of religious feelings that might lead to violence. Political authorities need to be careful to find a balance between sacrificing freedom of expression to extremism and avoiding violence. The private sector cannot alone take responsibility for such decisions.

75. The video clip on the film "The innocence of Muslims" had been produced in the US by a Coptic Christian.
76. See "Anti-Prophet Muhammed film: Pakistan blocks YouTube as two killed in violence", *The Times of India* (17 September 2012).
77. Pakistan blocks YouTube as two killed in Anti-Prophet Mohammed film, www.youtube.com/watch?v = z1LONsTyCMY.

2.1.6. Freedom of cultural expression

With the right to cultural diversity, a new right has emerged. It poses new challenges to the media and to business ("creative industries"), challenges which have been taken up in particular by UNESCO.[78] The UNESCO Convention on the Protection and Promotion of the Diversity of Cultural Expressions of 2005 puts cultural expression in the category of freedom of thought, expression and information. It explicitly refers to the rapid development of information and communication technologies which allow for enlarged interaction between cultures, and UNESCO's mandate to promote the free flow of ideas by word and image. The Convention aims to promote and respect cultural expression, as stemming from the creativity of individuals, groups and societies, but cautions that the exercise of cultural expression, including by cultural industries, must not infringe human rights and fundamental freedoms.[79]

The rights are mainly defined as limited to the territory of states but international co-operation should be promoted, including the use of new technologies.[80] In practice, this means that cultural expression can be permitted globally if it does not violate the human and fundamental rights of others. The Internet, however, increases the possibility of conflicts, for example, if certain cultural expressions are claimed by more than one state (or groups within states) as part of their own culture.

Cultural and linguistic diversity has also been given particular attention in WSIS documents.[81] This diversity allows promotion of cultural identity and preservation of cultural heritage. The Geneva Declaration considers cultural diversity as a "common heritage of mankind".[82] The diversity of languages is particularly relevant to this, in online content but also in alphabets and characters used for domain names and e-mail addresses in different languages. In this regard, the internationalisation of domain names and the introduction of non-Latin scripts to the Internet naming space are positive developments. Multilingualism promotes linguistic empowerment and helps to overcome the linguistic divide that is part of the digital divide.[83]

78. Frau-Meigs D. (2011), *Media matters in the cultural contradictions of the "information society" – Towards a human rights-based governance*, Council of Europe, p. 189 et seq.; see also on UNESCO in Chapter 8.
79. Cf. UNESCO (2005), Convention on the Protection and Promotion of the Diversity of Cultural Expressions, Preamble, Articles 1 and 4.
80. Ibid., Articles 6, 7 and 12 et seq.
81. Cf. Geneva Declaration of Principles, para. 52 and the Tunis Commitment, para. 32. See also on UNESCO in Chapter 8.
82. Geneva Declaration of Principles, para. 52.
83. Cf. Benedek and Rao (2012), *Background paper,* 12th Informal ASEM Seminar on Human Rights, "Human rights and information and communication technology", 27-29 June 2012, ASEM, Singapore, p. 71 et seq.

2.1.7. Freedom of science

Freedom of expression also includes freedom of science, although this is not specifically mentioned in the ECHR or the ICCPR. It comes under their protection of freedom of expression, which includes the freedom "to hold opinions and to receive and impart information and ideas without interference". It covers teaching, research and publication,[84] including value judgments on deficits in the academic system, and scientific conferences.[85]

Academic freedom and institutional autonomy are also supported by various UNESCO recommendations, in particular the recommendation on the Status of Higher Education Teaching Personnel.[86] In light of new media, academic freedom raises new challenges. While academic work had a global dimension before, the Internet has significantly increased access to scientific information and the possibilities for distribution of academic opinions and scientific results – which are not always welcome to states or private institutions. Therefore, the relevance of academic freedom as part of freedom of expression increases with the new communication tools and dimensions the Internet provides.

2.1.8. A new freedom? Internet freedom and openness

The Internet has brought new opportunities and challenges for the freedom of expression. Does this mean that freedom of expression on the Internet can be considered a new freedom? No, because the clarification "by any other media" contained explicitly in Article 19 ICCPR of 1966 and implicitly in Article 10 ECHR of 1950, and the subsequent jurisprudence of the Court, shows the openness of freedom of expression to technological and social innovation.

The Internet is characterised by the freedom and openness it offers to its users. Its history provides an account of the defence of this freedom against efforts from various sides, public and private, to limit it, and the struggle is ongoing. John Perry Barlow, an Internet activist, issued a declaration on the independence of the Internet as long ago as 1996, in which he emphasised the open and free character of the Internet.[87] Many NGOs follow his example and focus on the defence of Internet freedom, like the Electronic Frontier

84. *Lombardi Vallouri v. Italy* (20 October 2009), application No. 39128/05, para. 30 d; *Wille v. Liechtenstein* (28 October 1999), application No. 28396/95, para. 8, 36 et seq. See also Grabenwarter (2012), p. 312.
85. *Sorguc v. Turkey* (23 June 2009), application No. 17089/03, para. 35 et seq.
86. Cf. UNESCO (11 November 1997), Recommendation concerning the status of higher education teaching personnel.
87. Barlow J. P., *A declaration of the independence of cyberspace*, http://w2.eff.org/Censorship/Internet_censorship_bills/barlow_0296.declaration.

Foundation based in Canada, which Barlow heads.[88] Efforts to define the main principles of Internet governance regularly mention the principle of openness and the freedom of expression.[89]

The WSIS has specifically reaffirmed Article 19 of the UDHR in its Geneva Declaration of Principles,[90] but the declaration also reproduces Article 29 of the UDHR, which mentions the existence of duties and limitations in its next paragraph.[91] The Tunis Commitment of 2005, a document which came out of the second phase of the WSIS process, reaffirms the importance of the UDHR for the Information Society without referencing any particular rights.[92]

2.1.9. Right to anonymity

Anonymous (or pseudonymous) expression has a long tradition in the written press, among authors of books and critical reports, such as whistle-blowing. Anonymity on the Internet is therefore considered a part of freedom of expression. This has also been confirmed by the Special Rapporteur on Freedom of Opinion and Expression, in his report of 2011.[93] The problems that may come with anonymity, like defamation or online stalking, but in particular anonymous critiques of government action by whistle-blowers, can be irritating for governments. Some try to deal with anonymity by imposing obligations of registration or the use of special software. For example, people using cyber cafés in Iran have to register, and private service providers like comment pages of newspapers require registration. Social network services, such as Facebook, also insist on knowing the identity of their users.

Facebook has a real-name policy that went as far as deleting the account of the writer Salman Rushdie (of *Satanic Verses* fame), because that was a nom de plume and his real full name was Ahmed Salman Rushdie. They then changed the name on his profile to "Ahmed Rushdie". Such a policy can have a chilling effect on freedom of expression. Salman Rushdie took to Twitter and implored Facebook to give him back his name. In only "1 hour and 30 minutes" he managed to get the change reversed. As a commentator

88. See Electronic Frontier Foundation, www.eff.org/about.
89. Council of Europe, Committee of Ministers (21 September 2011), Declaration by the Committee of Ministers on Internet governance principles, http://wcd.coe.int/ViewDoc.jsp?id=1835773.
90. Cf. WSIS (12 December 2003), Declaration Principles, UN Doc. WSIS-03/GENEVA/DOC/4-E, para. 4.
91. Ibid., para. 55.
92. WSIS (18 November 2005), Tunis Commitment, UN Doc. WSIS-05/TUNIS/DOC/7-E, paras. 2 and 3.
93. Cf. La Rue F. (16 May 2011), *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, UN Doc. A/HRC/17/27, para. 84.

aptly put it: "Something tells me this would not have been possible if Rushdie didn't have over 115 000 followers."[94]

There is a danger that, by addressing illegal speech under the veil of anonymity, the right to anonymity online as part of freedom of expression may be undermined. Accordingly, any restrictions need to respect the criteria of Article 10 of the ECHR developed in the practice of the European Court of Human Rights.

2.1.10. Right to whistle-blowing

The practice of whistle-blowing is generally supported, even by certain governments, as a way to identify shortcomings in business or government and thus beneficial to a functioning democracy, for example by exposing corrupt practices. The Parliamentary Assembly, in its resolution of 2010 on protection of whistle-blowers, recognised the contribution of whistle-blowers in the fight against corruption and mismanagement.[95]

To use the freedom of expression in this way can also be controversial, for example when state secrets are at stake, as in the case of WikiLeaks. As there is hardly any way to fully prevent classified information being published on the Internet, it is a matter of responsibility where to draw the line. For example, to publish information on the Internet that might put the lives of dissidents or diplomats in danger might be disproportionate to the objective of revealing malpractices. However, the NGO Article 19 and others have rightly criticised measures taken by companies like Paypal, Amazon and EveryDNS.net to disable WikiLeaks' basis of operation, as these are also restrictions of freedom of expression.[96]

The jurisprudence of the European Court of Human Rights in whistle-blowing cases, such as *Heinisch v. Germany*,[97] can be usefully employed to give guidance. In any case, an outright prohibition of whistle-blowing would unnecessarily restrict freedom of expression online. In *Guja v. Moldova (GC)*, the Court found that the disclosure of confidential information by a civil servant denouncing illegal conduct or wrongdoing at the workplace was protected by Article 10, because of the strong public interest involved.[98]

94. Protalinski E. (15 November 2011), *Facebook name battle: Ahmed Salman Rushdie claims victory*, www.zdnet.com/blog/facebook/facebook-name-battle-ahmed-salman-rushdie-claims-victory/5358.
95. See Council of Europe, Parliamentary Assembly (29 April 2010), Resolution 1729 (2010) on Protection of "whistle-blowers"; see also Recommendation 1916 (2010) to the Committee of Ministers.
96. Cf. Association of Progressive Communications (APC), www.apc.org/en/pubs/briefs/wikleaks-human-rights-whistleblowers-under-attack. See also Chapter 6.
97. *Heinisch v. Germany* (21 July 2011), application No. 28274/08, para. 93.
98. *Guja v. Moldova (GC)* (12 February 2008), application No. 14277/04, para. 72.

2.2. Corollary rights: freedom of assembly and association, right to education and access to knowledge

There are several rights that are closely related to freedom of expression, and we examine three such rights here: the freedom of assembly and association online, the right to (digital) education and the right of access to digital knowledge.

The freedom of online assembly and association guarantees the right to meet on the Internet to exchange views and share opinions, as well as to collectively protest against anything considered undesirable. Anyone may associate with others on the Internet. This includes things like visiting websites or using electronic networks to meet for any legal purpose. Access to assemblies or associations using the Internet must not be subjected to blocking or filtering. Limitations on the right are similar to the ones on freedom of expression (Article 11 paragraph 2 ECHR). The relevance of this right for the freedom of expression is to provide everyone with the means to express his/her views or to seek information collectively by joining others on the Internet, or to take joint action by the means of the Internet.

The Arab Spring has been the most prominent example of the importance of this right. The Egyptian blackout that disabled use of this right has to be considered disproportionate, and could only be sustained by the government for a few days anyway.[99] In the meantime there were other cases of temporary blackouts and the Internet being closed down by governments attempting to stop citizens' activism. In practice, we find that most cases of blocking certain websites or filtering certain content have the same intention. This is legally justified only if it meets the criteria for restrictions of the right indicated in Article 11 paragraph 2 ECHR or in Article 21 ICCPR.

An interesting question is whether distributed denial-of-service (DDoS) attacks are covered by freedom of assembly. Nonviolent assemblies that block streets or, for short periods, the entrance to a specific shop, are recognised as a legitimate form of assembly, as are sit-ins. Using technology to make access to a specific site more difficult has been used as a form of protest as well.[100] However, states are also under the obligation to protect individuals against interference with their freedom of expression by third parties and hold the authors of such attacks accountable, which can result in a difficult

99. Kettemann M. C. (2012), "Das Internet als internationales Schutzgut: Entwicklungsperspektiven des Internetvölkerrechts anlässlich des Arabischen Frühlings" [The Internet as a global object of protection: perspectives on international Internet law in light of the Arab spring], *Heidelberg Journal of International Law 72*, pp. 469-482.

100. Scola N. (13 December 2010), *Ten ways to think about DDoS attacks and "legitimate civil disobedience"*, http://techpresident.com/blog-entry/ten-ways-think-about-ddos-attacks-and-legitimate-civil-disobedience.

balancing exercise.[101] The resilience of the Internet is a common concern to be addressed by multi-stakeholder co-operation.[102]

The right to education is also closely linked to freedom of expression. Its digital dimension includes the right to be educated about the Internet and the right to use the Internet for education. Awareness of possible uses of the Internet ("digital literacy") is a precondition for being able to exercise one's freedom of expression online. Freedom of information, as part of freedom of expression, is served by access to digital publications, teaching and learning platforms. The academic freedoms discussed above also belong to the right of education, contained in Article 2 of the First Protocol of the ECHR of 1952 and Article 13 ICESCR.[103]

A third corollary right, a right of Access to Knowledge (A2K), can be derived from Article 27 of the UDHR, which declares a right to "enjoy the arts and to share in scientific advancements and its benefits". This right is confirmed by Article 15 of the ICESCR and amounts to a right to cultural enjoyment of the Internet. This includes open-access initiatives like digital libraries, open courses and open-access journalism. The corollary to this is that everyone has the right to benefit from the protection of the moral and material interests resulting from any scientific, literary or artistic production of which he or she is an author (Article 15 paragraph 2, ICESCR), which can also be seen as the right to property such as copyright or intellectual property rights in general. Like the right to education, A2K can be a precondition for freedom of expression. Finding the correct balance between A2K and copyright is a key challenge today. Particular issues are raised by access to governmental information, regulated in many countries by Freedom of Information Acts.[104] The definition of public interest is of crucial importance in this context. This is a highly emotive issue and has prompted some of the most energetic activity related to freedom of information.

The institution of copyright is challenged in the digital environment, which allows for uploading of copyrighted content and downloading by users without permission.[105] An NGO called Article 19 organised a meeting of experts in London in December 2012 on the relationship between freedom of expression and intellectual property rights. It considers the licensing of

101. Cf. La Rue F. (16 May 2011), *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, UN Doc. A/HRC/17/27, paras. 51-52.
102. See Council of Europe, *International and multi-stakeholder co-operation on cross-border Internet*, Interim Report of the Ad-hoc Advisory Group on cross-border Internet, Doc. H/Inf (2010) 10.
103. Cf. Benedek W., "Right to education" (2012) in *Manual on human rights education*, 3rd edn, pp. 251-301.
104. Krikorian G. and Kapczynski A. (eds) (2010), *Access to knowledge in the age of intellectual property*, MIT Press.
105. Cf. EDRI, *Copyright: challenges of the digital era*, www.edri.org/files/paper07_copyright.pdf.

digital information as "intellectual property" as problematic for freedom of expression in the digital world. It is therefore now working on "Principles on freedom of expression and copyright in the digital age".[106]

Copyright is an exception to freedom of expression and information; it is meant to preserve the exclusive rights of authors, who should benefit from their work. The music industry in particular fights a fierce battle to maintain this system against what they consider to be little more than modern forms of piracy. In the case of *Neij and Sunde Kolmisoppi v. Sweden* (Neij and Sunde Kolmisoppi being the co-founders of Pirate Bay, one of the Internet's largest file-sharing services for music, films and computer games), the Court found that a criminal conviction and prison sentence were legitimate. They may have been against Article 10 on freedom of expression, but the major violation of Swedish copyright law took precedence.[107]

However, the legal situation differs between countries. For example, Dutch law allows private copy-exceptions for downloading,[108] while the French (Hadopi) law and the Digital Economy Act of the United Kingdom prescribe penalties in cases of illegal downloading which may lead to the user being disconnected. This raises the question of proportionality in penalties, and has resulted in serious concern about freedom of expression. Some countries approach the issue differently. The Austrian Government has for some time considered a general levy on hard disks to compensate authors for losses from illegal downloading, very like existing taxes on copying machines introduced before the dawn of the Internet. Similarly, the European Commission is developing proposals to modernise European copyright protection, with a new directive that could help harmonise divergent national laws and thus ensure more effective protection of both freedom of expression and authors' rights in a creative digital economy.[109]

2.3. Right to access to the Internet

A right to access to the Internet can be derived from the rights discussed above, but it is still controversial with some governments and parts of the interested community. However, access to online information and knowledge is crucial

106. Article 19, *Intellectual property*, www.article_19.org/pages/en/intellectual-property.html; see also its policy brief: *Balancing the right to freedom of expression and intellectual property protection in the digital age*.
107. *Neij and Sunde Kolmisoppi v. Sweden* (19 February 2012), application No. 40397/12, p. 9 et seq; see also 3.2.2 *infra*.
108. Cf. La Rue F. (16 May 2011), *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, UN Doc. A/HRC/17/27, para. 49.
109. European Commission, Press Release (5 December 2012), *Commission agrees way forward for modernising copyright in the digital economy*, http://europa.eu/rapid/press-release_MEMO-12-950_en.htm.

for personal development and the development of societies.[110] The argument for a right of access is that without it people could not fully exercise other rights, particularly freedom of expression but also the right to online assembly or to education. For this very reason, the right of access to the Internet is the first and most fundamental right of the Charter of Human Rights and Principles for the Internet.[111]

In its "Recommendation on the public service value of the Internet" in 2007, the Committee of Ministers of the Council of Europe emphasised that "access to and the capacity and ability to use the Internet should be regarded as indispensable for the full exercise and enjoyment of human rights and fundamental freedoms in the Information Society".[112] However, there are also arguments that hold that the Internet is just a technology that might change and therefore, as in the case of electricity, it is a utility rather than an object to which one can have a right.[113] Some also fear human rights inflation: the declaration of new human rights without corresponding effective protection.[114]

In this context, it is worth noting the concern of the Parliamentary Assembly of the Council of Europe that "[i]ntermediaries of ICT-based media might unduly restrict the access to, and dissemination of, information for commercial and other reasons without informing their users and in breach of user rights".[115]

Governments are often afraid of additional obligations and therefore most of them resist recognising access as a human right. However, numerous governments have provisions in their national (sometimes also constitutional) law providing a right of access to the Internet.[116]

---

110. See Global Information Society Watch (2009), *Focus on access to online information and knowledge – advancing human rights and democracy*, Association of Progressive Communications (APC) and Humanist Institute for Co-operation with Developing Countries (Hivos) Publishers, and subsequent annual editions, www.apc.org/en/node/11030; on access, see also Chapter 5.
111. See Charter of Human Rights and Principles for the Internet, http://internetrightsprinciples.org/site/charter.
112. Council of Europe, Committee of Ministers (7 November 2007), Recommendation on measures to promote the public service value of the Internet, CM/Rec (2007)16.
113. Cf. Cerf V. (4 January 2012), "Google's chief internet evangelist, Internet access is not a human right", in *New York Times*, www.nytimes.com/2012/01/05/opinion/internet-access-is-not-a-human-right.html.
114. Cf. de Hert P. and Kloza D. (2012), "Internet (access) as a new fundamental right. Inflating the current rights framework?", *European Journal of Law and Technology*, 3 (2012) 3, http://ejlt.org/article/view/123/268.
115. Council of Europe, Parliamentary Assembly (2012), Resolution 1877 on the protection of freedom of expression and information on the Internet and online media.
116. Cf. Akdeniz Y. (2012), *Freedom of expression on the Internet*, OSCE, The Representative on Freedom of the Media, Vienna.

The question of access has also been analysed by the European Court of Human Rights in the case of *Ahmet Yildirim v. Turkey*, in which the Court found a restriction of Internet access which violated Article 10.[117] A criminal court of first instance had ordered the blocking of an Internet site, because its owner had been accused of insulting the memory of Atatürk. The Turkish Telecom Directorate asked the court for an extension of the order blocking access to Google Sites, which hosted the site of the applicant, for technical reasons. As a result he was unable to access his own site, even after criminal proceedings against him were discontinued.

The Court recognised that the Internet had become one of the principal means of exercising the right to freedom of expression and information. Turkish law did not have a provision for blocking all access, as ordered by the Turkish court, nor did it authorise blocking an entire Internet domain like Google Sites. Besides which, Google Sites had not been informed that a particular site subject to criminal proceedings needed to be blocked. The Turkish Criminal Court had therefore failed to meet the Convention's foreseeability requirement and had not given the applicant the degree of protection he was entitled to. This meant the measure taken was arbitrary, amounting to a violation of Article 10.[118] In particular, the court held that the question of Internet access engaged the responsibility of the state under Article 10.[119]

The Special Rapporteur of the United Nations on Freedom of Opinion and Expression, Frank La Rue, concluded in his ground-breaking report of 2011 that "given that the Internet has become an indispensable tool to realise a range of human rights …, ensuring universal access to the Internet should be a priority for all States" and effective policy should be developed, in a multi-stakeholder approach "to make the Internet widely available, accessible and affordable to all segments of population".[120] Though this was hailed by some as a declaration of a new right of access by the UN, it was, if read closely, rather a recognition of importance of ensuring access as a policy priority. La Rue, however, understands the important role of Internet access as a catalyst for other human rights and an important facilitator for change. Indeed, it was La Rue who introduced the important separation of access to Internet content from physical access through accessible infrastructure.[121]

The same year, the annual joint declaration of the four international rapporteurs on freedom of expression made it clear that "giving effect to the right to freedom of expression imposes an obligation on States to promote universal

117. *Yildirim v. Turkey* (18 December 2012), application No. 3111/10.
118. Cf. Press Release by the Registrar of the Court (18 December 2012), ECHR 458 (2012).
119. *Yildirim v. Turkey* (18 December 2012), application No. 3111/10, para. 53, with reference to *Vereinigung demokratischer Soldaten Österreichs et Gubi v. Austria* (19 December 1994), para. 27.
120. La Rue F. (26 April 2011), *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, UN Doc. A/HRC/17/27, para. 85.
121. Cf. ibid.

access to the Internet. Access to the Internet is also necessary to promote respect for other rights, such as the right to education".[122]

The Internet Rights and Principles Coalition operating in the context of the Internet Governance Forum has elaborated a Charter on Human Rights and Principles of the Internet, with freedom of expression as one of the key rights. It stipulates a right of access to the Internet, derived from freedom of expression and other rights. It also confirms the freedom of the press and media, which is considered essential to the information society.[123]

We have seen in this chapter that accessing the Internet and forming, expressing, receiving and sharing opinions and information all enjoy broad protection. There are, however, limits to freedom of expression online. In some cases, these restrictions are misused by states to muzzle free speech and oppress their citizens. But some restrictions are legitimate. In the next chapter we see what conditions they have to meet in light of the relevant Court case law.

122. International mechanisms for promoting freedom of expression (1 June 2011), *Joint Declaration on Freedom of Expression and the Internet*, www.osce.org/form/78309.

123. *Charter of Human Rights and Principles for the Internet*, http://internetrightsandprinciples.org/wpcharter; see also 4.3.1 *infra*.

3. Restrictions on freedom of expression online

3.1. Principles and problems

With regard to restrictions on or interference with freedom of expression online, there are numerous challenges in practice, such as censorship through filtering or blocking of online content. They are elaborated in Chapter 5. The omnipresence of the Internet, its universal accessibility and the amplifying effect it has on information published online have to be taken into account, as do its empowering potential and technological characteristics, including its end-to-end orientation and decentralised nature. Nevertheless the rules for restrictions remain the same, according to the principle "what applies offline, also applies online". This principle was confirmed in July 2012 by the Human Rights Council in its ground-breaking resolution on the protection, promotion and enjoyment of human rights on the Internet.[124]

On the obligations from Article 19 of the ICCPR, Frank La Rue, Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, argued in his influential 2011 report that, in analogy to offline content, any restriction of online content to be imposed as an exceptional measure must pass a three-part, cumulative test:

- it must be provided by law, to meet the principles of predictability and transparency,
- it must pursue one of the purposes envisaged in Article 19 of the ICCPR, i.e. to protect the rights or reputation of others, or to protect national security or public order, health or morals, and
- it must be necessary and also the least restrictive means to achieve the respective objective (principle of proportionality).

Furthermore, the restricting legislation must be applied by an independent body in a non-arbitrary and non-discriminatory way, and there should be adequate remedies against abusive application of such legislation.[125] This is explained in more detail in the General Comment of the UN Human Rights

124. UN Human Rights Council (5 July 2012), Resolution A/HRC/20/8 on the promotion, protection and enjoyment of human rights on the Internet.
125. La Rue F. (16 May 2011), *Report of the Special Rapporteur on freedom of opinion and expression*, para. 69.

Committee on Article 19 of the ICCPR, based on its case law.[126] The criteria largely correspond to ECHR Article 10 paragraph 2, except that the legitimate grounds are fewer and there is no reference to a democratic society.

It is a peculiarity of the Internet that information uploaded is available globally (and therefore is ubiquitous) and thus is subject to a variety of international, national or supra-national rules, which can lead to different, if not contradictory treatment. One example is the existence of different approaches to freedom of expression in Europe and the United States. Due to the entrenchment of free speech in the First Amendment to the US Constitution, the ambit of freedom of expression in the US is significantly larger than in Europe. Forms of expression which are considered illegal under the ECHR are protected in the US, such as racist or hate speech, including Nazi propaganda and Holocaust denial.[127] For this very reason, the US has made a reservation to Article 20 of the ICCPR on the prohibition of hate speech and did not sign the Additional Protocol to the Cybercrime Convention, concerning criminalisation of acts of a racist and xenophobic nature committed through computer systems.[128] Although the US courts protect against the misuse of freedom of expression for child abuse, such as child pornography,[129] this aggravates the problem of addressing illicit speech, because European rules can be circumvented by using US or Australian servers, where other standards apply.

However, even within Europe standards can differ, as the treatment of Nazi propaganda illustrates. This situation results in numerous jurisdictional problems.[130] Conflicts of jurisdiction for human rights violations on the Internet are frequent.[131] The French *Yahoo!* case shows this impressively. Yahoo! France had to comply with French law, which prohibited Nazi memorabilia, while its US head office did not have such an obligation.[132] The ensuing conflict

126. Human Rights Committee (12 September 2011), General Comment No. 34 on Article 19: Freedoms of opinion and expression, CCPR/C/GC/34. See also the commentary by the rapporteur of the UN Human Rights Committee for this; O'Flaherty M. (2012), "Freedom of Expression: Article 19 of the International Covenant on Civil and Political Rights and the Human Rights Committee's General Comment No. 34", in *Human Rights Law Review* 12:4, pp. 627-654.
127. Internet & Jurisdiction Observatory (2013), 2012 in Retrospect, www.internetjurisdiction.net/wp-content/uploads/2013/03/2012-in-Retrospect.pdf.
128. Council of Europe (28 January 2003), Additional Protocol to the Cybercrime Convention concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, ETS No. 189.
129. Cuceranu D. (2008), *Aspects of regulating freedom of expression on the Internet*.
130. Cf. de la Chapelle B. and Fehlinger P. (2012), "Internet and jurisdiction, a global multi-stakeholder dialogue process", *Annual Report*, at www.Internetjurisdiction.net/wp-content/uploads/2013/01/Internet-Jurisdiction-Annual-Report-2012.pdf.
131. See Heissl, Gregor (2011), "Jurisdiction for human rights violations on the Internet", *European Journal of Law and Technology*, Vol. 2, No. 1, pp.1-15; see also Chapter 5.
132. Greenberg M. H. (2004-5), "A return to Lilliput: the Licra v. Yahoo! Case and the regulation of online content in the world market", *1192 Berkeley Technology Law Journal* (18), pp. 1191-1258, at www.btlj.org/data/articles/18_04_05.pdf, at 1206.

of laws and courts, explained in more in detail in Chapter 6, shows that pursuing common values by restricting speech is difficult in globalised media communication settings.

Obviously, because of the global nature of the Internet, it is more difficult to apply restrictions. There are often possibilities of circumvention, which can lead to an overreaction by governments, as shown by the Internet blackouts in Egypt or Syria and the increasing number of cases of censorship.[133]

3.2. Criteria for restrictions and the practice of the Court in Internet cases

Freedom of expression is not an absolute right. Article 10, paragraph 2, refers to duties and responsibilities engaged by the exercise of freedom of expression. Similarly, Article 19 of the ICCPR refers to "special duties and responsibilities" that are invoked by exercising freedom of expression. These make the right subject to certain restrictions which are, for Article 10 of the Convention, defined in paragraph 3.

3.2.1. Criteria for restrictions

Any measure that *prima facie* restricts freedom of expression needs to be justified. For that, three criteria have to be met. The measure:

- needs to be prescribed by law (legality),
- needs to pursue one or more of the legitimate aims (legitimacy),
- must be necessary in a democratic society, with necessity implying proportionality to the legitimate aim pursued (necessity).

Article 10, paragraph 2, of the ECHR contains a relatively long list of possible reasons for restrictions, ranging from national security, territorial integrity or public safety to the prevention of disorder or crime, the protection of health or morals, protection of the reputation or rights of others, prevention of the disclosure of information received in confidence and maintaining the authority and impartiality of the judiciary. They reflect the concerns of the era – 1950 – when the Convention was passed. But only if the restrictions are in fact "prescribed by law" and are "necessary in a democratic society" to pursue these goals will the Court consider them not to violate the Convention's guarantees. Hence we can base much of the discussion in this publication on the three-step test of legality, legitimacy and necessity, the last of which includes the element of proportionality.

133. Freedom House, *Freedom on the Net*, www.freedomhouse.org/report/freedom-net/freedom-net-2012.

In principle, the European Court of Human Rights applies its established practice also to the Internet. Therefore the wealth of case law that has emerged over time[134] is also applicable to cases related to the Internet. However, the Court does take the nature of the Internet into account, which is most evident when it deals with government measures that restrict the Internet.

3.2.2. The practice of the Court

In the case of *Ahmet Yildirim v. Turkey* in 2012, the Court reviewed whether interference with the right of the applicant to freedom of expression was prescribed by law, pursued legitimate aims and was necessary in a democratic society, as required by Article 10 paragraph 2 ECHR.[135] In this case the Court took the fact that the Internet had now become one of the principal means of exercising the right to freedom of expression and information as an aggravating factor in determining the illegality of the measures taken by the Turkish authorities. It did not question that there had been a legitimate ground for the restriction based on Turkish law regarding the website in question, but found that the restriction had been disproportionally excessive, by affecting the freedom of expression of a third person as a collateral effect, and thus not necessary to achieve the legitimate result.[136]

Because of the high relevance of freedom of expression in a democratic society, the possible limitations have to be interpreted strictly. According to the case law of the Court, interference is only necessary in a democratic society when it corresponds to a "pressing social need". The Court considers that its role is to review the action taken, looking at the case as a whole, and to "determine whether it was proportionate to the legitimate aims pursued" and whether the reasons given by the national authorities are "relevant and sufficient".[137]

The margin of appreciation

States have a margin of appreciation when determining whether or not there is a pressing social need, because the Court sees national authorities as best placed to assess the social realities. However, the margin is limited because it is applied under the supervision of the Court.[138] In *Ovchinnikov*, the Court found that, although certain information was already available on the Internet, the Russian Court's restrictive measure was to be upheld for the sake of protecting the privacy of a minor. Protecting minors from potentially harmful information was also the determining factor for the majority of the Grand

134. Verpeaux M. (2010), *Freedom of expressio*n, Council of Europe.
135. *Yildirim v. Turkey* (18 December 2012), application No. 3111/10.
136. Ibid., paras. 66-68.
137. *Mouvement Raëlien Suisse v. Switzerland,* First Section, para. 49, referring to *Stoll v. Switze*rland, para. 101.
138. Cf. *Aleksey Ovchinnikov v. Russia* (16 December 2010), application No. 24061/04, para. 46.

Chamber judges when they voted in *Mouvement Raëlien Suisse*. The NGO Article 19, acting as a third party, held that a state's margin of appreciation in cases involving dissemination of information on the Internet should be a narrow one. The removal of a reference or a link to a webpage which itself was left untouched could be considered as disproportionate.[139]

This position was supported by the dissenting opinion of several judges in *Mouvement Raëlien* who argued that "the Internet being a public forum *par excellence*, the State has a narrow margin of appreciation with regard to information disseminated through this medium", especially regarding hyperlinks to webpages not controlled by the site hosting the link.[140]

In his dissenting opinion, Judge Pinto de Albuquerque, *inter alia*, pointed to the principle of "Internet neutrality" and the public service value of the Internet, from which he concluded that users must have the greatest possible access to Internet-based content on a non-discriminatory basis. The majority had found in favour of a broad margin of appreciation similar to speech in commercial matters and advertising.[141]

The Court also considered that states had a particularly wide margin of appreciation when establishing laws regulating penalties for copyright violations, because political debate or expression were not at stake. In *Neij and Sunde Kolmisoppi v. Sweden* the Court found that a criminal conviction and civil damages for enabling copyright violations by running a file-sharing service ("The Pirate Bay"), while an interference with the right to freedom of expression, was necessary in a democratic society.[142]

It should be noted that, in the case of *Ovchinnikov*, the fact that the incriminated information had also appeared on the Internet in the meantime was not considered to make a substantive difference, because in this case the privacy and reputation of a minor was to be protected and there was no public interest in this case. However, reasons of curiosity did not justify the publishing of details like the name of the minor, which had appeared in the article in question.[143] Generally, the Court applies a rule according to which there is little room for restrictions on freedom of expression in political speech and in cases of public interest.[144]

---

139. *Mouvement Raëlien v. Switzerland (GC)*, para. 47. The decision was taken by the smallest possible majority of 9:8. There were also several (joint) dissenting opinions.
140. *Mouvement Raëlien v. Switzerland (GC),* Dissenting opinion of Judge Pinto de Albuquerque, at p. 56. Two other joint dissenting opinions of several judges come to the same finding, but with other reasons.
141. Dissenting Opinion of Judge Pinto de Albuquerque, ibid., pp. 46-68, at 54 et seq. and ibid., paras. 61-62.
142. *Neij and Sunde Kolmisoppi v. Sweden* (19 February 2013) admissibility decisions, application No. 40397/12, at 11.
143. *Ovchinnikov v. Russia*, para. 50.
144. European Court of Human Rights (2011), Research Division, *Internet: case law of the European Court of Human Rights*, at 12.

The role of context

The Court differentiates according to the context: in *Stoll v. Switzerland* it clearly said that "where the freedom of the 'press' is at stake, the authorities have only a limited margin of appreciation to decide whether a 'pressing social need' exists". In the case of *Editions Plon v. France*, the Court started from its standard practice that, in a matter of public interest like the serious illness of a head of state, the French authorities had a limited margin of appreciation in deciding on a "pressing social need". On this basis the authorities had banned the publication in question, a book entitled "The Grand Secret", and the Court accepted that initial response; but, when the ban was renewed, the Judges in Strasbourg could see no further need for it and therefore found the continued ban disproportionate. The fact that an electronic version of the text was available on the Internet, against which the French authorities felt unable to take legal action and which had been the subject of considerable media comment, meant that the preservation of medical confidentiality could no longer be an overriding requirement.[145]

The margin of appreciation usually depends on the context, which may be assessed in different ways, as can be seen in *Mouvement Raëlien*. As use of the Internet may bring with it new factors, contexts and dimensions in terms of, *inter alia*, authors, audience and victims, both content and context of the speech have to be assessed by the Court.[146] It therefore depends on the context whether publication on the Internet (as opposed to publication of the same content offline) affects the decision of the Court. The Judges in Strasbourg continue to apply different standards of necessity in online and offline cases when evaluating whether there is a pressing social need that makes suppressing certain speech necessary. The protection of the rights of minors or young people due to their vulnerability is given particularly high relevance. Freedom of expression in the digital era thus requires taking the new context of Internet publication into account just as much as the content.[147]

Protection of the rights of others

The Court has already had several cases in which it had to balance freedom of expression on the Internet with other rights. These mainly concern the right to private life. Indeed, the issue of Internet privacy and freedom of expression is also a major concern in international debates.[148] In the case of *K.U. v. Finland*, it stated the principle that, while:

145. *Stoll v. Switzerland* (10 December 2007), application No. 69698/01, para. 105, referring also to *Editions Plon v. France* (18 May 2004, final 18 August 2004), application No. 48148/00, paras. 44 and 51.
146. Cuceranu D. (2008), *Aspects of regulating freedom of expression on the Internet*, p. 179 et seq.
147. Karanasiou A. P. (2012), "Respecting context: a new deal for free speech in the digital era", in *European Journal of Law and Technology*, Vol. 3 (2012) 3.
148. See Mendel T., Puddephatt A., Wagner B., Hawkin D. and Torres N. (2012), *Global survey on Internet privacy and freedom of expression*, UNESCO Publishing, p. 50 et seq.

> users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected, such guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others.

The "rights of others" in this case represented respect for private life, protected by Article 8 of the ECHR. An unknown person had posted an advertisement of a sexual nature in the name of the applicant, who was 12 years old, on an Internet dating site without his knowledge. It gave details of him and stated that he was looking for an intimate relationship with a male. It also contained a link to his webpage with his picture and telephone number.

When the applicant became aware of the advertisement, he turned to the police, who tried to establish the identity of the person, which the service provider refused to disclose as they felt bound by confidentiality rules; the courts refused to order the service provider to disclose the identity, for lack of explicit legal provisions. The Court found a violation of the right to private life, in particular because of the potential threat to the physical and mental welfare of the young person at his vulnerable age. The government should have put a system in place to protect children from paedophiles as the danger of the Internet being used for criminal activities was well known: "it is nonetheless the task of the legislator to provide the framework for reconciling the various claims which compete for protection in this context."[149] The Court gives special attention to protection of the private life and reputation of minors and young people, for example when their names and identities are published on the Internet,[150] because they risk being targeted by online predators or becoming victims of other forms of child abuse.

So the buck stops with states: they are obliged to respect, protect and ensure all human rights on the Internet. Protecting the human rights of minors may involve forcing Internet intermediaries to disclose information on their clients in order to enable effective prosecutions. This may, of course, limit the freedom of expression of the parties, but Article 10 contains an exception for interference with freedom of expression that pursues the legitimate goal of safeguarding the rights of others.

In the case *Perrin v. the United Kingdom*, the applicant had claimed his freedom of expression to publish obscene material on a website. However, the Court found that the need to protect morals and the rights of others, especially children, justified the criminal conviction for the publication of a freely accessible preview webpage with no age checks, showing seriously obscene pictures and likely to be found by young people.[151]

149. *K. U. v. Finland* (2 December 2008), application No. 2872/02, paras. 41-50.
150. *Ovchinnikov v. Russia* (16 December 2010), application No. 24061/04, paras. 49-50.
151. *Perrin v. the United Kingdom* (18 October 2005), application No. 5446/03, Decision on Admissibility.

In the case of *Mouvement Raëlien Suisse v. Switzerland*, where a ban had been imposed on the display of a poster on the public highway showing the website address of an association that claimed to offer a message from extraterrestrials and propagated cloning, some of whose members were accused of sexual activities with minors, the Court by a small majority considered the ban proportionate and necessary to protect health and morals and to prevent crime.[152] In this case, the Grand Chamber was nearly equally divided; the minority expressed its views in several dissenting opinions, which are worth analysing as they also touch on the nature and role of the Internet.

In *Neij and Sunde Kolmisoppi v. Sweden* the Court concluded that "protecting the plaintiffs' copyright to the material in question" was a legitimate aim pursued by the restriction. The convictions and damages awarded therefore pursued the legitimate aim of the "protection of the rights of others" (and that of "prevention of crime").[153]

Information already available on the Internet

In *Ovchinnikov*, the Court found that the fact that certain information is already available on the Internet does not excuse journalists from respecting the private or family life of individuals in certain circumstances. In this case, a journalist had revealed the identity of a minor involved in a violent incident in a summer camp, and information on the incident had already appeared on the Internet.[154]

In other cases, like *Editions Plon v. France*, the Court held that the fact that the confidential information was already in the public domain including the Internet substantially diminished the interest in its protection and could no longer constitute an overriding requirement,[155] whereas in *Ovchinnikov* the Court considered that restricting information already in the public domain could be justified as the details did not come within the scope of any political or public debate on a matter of general importance. It reiterated its earlier line of reasoning in *Von Hannover v. Germany*,[156] that in the case of the publication of details of an individual's private life with the sole purpose of satisfying the curiosity of readers, the protection of the private life of the individual prevails over the journalist's freedom of expression.[157]

Specific responsibilities of the media

In *Fatullayev v. Azerbaijan*, the Court found that specific responsibilities of journalists related to exercising their freedom of expression also apply

152. *Mouvement Raelien Suisse v. Switzerland* (13 July 2012), application No. 16354/06, para. 72, confirming the Judgment of the Chamber of 13 January 2011.
153. *Neij and Sunde Kolmisoppi v. Sweden* (19 February 2013), application No. 40397/12, at 10.
154. *Ovchinnikov v. Russia* (16 December 2010), application No. 24061/04, paras. 50-52.
155. *Editions Plon v. France* (18 May 2004), application No. 58148/00, para. 53.
156. *Von Hannover v. Germany* (24 June 2004), application No. 59320/00, para. 65.
157. *Ovchinnikov v. Russia*, para. 50.

if they publish information on the Internet, for example on public Internet forums.[158] The applicant was the founder and chief editor of two newspapers which were often critical of the government, resulting in several defamation actions and convictions. For example, he made serious allegations against Azeri troops on a publicly accessible Internet forum indirectly linked to one of his newspapers. Legal action resulted in a criminal conviction with a prison sentence. After carefully weighing the arguments the Court came to the conclusion that the author, while making "exaggerated and provocative assertions", did not cross the limits of journalistic freedom in performing his duty to impart information on matters of general interest. His conviction of defamation for the Internet posts did not meet a "pressing social need", and the requirement of proportionality was not satisfied.[159] The Court reiterated that the imposition of a prison sentence for a press offence against journalists is compatible with Article 10 only in exceptional circumstances where other fundamental rights are seriously impaired, as in cases of hate speech or incitement to violence. Finding a violation in both criminal convictions, the court ordered the immediate release of the applicant.[160]

With regard to responsibilities for Internet archives, in *Times Newspapers Limited v. The United Kingdom* the Court did not consider that the requirement to publish an appropriate qualification to an article contained in an Internet archive constituted a disproportionate interference with the freedom of expression, though it was aware that libel action was taken against the same article published in the written press.[161] Generally, the maintenance of Internet archives was considered a valuable secondary role of the press in making available to the public an important source for education and historic research.[162]

Responsibilities of politicians

In the case of *Féret v. Belgium*, which dealt with xenophobic remarks made by a politician on his website, the Court saw a pressing social need to protect the rights of the immigrant community as a reason for the conviction. It found that the language employed clearly did incite to discrimination and racial hatred, which could not be excused by an electoral process.[163] However, the criminal conviction of a webmaster for publicly insulting a mayor – *inter alia*, as a Ceauşescu urban dictator, as part of a critique of urban projects, published on the website of an association chaired by the webmaster – was considered excessive, because these were mainly value judgments related to a critique

158. *Fatullayev v. Azerbaijan* (22 April 2010), application No. 40984/07, paras. 94 and 95; see also Chapter 2.
159. On defamation and the Internet see also 5.7.
160. *Fatullayev v. Azerbaijan,* paras. 100, 101, 103 and 177.
161. *Times Newspapers Ltd. v. The United Kingdom* (10 March 2009), application Nos. 1 and 2, application Nos. 3002/03 and 23676/03, para. 47.
162. Ibid., para. 45.
163. *Féret v. Belgique* (16 July 2009), application No. 15615/07.

of municipal policy and thus related to a political debate, protected by the Convention, which made the condemnation disproportionate.[164]

However, in *Willem v. France*, the Court found that incitement by a mayor, as an elected representative, calling for an act of discrimination against products from Israel to protest against its policy on Palestine, and reiterated as an open letter on the municipality's website, did not belong to the free discussion of a subject of general interest. The discriminatory – and thus reprehensible – nature of a political message is exacerbated by its publication on the Internet. In this conclusion, the function of a mayor was considered important as was protection of the political debate. As mayor, he had an obligation to keep a certain neutrality and restraint as he was engaging the territorial collectivity he was representing. By involving the municipal services in a discriminatory act, without a debate or vote in the municipal council, the applicant did not promote free discussion of a subject of general interest.[165]

3.3. Conclusion

We can therefore see that the Internet has not changed fundamentally the nature of freedom of expression or the limits to its protection. Freedom of expression is an essential catalyst for a number of human rights. But as the Internet also intensifies violations of human rights and increases their potential harm, the law and practice of restrictions has to develop accordingly. Rather than reinvent the wheel of legitimate restrictions to freedom of expression, the commonly used three-part test applies also in cases with an online connection. Some nuancing will continue to be necessary, but the principle stands: what is legal offline, is legal online; and what is forbidden offline is not protected online, but the character of the Internet with its amplifying and globalising effect needs to be taken into account.

In doing this, the European Court of Human Rights in its evolving case law has to meet two challenges: upholding its standards developed in its jurisprudence on freedom of expression and applying them to the Internet – taking its special characteristics, including its ubiquity and asynchronicity and amplifying nature, into account and carefully considering its empowering potential. The Court has not yet been able to address all challenges related to freedom of expression online as exemplified in Chapters 5 and 6. It has another opportunity to deal with access to the Internet in *Yankovskis v. Lithuania*[166] and in other cases pending.[167] The coming years will thus allow the Court to more clearly delimit freedom of expression online.

164. *Renaud v. France* (25 February 2010), application No. 13290/07, paras. 36-43.
165. *Willem v. France* (16 July 2009), application No. 10883/05, paras. 36-38.
166. See *Jankovskis v. Lithuania*, application No. 21575/08.
167. See, for example, *Akdeniz v. Turkey*, application No. 20877/10.

4. Standard-setting by the Council of Europe and non-state actors

The protection of freedom of expression has many facets (as described in Chapter 2) and knows certain restrictions (as analysed in Chapter 3). The role of freedom of expression online, however, does not end with delineating state duties to respect, protect and implement human rights norms as developed by the European Court of Human Rights. In this chapter we show how the Council of Europe and non-state actors set standards for the implementation of freedom of expression by their guidelines, recommendations, codes of conduct and positive practice. We focus first on commitments to the importance of human rights in Internet governance. Then we discuss the activities of the Council of Europe, its recommendations and declarations, and its guidelines for transnational corporations. Non-state actors have also made important contributions to freedom of expression online. We look especially at the importance of transparency in the protection of freedom of expression.

4.1. The context: the role of human rights in Internet governance

Human rights and Internet governance are closely linked. But the road to the 2012 resolution of the Human Rights Council, confirming that online human rights enjoy the same protection as offline human rights, was long and rocky. Efforts towards regulation of the Internet in the framework of the World Summit on the Information Society (WSIS), which took place in two phases (Geneva 2003 and Tunis 2005), quickly raised the issue of the proper role of human rights in Internet governance, an issue taken up in particular by the Human Rights Caucus of civil society.[168] An international symposium on the Information Society, Human Rights and Human Dignity in 2003 highlighted the challenges of human rights for Internet governance.[169]

Both the Geneva and Tunis documents contain clear references to the Universal Declaration of Human Rights and to freedom of expression in

168. See Jørgensen R. F. (ed.) (2006), *Human rights in the global information society*, and Jørgensen (2013), *Framing the net: the Internet and human rights*; also Benedek W. (2008), "Internet governance and human rights" in Benedek, Bauer and Kettemann (eds), *Internet governance and the information society*, pp. 31-49.

169. Statement on human rights, human dignity and the information society, www.pdhre.org/wsis/statement.doc. The symposium was organised by the NGO PDHRE in co-operation with the European Commission and the OHCHR with the support of the Swiss Government.

particular. The Geneva Declaration of Principles of 2003 contains a reaffirmation of Article 19 UDHR on freedom of opinion and expression and more specifically of the freedom of the press and freedom of information as well as of the independence, pluralism and diversity of the media as essential to the Information Society.[170] The Tunis Commitment of 2005 reaffirms paras. 4 and 55 of the Geneva Declaration of Principles and further requires "that freedom of expression and the free flow of information, ideas, and knowledge are essential for the Information Society and beneficial for development".[171]

4.2. Activities of the Council of Europe: awareness raising and standard-setting

The Council of Europe has established itself as the main international organisation developing the role of human rights in the information society by raising awareness and pursuing a trilateral approach: through conventions, standards and capacity building.[172] Here we analyse its standard-setting role in freedom of expression online. The various recommendations adopted over the years by the Committee of Ministers in particular are usually addressed to the member states. They are also used in the jurisprudence of the European Court of Human Rights, which regularly refers to them to elucidate the meaning of Article 10 in the context of the Internet,[173] and they are a valuable contribution to international dialogue on Internet governance and human rights.

Already in May 2003, the Council of Europe adopted the Declaration on freedom of communication on the Internet, in which it reaffirmed freedom of expression and free circulation of information on the Internet. In its operative part, the Declaration identified seven principles for member states, which are all relevant to freedom of expression – in particular, that restrictions on content on the Internet should not go further than restrictions on content delivered by other means, that states should not establish any prior controls of information on the Internet through blocking or filtering, that there should be only a limited liability of service providers for Internet content and that the decision of users not to disclose their identities through anonymity should be respected.[174]

Later, the Council of Europe established the Group of Specialists on Human Rights and the Information Society, which during its 10 sessions between

170. WSIS (12 December 2003), Doc. WSIS-03/GENEVA/DOC/4-E, paras. 4 and 55.
171. WSIS (18 November 2005), Doc. WSIS-04/TUNIS/DOC/7-E, para. 4.
172. Benedek W. and Kettemann M. C. (2010), "The Council of Europe and the information society" in Kicker R. (ed.), *The Council of Europe, Pioneer and guarantor for human rights and democracy*, pp. 109-115.
173. See e.g. *Editorial Board of Pravoye Delo and Shtekl v. Ukraine*, para. 30 and *Yildirim v. Turkey*, para. 26.
174. Committee of Ministers (28 May 2003), Declaration on Freedom of Communication on the Internet.

2005 and 2011 produced important initiatives and advice through the Steering Committee on the Media and New Communication Services (CDMC) for the Committee of Ministers.[175]

4.2.1. Recommendations and declarations

In 2005, the Committee of Ministers of the Council of Europe adopted a Declaration on human rights and the rule of law in the information society, which reiterated the principle that "freedom of expression, information and communication should be respected in a digital as well as in a non-digital environment and should not be subject to restrictions other than those provided for by Article 10 of the ECHR".[176]

The 3rd Summit of Heads of State and Government of the Council of Europe in Warsaw in 2005 called on the organisation to elaborate principles and guidelines to ensure respect for human rights and the rule of law in the information society and to address challenges created by the use of information and communication technologies (ICTs) to protect human rights against violations stemming from the abuse of such technologies.[177]

In 2007, the Committee of Ministers of the Council of Europe adopted a Recommendation on promoting freedom of expression and information in the new information and communication environment, in which it emphasised the empowerment of individual users and access to the new information and communication environment, but also stated that "a fair balance should be struck between the right to express freely and to impart information in this new environment and respect for human dignity and rights of others".[178]

The Recommendation of the Committee of Ministers on measures to promote the public service value of the Internet of the same year is of fundamental importance. The public service value is understood as "peoples' significant reliance on the Internet as an essential tool for their everyday activities (communication, information, knowledge, commercial transactions) and the resulting legitimate expectation that Internet services be accessible and affordable, secure, reliable and ongoing".[179] It requires that "member states should adopt or develop policies to preserve and, whenever possible, enhance the protection

175. See, for an overview of all activities: www.coe.int/t/dghl/standardsetting/media/MC-S-IS/default_en.asp.
176. Committee of Ministers (13 May 2005), Declaration on human rights and the rule of law in the information society, CM/Rec(2005)56 final.
177. See Action Plan attached to the Warsaw Declaration (17 May 2005), Doc CM(2005)80, para. 5.
178. See Committee of Ministers (26 September 2007), Recommendation CM/Rec(2007)11 on promoting freedom of expression and information in the new information and communication environment.
179. See Committee of Ministers (7 November 2007), Recommendation CM/Rec(2007)16 on measures to promote the public service value of the Internet.

of human rights and respect for the rule of law in the information society". Particular attention should be paid to the right to freedom of expression, information and communication on the Internet. Member states should ensure that restrictions are in line with Article 10 ECHR as interpreted by the Court.[180]

An application of these recommendations can be found in the Recommendation of the Committee of Ministers on measures to promote the respect for freedom of expression and information with regard to Internet filters of 2008. According to this recommendation, users' awareness, understanding of and ability to effectively use Internet filters are considered as key to fully exercising their human rights, in particular the right to freedom of expression and information. For this purpose, a number of recommendations are made to member states, to be implemented in co-operation with the private sector and civil society.[181]

Freedom of expression can also be affected by restrictions of the principle of network neutrality, by which "users should have the greatest possible access to Internet-based content, applications and services of their choice, whether or not they are offered free of charge, using suitable devices of their choice".[182] According to the Declaration of the Committee of Ministers on network neutrality, exceptions to this principle must be justified by overriding public interest, paying due attention to Article 10 ECHR and the case law of the Court.[183]

In a wider sense, the right to freedom of expression and the corresponding public service value of the Internet depend on preserving the Internet's universality, integrity and openness. Therefore, in its Recommendation on the protection and promotion of the universality, integrity and openness of the Internet, the Committee of Ministers expressed concern about risks of disruption of the stable and functional Internet by technical failures or by interference with its infrastructure.

In order to promote its integrity, stability and resilience, member states were asked to respect specific principles like 'do no harm', co-operation, due diligence, information sharing, consultation and mutual assistance, and to incorporate the protection of human rights and fundamental freedoms in the management of critical resources of the Internet.[184] This recommendation was the outcome of work done in response to a Resolution on Internet governance and critical Internet resources by the ministerial meeting in Reykjavik in 2009.[185]

180. Ibid.
181. Committee of Ministers (26 March 2008), Recommendation CM/Rec(2008)6 on measures to promote the respect for freedom of expression and information with regard to Internet filters.
182. Committee of Ministers (29 September 2010), Declaration on network neutrality, para. 4.
183. Ibid., para. 6.
184. Council of Europe, Committee of Ministers (21 September 2011), Recommendation CM/Rec(2011)8 on the protection and promotion of the universality, integrity and openness of the Internet.
185. 1st Council of Europe Conference of Ministers responsible for Media and New Communication Services (29 May 2009), Resolution on Internet Governance and critical Internet resources, Doc. MCM(2009)011.

As this recommendation addressed basic questions of Internet governance, the Council of Europe, assisted by an expert group, elaborated 10 key principles of Internet governance,[186] which were endorsed by the Declaration of the Committee of Ministers on Internet governance principles.[187] The first principle is "human rights, democracy and the rule of law"; another is "empowerment of Internet users" to exercise their rights and freedoms. This work proves that the close linkages between human rights and Internet governance have been recognised, at least in the framework of the Council of Europe. With this declaration, the Council of Europe has contributed to the global debate on principles of Internet governance, which intensified in 2011. An even stronger focus on human rights is found in the *10 Internet Rights and Principles* issued by the Internet Rights and Principles Coalition in 2011.[188]

The 1st Council of Europe Conference of Ministers responsible for Media and New Communication Services in Reykjavik in 2009 was devoted to "a new notion of media?" In a pertinent resolution, the ministers committed to further standard-setting in the fields of freedom of expression and information and freedom of the media, with the necessary political backing, and they recognised the positive impact of such efforts in the new information and communication environments. The resolution contained an action plan to examine a new notion of the media and to elaborate, *inter alia*, a policy document reviewing the concept of the media to include relevant new media and services.[189]

This process resulted in the Recommendation of the Committee of Ministers on a new notion of media of 2011, which is based on the relevance of media as the most important tool for freedom of expression and once again highlights the importance of freedom of expression for genuine democracy and democratic processes. Developments in the media ecosystem by the digital media and new actors are found to require a new notion of the media, with a graduated and differentiated approach, for the purpose of which criteria and indicators are identified in the appendix to the recommendation.[190] The issue here is about identifying under what circumstances communication in new digital contexts can be categorised as a new kind of media, which would allow it to be treated by member states accordingly. For example, public blogs can reach a wide audience today and bloggers may pursue journalistic roles.

186. The Ad hoc Advisory Group on cross-border Internet was established in 2009 and completed its mandate after four meetings in 2011; www.coe.int/t/dghl/standardsetting/media/MC-S-CI/default_en.asp.
187. Council of Europe, Committee of Ministers (21 September 2011), Declaration on Internet Governance Principles; see also Kleinwächter W. (2011), *Internet principle hype: how soft law is used to regulate the Internet,* www.news.dot-nxt.com/2011/07/27/internet-principle-hype-anon.
188. See *10 Internet Rights and Principles* at www.internetrightsandprinciples.org.
189. See the Resolution of the 1st Council of Europe Conference of Ministers responsible for Media and New Communication Services, Towards a new notion of media, Doc. MCM(2009)011.
190. Council of Europe, Committee of Ministers (21 September 2011), Recommendation CM/Rec(2011)7 on a new notion of media.

Ordinary citizens by sharing pictures on the Internet may become "citizen journalists", but usually lack the protection citizens enjoy. Why, we may ask, should students filming a police crackdown with their smartphones deserve less protection than a BBC team filming the same situation?[191]

Accordingly, the resolution in the appendix to the recommendation identifies several criteria, such as the intent to act as media, the purpose of media, editorial control or professional standards, outreach and public expectation. These criteria are supported by sets of indicators. The recommendation further develops standards to be applied to media in the new ecosystem, including freedom of the media, freedom from censorship and protection against misuse of defamation laws, protection of journalists and their sources, media pluralism and media responsibilities like respect for dignity and privacy or providing remedies for third parties. The new notion of media thus significantly widens the concept by including digital media, which also benefit from the right to freedom of expression and information, if they meet the identified criteria. It also deals with downsides of freedom of expression on the Internet like hate speech and the need to protect children against online harassment and grooming.

Freedom of expression on the Internet can also be affected by pressures exerted on Internet platforms and Internet service providers (ISPs). In its Declaration on the protection of freedom of expression and freedom of assembly and association with regard to privately operated Internet platforms and online service providers of 2011, the Committee of Ministers highlights the relevance of blogging websites and other means of mass communication by which civil society, whistle-blowers and human rights defenders can exchange information, publish content, interact and associate with each other. Those platforms are considered as an integral part of the new media ecosystem. Although privately operated, they are a significant part of the public sphere because they facilitate debates on issues of public interest. Like traditional media, they can assume the role of social watchdogs.

The Committee of Ministers expresses concern about direct or indirect political influence and pressure on new media, which can lead to interference with freedom of expression nationally or internationally. Among new challenges to freedom of expression online it mentions particular forms like distributed denial-of-service attacks against independent media websites and recalls the need to reinforce policies to uphold freedom of expression and information.[192]

Finally, the Committee of Ministers in March 2012 adopted its comprehensive strategy on Internet governance for the period 2012-2015.[193] Starting from

191. On citizen journalists, see also Chapter 2.

192. Committee of Ministers (7 December 2011), Declaration on the protection of freedom of expression and freedom of assembly and association with regard to privately operated Internet platforms and online service providers.

193. Committee of Ministers (14 March 2012), Council of Europe Strategy 2012-2015 on Internet Governance.

human rights, democracy and the rule of law on the Internet as a Council of Europe priority, it emphasises the role of freedom of expression and information regardless of frontiers, and as a catalyst for other rights. One main line of action identified is "maximising rights and freedoms for Internet users", for which purpose the strategy foresees the "drawing up of a compendium of existing human rights for Internet users". This should help users also to seek effective recourse from Internet actors and government agencies when their rights and freedoms have been adversely affected. To elaborate such a compendium a Committee of experts on rights of Internet users was established in September 2012,[194] to prepare the compendium within about one year.

Other recommendations that are indirectly relevant to freedom of expression online are the Declaration on freedom of expression and information in the media in the context of the fight against terrorism, adopted by the Committee of Ministers in 2005 and complemented by a pertinent resolution by the Council of Europe Conference of Ministers responsible for Media and New Communication Services in Reykjavik in 2009.[195]

According to the Council of Europe Declaration of 2005 on human rights and the rule of law in the information society, the same treatment of freedom of expression, information and communication should apply online as offline – in digital and non-digital environments equally.[196] In a similar way, the Guidelines of the Committee of Ministers of the Council of Europe on protecting freedom of expression and information in times of crises of 2007 deserve to be mentioned. They are also concerned with the safety of media professionals, access to information and undue limitations on freedom of expression.[197]

Also of indirect relevance is the Declaration of the Committee of Ministers on enhanced participation of member states in Internet governance matters – Governmental Advisory Committee (GAC) of the Internet Corporation for Assigned Names and Numbers (ICANN) of 2010, which encourages a more active role for Council of Europe member states in the GAC with the purpose of promoting Council of Europe standards and values in Internet governance and seeking observer status for the Council of Europe. In this context the Council of Europe has made valuable contributions to Internet governance, such as a study on freedom of expression and freedom of association regarding

194. See Committee of experts on rights of Internet users, www.coe.int/t/dghl/standardsetting/media/MSI-DUI/default_en.asp.
195. See Declaration on freedom of expression and information in the media in the context of the fight against terrorism (2 March 2005) and Committee of Ministers (28 and 29 May 2009), Resolution on Developments in anti-terrorist legislation in Council of Europe member states and their impact on freedom of expression and information, MCM(2009)11.
196. Committee of Ministers (13 May 2005), Declaration on human rights and the rule of law in the information society, CM/Rec(2005)56 final, para. 2.
197. See Council of Europe, Committee of Ministers (26 September 2007), Guidelines on protecting freedom of expression and information in times of crises.

the new generic top-level domains,[198] which should provide guidance to the GAC in taking human rights properly into account when providing advice on new generic top-level domains (gTLDs) to ICANN.

Already in 2011, the Committee of Ministers had adopted a Declaration on the protection of freedom of expression and information and freedom of assembly and association with regard to Internet domain names and name strings.[199] In this declaration, the Committee of Ministers stated that expressions contained in names of Internet websites, such as domain names and name strings, should not be excluded a priori from the application of legal standards of the freedom of expression and the right to information. In this context, the declaration expressed concern about measures in certain Council of Europe member states prohibiting the use of certain words or characters in domain names and name strings, both with regard to the right to freedom of expression and the freedom of assembly and association. Over-regulation in this field could become a form of interference, in which case it would have to meet the conditions of articles 10 and 11 ECHR and the related case law of the Court.[200]

4.2.2. Guidelines and recommendations for business

Contributing to the rules of Internet governance, the Council of Europe has so far adopted four guidelines or recommendations on how to address human rights issues in Internet governance in selected business fields. The first two were the *Guidelines for online game providers* and the *Guidelines for Internet service providers (ISPs),* both adopted in 2008.[201] In these voluntary guidelines, the Council of Europe adopted a multi-stakeholder approach by working closely with the industries that were to follow the guidelines. This effort of co-regulation should increase the rate of compliance by the industry concerned.

The *Human rights guidelines for online game providers* (who are not to be confused with providers of online gambling services, which are not covered by these), contain the guidelines themselves and extracts from relevant

198. Council of Europe, Directorate General on Human Rights and the Rule of Law, Comments relating to freedom of expression and freedom of association with regard to new generic top level domains, by Benedek W. (with Gragl P. and Kettemann M. C.), Liddicoat J. and van Eijk N., DG-I (2012) 4 of 12 October 2012.
199. Committee of Ministers (21 September 2011), Declaration on the protection of freedom of expression and information and freedom of assembly and association with regard to Internet domain names and name strings.
200. See ibid.
201. Council of Europe, *Human rights guidelines for online game providers,* developed by the Council of Europe in co-operation with the Interactive Software Federation of Europe, Doc. H/Inf (2008) 8; and *Human rights guidelines for Internet service providers,* developed by the Council of Europe in co-operation with the European Internet Service Providers Association (Euro. ISPA), Doc. H/Inf (2008) 9.

recommendations and declarations of the Committee of Ministers of the Council of Europe. With regard to the relevance of these guidelines to the right to freedom of expression, the guidelines are mainly concerned with avoiding illegal and harmful content or labelling sensitive content, in particular for the purpose of child protection.

In this context, they refer to the 2008 Recommendation of ministers on measures to promote respect for freedom of expression and information with regard to Internet filters; these measures include some guidelines, but they have not been drafted for any particular business sector.[202] The guidelines are followed by extracts from relevant Council of Europe standards, in particular a 1992 recommendation on video games with racist content and a 1997 recommendation on portraying violence in electronic media. The latter contains guidelines for non-state actors and the responsibilities of member states.[203] Also attached are the pertinent Declaration of the Committee of Ministers on protecting the dignity, security and privacy of children on the Internet[204] of 2008 and Recommendation CM/Rec(2008)6 on measures to promote respect for freedom of expression and information with regard to Internet filters.[205]

The *Human rights guidelines for Internet service providers*, also published in 2008, provide human rights benchmarks for ISPs, which fulfil several functions: as access providers ("gatekeepers of the Internet"), as content providers and/or as host providers. Accordingly, their responsibilities may differ, depending on the type of service provided. Of particular relevance to freedom of expression are attempts to put ISPs under an obligation to monitor content and traffic data. This should only happen in specific cases defined by law and upon a specific order by a legitimate authority. According to the guidelines, ISPs should make available information on the risks of encountering illegal or harmful content, in particular concerning children, regarding online pornography, glorification of violence, discriminatory and racist expressions and various forms of harassment. Users should also be informed on hotlines about illegal content and how they can protect themselves, for example by information on available software tools.

Any filtering or blocking of services of ISPs should be legitimate, proportional and transparent, and only after verification of the illegality of the content. The Recommendation on measures to promote respect for freedom of expression in information with regard to Internet filters needs to be applied and

202. See Council of Europe, Committee of Ministers (26 March 2008), Recommendation CM/Rec(2008)6 on measures to promote the respect for freedom of expression and information with regard to Internet filters.
203. See Recommendation No. R (92) 19 on video games with racist content and Recommendation No. R (97) 19 on the portrayal of violence in the electronic media.
204. Council of Europe, Committee of Ministers (20 February 2008), Declaration on protecting the dignity, security and privacy of children on the Internet.
205. See Council of Europe, Committee of Ministers (26 March 2008), Recommendation CM/Rec(2008)6.

also reprinted. A right to reply should be offered to users. Extracts from relevant Council of Europe recommendations and declarations are reprinted with the guidelines, like the Declaration on freedom of communication on the Internet along with the principle of limited liability of service providers for Internet content and the principle that there is no general obligation of service providers to monitor the information on the Internet to which they give access, which is based on Article 15 of the EU Directive on Electronic Commerce of 2000.[206] ISPs should also not be obligated to actively seek facts or circumstances indicating illegal activity, since this might have the effect of curbing freedom of expression. CM Rec(2007)16 on measures to promote the public service value of the Internet is reproduced in the annex.

Clearly, these guidelines and other relevant Council of Europe standards are of particular practical importance. Most ISPs seem to have accepted the guidelines, which, however, because of their voluntary nature, lack monitoring and enforcement tools.

It took several years before the Council of Europe issued another set of guidelines, this time in the form of recommendations by the Committee of Ministers, giving the guidelines more authority. These guidelines were elaborated with the assistance of the Committee of Experts on New Media, which operated between 2009 and 2011.[207] The two recommendations on the protection of human rights with regard to search engines and social networking services of 2012[208] address first of all member states, which should develop and promote, in consultation with the private sector and civil society, coherent strategies to protect freedom of expression, access to information and other human rights in relation to search engines. Member states need to do this by engaging research engine providers to strive towards several objectives relevant to freedom of expression, such as enhancing transparency in how access to information is provided, ensuring pluralism and diversity of information, and reviewing search ranking and indexing of content that is not intended for mass communication, taking into account the intentions of the producers.

The European Commission later reviewed the practice of Google in particular and expressed concern that it was ranking search results to its own products higher than others, which was affecting fair competition.[209] After the US Federal Trade Commission had decided not to take formal steps, following a similar inquiry that found unfair business practices, the European Commission announced that its investigations would not be affected by the

206. See Directive 2000/31/EC (8 June 2000).

207. Committee of Experts on New Media, www.coe.int/t/dghl/standardsetting/media/MC-NM/default_en.asp.

208. Council of Europe, Committee of Ministers (4 April 2012), Recommendation CM/Rec(2012)3 on the protection of human rights with regard to search engines and Recommendation CM/Rec(2012)4 on the protection of human rights with regard to social networking services.

209. European Commission (30 November 2010), *Antitrust: commission probes allegations of antitrust violations by Google,* Press Release, IP/10/1624.

US decision. Presently, the issue remains unresolved and highly controversial. In addition, Google is under criticism by European data-protection authorities for linking user data from different Google services without the consent of the users, who have no possibility to object. The French data-protection authority CNIL, acting on behalf of European data-protection authorities, is now considering "repressive measures".[210]

Furthermore, member states should encourage search engine providers to discard search results only in accordance with Article 10 paragraph 2 ECHR and to inform the user about the origin of the request.[211] The recommendation points out that in many countries search engine providers de-index or filter particular websites at the request of public authorities or private parties. In this context, member states should ensure that the right to freedom of expression and information is fully respected. The filtering and blocking should be transparent to the user and should respect the principle of due process and the availability of independent and accountable redress mechanisms. Interaction between different stakeholders like the state and private actors or civil society is expected to contribute to standard-setting protecting human rights. Self- and co-regulatory regimes should not hinder the individual's freedom of expression and information, for the protection of which self-regulatory codes of conduct are encouraged. Users should be informed and educated about the functioning of different search engines.[212]

Of particular relevance for freedom of expression is the Recommendation of the Council of Ministers on the protection of human rights with regard to social networking services.[213] The recommendation highlights the potential of social networking services in promoting freedom of expression and their public service value of facilitating democracy and social cohesion. Among the threats to freedom of expression identified by the recommendation are sheltering discriminatory practices, lack of legal and procedural safeguards, and inadequate protection of children against harmful content. Self- and co-regulatory mechanisms, which exist in certain member states, have to respect procedural safeguards like the right to fair trial. Member states, in consultation with the private sector and civil society, are recommended to develop coherent strategies to protect and promote human rights with regard to social networking services, for example by raising user awareness of possible challenges to human rights and protecting users from harm, without limiting freedom of expression and access to information.

---

210. EU-Info Deutschland (18 February 2013), *Europäische Datenschutzbehörden wollen Sanktionen gegen Google,* www.eu-info.de/dpa-europaticker/226952.html.
211. Committee of Ministers (4 April 2012), Recommendation CM/Rec(2012)3 on the protection of human rights with regard to search engines, para. 8.
212. See ibid., Appendix, paras. 12 et seq. and 17-20.
213. Council of Europe, Committee of Ministers (4 April 2012), Recommendation CM/Rec(2012)4 on the protection of human rights with regard to social networking services.

The appendix to the recommendation, which provides specific lines of action, focuses on empowering the user to control access to their personal data. However, sharing access to data can also be part of freedom of expression. Particular freedom-of-expression issues arise with regard to protection of children and young people against harmful content, for which purpose several recommendations are made. As a general principle, member states should refrain from the general blocking and filtering of offensive or harmful content in order to respect their obligations under Article 10 paragraph 2.[214] Again reference is made to the Recommendation on promoting respect for freedom of expression and information regarding Internet filters.[215]

In conclusion, the Council of Europe has elaborated comprehensive guidelines for state and non-state actors on dealing with various challenges for freedom of expression on the Internet. They are not legally binding, but constitute authoritative interpretations of the obligations of these actors to be derived from applying freedom of expression to the Internet. The various actors are encouraged to seek solutions based on the principles identified, which can be done by way of self-regulation or co-regulation. Thus the approach of the Council of Europe can be described as guided self-regulation. Multi-stakeholder approaches are clearly preferred. The empowerment of users to enjoy their right to freedom of expression and information is given particular attention. The elaboration of a compendium of user rights, derived from existing human rights, is a logical further step.

Generally, we can observe a significant widening of coverage of pertinent human rights like freedom of expression as a consequence of an enlarged concept of the media and their public service value. This requires also a renewed effort to enlarge the field of application of human rights like freedom of expression to include private actors assuring their responsibility in providing a public space for searching or for social networking and thus assuming public functions, including the responsibility to respect and promote human rights.

4.3. Activities of non-state actors

4.3.1. The Charter on Human Rights and Principles for the Internet

The concern with human rights in the governance of the Internet was also strongly promoted by non-state actors like the Internet Rights and Principles Coalition, the Dynamic Coalition on Freedom of Expression and the Global Network Initiative. Their efforts should therefore be introduced as examples of good practice.

214. See Appendix to Recommendation CM/Rec(2012)4.
215. Committee of Ministers (26 March 2008), Recommendation CM/Rec(2008)6 on measures to promote the respect for freedom of expression and information with regard to Internet filters.

The Internet Rights and Principles Coalition is the result of efforts to give human rights more attention in the work of the Internet Governance Forum (IGF). It is actually the outcome of a merger of two dynamic coalitions, the Dynamic Coalition on an Internet Bill of Rights (IBR) and the Dynamic Coalition on a Framework of Principles for the Internet, which merged in 2008 at the IGF in Hyderabad (India). It is a multi-stakeholder group with civil society as the driving force and uses the space created by the IGF for dynamic coalitions to promote its objective, the mainstreaming of human rights in all activities of the IGF during and between its meetings.

In 2009, at the IGF in Sharm el Sheikh, Egypt, it decided to elaborate a "Charter on Human Rights and Principles for the Internet", which was presented at the IGF in Vilnius in 2010 and, in a more developed version, at Nairobi in 2011.[216] Its structure follows the Universal Declaration on Human Rights (UDHR), which has been referred to in the Geneva and Tunis documents of the WSIS and therefore constitutes an agreed basis. However, at the beginning, it states a right of access to the Internet, because without such a right (which, according to its authors, can be derived by implication from other human rights like freedom of expression or the right to education) human rights cannot be enjoyed online.[217] Following the holistic approach of the UDHR, the "Charter" also covers economic, social and cultural rights not contained in the ECHR. It builds on various efforts like the Internet Rights Charter of 2006 of the Association for Progressive Communications (APC), a leading NGO in the field of Internet governance and human rights, and the work done in the framework of the Council of Europe and other forums.[218] The Charter spells out freedom of expression and information on the Internet, along the lines of Article 19 UDHR and ICCPR, and identifies several Internet-related elements of the right like "freedom of online protest", "freedom from (online) censorship", "right to information", "freedom of the media" and "freedom from hate speech".

Of obvious relevance to the topic of this publication is the work of the Dynamic Coalition on Freedom of Expression, which was established after the first IGF in Athens in 2006. It regularly organises workshops in the framework of the IGF, but generally is less active than the Internet Rights and Principles Coalition. It is particularly concerned with restrictions of freedom of expression worldwide, by censorship, filtering and blocking ordered by governments, but also by the role of the private sector in restricting freedom of expression.[219]

---

216. *Charter on Human Rights and Principles for the Internet* at www.internetrightsandprinciples.org/wpcharter.
217. See Internet Rights & Principles Coalition (October 2011), *Commentary to the Charter on Human Rights and Principles for the Internet*, /www.law-democracy.org/wp-content/uploads/2011/10/Charter-Commentary.pdf.
218. See Preamble of the Charter, note 216 *supra*.
219. See the activities of the Dynamic Coalition on Freedom of Expression, www.dcexpression.wordpress.com.

4.3.2. Standard-setting in the private sector

The Parliamentary Assembly of the Council of Europe in its resolution on the protection of freedom of expression and information on the Internet and online media has highlighted the role of the private sector in respecting and promoting freedom of expression.[220]

According to this resolution "the Assembly is concerned that ICT-based media might unduly restrict access to, and dissemination of, information for commercial and other reasons without informing their users", which would be breaching user rights. Therefore, the Assembly calls on the media to set up self-regulatory codes of conduct to respect the rights of their users to freedom of expression and information and to ensure transparency of their corporate policies.[221] In addition the Assembly, in its Recommendation 1998 (2012) on the protection of freedom of expression and information on the Internet online media, recommends that the Committee of Ministers develop guidelines on domestic jurisdiction over, and the legal and corporate responsibility of, private intermediaries for ICT-based media for the functioning of the Internet and the respect for freedom of expression and information. Together with EU bodies a common application of Article 10 ECHR and Article 11 of the EU Charter of Fundamental Rights regarding freedom of expression and information on ICT-based media should be ensured.[222]

The responsibility of the business sector in protecting and respecting human rights, and providing remedies for their violation, has been elaborated by the Special Representative of the Secretary General of the United Nations, John Ruggie, in his reports delivered in 2008 and 2011, in which he proposed a framework and principles for corporate social responsibility.[223] The 'responsibility to protect, to respect and to remedy' framework and the 31 guiding principles on business and human rights are also applicable to the private sector in the field of ICT. For example, in order to identify and prevent adverse human rights impacts, business enterprises are to carry out human rights due diligence. This should involve meaningful consultation with potentially affected groups and other relevant stakeholders, taking appropriate action,

220. See Parliamentary Assembly (25 April 2012), Resolution 1877 (2012) on the protection of freedom of expression and information on the Internet and online media.
221. Ibid., paras. 10 and 11.
222. Parliamentary Assembly (25 April 2012), Recommendation 1998 (2012) on the protection of freedom of expression and information on the Internet online media.
223. See Ruggie J. (7 April 2008), Human Rights Council, Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, *Protect, respect and remedy: a framework for business and human rights*, UN Doc. A/HRC/8/5 and *Guiding principles on business and human rights, implementing the United Nations "Protect, respect and remedy" framework*, Annex to the Final Report of the Special Representative to the Human Rights Council, UN Doc. A/HRC/17/31 and adopted by the Human Rights Council (16 June 2011) by Resolution 17/4.

monitoring the effectiveness of the response and communicating their action as part of their accountability.[224]

The Global Network Initiative (GNI) was set up in 2008 as a collaborative project of major Internet firms, starting with Microsoft, Google and Yahoo! Together with some NGOs and academia it aims to strengthen respect for human rights in the work of relevant business actors, which therefore are invited to join. It focuses on freedom of expression and privacy, which explains its relevance for our topic.[225] Its activities so far have included drafting principles and implementation guidelines[226] and an accountability and learning framework.

The GNI acknowledges that the Ruggie framework has been a prime influence in its work.[227] Besides dialogue with companies on risks to freedom of expression and privacy, efforts to increase its membership and activities of shared learning, it monitors an assessment process in three phases: self-reporting, independent assessment of implementation of GNI principles based on criteria and an assessment template, and case studies. It also undertakes other initiatives like studies for taking freedom of expression and privacy better into account.[228]

4.3.3. Transparency to protect freedom of expression

One GNI member, Google, publishes semi-annual "transparency reports", which inform readers about requests from government agencies and courts for Google to removal content, mainly references to certain websites in the search results, or to hand over user data.

By far the largest number of requests, however, are related to requests for removals because of alleged copyright infringements, reaching 14 million requests in one month in 2012. As such requests constitute interference with freedom of expression, they have to respect the requirements indicated in Article 10 paragraph 2 ECHR or Article 19 ICCPR, which is difficult to assess as the transparency reports publish trends in requests rather than details of the requests themselves. However, they also give information on the reaction of Google to the requests, which do not only come from courts, but more often

224. Ibid., Guidelines 17-21. See also Mares R. (ed.) (2012), *The UN Guiding principles on business and human rights, foundation and implementation*, Martinus Nijhoff.
225. See Global Network Initiative, *Protecting and advancing freedom of expression and privacy in information and communications*, www.globalnetworkinitiative.org.
226. See Global Network Initiative, www.globalnetworkinitiative.org/principles/index.php.
227. See Global Network Initiative, *Inaugural Report 2010, Our Work. Our vision. Our progress*, p. 7, www.globalnetworkinitiative.org/files/GNI_Annual_Report_2010.pdf.
228. Hope D. A. (2011), *Protecting human rights in the digital age: understanding evolving freedom of expression and privacy risks in the ICT industry*, https://globalnetworkinitiative.org/sites/default/files/files/BSR_ICT_Human_Rights_Report.pdf.

from ministries or private associations. In any case, it can be concluded that the number of requests is increasing.[229]

In the last six months of 2012, Google received some 22,000 requests for user information, a 17 % increase from 2011. The company complied with 90 % of US-based requests but with none of some other countries, such as Turkey.[230] Of US-based requests to Google, 70 % came from government entities and did not usually involve judges. Only 20 % were brought under the Electronic Communications Privacy Act (ECPA), which requires the determination of a "probable cause" by a judge.[231] Google explained that it took a very careful approach to ensuring that requests satisfy "the law and our policies". It must be "in writing, signed by an authorised official of the requesting agency and issued under an appropriate law" and not overly broad. Once a request is received Google notifies the users, when appropriate, of the legal demands so they can contact the entity requesting the information or seek legal representation. Google also emphasised that, in criminal investigations, a search warrant is necessary to force the company to provide a user's search query information and private content stored in a Google account. The company argues that "a warrant is required by the Fourth Amendment to the U.S. Constitution, which prohibits unreasonable search and seizure and overrides conflicting provisions in ECPA".[232] Though this is an admirable position from a freedom-of-expression standpoint it raises interesting questions about the role of companies in interpreting legal provisions.

Twitter has also started to publish a Transparency Report on its website.[233] Since 1 January 2012 the company has received 1,858 information requests, 48 removal requests and 6,646 copyright notices. Among the 1,009 information requests received in the second half of 2012, the company complied with 57 %. Of the 815 requests originating in the US, Twitter complied with 69 %. It did not comply with requests from certain states, such as India, Switzerland and Turkey, and with only 4 % and 5 % of requests made from the United Kingdom and Japan.[234]

There was a clear upturn in removal requests (where Twitter was asked to remove or withhold content by governments or "authorised reporters") after the first half of 2012. Between January and July 2012 Twitter received only

229. See Google, Transparency Report, at www.google.com/transparencyreport/removals.
230. Google, Transparency Report, www.google.com/transparencyreport.
231. Google, Salgado R. (23 January 2013), "Transparency Report: What it takes for governments to access personal information", *Google public policy blog*, www.googlepublicpolicy.blogspot.co.at/2013/01/transparency-report-what-it-takes-for.html.
232. Drummond D. (28 January 2013), "Google's approach to government requests for user data", *Google blog,* www.googleblog.blogspot.com/2013/01/googles-approach-to-government-requests.html.
233. Twitter, Transparency Report, at www.transparency.twitter.com.
234. Twitter (1 July - 2 December 2012), Transparency Report, Information requests, www.transparency.twitter.com/information-requests-ttr2.

six such requests, whereas it received 42 in the second half of the year. There was a slight downturn in copyright notices in the second half of 2012, down to 3,268 from 3,378 in the first half.[235] Twitter complied with about 50 % of all copyright-based takedown notices. All actionable takedown notices and counter notices are communicated to the website Chilling Effects, which monitors limits to online freedom of expression.[236]

While it is important for Internet companies to protect the privacy of their users and their right to engage in freedom of expression, certain limits are not only possible but even required by international human rights law. On 24 January 2013, for instance, a French court ruled that Twitter had to identify authors of anti-Semitic messages "within the framework of its French site". The ruling had come after France's Union of Jewish Students had sued Twitter for failing to police more effectively the misuse of the site as a forum for anti-Semitic slurs under #unbonjuif (#agoodjew).[237] Twitter complied with the ruling.

The standards described in this chapter show that states, international organisations, civil society and companies often work together to ensure a higher level of protection for freedom of expression on the Internet. No single institution or actor can safeguard freedom of expression online in light of today's challenges. The issues that emerge touch upon many aspects of society and only through the co-operation of all actors, in a multi-stakeholder model, can we hope to ensure adequate protection of freedom of expression in light of its legitimate restrictions. Some of the most pressing societal issues that arise when freedom of expression and other rights come into conflict will be discussed in the following chapter.

235. Ibid., Copyright Notices, at www.transparency.twitter.com/copyright-notices and www.transparency.twitter.com/copyright-notices-ttr2.
236. Chilling Effects, at www.chillingeffects.org.
237. AFP (24 January 2013), *French court says Twitter must identify racist tweeters*.

5. Specific issues

The Internet has substantially affected all fields of human activity and has multiplied the possibilities to communicate: more actors can now use more communicative means to convey more messages more quickly to an increasing number of people. What the agora was to the denizens of the Greek city states and the forum was to the Romans, the Internet is to today's community of citizens engaged in a communicative matrix: a place to interact with others, to discuss current events, and to define their individual and group identity.

The Internet has influenced the eco-political and socio-cultural conditions under which meaning is produced online and goods are purchased, but also the conditions under which rights are exercised and violated. The expansion of freedom of expression on the Internet has sociological, economic and cultural consequences with impacts on our civil and political self-identity. We covered the protection of freedom of expression in Chapter 2 and the restrictions of the right in Chapter 3, and we discussed standard-setting mechanisms by the Council of Europe and non-state actors in Chapter 4.

Now, we draw from those chapters to look at some specific aspects of freedom of expression on the Internet. They are only facets of the communicative revolution, but taken together they provide a clear picture of the challenge of ensuring freedom of expression while countering socially corrosive trends. Indeed, the hermeneutics of protecting freedom of expression and the roles allocated to the different actors in this process (and their interaction) form the anvil on which the future of human rights protection on the Internet will be hammered out.

We first ask a fundamental question: do we need content regulation at all? What should legislators take into account when considering legislation that may inhibit freedom of expression? We then turn to a fundamental right in the Internet age: the right to access the Internet as a precondition for freedom of expression online. But access alone is not sufficient, as subsequent chapters will show: the technological neutrality of human rights norms and the principle of network neutrality together increase the protection of freedom of expression online. We then turn to some elemental characteristics of protected and unprotected speech online before focusing on how to most effectively fight hate speech.

The European Court of Human Rights took some time in reading a right to reputation into the right to privacy. Since then, a nuanced weighing of protection of reputation versus freedom of expression is necessary. We also consider the special protection children need on the Internet.

Not only blogs and social networks allow the exercise of freedom of expression online; even domain names can be used to express one's views, aggregate support and articulate ideas, especially critical ones. But how is freedom of expression online limited with regard to domain names, which are more intensively regulated than many other online resources?

We also look at the increasingly important role of Internet intermediaries as gatekeepers of the Internet-based information flows and communication networks and their role in ensuring (and limiting) freedom of expression in social networks. We conclude this chapter with a key challenge for the future development of the information society: As private Internet intermediaries take over the running of public debates, does that change the very nature of the privately owned communicative spaces they have created and run under private law-based terms of service? What are the responsibilities of social networks as the public spaces of the future?

5.1. Internet content regulation and freedom of expression

It is one of the tropes of the Internet age that the online world is one without laws, that governments have no authority over online activities and no effective means of execution. As social relations on the Internet have become more complex, states have increased their role in online environments. States exercise sovereignty over Internet-related situations emerging within their jurisdiction, and indeed they have to. As the case of *K.U. v. Finland*[238] shows, states have an obligation, under the European Convention of Human Rights, to ensure that the human rights of persons under their jurisdiction are protected – offline just as online. This protection, central to freedom of expression online, must be effective. In deciding how best to ensure protection, legislators must consider three levels of question.[239]

First, legislators have to consider whether to regulate or not. It is always difficult to pinpoint exactly when a social situation demands legal norms and up to what point social norms are enough. If a state introduces too strict a rule too early in time, this may hamper technological development. Then again, not ruling at all may lead to anarchy and human rights violations. Second, legislators need to decide which entity should be the regulator. Often the

238. *K.U. v. Finland* (2 December 2008), application No. 2872/02.

239. Cf. Kettemann M. C. (2011), "Building the legal framework of the information society: lessons from combating hate speech", in Schweighofer E. and Kummer F. (eds), *Europäische Projektkultur als Beitrag zur Rationalisierung des Rechts. Tagungsband des 14. Internationalen Rechtsinformatik Symposiums IRIS 2011* [European project culture as a contribution to the rationalisation of law: contributions to the 14th International Symposium on Legal Informatics], ÖCG, Vienna, pp. 179-182.

self-regulatory powers of stakeholders will be enough but sometimes governments, as the traditional rule-making authority, come into play. Third, the technical question of how to regulate needs to be answered. Depending on the normative goal, the normative and technological means will differ.

Let us illustrate this approach with the example of hate speech. First, a state has to consider whether to fight (certain) online hate speech or allow it. International law helps answer that question because it sets down certain standards that all states must obey, such as the prohibition of incitement to genocide. But with regard to other hate speech, such as negationism, a country with a different historical experience from, say, Germany, may decide not to penalise Holocaust denial. Some states, such as France or Switzerland, may also decide to penalise denial of other genocides while other states consider these denials covered by freedom of expression. On the second level, states have to consider which actor is best suited to implementing the prohibition of hate speech. States may consider censorship by Internet service providers, relying on unofficial blacklists maintained by non-governmental organisations, to be more effective or they may rely on their own criminal law – or a combination of both. On the third level, states may also consider whether it makes more sense to blacklist sites or to have servers physically remove (access to) them.

In assessing the different approaches, states have to keep in mind that they should always choose the least invasive one – in keeping with international human rights law and its principles of necessity and proportionality.

5.2. Access to the Internet as a precondition for freedom of expression online

Access is a key precondition to exercising online freedom-of-expression rights. In that sense the Internet is an enabler of human rights.[240] But access – often understood primarily in the physical, or infrastructure, dimension – is only one of two dimensions of access. Distinct from access to the Internet is the right to access online content. Ensuring both poses specific, but interrelated human rights challenges. Using the Internet as a facilitator for other human rights presupposes access to the Internet in the first place (connectivity) and then unfiltered access to content.[241]

Access to information online has played a role in a number of judgments of the European Court of Human Rights. If information can be found online, it may have a more intensive impact than offline information. Therefore, the standards applied to publishing information offline have to be refined in light of the

240. See *supra*, 2.3.

241. Cf. La Rue F. (16 May 2011), *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, UN Doc. A/HRC/17/27.

increased impact. Further, information that is freely available online can also be accessed by minors. Taken together, these two elements may dip the scale towards a state's right to restrict certain information in accordance with Article 10 paragraph 2, as the Court ruled in *Mouvement Raëlien Suisse v. Switzerland.*[242]

Access to the Internet, in both physical and content dimensions, is more directly at stake in a case that is still before the Court. In *Jankovskis v. Lithuania*[243] the Court will have to decide whether prison authorities can refuse to give convicted prisoners access to the Internet. In this case, Mr Jankovskis, a prisoner, wished to enrol in an online course but the Supreme Administrative Court ruled that use by prisoners of the Internet was not permitted by law, as prison authorities would be hampered in their fight against crime committed by inmates. Mr Jankovskis maintains that the refusal to allow prisoners access to the Internet violates their right to receive and impart information and ideas.

Courts have already given some important protection to the right of access to the Internet and information online. With its decisions in *Scarlet Extended*[244] and *SABAM*[245] the Court of Justice of the European Union has made two important inroads for access in both dimensions. In *Scarlet Extended*, the court found that a requirement for Internet service providers to install filtering software in order to conduct blanket searches for unlawful content would amount to an infringement of data-protection rules and, since lawful communications might be blocked as well, of freedom of expression online.

In *SABAM*, the court confirmed that owners of social networking sites cannot be obliged to install general filtering systems to cover all their users, even if these filtering systems would be effective in preventing the unlawful use of copyrighted material.[246] Again, the court reasoned that violations of data-protection rules, the freedom to conduct business and the freedom to receive or impart information were to be given more weight than narrowly construed property rights.[247]

In human rights terms, an even clearer case for protection of freedom of expression was made by the European Court of Human Rights in *Yildirim v. Turkey*,[248] the first case decided in Strasbourg that assesses the formal and material criteria for Internet censorship. The applicant complained that a blocking order (unrelated to him) by a Turkish criminal court made access to Google Sites no longer possible. After the blocking order was executed by the Telecommunications

242. *Mouvement Raëlien Suisse v. Switzerland* (13 July 2012), application No. 16354/06, paras. 54-8.
243. *Jankovskis v. Lithuania*, application No. 21575/08, communicated on 27 September 2010.
244. *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* (24 November 2011), ECJ C-70/10.
245. *SABAM v. Netlog NV* (16 February 2012), ECJ C-360/10.
246. See also Kettemann M. C. (2013), *The future of individuals in international law: lessons from international Internet law*, Utrecht: Eleven International, p. 155.
247. See also 1.5. to 1.7.
248. *Yildirim v. Turkey* (18 December 2012), application No. 3111/10.

Directorate (TİB) he could no longer access his academic work, which he published on a website hosted by the same service. The Court noted that the blocking order amounted to a restriction on Internet access. The restriction was serious because the Internet has developed into "one of the principal means for individuals of exercising the right to freedom of expression and information".[249]

The Court then analysed whether the rule was justified under the exception regime of Article 10 paragraph 2 ECHR. The Court first found that the blocking order was not foreseeable, since the criminal proceedings concerned a third party and the blanket ban on Google Sites, legal under Turkish law, amounted to an unforeseeable restriction. The Court also criticised the fact that the court issuing the blocking order had to weigh the interests at stake before denying access to Google Sites. The Court therefore ruled that the interference did not meet the foreseeability criterion of Article 10 paragraph 2, nor did it allow the applicant the level of protection necessary under rule-of-law considerations in a democratic society. Further, the Turkish law allowing the blocking order was in direct violation of the protection of the right to freedom of expression "regardless of frontiers" as per Article 10 paragraph 1.

In coming to this conclusion the Court also gives an overview of international commitments on Internet access.[250] These include, the Court wrote, the Declaration of the Committee of Ministers on human rights and the rule of law in the information society[251] (recognising "that limited or no access to ICTs can deprive individuals of the ability to exercise fully their human rights"), the Declaration on freedom of communication on the Internet of 2003,[252] the Recommendation on measures to promote the public service value of the Internet,[253] Recommendation CM/Rec(2007)11 to member states on promoting freedom of expression and information in the new information and communications environment, adopted on 26 September 2007, the Recommendation on measures to promote the respect for freedom of expression and information with regard to Internet filters[254] and the Recommendation on the protection of human rights with regard to search engines.[255]

249. Ibid., para. 54: "[L]'Internet est aujourd'hui devenu l'un des principaux moyens d'exercice par les individus de leur droit à la liberté d'expression et d'information." [our translation]
250. Ibid., paras. 19 et seq.
251. Council of Europe, Committee of Ministers (13 May 2005), Declaration of the Committee of Ministers on human rights and the rule of law in the Information Society, CM(2005)56 final.
252. Council of Europe, Committee of Ministers (28 May 2003), Declaration on freedom of communication on the Internet.
253. Council of Europe, Committee of Ministers (7 November 2007), Recommendation CM/Rec(2007)16 to member states on measures to promote the public service value of the Internet.
254. Council of Europe, Committee of Ministers (26 March 2008), Recommendation CM/Rec(2008)6 to member states on measures to promote the respect for freedom of expression and information with regard to Internet filters.
255. Council of Europe, Committee of Ministers (4 April 2012), Recommendation CM/Rec(2012)3 to member States on the protection of human rights with regard to search engines.

This list shows how important in aggregate are the recommendations of the Council of Europe's Committee of Ministers, discussed in more detail in Chapter 7.[256] They provide guidance that the Court can take into account when developing its case law. The Court also took note of the European Parliament recommendation on strengthening security and fundamental freedoms on the Internet and of the CJEU's *Scarlet Extended* case, in a nod to its Luxembourg sister court.[257] Finally, it referenced General Comment No. 34 of the Human Rights Committee, the quasi-judicial body overseeing the ICCPR, in which the Committee described the challenges of protecting human rights online in words that merit a full quotation:

> 15. States parties should take account of the extent to which developments in information and communication technologies, such as internet and mobile based electronic information dissemination systems, have substantially changed communication practices around the world. There is now a global network for exchanging ideas and opinions that does not necessarily rely on the traditional mass media intermediaries. States parties should take all necessary steps to foster the independence of these new media and to ensure access of individuals thereto.[258]

One important factor in ensuring access for all to content is that Internet service providers do not discriminate against certain content. The principle of not discriminating on the basis of content – "network neutrality" – is closely linked to freedom of expression as an enabling factor.

5.3. Technological neutrality and freedom of expression

On 5 July 2012, the UN Human Rights Council (HRC) adopted by consensus a key resolution on the promotion, protection and enjoyment of human rights on the Internet.[259] The resolution affirms in paragraph 1 that "the same rights that people have offline must also be protected online". This commitment represents the backbone of the argument made in this book that human rights online are the same as offline and only the challenges are new. As we explained in Chapter 2, the Internet has become a catalyst for individuals all across the

256. For a full overview of relevant documents, see List of Committee of Ministers' Recommendations, Resolutions and Declarations adopted in the media field, www.coe.int/t/dghl/standardsetting/media/Doc/CM_en.asp.
257. European Parliament (26 March 2009), Recommendation A6-0103/2009 to the Council on strengthening security and fundamental freedoms on the Internet, www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A6-2009-0103&language=EN.
258. Human Rights Committee (12 September 2011), General Comment No. 34 on Article 19: Freedoms of opinion and expression, CCPR/C/GC/34.
259. UN Human Rights Council (5 July 2012), Resolution A/HRC/20/8 on the promotion, protection and enjoyment of human rights on the Internet. For an analysis, see Cf. Kettemann M.C. (1/2012), "The UN Human Rights Council Resolution on Human Rights on the Internet: Boost or Bust for Online Human Rights Protection", *Human Security Perspectives,* pp. 145-169.

world to exercise a broad range of human rights. It is a key means by which freedom of expression can be exercised,[260] and freedom of expression in turn is not only a human right by and of itself but also enables the enjoyment of other human rights, including economic, social and cultural rights and civil and political rights, such as freedom of association and assembly.[261]

The Human Rights Council, in its resolution on online human rights, specifically refers to freedom of expression and cites the language of Article 19 of the Universal Declaration of Human Rights (UDHR), which guarantees everyone "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".

Article 19's language is based on technological neutrality ("through any media") and recognises the importance of entering into universal processes of seeking and imparting information and ideas ("regardless of frontiers"). It thus seems to have anticipated developments in ICTs and the growing internationalisation of content flows. Similarly, Article 19 of the ICCPR protects freedom of expression independent of borders. Its paragraph 2 enshrines the right to freedom of expression, including the "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 [one's] choice". Again we find the dual preconditions of technological neutrality – "through any [media] of [one's] choice" – and the universality of the information processes – "regardless of frontiers".

This clear commitment to the technological neutrality of human rights, based on the Universal Declaration of Human Rights, contained in the ICCPR and largely reflected in international customary law, has been confirmed by the Human Rights Council resolution. It is thus part of international human rights law. We examine now how the case law of the European Court of Human Rights reflects the importance of technological neutrality in human rights protection.[262]

5.4. Network neutrality and freedom of expression

Network neutrality (or net neutrality) is a design paradigm according to which the network must not prioritise some information over other, for example by charging different rates or providing different

260. La Rue F. (16 May 2011), *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, UN Doc. A/HRC/17/27, para. 20.
261. Cf. the main elements of the right as explained in 2.1.
262. Cf. Kettemann M.C. (1/2012), "The UN Human Rights Council Resolution on Human Rights on the Internet: boost or bust for online human rights protection", *Human Security Perspectives*, pp. 145-169.

bandwidths.[263] Network neutrality is closely related to the demand for openness of the Internet[264] and can be violated by blocking, monopolistic pricing, preferential treatment to certain providers (or certain content) and failures in transparency.[265] The main problem is that certain commercial uses may be given preference over others, for example educational uses, or that certain Internet service providers may wish to penalise users of file-sharing services by slowing down their connections. But checking the content that runs through the network is only possible through Deep Packet Inspection, a practice that meets serious human rights challenges,[266] especially in light of the closed process of standard-setting in which the World Telecommunication Standardisation Assembly of the International Telecommunication Union passed its new Requirements for Deep Packet Inspection in Next Generation Networks.[267]

In 2010, the Council of Europe's Committee of Ministers declared its commitment to the principle of network neutrality and stressed that any exceptions to network neutrality would have to be in accordance with the human rights protection framework.[268] Again, we have a situation where both states and private Internet companies have to be reminded of their human rights obligations regarding freedom of expression on the Internet. This is not to say that network operators are not allowed to manage Internet traffic. Indeed, certain management steps are necessary to ensure quality of service and network stability. Yet, just as police must regulate traffic in order to ensure safe travel but must not discriminate against certain drivers, network managers must, as a principle, not depart from network neutrality.

Exceptions are possible only when "overriding public interests" are at stake. Even – or especially – in these situations, states have to take into account the protective ambit of Article 10 and the case law of the European Court of Human Rights:[269] restrictive measures thus need to meet the three-part test of being provided by law, necessary in a democratic society for the pursuit of a legitimate goal and proportionate (i.e. appropriate and avoiding unjustified discrimination).[270] In addition, the Council of Europe recommended that any measures that violate network neutrality should be subjected to periodic

263. Wu T. (2003), "Network neutrality, broadband discrimination", *Journal of Telecommunications and High Technology Law*, Vol. 2, p. 141; Yoo C. (Fall 2005), "Beyond network neutrality", *Harvard Journal of Law and Technology*, Vol. 19.
264. Cf. 2.1.8.
265. Wu T., at http://timwu.org/network_neutrality.html.
266. Cf. Center for Democracy and Technology (28 November 2012), *Adoption of traffic sniffing standard fans WCIT flames*, www.cdt.org/blogs/cdt/2811adoption-traffic-sniffing-standard-fans-wcit-flames.
267. ITU-T (November 2012), Recommendation Y.2770 on Requirements for deep packet inspection in next generation networks, www.itu.int/rec/T-REC-Y.2770-201211-P.
268. Council of Europe, Committee of Ministers (29 September 2010), Declaration of the Committee of Ministers on network neutrality, http://wcd.coe.int/ViewDoc.jsp?id = 1678287, para. 9.
269. Cf. ibid., para. 6.
270. For more detail on restrictions generally, see Chapter 3.

review and maintained only as long as they are necessary. Network operators need to inform users when, under which conditions, and for what reasons they violate network neutrality and states need to provide for adequate avenues to challenge network management decisions.[271]

The human rights issues that are involved when companies violate network neutrality became evident when Deutsche Telekom, Germany's most important Internet access provider, announced that it would – for future clients – reduce downstream transfer speed to 384 kBit/s after transfer volumes of 74 to 400 GByte had been reached (depending on contract). This is problematic since Telekom can thus effectively limit users' access to Google's YouTube, Amazon's Lovefilm and ProSiebenSat1's Maxdome services.[272] The announcement met with strong criticism, but aptly illustrates how the lack of a coherent international framework for ensuring net neutrality is problematic.

5.5. Characteristics of protected and unprotected speech online

National discourses are held under national laws. The internationalisation of discourses and the assessment of expressions under different jurisdictions has made it difficult to find clear answers to the question of what content is (or should be) prohibited. Cultural, historical and religious reasons can be (and have been) used to find exception to the universality of the right to freedom of expression. In assessing expressions, it helps to keep three types of expression strictly apart, as they necessitate different reactions by states:

> (a) expression that constitutes an offence under international law and can be prosecuted criminally;
>
> (b) expression that is not criminally punishable but may justify a restriction and a civil suit; and
>
> (c) expression that does not give rise to criminal or civil sanctions, but still raises concerns in terms of tolerance, civility and respect for others.[273]

States are obliged to prohibit content falling under category (a). The category includes expression that is prohibited by international law:

- images of sexual exploitation of children (to protect the rights of children);
- advocacy of national, racial or religious hatred amounting to incitement to discrimination, hostility or violence (to protect the rights of others, such as the right to life);

271. Council of Europe, Committee of Ministers (29 September 2010), Declaration of the Committee of Ministers on network neutrality, para. 8.
272. Cf. Heise.de, Telekom kappt Festnetz-Flatrates [Telekom kills flatrates for fixed lines], 22 April 2013, www.heise.de/newsticker/meldung/Bandbreiten-Drossel-Telekom-kappt-Festnetz-Flatrates-1847224.html.
273. UNGA (10 August 2011), Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/66/290, para. 18.

– direct and public incitement to commit genocide (to protect the rights of affected communities); and
– incitement to terrorism.[274]

Originally, the Special Rapporteur on Freedom of Expression also included defamation in this category,[275] but later argued that it should not be criminalised because of the potential chilling effect on freedom of expression.[276] Of course, states also have to ensure that they provide for a system of laws and courts that allows those victimised by expressions under (b) to file claims invoking civil liability. States also have an important role to play in awareness raising and thus minimising the number of civility-offences under (c), and should, rather than criminalise such expressions, address the underlying causes of discrimination in their society.[277] In their quest to fight hate speech and adopt non-legal and legal measures, states have to carefully craft their responses. Laws that request intermediaries to screen and remove user content, force registration requirements upon users or arbitrarily block websites are as bad as vaguely worded laws with disproportionate sanctions.[278]

Instead, states have to very carefully draft laws that safeguard legitimate expressions but fight serious and actual hate speech. Content that is not illegal, however, be it potentially harmful, offensive or objectionable or just undesirable, must not be the target of state censorship. It is precisely shocking, offending and disturbing ideas that need protection, as the Court laid down in *Handyside v. UK*.[279] But what if expression does not only shock, offend and disturb, but also endanger, discriminate and denigrate others? What about, in short, "hate speech" and how can we differentiate, if at all, between hate speech and incitement to discrimination, violence and racism online?

5.6. Fighting online hate speech

Hate speech is a phenomenon that predates the Internet age.[280] Racism, xenophobia, anti-Semitism, aggressive nationalism and discrimination against minorities and immigrants[281] are present online as well. Indeed, the very

274. Cf. ibid., paras. 20-36.
275. La Rue F. (16 May 2011), *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, UN Doc. A/HRC/17/27, para. 25.
276. Ibid., para. 40.
277. Ibid.
278. Report of the Special Rapporteur on Freedom of Expression (2012), para. 32.
279. Cf. *Handyside v. the United Kingdom* (7 December 1976), application No. 5493/72, para. 49.
280. Cf. Council of Europe, Committee of Ministers, Recommendation No. R 97 (20) on "hate speech" and Recommendation 1805 (2007) of the Parliamentary Assembly of the Council of Europe on blasphemy, religious insults and hate speech against persons on grounds of their religion.
281. Council of Europe, Committee of Ministers, Recommendation No. R 97 (20) on "hate speech".

nature of the Internet makes it easier for authors of hate speech to get their message of hate across and more difficult for authorities to fight it.[282]

The biggest challenge underlying the fight against hate speech is finding the right balance between the right of individuals to voice opinions that "offend, shock or disturb", as the Court had already ruled in 1976 in *Handyside*,[283] and the right of others not to be subjected to messages of hate.[284] "[T]olerance and respect for the equal dignity of all human beings", the Court emphasised in *Erbakan,*[285] "constitute the foundations of a democratic, pluralistic society". Of course, not all opinions are based on tolerance and respect for the equal dignity of all. But only those opinions that go beyond offending, shocking or disturbing and, as the Court noted in *Erbakan*, "spread, incite, promote or justify hatred based on intolerance" can (and indeed have) to be punished in democratic societies. It is essential to understand both the content of hate speech and its context. A statement that amounts to hate speech in certain contexts may not be hate speech in others; and the content of hate speech cannot be analysed in the abstract because a statement may be considered humorous by some, but hate speech by others.[286]

The Internet has increased the visibility of hate speech, which has been made more acute by increases in immigration, social and economic turmoil and the emergence of terrorism. Rather than solving these problems, national laws have sometimes compounded them. Special Rapporteur Frank La Rue in his 2012 report especially criticised "flawed national security and anti-terrorism laws and policies, such as racial profiling, demagogic statements by opportunistic politicians and irresponsible reporting by the mass media".[287]

The Internet has also made it easier to engage in hate speech. Special Rapporteur La Rue reminds us that it is usually politicians and the media who play the central role in fostering offline hate, but the Internet has enabled anyone to become the author of visible hate speech, even anonymously.[288]

Already in 2000, ECRI published its General Policy Recommendation No. 6 on Combating the dissemination of racist, xenophobic and anti-Semitic material via the Internet. The Committee showed itself "deeply concerned by the fact that the Internet is also used for disseminating racist, xenophobic and anti-Semitic material, by individuals and groups aiming to incite to intolerance or racial and ethnic hatred".[289]

---

282. See Akdeniz Y. (2010), *Racism on the Internet*, Council of Europe.
283. *Handyside v. the United Kingdom* (7 December 1976), application No. 5493/72, para. 49.
284. Cf. also the role of the concept of margin of appreciation, explained in 3.2.2.
285. *Erbakan v. Turkey* (6 July 2006), application No. 59405/00, para. 56.
286. Herz M. and Molnar P. (eds) (2012), *The content and context of hate speech. rethinking regulation and responses*, Cambridge: Cambridge University Press.
287. La Rue, F., *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, UN Doc. A/67/357 of 7 September 2012, at 24.
288. Ibid., at 30.
289. Council of Europe, ECRI (15 December 2000), General Policy Recommendation No. 6: Combating the dissemination of racist, xenophobic and antisemitic material via the internet.

In its jurisdiction, the Court has developed parameters in order to distinguish between merely offending language, which is protected, and hate speech, which is not. These parameters, developed originally without reference to the Internet, are nevertheless applicable to online surroundings. Online (and offline) hate speech has been excluded from the protection of the ECHR by way of Article 17 (which prohibits the abuse of rights) or by an application of the limitations contained in articles 10 and 11, namely restrictions deemed necessary in the interests of national security, public safety, the prevention of disorder or crime, the protection of health or morals and the protection of the rights and freedoms of others.

The case law of the Judges in Strasbourg contains important distinctions between what is considered protected speech and what lies outside the protective ambit of the Convention. In *Féret v. Belgium*[290] the Court ruled that aggressive political slogans distributed on leaflets could amount to incitement of racial discrimination. They carried strong resonance in an election, and Belgium had been justified in limiting freedom of expression in the interests of preventing disorder and protecting the rights of others. The Court's reference to the strong resonance of political slogans in an electoral context can have an impact in assessing the limits of Article 10 on the Internet, because online publications can be of much stronger resonance than purely offline ones.

Similarly, in *Léroy v. France*,[291] the Court found that glorification of terrorism through cartoons published in a local newspaper went beyond protected freedom of expression. Interestingly, the Court argued that the limited circulation of the newspaper did not diminish the seriousness of the violation of the rights of others. In light of the Internet's inherent unlimited accessibility, this approach can be used to argue for stronger protection from hate speech.

The Court's case law, from *Jersild v. Denmark*[292] onwards, also exhibits a difference in the treatment of authors of racist remarks and those who report on them. In *Jersild*, a Danish journalist who had made a documentary that contained footage of a group of people making racist remarks was found not to have overstepped the limits of freedom of expression. This difference between racist comments (that can be prohibited or punished) and reporting on racist comments is important, especially in the age of citizen journalists and bloggers. The Danish court's punishment of the journalist was considered a violation of his freedom of expression in the form of his critical presentation of the group making racist remarks.

The Court has also ruled that serious and prejudicial allegations based on sexual orientation could be considered as serious a discrimination as those based on other grounds. Therefore, in *Vejdeland and Others v. Sweden*,[293] the

290. *Féret v. Belgium* (16 July 2009), application No. 15615/07.
291. *Leroy v. France* (2 October 2008), application No. 36109/03.
292. *Jersild v. Denmark* (23 September 1994), application No. 15890/89.
293. *Vejdeland and Others v. Sweden* (9 February 2012), application No. 1813/07.

Court found that Swedish authorities had not erred in punishing the author and distributor (at a school) of an anti-homosexual leaflet.

A further category of hate speech that is prohibited offline and online is hate speech based on religion. In two similar cases the Court found that states could legitimately criminalise expressions linking a religious group (Islam) to terrorism (*Norwood v. the United Kingdom*)[294] or inciting hatred towards Jewish people (*Pavel Ivanov v. Russia*).[295] In the *Norwood* case the applicant had put a poster in his window showing the Twin Towers in flames with the caption "Islam out of Britain – Protect the British People". The Court found that he could not claim protection of Article 10 against this conviction of aggravated hostility towards a religious group by the British authorities. What applies to putting a poster in a window must also apply *a minori ad maius* to putting a post on one's social network profile. If the network is closed and only a limited number of people can see the posting, the conclusion may be different, but the open character of most social networks argues for a broad reading of *Norwood*.

The Internet is also a repository for Holocaust denials. Citizens of states where Holocaust denial is criminalised (such as Austria and Germany) can more easily access information published by Holocaust deniers that would not be available in printed form in their home countries. Some websites have used geo-locational filtering (as was suggested in the *Yahoo!* case), but it is often search engines that change their algorithms according to the laws of different countries in order to comply with anti-negationism statutes. The Court had clearly ruled in *Honsik v. Austria*[296] and later in *Garaudy v. France*[297] that Holocaust denial amounted to "one of the most serious forms of racial defamation of Jews and of incitement to hatred of them". Revisionist arguments were not protected by freedom of science or expression, but were rather attempts to spread hate by falsifying history.

Social media have enabled political activism on a much larger scale than in the pre-Internet age. This is also important for assessing whether expression can amount to a threat of public order. In *Karatas v. Turkey*,[298] the Court ruled that the higher the impact of speech, the higher its potential to disrupt public order.

Activists have also dynamised and internationalised discourses, exemplifying a phenomenon Cass R. Sunstein described as "going to extremes".[299] Within groups, extremists are usually confident of (what little) they know; since they are confident, they will not moderate their opinions and thus ensure higher group polarisation. Not all polarised statements are to be prohibited. Indeed, as per *Handyside*, statements that shock and disturb are protected. What the

294. *Norwood v. the United Kingdom* (16 November 2004), application No. 23131/03, admissibility decision.
295. *Pavel Ivanov v. Russia* (20 February 2007), application No. 35222/04, admissibility decision.
296. *Honsik v. Austria* (18 October 1995), application No. 25062/94.
297. *Garaudy v. France* (24 June 2003), application No. 65831/01, admissibility decision.
298. *Karatas v. Turkey* (8 July 1999), application No. 23168/94, para. 52.
299. Sunstein C. R. (2009), *Going to extremes: how like minds unite and divide*, Oxford: OUP, p. 41.

Court does not accept are applications for the protection of statements that are based on a totalitarian doctrine, militate for restoration of a totalitarian regime or are imbued with ideas endangering democracy.[300]

The Court laid the foundation for this approach in *Communist Party of Germany v. the Federal Republic of Germany*[301] and *B.H. et al. v. Austria*,[302] and strengthened it in *Refah Partisi.*[303] Political speech that poses, in aggregate, a real threat to democracy is therefore not protected under Article 10. However, criticism of a government, including criticism of its anti-terrorism politics and treatment of convicted terrorists, is protected,[304] especially if (even controversial) statements and strongly worded critiques are published with relation to a public debate or a matter of public interest.[305] As the Internet expands the possibility for public debate, the field of protected speech is also enlarged. While negationism or Holocaust denial veiled in the cloak of historical debate is not protected by the Convention, journalists and bloggers that question national historical narratives, as Firat (Hrank) Dink did, fall within the ambit of freedom of expression.[306]

The Council of Europe has also developed a conventional approach to fighting cybercrime and racist or xenophobic acts online. In 2003, it adopted an Additional Protocol to the Convention on Cybercrime, on the criminalisation of acts of a racist and xenophobic nature committed through computer systems.[307] Article 2 paragraph 1 of the 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.

States that have acceded to the Protocol commit to adopt those legislative and other measures necessary to establish as criminal offences under domestic law the intentional distribution, or otherwise making available, of racist and xenophobic material to the public through a computer system (Article 3 paragraph 1). Articles 4 and 5 oblige states to criminalise racist and xenophobic motivated threats and insults. Under Article 6 states agree to adopt legislation

300. Cf. European Court of Human Rights (June 2012), Press Unit, Hate Speech Factsheet.
301. *Communist Party of Germany v. the Federal Republic of Germany* (20 July 1957), application No. 250/57.
302. *B.H; M.W; H.P; G.K. v. Austria* (12 October 1989), application No. 12774/87.
303. *Refah Partisi (The Welfare Party) and Others v. Turkey* (13 February 2003), application Nos. 41340/98, 41342/98, 41343/98 and 41344/98.
304. *Faruk Temel v. Turkey* (1 February 2011), application No. 16853/05.
305. *Otegi Mondragon v. Spain* (15 March 2011), application No. 2034/07.
306. *Dink v. Turkey* (14 September 2010), application Nos. 2668/07, 6102/08, 30079/08, 7072/09 and 7124/09.
307. Council of Europe, Additional Protocol to the Convention on Cybercrime (28 January 2003), concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, CETS No. 189, www.conventions.coe.int/Treaty/en/Treaties/Html/189.htm.

necessary to criminalise the denial, gross minimisation, approval or justification of genocide or crimes against humanity as defined by international law and recognised as such by final and binding decisions of an international court established by relevant international instruments and whose jurisdiction is recognised by the state. As of 1 January 2013, the Protocol has been ratified by 20 states and signed by 15 more.

In implementing their duties under the Protocol, states can draw inspiration from the 2013 publication of the OCHCR's Rabat Plan of Action on the prohibition of advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence,[308] a plan which emanated from a universal, expert-led process. The Plan of Action recommended states to quickly adopt comprehensive legislation against discrimination, combining preventive and punitive action. Only thus can states hope to effectively combat incitement to hatred and empower minorities and vulnerable groups.[309]

The Rabat Plan of Action recognises that new technologies, including the Internet, "vastly … enhance the dissemination of information and open up new forms of communication".[310] The Plan of Action also contains input from the British NGO Article 19 on the circumstances under which hate speech amounts to advocacy constituting incitement to discrimination, hostility or violence pursuant to Article 20 paragraph 2 of the International Covenant on Civil and Political Rights.[311]

With regard to the Internet, explicit recognition of the three-part test of legality, necessity and proportionality continues to apply. Article 19, the NGO, suggests assessing all incitement cases under a six-part test.[312] This test considers:

1. the context of the expression (the existence of conflicts within society, a history of institutionalised discrimination, a history of clashes between audience and the targeted groups, the legal and the media framework);
2. the speaker of the expression (his/her official position, level of authority, the capacity in which s/he makes the statement);
3. the intent of the speaker (especially the volition to engage in hate speech and to target a protected group on prohibited grounds including the knowledge of certain consequences);

308. Rabat Plan of Action on the prohibition of advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence (2013), Conclusions and recommendations emanating from the four regional expert workshops organised by OHCHR in 2011 and adopted by experts in Rabat, Morocco on 5 October 2012, www.ohchr.org/Documents/Issues/Opinion/SeminarRabat/Rabat_draft_outcome.pdf.
309. OHCHR, *Between free speech and hate speech: the Rabat plan of action, a practical tool to combat incitement to hatred*, www.ohchr.org/EN/NewsEvents/Pages/TheRabatPlanofAction.aspx.
310. Rabat Plan of Action (2013), at p. 28.
311. Article 19, Prohibiting incitement to discrimination, hostility or violence, Policy Brief, 2012, at www.article19.org/data/files/medialibrary/3572/12-12-01-PO-incitement-WEB.pdf, p. 2.
312. Ibid., p. 29 et seq.

4. the language used by the speaker (his/her objectives, the scale and repetition of the communication);
5. the content of the expression (especially the style and the form: artistic expression, public discourse, religious expression, academic discourse, a statement of fact or a value judgment); and
6. the likelihood of the advocated action actually occurring, including its imminence.

Applying this incitement test to Internet-based hate speech will allow for a nuanced treatment of incitement, and the suppression and criminal prosecution of only those cases that actually amount to incitement or hate speech and transcend the protection ground of opinions that merely "shock, offend and disturb".

5.7. Defamation, reputation and freedom of expression online

Just like the *fama* in Virgil's Aeneid (the etymological root of de*fam*ation), negative rumours harmful to someone's reputation prosper on the Internet.

> [Fama] flourishes by speed, and gains strength as she goes:
> first limited by fear, she soon reaches into the sky,
> walks on the ground, and hides her head in the clouds.
> … fleet-winged
> and swift-footed, …
> who for every feather on her body has as many
> watchful eyes below …, as many
> tongues speaking, as many listening ears.[313]

Internet platform providers, site moderators and bloggers have to take care not to engage in defamation, and journalists reporting on events and news have to be careful not to publish content that is objectively defamatory. Although truth is an absolute defence against a claim of defamation, very often it can be difficult to establish or very costly do so.[314] A customer on a travel forum, for instance, might say that a specific hotel was a bad choice because of the small rooms and broken appliances. This includes their opinion ("bad choice") but it also contains a statement of fact ("broken appliances"). If the hotel identified in the review asks the website owner to take down the post (arguing that it is defamatory) the owner has a clear choice: either delete the post and thus arguably infringe the freedom of expression of its users or keep the post and thus, having owned up to it, risk a defamation-based suit by the hotel. The risk in the defamation suit is how to prove the veracity of the statement.

313. Virgil, *Aeneid: Book IV*, transl. by A.S. Kline (2002) at www.poetryintranslation.com/PITBR/Latin/VirgilAeneidIV.htm, lines 173-97.
314. Cf. Dario M. (2008), *Defamation and freedom of speech*, Oxford: Oxford University Press.

Unfortunately for the owner of the travel website, that duty now falls upon them. Though the original poster may help, he or she is under no obligation to do so. The website owner may have a hard time proving that at a certain date the appliances in one specific hotel room were faulty.

Voicing opinions (value judgments) online cannot amount to defamation; only statements of fact can be defamatory. As the European Court of Human Rights ruled in *Lingens*, "[t]he existence of facts can be demonstrated, whereas the truth of value judgments is not susceptible of proof".[315] However, the Court looks at the context of a statement to determine whether it is a true opinion or rather a statement of fact disguised as a value judgment.

Freedom of expression and the right to reputation as a weapon against defamation often conflict. The European Convention on Human Rights mentions reputation in Article 10 paragraph 2 only as a legitimate aim that would allow a restriction of freedom of expression: "for the protection of the reputation or the rights of others". In a number of cases, centrally *Pfeifer v. Austria*[316] (with regard to Article 8) however, the Court has developed a right to reputation from this basis as being part of a person's right to respect for private life.[317] More recently, in *Karakó v. Hungary*,[318] the Court seemed to qualify its strong position in *Pfeifer*, arguing that only "factual allegations [of a] seriously offensive nature [with an] inevitable direct effect on the applicant's private life" warrant protection, a position it largely held in *Polanco Torres and Movilla Polanco v. Spain*.[319]

In *Polanco Torres* (regarding an article alleging unlawful dealings and dirty money, published first in the *El Mundo* newspaper) the Court ruled that the journalist had sufficiently verified the veracity allegations contained in the article. The right to impart information that was in the general interest was given more weight than the right of reputation. What makes this case especially interesting for freedom of expression online is that the article under review was republished by another newspaper, *Alerta*, which was also charged with defamation but unlike *El Mundo* was convicted of it in the national courts because the journalists at *Alerta* had simply copied the article from *El Mundo* without checking the veracity of the allegations. The Court found no fault with the national decision regarding *Alerta*. From that we can deduce for the protection of freedom of expression online that merely republishing defamatory allegations without ensuring their veracity is highly problematic.

It remains unclear though whether the treatment of *Alerta* in *Polanco Torres* gives a preview of how non-journalists will be treated if they copy potentially

315. *Lingens v. Austria* (8 July 1986), application No. 9815/82, para. 46.
316. *Pfeifer v. Austria* (15 November 2007), application No. 12556/03.
317. Cf. Smet S. (2011/1), "Freedom of expression and the right to reputation: human rights in conflict", *American University International Law Review* 26, pp. 183-236.
318. *Karakó v. Hungary* (28 April 2009), application No. 39311/05.
319. *Polanco Torres and Movilla Polanco v. Spain* (21 September 2010), application No. 34147/06.

defamatory statements from trusted news sites to their own blogs without checking their veracity, or whether the standard should be applied only to journalists.

In the 2011 case of *Editorial Board of Pravoye Delo and Shtekel v. Ukraine*[320] the Court had another opportunity to assess the limits of defamation. The Court ruled that Article 10 must be interpreted as imposing on states an obligation to create an appropriate regulatory framework to ensure effective protection of freedom of expression on the Internet for journalists. *Pravoye Delo* is therefore to journalistic freedom online what *K.U. v. Finland* is to protection of minors on the Internet. The editorial board of the Ukrainian newspaper had been fined for publishing defamatory statements taken from the Internet accompanied by an editorial in which they distanced themselves from the statements. The Court found fault with the reluctance of the local courts to apply protections for offline media to online surroundings. The Court agreed that:

> [the] risk of harm posed by content and communications on the Internet to the exercise and enjoyment of human rights and freedoms, particularly the right to respect for private life, is certainly higher than that posed by the press. Therefore, the policies governing reproduction of material from the printed media and the Internet may differ. The latter undeniably have to be adjusted according to the technology's specific features in order to secure the protection and promotion of the rights and freedoms concerned.[321]

Just because the legal treatment of offline and online publications may differ, not applying safeguards at all is a violation of Article 10. This does not mean, however, that newspapers have to make individuals aware of potentially defamatory information. In *Mosley v. the United Kingdom*[322] the Court ruled that the United Kingdom could not be faulted for not giving a public figure whose sexual activities had been recorded and published in the form of images and videos on a newspapers' website the possibility of an injunction to prevent publication, even if the publication did violate his right to private life.

Journalistic ethics also have to develop to keep up with the growing challenges of electronic media and the growing number of media actors.[323] As journalists have started to use new media, with well-known journalists now routinely using Twitter and other social media, the Court has also had to face the question whether a statement by a journalist on his real-name Twitter account was a factual statement to be measured against journalistic ethics. In *Fatullayev v. Azerbaijan* the Court refused to differentiate between journalistic writings in newspapers and the writings of a journalist on a public Internet forum. Independent of the medium used, "accusing specific individuals of a specific

320. *Editorial Board of Pravoye Delo and Shtekel v. Ukraine* (5 May 2011), application No. 33014/05.
321. Ibid., p. 6.
322. *Mosley v. the United Kingdom* (10 May 2011), application No. 48009/08.
323. *Stoll v. Switzerland* (10 December 2012), application No. 69698/01, para. 149.

form of misconduct entails an obligation to provide a sufficient factual basis for such an assertion".[324]

Taken together, the case law of the European Court of Human Rights contains important markers for navigating between the right of freedom of expression and the right to private life, between legitimate publication in the public interest and defamatory comments. A key lesson, however, is – again – that states need to apply offline free expression protection guarantees to online situations, even if these have to be developed in recognisance of the special impact Internet publications often have.

This potential of the Internet to exacerbate violations of the right to reputation and the role of the Internet as a catalyst for freedom of expression are present, even in the title, of the 2012 Declaration of the Committee of Ministers on the desirability of international standards dealing with forum shopping in respect of defamation, "libel tourism", to ensure freedom of expression.[325] Recognising the special role of freedom of expression on the Internet in creating a public sphere necessary for democracy, the Declaration recalls that Article 10 refers to "duties and responsibilities" carried by the exercise of freedom of expression. Nevertheless, only limits necessary to protect the reputation or rights of others are allowed. They must also be "prescribed by law and … necessary in a democratic society". Referring to Parliamentary Assembly Recommendation 1814 (2007) on the decriminalisation of defamation,[326] the declaration recommends states to proactively review their defamation laws in light of the Court's case law.

The Internet is a universal network and knows no boundaries. Therefore authors of defamatory statements may see themselves facing a more stringent jurisdiction. While the Strasbourg Court usually leaves to the national judiciary to find the "fine balance [to be] struck between guaranteeing the fundamental right to freedom of expression and protecting a person's honour and reputation", different member states within the Council of Europe follow different ideas of proportionality and balancing of interests.

These differences have given rise to what is called libel tourism, a form of "'forum shopping' when a complainant files a complaint with the court thought most likely to provide a favourable judgment … and where it is easy to sue".[327] The risk of libel tourism is growing because of decreasing storage costs and the universal availability of much (defamatory) information online. Libel tourism

324. *Fatullayev v. Azerbaijan* (22 April 2010), application No. 40984/07, para. 95.
325. Council of Europe, Committee of Ministers (4 July 2012), Declaration on the desirability of international standards dealing with forum shopping in respect of defamation, "libel tourism" to ensure freedom of expression.
326. Council of Europe, Parliamentary Assembly Recommendation 1814 (2007), Towards decriminalisation of defamation.
327. Council of Europe, Committee of Ministers (4 July 2012), Declaration on the desirability of international standards dealing with forum shopping in respect of defamation, "libel tourism", to ensure freedom of expression, p. 5.

can have a detrimental effect on the availability of information because content providers may choose to proactively withdraw (even legal) content before risking costly defamation proceedings in an unfamiliar forum. It may sometimes be seen as "the attempt to intimidate and silence critical or investigative media purely on the basis of the financial strength of the complainant". This inequality of arms is particularly worrisome when small media providers are targeted by powerful companies (and their large legal departments).[328] The Court has provided some protection by ruling that disproportionately large awards to claimants can, as per *Tolstoy Miloslavsky v. United Kingdom*,[329] violate Article 10. But what can be done against libel tourism?

One approach would be to restrict jurisdiction in libel cases to those states where a "real and substantial connection" exists.[330] With this approach, a Danish journalist writing a potentially defamatory blog entry about a Danish company could not be sued by the company's parent in, say, Germany. Other measures could include in-depth reviews of national laws in light of the Court's case law and attempts to ensure legal certainty on jurisdiction and limits of awards.[331]

5.8. Protection of children in light of freedom of expression

Freedom of expression also encompasses the right to impart ideas that may be unsuitable for some age groups, such as offensive information. Therefore, freedom of expression may have to be subjected to more stringent limits when the speech could come in contact with children. As children are vulnerable because of their age, the law needs to protect them.

Two important cases of the European Court of Human Rights help set the stage for balancing freedom of expression and the need to protect children. In *Perrin v. UK*[332] the Court refused the complaint of an owner of a website who had been convicted on obscenity charges, reasoning that he could have avoided exposing minors to the obscene pictures had he used age checks on the free preview page.

But states need to do more to protect children. In *K.U. v. Finland*[333] an unknown person had published the personal details of a 12-year-old on a dating website.

328. Cf. ibid., p. 6.
329. *Tolstoy Miloslavsky v. United Kingdom* (13 July 1995), application No. 18139/91, para. 51.
330. International Mechanisms for Promoting Freedom of Expression, Joint Declaration on Freedom of Expression and the Internet, 1 June 2011, www.osce.org/fom/78309.
331. Council of Europe, Committee of Ministers (4 July 2012), Declaration of the committee of ministers on the desirability of international standards dealing with forum shopping in respect of defamation, "libel tourism", to ensure freedom of expression, pp. 11-12.
332. *Perrin v. the United Kingdom* (18 October 2005), application No. 5446/03.
333. *K.U. v. Finland* (2 December 2008), application No. 2872/02, paras. 41-50.

This obviously put the child in danger of sex predators. Since Finnish law at that time did not allow the police to ask Internet service providers to reveal the identity of the person who had published the profile, it was found to violate the right to privacy of K.U. As the anonymity that characterises much communication on the Internet makes it harder for the police to ensure the human rights of victims of privacy violations, states have to provide a legal framework sufficient to pierce the veil of anonymity in serious cases.

Children are especially vulnerable in social networks where they may communicate unknowingly with sex predators, share personal information with serious negative effects, engage in harmful behaviour or come into contact with harmful content. Cyber-bullying and cyber-grooming are present dangers. Though children, especially older children and young people, should use social networks in their self-actualisation processes and in the development of their self-identity, social network service providers need to introduce safeguards (and if they fail to do so, states need to enforce the protection framework in light of *K.U. v. Finland*).

In its Recommendation on the protection of human rights for social networks, the Council of Europe added specific language targeted at protecting children. Safeguards might include precautionary measures by social networks, including filtering for keywords, but must at least include *ex post* moderation of content flagged as inappropriate for young users. Some social networks rely on age verification systems or on self-declaration of maturity, but these systems (and the declarations) are not failsafe.[334] In all attempts to avoid content unsuitable for children, social network providers need to avoid falling into the trap of restricting the freedom of expression of others who may be interested in shocking information.

5.9. Freedom of expression and Internet domain names

Internet domain names are identifying strings that make the Internet easier to use for humans who are at a loss to remember 193.164.229.51, the Internet Protocol (IP) address, but can easily recall http://hub.coe.int if they wish to visit the Council of Europe's website. The ".int" in this address is the top-level domain (TLD), the highest level of identifiers in the Internet's domain name system (DNS); "hub" and "coe" are domain and subdomain name. Among TLDs, we can further differentiate between country code TLDs (ccTLDs), such as .at for Austria and .de for Germany, and generic TLDs (gTLDs) such as .com, .biz or .edu.

334. Council of Europe, Committee of Ministers, Recommendation CM/Rec(2012)4 on the protection of human rights with regard to social networking services, Appendix, pp. 5-10.

As the Council of Europe recognised, the choice of domain name or name string can be used

> to identify and describe content hosted in their websites, to disseminate a particular point of view or to create spaces for communication, interaction, assembly and association for various societal groups or communities.[335]

In 2011, the Committee of Ministers of the Council of Europe passed the Declaration on the protection of freedom of expression and information and freedom of assembly and association with regard to Internet domain names and name strings.[336] In rather cautious language, the Declaration confirms that:

> [e]xpressions contained in the names of Internet websites, such as domain names and name strings, should not, a priori, be excluded from the scope of application of legal standards on freedom of expression and the right to receive and impart information and should, therefore, benefit from a presumption in their favour.[337]

As we show below, however, the Court's clear case law on freedom of expression and its limits, and on trademarks, can be interpreted to provide nuanced protection to domain names that recognises both their address function and their expressive function. Just as freedom of expression extends to a company's name, within the usual limitations described in Chapter 3, domain names are therefore also protected. The Council of Europe has criticised the prohibition of certain words or characters in domain names and name strings, especially as these prohibitions might have negative consequences in a cross-border context.[338]

Challenges to freedom of expression are posed by state attempts to regulate both domain names and top-level domains. While TLD management is historically part of the key responsibility of ICANN, the Internet Corporation of Assigned Names and Numbers, the recently implemented liberalisation and internationalisation of both domain names and TLDs raises important public policy and human rights concerns. The Council of Europe has pointed out that, in the process of TLD liberalisation – the introduction of new TLDs like .nike or .berlin – freedom of expression is relevant to the policy development processes.[339]

In light of the Council of Europe's commitment to "support … the recognition by member states of the need to apply fundamental rights safeguards to the

335. Council of Europe, Committee of Ministers (21 September 2011), Declaration on the protection of freedom of expression and information and freedom of assembly and association with regard to Internet domain names and name strings, www.wcd.coe.int/ViewDoc.jsp?id=1835805&Site=CM.
336. Ibid.
337. Ibid., para. 7.
338. Ibid., para. 9.
339. Ibid., para. 10.

management of domain names",[340] the following standards developed from the European Court of Human Rights' case law on freedom of expression[341] can be applied both to Internet domain names and to existing and new generic top-level domain (gTLD) strings.[342]

Domain names and new gTLD strings may not negate the Convention's fundamental values and can be restricted in accordance with paragraph 2 of articles 10 and, *in eventu*, 11, if this restriction is necessary in the pursuance of a legitimate aim and proportionate. Domain names and new gTLD strings promoting racial hatred, supporting terrorism, vehemently attacking particular religions, inciting to violence, negating the Holocaust or calling for installing totalitarian regimes are not permissible. In light of the high visibility of gTLDs in certain cases, they can be considered to have a substantial impact on public order.

The Court will most likely allow national authorities a broad margin of appreciation in assessing whether prohibiting a certain gTLD answers a pressing social need. The margin can be smaller when there is a link to media or political discourse. The Court will most likely look at domain names and gTLD strings in the context of the website, as it follows a comprehensive approach to assessing limits to Article 10. In the case of *Raëlien Suisse v. Switzerland*[343] the Court assessed the content of a website when judging whether taking down the poster announcing the website had violated Article 10. Similarly, domain name, web string and content will have to be considered as a whole.

Domain names and gTLD strings that are aimed at selling a product are considered commercial speech, while those having other aims, such as furthering public discourse on a socially relevant topic, will not.[344] The Court's differentiation between commercial and non-commercial speech is categorical.[345] In *X and Church of Scientology v. Sweden*[346] the now defunct Commission introduced the distinction between advertisements aimed at promoting a religion and those aimed at selling a product. The distinction to be made is thus based on the purpose pursued by the speech. If domain names and gTLD strings are commercial in their nature, e.g. www.BuyJohnsBread.now, they will be imbued with less protection than the

340. Ibid., para. 11.
341. For the Court's case law on hate speech, see also 3.2.
342. Benedek W., Gragl P., Kettemann M. C., Liddicoat J., van Eijk N. (October 2012), "Comments relating to freedom of expression and freedom of association with regard to new generic top level domains", *DG-I*, 2012/4.
343. *Mouvement Raëlien Suisse v. Switzerland* (13 July 2012), application No. 16354/06, paras. 54-58, para. 68.
344. Cf. Hertig Randall M. (2006), "Commercial speech under the European Convention on Human Rights: subordinate or equal?", *Human Rights Law Review,* 6 (1), pp. 53-86.
345. Cf. ibid., p. 58.
346. *X and Church of Scientology v Sweden* (5 May 1979), application No. 7805/77, admissibility decision.

expression of political ideas or contributions to socially relevant topics, such as www.IsBreadGoodForYouOrShouldWeAllEatMore.Fruit?[347]

If a domain name and a gTLD string are considered commercial speech, the Court will then (as can be deduced from its previous jurisprudence regarding non-Internet related cases) only review the justifiability of the national decision and its proportionality,[348] while giving states a wide margin of appreciation. This margin is reduced, as stated before, when the domain name and gTLD are contributions to a more general debate on issues bearing on the public interest.[349] There is not yet enough case law to safely say how the Court will rule on cases that contain both commercial and non-commercial elements. As a rule, however, when both commercial and non-commercial elements of speech are present, the Court will assess whether the advertising effect is primary or secondary and whether state interests of pursuing a legitimate aim can be seen as more important than the legitimate interest of the public in the information provided.[350]

Rights of others, including trademarks, are also legitimate limits to freedom of expression, provided they are not abused. Usually, trademark law gives trademark holders the right to prevent use of identical signs on identical goods or the right to prevent economic harm to the distinctive character of a trademark.[351] The use of trademarks falls within the scope of Article 10 and can be restricted to protect trademark rights. Furthermore, in *Anheuser-Busch Inc. v. Portugal*[352] the Court held that a trademark constituted intellectual property and thus a "possession" within the meaning of Article 1 of Protocol No. 1.

The Court held in *Paeffgen GmbH v. Germany*,[353] its only decision so far bearing directly on domain names, that non-physical goods are covered by the Convention's protection of "property rights" and are thus "possessions" for the purpose of Article 1 of Protocol No. 1. Accordingly, the prohibition against using certain domain names and gTLDs that infringe domestic trademark law reflect a legitimate general interest in upholding an effective system of trademark protection.

The prohibition on submitting negative statements regarding certain trademarks via gTLDs (such as www.[Car name]sucks.com) does not violate Article 10, paragraph 2, if such interference is necessary to prevent statements of a disparaging nature and if the applicants can still pursue alternative avenues of

347. The URLs used in this section are fictional examples. No similarity to existing URLs is intended.
348. *Casado Coca v. Spain* (24 February 1994), application No. 15450/89.
349. *Krone Verlag GmbH & Co KG v. Austria* (11 December 2003), application No. 39069/97, No. 3.
350. *VgT Verein gegen Tierfabriken v. Switzerland* (28 June 2001), application No. 24699/94, para. 71.
351. Cf. Sakulin W. (2011), "Trademark protection and freedom of expression", Wolters Kluwer, pp. 1-2.
352. *Anheuser-Busch Inc. v. Portugal* (11 October 2005), application No. 73049/01, para. 46.
353. *Paeffgen GmbH v. Germany* (declared inadmissible), application Nos. 25379/04, 21688/05, 21722/05, 21770/05.

communicating the idea they wish to convey.[354] In light of the broad variety of communicative outlets on the Internet, such an alternative avenue to voice one's ideas or opinions will often exist. Nevertheless, views that shock, offend and disturb can not only be voiced against ideas, religions, historical narratives and concepts, but also against companies, names and trademarks, especially in an age where certain products take on a near-mythical status and companies often take over from religions the role of producers of self-identity and affirmation.

5.10. The role of Internet intermediaries

Internet intermediaries such as Internet service providers (ISPs) and Internet content providers control the spaces in which search individuals access and share information online and express their opinion.[355] In the past, most states relied on ensuring an underlying framework of laws and trusted in self-regulation of intermediaries to ensure that no illegal content was available on sites.[356] However, states have increasingly turned to intermediaries to police Internet users and have forced intermediaries to implement national laws that are often at variance with international legal commitments.[357] Technically, the liability of Internet intermediaries for content of users is engaged through "notice-and-take-down" procedures. Yet these can be misused both by state and private actors.[358]

A big difference between traditional and new media lies in the amount of information published by newspapers versus that uploaded to popular websites. In 1999, the European Court of Human Rights could still confidently claim in *Sürek v. Turkey*[359] that the owner of a journal was responsible for having published aggressively written letters to the editor, even if he had not personally associated himself with these. His conviction did not violate Article 10 because of the threat contained in these letters to particular individuals.

Extending *Sürek* to Internet intermediaries would mean burdening them with an impossible task. However, Internet intermediaries are not the prima facie editors of the information contained on their sites. Even the webmaster of the site of an organisation is not necessarily responsible for all content published on that site, as in the case of *Renaud v. France*[360] where the Court deemed

354. *Appleby v. United Kingdom* (6 May 2003), application No. 44306/98.
355. For the standard-setting function of the private sector, and company-led best practices, see 4.3.2, *supra*.
356. Regarding the role of hotlines in monitoring Internet content, see 6.3, *infra*, and for the role of business in promoting freedom of expression, see 6.5, *infra*.
357. York J. C. (September 2010), "Policing content in the quasi-public sphere", *OpenNet*, at opennet.net/policing-content-quasi-public-sphere.
358. La Rue F. (16 May 2011), *Report by the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, UN Doc. A/HRC/17/27, paras. 34-36.
359. *Sürek v. Turkey* (8 July 1999), application No. 26682/95, No. 1.
360. *Renaud v. France* (25 February 2010), application No. 13290/07.

exaggerated the conviction of a webmaster for remarks published, within an emotional public debate, on the association's site.

In that light the Court's decision in *Delfi AS v. Estonia*[361] (pending) seems like a foregone conclusion. In that case the operators of an Internet news portal were held responsible in national courts for defamatory comment posted by a non-identifiable user below an article. Commenting was possible through a non-moderated system, as the technology was in place to delete messages on the request of third parties and to filter out certain language. The portal deleted the impugned comment without delay but was nevertheless convicted.

Limiting the *ex ante* content-moderation obligations of Internet intermediaries is essential for keeping the flow of ideas on the Internet open. Navigating between state laws and its own content-moderation rules is often difficult for international Internet intermediaries, and especially social networking sites, who are faced with conflicting demands and threats by states to disallow access altogether in case of non-removal of impugned information.[362] The *Yildirim* case confirmed that a wholesale ban on a whole service in reaction to illegal content on a certain site violates Article 10.

Attempts by some states, such as India, to oblige Internet intermediaries to pre-censor content have met with strong international opposition. The Internet thrives on openness and the quick and free exchange of ideas. Therefore the responsibilities of Internet service providers cannot be understood to extend to *ex ante* moderation. Distinguishing *Sürek* and relying on *Renaud*, this is what *Delfi AS* can be expected to come down to.

Freedom of expression in social networks can be threatened not only by state attempts to regulate content but also by the social networks themselves. They can be simultaneously a threat to freedom of expression online and its advocate, as the following section illustrates.

5.11. Freedom of expression in social networks

Social networks play an essential role in creating and increasing the value of the Internet as a discourse forum. They enable the exercise of human rights, especially the freedom of expression (but also of assembly) and can act as a catalyst for democratic participation and thus for democracy. But at the same time, human rights may be threatened on social networks by terms of service that are insensitive to human rights, as we see next. Threats can arise, as the Council of Europe's Council of Ministers' Recommendation on

361. *Delfi AS v. Estonia* (communication of 11 February 2011), application No. 64569/09.
362. Benesch S. and MacKinnon R. (5 October 2012), "The innocence of YouTube", *Foreign Policy*, www.foreignpolicy.com/articles/2012/10/05/the_innocence_of_youtube.

the protection of human rights with regard to social networking services[363] reminds us:

> from lack of legal, and procedural, safeguards surrounding processes that can lead to the exclusion of users; inadequate protection of children and young people against harmful content or behaviours; lack of respect for others' rights; lack of privacy-friendly default settings; lack of transparency about the purposes for which personal data are collected and processed.[364]

Especially freedom of expression can be threatened by terms of service that disallow certain content because of economic considerations. A case in point is the regulation of content on the social networking site Facebook.com. User behaviour and the treatment of content uploaded to Facebook sites are covered by the Facebook Principles,[365] the social network's Statement of Rights and Responsibilities[366] and the Facebook Community Standards.[367]

The Facebook Principles do not refer to dignity or human rights or reference any human rights codification, but lay down the "freedom to share and connect": "People should have the freedom to share whatever information they want, in any medium and any format." This commitment to sharing "whatever information they want" is limited substantially, as we will soon see.

Anyone who uses or accesses Facebook thereby "agrees" to the Statement of Rights and Responsibilities, which includes prohibitions on harassing other users (3.6), using Facebook in a discriminatory manner (3.10) or taking "any action on Facebook that infringes or violates someone else's rights or otherwise violates the law" (5.1). Convicted sex offenders may not use Facebook (4.6). A user who violates "the letter or spirit of this Statement, or otherwise create[s] risk or possible legal exposure" can be penalised by the company ceasing to "provid[e] all or part of Facebook to [the user]" (15). Facebook also obliges users to "comply with all applicable laws when using or accessing Facebook" (19.11) but it does not refer to human rights.

In the Facebook Community Standards, the social network site commits to removing, and possibly escalating to law enforcement, posts considered to be a "direct threat to public safety. … Organisations with a record of terrorist or violent criminal activity are not allowed to maintain a presence on our site". Any promotion or encouragement of self-mutilation, eating disorders or hard drug abuse is also removed. The social network also does not "permit hate speech" but distinguishes it from "humorous speech". In keeping with anti-discrimination law, "attack[s on] others based on their race, ethnicity,

363. Council of Europe, Committee of Ministers, Recommendation CM/Rec(2012)4 on the protection of human rights with regard to social networking services.
364. Ibid., para. 3.
365. Facebook, Principles, www.facebook.com/principles.php.
366. Facebook, Statement of Rights and Responsibilities (11 December 2012), www.facebook.com/legal/terms.
367. Facebook, Community Standards, www.facebook.com/communitystandards.

national origin, religion, sex, gender, sexual orientation, disability or medical condition" are also prohibited. Graphic content is not prohibited per se, but is balanced against "the needs of a diverse community". Facebook also has a "strict policy against the sharing of pornographic content and any explicitly sexual content where a minor is involved. We also impose limitations on the display of nudity." While vague in references to the "needs" of the community and the "limitations" that may be imposed, the Community Standards are mainly in keeping with freedom-of-expression norms, in particular with their prohibition of hate speech and sexual exploitation of children.

But Facebook can be faulted for not presenting the whole picture. The social network's terms of service do not contain all rules relevant to the treatment of postings. In 2012, a website leaked Facebook's Abuse Standards 6.2: Operation Manual for Live Operators,[368] a document supplied to Facebook employees who assess postings that have been flagged as inappropriate by users. The document allows assessment of Facebook's moderation process in more depth.

When users report pictures, videos and wall posts, outsourced content-moderation teams wade through the stream of reported items and, using the Abuse Standards, they can confirm the flag and delete the content, unconfirm the flag and allow the content to stay or "escalate" the flag, thus turning it over to a higher-level Facebook employee. The standards, for instance, disallow pictures with "sexual activity [...] Cartoons/art included. Foreplay allowed (Kissing, groping, etc.) even for same-sex individuals". Users are also not allowed to "describe sexual activity in writing, except when an attempt at humor or insult". Pictures showing marijuana use are allowed, "unless context is clear that the poster is selling, buying or growing it". Facebook also bans "[s]lurs or racial comments of any kind", hate symbols and "showing support for organisations and people primarily known for violence". But the Guidelines caution that "[h]umor overrules hate speech UNLESS slur words are present or the humor is not evident".

Most of the prohibitions contained in the Standards do not meet human rights standards, if applied to the public sphere. The problem here is dual. First, it seems arbitrary of Facebook to single out certain content that is not allowed without reference to human rights. Second, the application of the Abuse Standards (that are not officially known to the public) is problematic as individuals do not know against which standards their postings are measured. True, some of the Abuse Standards, especially those regarding hate speech, are in line with general human rights commitments. But most of them go far beyond what the European Court of Human Rights would consider to fall outside the realm of protected expression.

368. oDesk, *Abuse Standards 6.2. operation manual for live operators*, www.scribd.com/gawker/d/81877124-Abuse-Standards-6-2-Operation-Manual.

From an international freedom-of-expression perspective the Abuse Standards section entitled "IP Blocks and International Compliance" is particularly interesting. All of the content found has to be "escalated", that is, forwarded to a higher-ranking Facebook content controller for review. Facebook will thus clearly block "Holocaust denial which focuses on hate speech; All attacks on Ataturk (visual and text); Maps of Kurdistan (Turkey); Burning Turkish flag(s)". Other content, including "Any PKK support or content with no context" and "Content supporting or showing Abdullah 'Apo' Ocalan" has to be "confirmed", that is, the flagged content has to be deleted. The Standards add: "Ignore if clearly against PKK and/or Ocalan."

This content seems to stem from international requests to Facebook, which found itself confronted by the obligation of either acceding to deletion of the content in question or facing a complete blocking of all Facebook sites. That this is no idle threat by Turkey is exemplified by the 2012 decision in the *Yildirim* case, where the Court ruled (after the Turkish authorities had blocked access to certain Google sites) that restriction of Internet access without a strict legal framework regulating the scope of the ban and affording the guarantee of judicial review to prevent possible abuses amounted to violation of freedom of expression.[369] While deleting negationist posts is in keeping with the European Court of Human Rights' case law, escalating and deleting all maps of Kurdistan most certainly raises serious freedom-of-expression issues.

Other content that Facebook "escalates" includes images of sexual exploitation of children, threats of school violence, necrophilia and bestiality, credible threats and indications against public figures (under certain circumstances), indications of past/future crime and organised crime; any indication of terrorist activity and posts containing evidence of poaching of endangered species. These limits are partly required by international law (prohibition of sexual exploitation of children) and partly reflective of national criminal laws. However, we have to keep in mind that, with some crimes (e.g. poaching), talking and posting about it may not be wise (as it may give evidence to prosecuting authorities) but it is not a crime as such.

Since the role of Facebook as an international forum of aggregation and articulation of ideas is growing, the Abuse Standards are *de facto* the law in force regarding freedom of expression in an important international forum. It is not without problems to leave the establishment of freedom-of-expression standards to a private company that is not primarily interested in ensuring freedom of expression. Such a document, indeed any standard developed by social networking firms, needs to be vetted more carefully against the international law on freedom of expression.

One way out of the dilemma would be for Facebook to more actively engage with the community of users by publishing an authorised version of the standards of

369. *Yildirim v. Turkey* (18 December 2012), application No. 3111/10.

review, clarifying the moderation process, and starting a vigorous debate among its users on the international standards of freedom of expression.

Such an approach would be fully in line with the suggestions made by the Council of Europe in its Recommendation on social network providers. Recognising that different self- and co-regulatory mechanisms have already been set up to develop and discuss standards to be used by social network providers, the Council recommended that states ensure that the procedural safeguards for users foreseen in these mechanisms include a right by users to be heard and to review or appeal against decisions by social network providers. These might include in appropriate cases the pursuance of legal measures within state judiciaries.

Social networking providers may wish to avoid the possibility that users have recourse to the judicial system and will rather not risk the danger of courts considering that some social networks have developed into quasi-public spheres and have thus forfeited some of the immunity from human rights-based claims accorded traditionally to private actors with regard to their terms of service. Therefore, they have to implement a human rights-based approach in their terms of service and include strong protections for freedom of expression with exceptions only in keeping with the case law of the European Court of Human Rights. This includes the duty of social network providers to raise the awareness of users of their human rights by means of clear and understandable language.[370]

The trend towards deprivatisation of private spheres on the Internet, in order to increase the Internet's public service value and ensure a higher level of human rights protection, merits closer scrutiny.

5.12. Private and public spaces on the Internet

The Internet has a substantial public service value.[371] This function of the Internet implies, as the Council of Europe formulated in its Recommendation on measures to promote the public service value of the Internet of 2007, certain duties for states. These include adopting human rights-consistent Internet policies, developing and implementing e-democracy, e-participation and e-government policies, ensuring access, affirming freedom of expression and the free circulation of information on the Internet (and balancing them, where necessary, with other legitimate rights and interests) and ensuring that ICT content is reflective of all regions, countries and communities in order to ensure representation of all peoples, nations, cultures and languages.

370. Council of Europe, Committee of Ministers, Recommendation CM/Rec(2012)4 on the protection of human rights with regard to social networking services.

371. Cf. the standard-setting function of the Council of Europe, evidenced by its 2007 Recommendation on measures to promote the public service value of the Internet, in 4.2.1 *supra*.

One of the key roles of the Internet with regard to freedom of expression is its enabling function. The Internet enables the exercise of freedom of expression by creating a huge resonance space, allowing people to share ideas and concerns, wishes and complaints. The Internet is a denationalised discourse space, a progressive public sphere made up of private spheres where, nevertheless, issues of public interest are discussed.[372] In times before the Internet, the Roman forum and the Greek agora fulfilled that function. They were the original public spaces where discussions could be held, goods bought and sold, and political ideas voiced.

Of course, the Internet is more of a public sphere in the sense of Jürgen Habermas than the Roman forum or Greek agora ever were. In particular, some characteristics of today's perception of a public sphere (private individuals debating issues of public concern in rationalised discourses, independent of their status, with the best argument winning the day) are inventions seldom seen before the Enlightenment.

The very notion of the public sphere is that of a place where private citizens can "speak truth to power". In the Internet, however, a lot of discourse spaces are not public in the sense of being open to anyone. Rather, one can only speak truth to power after submitting to a different form of power, namely the terms of service of powerful Internet companies. These terms of service, required by practically all Internet Service Providers, social network providers and blogging services, turn these loci of conversation into *de jure* private places. But the discussions held in the private places managed by Internet gatekeepers still fulfil an important public role.

This is problematic because it gives private actors the possibility to regulate expression which is in the public interest. These places are thus no longer only private (because the discourse held there is in the public interest) nor only public (because private companies run them and apply their private law-based terms of service). Rather, they are semi-public or quasi-public. As a 2010 OpenNet Initiative report on public and private spheres put it:

> Instead of an unregulated, decentralised Internet, we have centralised platforms serving as public spaces: a quasi-public sphere. This quasi-public sphere is subject to both public and private content controls spanning multiple jurisdictions and differing social mores.

The Council of Europe has recognised this challenge. In its Declaration on the protection of freedom of expression and freedom of assembly and association with regard to privately operated Internet platforms and online service providers,[373] the Committee of Ministers underscored the fact that social

372. Cf. Jørgensen R.F. (2013), *Framing the net. the Internet and human rights*, Edward Elgar, and 2.2.

373. Council of Europe, Committee of Ministers (7 December 2011), Declaration on the protection of freedom of expression and freedom of assembly and association with regard to privately operated Internet platforms and online service providers.

networks, blogging sites and Internet-based companies offering other means of mass communications for civil society, whistle-blowers and human rights defenders to exchange information, publish content, interact and associate with each other have an important role in ensuring a human rights-based media ecosystem. They contribute significantly to public debate by providing room for discussions of public interest. This, however, engages their responsibility.

Companies tend to be stricter in regulating private spaces than countries are in regulating public spheres. They also tend to use one set of terms of service, usually from the company's home state, for users from different countries. This is positive in those cases when users from more oppressive countries access a platform from a more liberal country.

However, terms of service are sometimes in violation of human rights, especially privacy rights. Companies have to face the dilemma of navigating between "keep[ing] users happy", "operat[ing] within a viable business model" and "working to keep their services available in as many countries as possible by avoiding government censorship".[374] Too often, companies err on the side of caution and forbid much more speech than states would have to prohibit because of their human rights obligations. Of course, as the NGO Freedom House shows in their annual report on Freedom on the Net, Internet freedom and freedom of expression online are under attack in a growing number of countries.[375]

In these countries, the "enemies of the Internet", as Reporters Without Borders term them,[376] Internet companies have a special role to play in securing the openness of their semi-public spheres and supplanting the non-existent (or bitterly fought) public discourse space with one the company provides. In more human rights-sensitive states, however, companies will usually introduce limits to freedom of expression that are stronger than those required by the states' laws, making recourse to their character as a private sphere to legitimise these restrictions. It is in these countries that the qualification of a platform as a semi-public sphere becomes important.

Qualifying a private space as public (or semi-public) implies that not only terms of service will apply but also general human rights (apart from the most basic human rights, which are applicable everywhere). Let us illustrate this notion: Holocaust deniers are not protected by freedom of speech, regardless of whether they carry out a demonstration or create a group on a social networking site. In this case, the protection of freedom of speech in the public

374. York J. C. (September 2010), "Policing content in the quasi-public sphere", *OpenNet*, www.opennet.net/policing-content-quasi-public-sphere.

375. Kelly S. and Cook S. (24 September 2012), "Evolving tactics of Internet control and the push for greater freedom", in Kelly S., Cook S. and Truong M. (eds), *Freedom on the Net 2012: a global assessment of Internet and digital media*, Freedom House, pp. 1-18 (1-2).

376. Reporters Without Borders (2013), *Enemies of the Internet 2013*, http://surveillance.rsf.org/en.

and in the private sphere are the same. What about an image showing animals being slaughtered as part of campaign for a vegetarian lifestyle?

Offline, in the public sphere, a demonstration using such an image would be protected by freedom of expression (and assembly). But in a number of social networks, such an image would be deleted and the user's account might be deactivated for violating the terms of service. In this case, the terms of service do not serve primarily to protect other users from these images (though this can be a reason), but rather to ensure that the social network stays attractive and keeps its (other) users happy. Shocking, offending and disturbing pictures – explicitly protected under *Handyside* – are in danger of being deemed bad for business. In a private sphere where only terms of service apply, there would be little recourse. This is where the notion of a semi-public sphere becomes relevant. In such a sphere, national laws (especially those protecting human rights) complement the level of protection provided by the terms of service for freedom of expression.

Both American law and the case law of the European Court of Human Rights contain arguments for the case for the semi-public sphere. In *New Jersey Coalition Against War in the Middle East v. J.M.B. Realty Corp.* (1994),[377] the Supreme Court of New Jersey established the right of individuals to hand out protest literature in private shopping malls. The Court held that owners of shopping centres have to allow leafleting expressive speech within their malls, if they are *de facto* public forums. Therefore it would be unreasonable to allow private parties (the owners of the mall) to limit free speech. The Court backtracked from this more limited understanding of property rights in the 2000 case *The Green Party of New Jersey v. Hartz Mountain Industries, Inc.*[378] and adopted a test in which the private property rights of mall owners have to be weighed against the rights to free speech and assembly.[379]

In the only relevant case so far, the European Court of Human Rights has followed a similar approach, even if it appears to be less sensitive to concerns about freedom of expression (and allows the state a broader margin of appreciation, a notion that did not matter for the New Jersey Supreme Court). In *Appleby*,[380] the Court had to balance the right to property of a mall owner against the freedom of expression of a group wishing to collect signatures for a petition inside. Admitting that freedom of expression constituted one of the preconditions for a functioning democracy, the Court

377. *New Jersey Coalition Against War in the Middle East v. J.M.B. Realty Corp.* (1994), 138 NJ 326, 650 A.2d 757. Critically, see Friedelbaum S. H. (1999), "Private property, public property: shopping centers and expressive freedom in the States", *Albany Law Review 62*, pp. 1252-1262.

378. *The Green Party of New Jersey v. Hartz Mountain Industries, Inc.*, 2000 WL 758410 (N.J.).

379. Cromie J. D. and Jacobus J., "Court stakes a middle ground on free speech in shopping malls", *2000 New Jersey Law Journal*, www.connellfoley.com/content/page/court-stakes-middle-ground-free-speech-shopping-malls.

380. *Appleby v. United Kingdom* (6 May 2003), application No. 44306/98.

nevertheless pointed out that freedom of expression was not necessarily linked to a particular forum (the shopping mall), if alternative means were feasible. The applicants could have, the Court ruled, "employed alternative means, such as calling door-to-door or seeking exposure in the local press, radio and television".[381]

What can we take from this approach for the future of private, semi-public and public spheres online? The Court seems ready to accept that the right to property (and the right to keep privately owned social networks private and subject only to terms of service) has to be weighed against the right to expression. If disallowing certain legal content to be published on a social network amounted to negation of the right to freedom of expression, a state would be obliged to make the private actor (the social network provider) allow the expression. If, however, alternative avenues exist and applicants are not *de facto* denied their right to make their cause heard, the terms of service will remain untouched.

In light of the plethora of avenues of expressing one's opinion online, the argument of there being no alternative forum would be difficult to make. But it is not inconceivable that at some future date one or two companies may make up such a big share of the social networking market that exclusion of views from them amounts to *de facto* negation of the right.

Until then, however, it makes sense to address social network providers directly and oblige them to make their terms of service more consistent with human rights, especially in light of data-protection and privacy laws, but also in light of the recourse they offer when expressions are challenged. This approach has been chosen by the 2011 Declaration on the protection of freedom of expression and freedom of assembly and association with regard to privately operated Internet platforms and online service providers.[382]

Internet gatekeepers have an important role not only as "watchdog[s]" but even more broadly as providers of the spaces where the watchdogs – NGOs, citizens activist – can gather to effect "positive real-life change".[383] Two consequences flow from this increasingly important role of social networks providers for the public debate: an obligation on their part to foster such a debate (even to the short-term detriment of their business interests) and an obligation for states to not exert politically motivated pressure on privately operated Internet platforms and online service providers but respect all human rights, especially freedom of expression.[384]

381. Ibid., para. 48.
382. Council of Europe, Committee of Ministers (7 December 2011), Declaration on the protection of freedom of expression and freedom of assembly and association with regard to privately operated Internet platforms and online service providers.
383. Ibid., p. 2.
384. Ibid., p. 7.

5.13. Transcending the national level

The issues covered in this chapter – from network neutrality to the private, public or semi-public character of social networks – have in common that they transcend national boundaries. Yet, national policies also shape the evolution and use of the Internet, and national decisions of judicial and quasi-judicial bodies greatly influence the impact of information and communication technologies and their use in the exercise of freedom of expression. Therefore, in Chapter 6, we study selected cases and developments from the national level, study their similarities and differences, and analyse their impact on freedom of expression on the Internet. The challenges we identify through those case studies will allow us then to demonstrate the added value that European monitoring mechanisms, presented in Chapter 7, and the promotional activities of international organisations and individual states, discussed in Chapter 8, can bring to the protection of freedom of expression online.

6. Relevant practice on the national level

The use of the Internet has affected all sectors of society and all aspects of our lives. Each and every country in the world has experienced the political, social and economic consequences of the increased use of information and communication technologies. But, though all countries are confronted by similar challenges, their political and legal responses have varied greatly. Some states have introduced strict laws targeting freedom of expression online, some have waited for judges to apply (or not apply) existing laws and others have developed legislation that actively encourages citizens to use the Internet as a sphere for public discourse.

National practice on freedom of expression on the Internet varies widely. Regulating freedom of expression online is highly complex and touches upon, as we have seen in previous chapters, a vast number of societal issues – from anonymity to hate speech, from protecting intellectual property rights to the historic reasons why a country has opted to criminalise Holocaust denial. We therefore need to be selective.

In the following, we concentrate on selected practice on the national level in Europe (and from across the world where especially relevant), provide short case studies and present the lessons to be learned. As the speed of technological change continues to accelerate, examples of good practice on the national level can inspire states to frame their political and legal responses in a way that respects, protects and promotes human rights on the Internet, and especially freedom of expression online. But examples of bad practice can also provide important lessons – for states and the other relevant stakeholders, companies and civil society – in what not to do.

These selected cases are structured by a number of questions related to freedom of expression online: How do states establish jurisdiction in freedom-of-expression cases on the Internet? What legislative and judicial measures are taken to ensure Internet access (as a human right)? How can copyright protection and freedom of expression online be reconciled? Are there differences between public and private violations of freedom of expression online? How do powerful Internet companies engage with national law – or are they beyond the law? And what role can business play in protecting and promoting freedom of expression on the Internet?

Across the cases we see three interlinked phenomena: the important role of national courts and organs in developing and applying, at local and regional

level, international human rights commitments; the function of appeals courts in correcting the application of lower court judgments that have misapplied human rights protection guarantees in freedom-of-expression contexts (such as in the British *Twitter* and the Italian *Google* cases); and the key role of the European Court of Human Rights in laying down fundamental principles and reviewing controversial cases.

6.1. Jurisdiction and freedom of expression online

6.1.1. *France v. US* and *Yahoo! v. LICRA*: a tale of two countries and two courts

One of the first key cases bringing to the fore issues of jurisdiction over Internet content, the responsibility of private actors and the jurisdictional limits of states was the French Yahoo! case: *LICRA (Ligue Contre le Racisme et l'Antisémitisme) and the Union of Jewish Students of France v. Yahoo!* The case started when Yahoo! Inc. declined to withdraw from its auctions Nazi memorabilia which the applicants considered to be in violation of French anti-hate speech laws. Yahoo! Inc. contested the jurisdiction of the French court, but the court imposed a fine and ordered the website to block access for French users to the more than "1.500 Nazi and Third Reich related objects offered for sale on the Yahoo U.S. site [as of 2000]".[385]

Rather than engaging in a defence in France, Yahoo! Inc. decided to ask US courts to confirm the impossibility of enforcement of the French sentence. The District Court for the Northern District of California confirmed that obliging Yahoo! Inc. to use geo-location filtering software to stop French users from accessing the auction sites was in violation of First Amendment rights and could not be enforced. But the United States Court of Appeals, Ninth Circuit, in a 2006 decision,[386] reversed this on technical grounds but hinted that it was not convinced by the arguments of Yahoo! Inc.:

> In other words, as to the French users, Yahoo! is necessarily arguing that it has a First Amendment right to violate French criminal law and to facilitate the violation of French criminal law by others. As we indicated above, the extent – indeed the very existence – of such an extraterritorial right under the First Amendment is uncertain. … In sum, it is extremely unlikely that any penalty, if assessed, could ever be enforced against Yahoo! in the United States. Further, First Amendment harm may not exist at all, given the possibility that Yahoo! has now "in large

385. Cf. Greenberg M. H., "A return to Lilliput: *the Licra v. Yahoo!* case and the regulation of online content in the world market", *1192 Berkeley Technology Law Journal* (18) (2004-5), www.btlj.org/data/articles/18_04_05.pdf, pp. 1191-1258, at p. 1206.

386. United States Court of Appeals, Ninth Circuit (12 January 2006), 433 F.3d 1199, *Yahoo! Inc. v. LICRA and UEJF*, http://law.justia.com/cases/federal/appellate-courts/F3/433/1199/546158.

measure" complied with the French court's orders through its voluntary actions, unrelated to the orders.[387]

The different treatment of freedom of expression shows the challenges involved in safeguarding freedom of expression online in a globalised context in the light of divergent concepts on the two sides of the Atlantic. What we can take from the Yahoo! Inc. cases is that pursuing legal cases in different jurisdictions may lead to different results. Relying only on legal approaches may be less effective (and less promising for human rights protection) than calling upon the corporate social responsibility of international Internet companies.

6.1.2. UK: the Internet comes under national jurisdiction

In *Perrin v. UK*[388] (dealing with the criminal conviction of the owner of an adult entertainment material website who had not used age testing for his service's preview pages) the Court emphasised that the lawfulness of adult material in certain other states (the US) does not preclude a conviction in a European state (UK) because of the large margin of appreciation given to member states, especially in the area of morals. Jurisdiction can be established because the material can be accessed from the UK. The decision also confirmed the rights of states to extend their jurisdiction, under the ECHR, to regulating new aspects of freedom of speech on the Internet.[389] How many cases connected to freedom of expression on the Internet are imbued with questions of jurisdiction is well illustrated by the overviews the international think tank Internet & Jurisdiction Observatory collects.[390]

6.2. Access and freedom of expression online

Is Internet access a human right? Council of Europe member states have answered this question differently. But Egypt's shutdown of its Internet during the demonstrations on Tahrir Square in 2011 cannot be reconciled with international law. Blackouts violate freedom of expression online (and other human rights, such as the freedom of assembly). By now, 20 Council of Europe member states have, to some degree, implicitly or expressly, made Internet access a protected right. In Germany, a recent decision of the *Bundesgerichtshof* confirmed that the Internet was an essential part of life, while Finland pursues a more technology-focused approach by decreeing a right to broadband access.

387. Ibid., paras. 103 and 104.
388. *Perrin v. United Kingdom* (18 October 2005), application No. 5446/03.
389. Cuceranu D. (2008), *Aspects of regulating freedom of expression on the Internet*, Intersentia, p. 212.
390. Internet & Jurisdiction Observatory (2013), 2012 in Retrospect, www.internetjurisdiction.net/wp-content/uploads/2013/03/2012-in-Retrospect.pdf.

6.2.1. Egypt: Internet shutdowns

On 28 January 2013, at 12:12 a.m., Telecom Egypt, a key ISP, started shutting down its part of the Egyptian Internet. Only minutes later Raya, Link Egypt, Etisalt Misr and Internet Egypt followed.[391] This co-ordinated shutdown was ordered by the Egyptian Government as a reaction to the protests of what would become the Arab Spring. The shutdown was in violation of Article 19 of the ICCPR (and Article 19 of the UDHR) and, had Egypt been a member state of the Council of Europe, also of the European Convention of Human Rights.

Using the well-established three-part test, already the legality requirement is not met, as the shutdowns were not based on law but rather on executive decisions. But even if we go one step further, to the necessity test, we are reminded by the Human Rights Committee overseeing the implementation of the ICCPR that:

> [t]he legitimate objective of safeguarding and indeed strengthening national unity under difficult political circumstances cannot be achieved by attempting to muzzle advocacy of multi-party democracy, democratic tenets and human rights; in this regard the question of deciding which measures might miss the "necessity" test in such situations does not arise.[392]

Similarly, in the Siracusa Principles the High Commissioner for Human Rights noted that national security and public order are often used as pretexts to safeguard the government. "National security" may never be used as a reason for "arbitrary restrictions".[393] Even repressing opinions in selected cases is only allowed when there is a serious political or military danger to the state.[394] Complete Internet shutdowns will hardly ever meet the necessity test.

The third level of the three-part test, the proportionality test, is also not met by blanket Internet blackouts. A state has to show that any blackout decision is proportionate in light of the legitimate goal.[395] As the Human Rights

391. Cf. Cowie J. (28 January 2011), *Egypt leaves the Internet*, www.renesys.com/blog/2011/01/egypt-leaves-the-internet.shtml.
392. Human Rights Committee (1994), *Mukong v. Cameroon*, UN Doc. CCPR/C/51/D/458/1991, Abs. 9.7.
393. Siracusa Principles on the Limitation and Derogation of Provisions in the International Covenant on Civil and Political Rights (1984), Annex, UN Doc. E/CN.4/1984/4, para. 31, at www.uio.no/studier/emner/jus/humanrights/HUMR5503/h09/undervisningsmateriale/SiracusaPrinciples.pdf.
394. Partsch K.-J. (1981), "Freedom of conscience and expression, and political freedoms", in Henkin L. (ed.), *The International Bill of Rights: The Covenant on Civil and Political Rights*, New York: Columbia University Press, pp. 209, 221.
395. Human Rights Committee (2004), General Comment No. 31: Nature of the general legal obligation imposed on states parties to the Covenant, UN Doc. CCPR/C/21/Rev.1/Add.13, para. 3. Cf. Human Rights Committee, *Park v. Korea,* Comm. No. 628/1995, Abs. 10.3; *Laptsevich v. Belarus*, Comm. No. 780/1997, para. 8.2.

Committee writes in its Comment No. 34, on freedom of expression, the freedom itself may not be put in jeopardy.[396]

This is not say, however, that a partial blackout must always be illegal.[397] Imagine a conflict fuelled by social media that threatens to escalate into serious violence. If the authorities are technologically unable to shut down the network services that fuel the conflict, and an appropriate law has been democratically passed, it might be proportionate, in order to safeguard the lives of others, to introduce brief regional Internet shutdowns as an *ultima ratio*.

6.2.2 Internet access as a protected right in 20 Council of Europe member states

Though only a few states have laws containing an explicit right to Internet access, accessing the Internet can be protected as an enabling aspect of the right to freedom of expression.[398] In *Yildirim v. Turkey*[399] the European Court of Human Rights wrote that Court research had led to the conclusion that "in theory Internet access is protected by constitutional guarantees regarding freedom of expression, freedom to receive ideas and information" in 20 Council of Europe member states: Germany, Austria, Azerbaijan, Belgium, Spain, Estonia, Finland, France, Ireland, Italy, Lithuania, the Netherlands, Poland, Portugal, the Czech Republic, Romania, United Kingdom, Russia, Slovenia and Switzerland.[400]

This right to access is inherently connected, the Court continued, with the right to access information and communication, which is protected by national constitutional provisions. It includes, according to the Court, the right of everyone to participate in information society and the obligation for states to guarantee everyone access to the Internet. "Taken together, the general guarantees regarding freedom of expression constitute an adequate basis for recognising a right to unhindered Internet access."[401]

Germany: the Internet as an essential part of life

On 24 January 2012 the German Federal Court of Justice – the *Bundesgerichtshof* – ruled that Internet access is of central importance to

396. Human Rights Committee, General Comment No. 34 on Article 19: Freedom of opinion and expression of 21 July 2011, UN Doc. CCPR/C/GC/34 of 12 September 2011, para. 21: "when a State party imposes restrictions on the exercise of freedom of expression, these may not put in jeopardy the right itself. The Committee recalls that the relation between right and restriction and between norm and exception must not be reversed."
397. Cf. more generally on restrictions to freedom of expression online, Chapter 3 *supra*.
398. Cf. *supra* 2.3.
399. *Yildirim v. Turkey* (18 December 2012), application No. 3111/10.
400. Ibid., at 31.
401. Ibid. [our translation]: "L'ensemble des garanties générales consacrées à la liberté d'expression constitue une base adéquate pour reconnaître également le droit d'accès, sans entraves, à Internet."

life and its lack has significant impact on the material basis of life. Users can therefore demand damages from their ISPs if they cannot get online.[402] The judgment is important for freedom of expression online because it clarifies the case of a user whose telecommunications provider could not provide fax, phone and Internet access; in this situation, the telecommunications provider was liable to pay damages (and not merely compensation) for lost Internet access. Fax, the court ruled, had lost much of its importance; a fixed telephone connection, which was considered essential by the court, could be replaced by a mobile phone; but using the Internet amounted to an economic good and lack of access could significantly disrupt the material basis of life.[403] The Internet, the court argued, encompasses various material as text, image, video or audio, including entertainment, answers to questions relevant to daily life and highly scientific texts. This makes it very special and therefore the impact of not having access is immediately and severely felt.[404] This line of reasoning is important as it helps us understand what a central role the Internet has grown to play in the life of the European public. Especially as the first generation of Internet natives is starting to enter the workplace, the role of the Internet will only increase.

The 2012 judgment is in line with a previous judgment of Germany's Federal Constitutional Court, which concluded that it is the duty of the state to ensure that everyone can participate in current communication channels, including the Internet. This can be deduced from Article 1 of Germany's Fundamental Law – or *Grundgesetz* – ensuring human dignity, and the principle of the social state, which taken together ensure for all the "possibility to conduct relations with other people" and "take part in the social, cultural and political life" of the state.[405]

Finland: a right to broadband?

From 1 July 2010 every Finnish citizen was guaranteed the right to access to a 1 megabit per second (Mbps) broadband connection.[406] This technological commitment by the state on behalf of ICT companies is part of an effort by the Finnish Government to provide a 100 Mbps connection to all citizens by 2015. This initiative seems to be well on track, though some regulatory and technological issues remain. As a recent review of Finnish broadband policy demonstrated, already in 2013 almost 90% of Finns lived within 2 km of a

402. Bundesgerichtshof (Federal Court of Justice) (24 January 2013), Urteil des III. Zivilsenats (Judgment of the Third Civil Senate), III ZR 98/12, http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=pm&Datum=2013&nr=63259&linked=urt&Blank=1&file=dokument.pdf.

403. Ibid., at 17.

404. Ibid.

405. German Constitutional Court (9 February 2010), 1 BvL 1/09, para. 135.

406. Cf. BBC (1 July 2010), *Finland makes broadband a 'legal right'*, www.bbc.co.uk/news/10461048.

100 Mbps connection.[407] The commitment by the Finnish Government does not amount to paying for everyone's Internet access. But the governmental guarantee of a minimum level of service and access in implementation of the EU's Universal Services Directive is an important step towards ensuring access in rural areas, a policy that could reverse demographic trends of rural depopulation and reinvigorate local creativity in the growing knowledge economies.

A similar provision is included, for instance, in Spain's Law 2/11 of 4 March 2011 on the sustainable economy. Article 52 (1) obliges the government to ensure broadband connection to the public communications web at a minimum speed of 1 Mbps for everyone.[408]

6.3. Copyright and freedom of expression online

6.3.1. France: the limits to enforcing copyright

Finding common ground between enforcing copyright law and guaranteeing freedom of expression is difficult. The debate about the implementation of ACTA in Europe and of SOPA and PIPA in the US has shown that striking the balance between rights of authors and rights of users is not easy, especially when governments are perceived as responding more to pressure from economic entities wishing to safeguard their profit margins.[409]

Long before ACTA, a 2009 decision of the French *Conseil Constitutionnel*[410] provided for an important connection between freedom of expression and Internet access. At issue was a law, HADOPI I, allowing denial of Internet access to users in certain cases of copyright violation (laws in this spirit are often called three-strikes laws because they oblige ISPs to stop providing Internet access to users who have thrice violated copyright law).

The *Conseil Constitutionnel* struck down the law on constitutional grounds, arguing that the 1789 Declaration of Human and Citizen Rights provided for freedom of communication of ideas and expression. The meaning of this right has changed. In light of the realities of modern communications and the growing importance of Internet-based services for participation in democratic

407. Ars Technica (31 October 2012), *Finland: Plan for universal 100Mbps service by 2015 on track*, http://arstechnica.com/business/2012/10/finland-plan-for-universal-100mbps-service-by-2015-on-track.

408. Gobierno de Espana (Government of Spain), Ley 2/2011, de 4 de marzo 2011 de Ecomomia Sostenible, www.boe.es/diario_boe/txt.php?id = BOE-A-2011-4117.

409. For the implications of copyright for freedom of artistic expression and cultural expression, see *supra* 2.1.5 and 1.6, respectively.

410. Conseil constitutionnel, Decision No. 2009-580 DC of 10 June 2009, Loi favorisant la diffusion et la protection de la création sur internet, www.conseil-constitutionnel.fr/decision/2009/2009-580-dc/decision-n-2009-580-dc-du-10-juin-2009.42666.html.

life and the expression of ideas and opinions, the French constitutional arbiter argued, this right now includes "la liberté d'accéder à ces services" (freedom to access [Internet] services). The *Conseil Constitutionnel* also laid down important markers for the conditions under which Internet access can be restricted: only after the decision of a judge, after a fair process and in implementing a proportionate sanction. Any provisional measures have to be strictly necessary for the preservation of the author's rights at issue. The legislative response to the unconstitutionality of HADOPI 1 was to adopt a new law, HADOPI 2, which transferred the power to disconnect users to a judicial authority.[411]

The French court's judgment proved influential. The European Court of Justice's *Scarlet Extended*[412] decision evidenced the same approach, when it found that a requirement for Internet service providers to install filtering software in order to conduct blanket searches for unlawful content would amount, *inter alia*, to a violation of freedom of expression online. The French decision was also quoted at length in *Yildirim v. Turkey*,[413] the first ECHR case dedicated to Internet access.

6.3.2. European Union: citizen activism for freedom of expression

Freedom of expression has often been contrasted with intellectual property rights, and never more so than during the debate on the Anti-Counterfeiting Trade Agreement (ACTA)[414] in Europe. This showcased the dynamics of an international human rights-based discourse and the newly emerged sensibilities of an Internet-focused polity.

ACTA is (the draft for) an international trade agreement between the EU and non-EU states, including Japan, the US and Canada, that seeks to ensure effective international enforcement of intellectual property rights. Negotiations on ACTA started in June 2008 and were concluded in 2010. In late 2011, EU member states authorised the Commission to sign ACTA, and agreed to sign and ratify it themselves. But during the first phase of national ratification processes, civil society opposition intensified. A number of EU member states, with Poland in the lead, stopped plans for ratification, and demonstrations

411. Cf. Lucchi N. "Access to network services and protection of constitutional rights: recognising the essential role of Internet access for freedom of expression", *Cardozo Journal of International and Comparative Law* (2011), pp. 645-78 (at 672).

412. *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* (24 November 2011), ECJ C-70/10.

413. *Yildirim v. Turkey* (18 December 2012), application No. 3111/10.

414. Council of the European Union (23 August 2011), *Anti-Counterfeiting Trade Agreement between the European Union and its Member States, Australia, Canada, Japan, the Republic of Korea, the United Mexican States, the Kingdom of Morocco, New Zealand, the Republic of Singapore, the Swiss Confederation and the United States of America*, Doc. No. 12196/11, http://register.consilium.europa.eu/pdf/en/11/st12/st12196.en11.pdf.

occurred in a number of European capitals. The European Commission finally decided to have the Court of Justice of the European Union make the determination of whether ACTA is consistent with the Fundamental Rights Charter and other primary law-based fundamental rights guarantees on the EU level.[415] The European Parliament decided not to adopt the draft anyway.

Good practices for freedom of expression online lie on the one hand in the recognition by governments that excluding parliamentarians and civil society from treaty-making processes (and, by extension, national legislative processes), especially when human rights on the Internet are concerned, is a perilous approach for norm makers. They run the risk of facing a crisis of legitimacy for the normative solution reached in a process that did not include multiple stakeholders.

With ACTA, the European Commission argued that the critique regarding the exclusion of parliament and civil society was unfounded,[416] as "7 successive draft texts of the agreement; 3 detailed written reports on the negotiation rounds; 14 notes and internal working papers"[417] had been shared with the European Parliament. But the rapporteur of the European Parliament for ACTA resigned, criticising the non-transparent approach followed.[418] The negotiations, partly for reasons of EU competency, were mainly a Commission- and state-led exercise, but the (former) ACTA rapporteur for the European Parliament argued that the whole process was faulty: "no consultation of the civil society, lack of transparency since the beginning of negotiations, repeated delays of the signature of the text without any explanation given, rejection of Parliament's recommendations as given in several resolutions of our assembly."[419]

The example of ACTA allows us to conclude that a certain sense of ownership of Internet-related legislation has emerged internationally that is much stronger than in certain non-Internet-related fields of regulation, such as tax law. The big challenge that both states and other stakeholders face is developing clear and legitimate avenues of participation for all relevant stakeholders in (international) normative processes.[420]

---

415. Cf. European Commission (22 February 2012), Commissioner De Gucht K., *Statement on ACTA,* at trade.ec.europa.eu/doclib/press/index.cfm?id = 778. He expresses the Commission's opinion that "ACTA will change nothing about how we use the internet and social websites today – since it does not introduce any new rules. ACTA only helps to enforce what is already law today".
416. European Commission (13 February 2012), *Transparency of ACTA negotiations*, trade.ec.europa.eu/doclib/docs/2012/february/tradoc_149103.pdf.
417. Ibid.
418. Lee D., European Parliament rapporteur quits in Acta protest, 27 January 2012, www.bbc.co.uk/news/technology-16757142.
419. As quoted in ibid.
420. Cf. Kettemann M. C. (2013), *The future of individuals in international law: lessons from international Internet law*, Eleven, p. 138.

6.4. Public and private violations of freedom of expression online

6.4.1. United Kingdom: limits of freedom of expression online – and the limits of these limits

Though freedom of expression has a long history in the United Kingdom, and some of the continent's first documents containing predecessors of today's human rights emerged on the British isle, the use of Twitter is not without its dangers in Britain. In our introduction, we recalled the case of Paul Chambers, who tweeted, when advised that adverse weather had forced his local airport to close, "Crap! Robin Hood airport is closed, you've got a week and a bit to get your shit together otherwise I'm blowing the airport sky high!!" [*sic*]. He was convicted of making statements of a menacing character and only the highest court of the United Kingdom overturned the judgment.[421] The Lord Chief Justice quashed the lower court's convictions arguing, *inter alia*, that users "are free to speak not what they ought to say, but what they feel".[422]

Of course, this standard is not without its problems. A Twitter user may "feel" angry, may speak with a discriminatory intent, may want to actively incite violence. In October 2012, a British teenager who made "sick jokes" on Facebook about a missing girl was sentenced to 12 weeks in jail. Just a day later, another man was sentenced for having authored an abusive post about British soldiers who had died.[423]

The three-part test that the European Court of Human Rights uses – in defining whether a statement is protected by freedom of expression or can be legitimately penalised – is a much clearer standard than references to what users may "feel". Apart from penal law, however, a broader awareness-raising approach is necessary. In light of the growing number of Twitter-related cases, the director of the UK Crown Prosecution Service admitted that social media was raising "difficult issues of principle" and these had to be "confronted not only by prosecutors but also by others including the police, the courts and service providers". Not all statements, even offensive remarks, need to face criminal prosecution. Rather, as the chief prosecutor argued, "the time has come for an informed debate about the boundaries of free speech in an age of social media".[424]

421. Bowcott O. (27 July 2012), "Twitter joke trial: Paul Chambers wins high court appeal against conviction", *The Guardian*, www.guardian.co.uk/law/2012/jul/27/twitter-joke-trial-high-court.
422. *Paul Chambers v. DPP* (27 July 2012), [2012] EWHC 2157.
423. Sabbagh D. (9 October 2012), "Facebook and Twitter could be asked to increase moderation of networks", *The Guardian*, www.guardian.co.uk/media/2012/oct/09/dpp-criminal-tweets-facebook-posts.
424. Keir Starmer QC (20 September 2009), Director of Public Prosecutions, Crown Prosecution Service, *DPP statement on Tom Daley case and social media prosecutions*, http://blog.cps.gov.uk/2012/09/dpp-statement-on-tom-daley-case-and-social-media-prosecutions.html.

6.4.2. Twitter in France, Germany and the US: testing boundaries of free speech

While it is important for Internet companies to protect the privacy of their users and their right to engage in freedom of expression, certain limits are not only possible but even required by international human rights law.[425] On 24 January 2013, for instance, a French court ruled that Twitter had to identify authors of anti-Semitic messages "within the framework of its French site". The ruling had come after France's Union of Jewish Students had sued Twitter to police more effectively the misuse of the site as a forum for anti-Semitic slurs under #unbonjuif ("#agoodjew").[426] Twitter complied with the ruling.

Similarly, Twitter suspended account privileges for a German neo-Nazi group after a request from Germany. It also turned over to New York prosecutors tweets of an activist arrested during the Occupy Wall Street movement.[427] Manhattan Criminal Court Judge Matthew Sciarrino Jr was quoted as saying: "If you post a tweet, just like if you scream it out the window, there is no reasonable expectation of privacy." A lawyer for Twitter replied arguing that "Twitter users own their tweets. They have a right to fight invalid government requests, and we continue to stand with them in that fight."[428]

6.4.3. United Kingdom: private censorship through hotlines

The UK Internet Watch Foundation (IWF), with its hotline against illegal content, has been criticised for including non-illegal websites in its blacklist with immediate negative effects for website owners and Internet users, without any notice of blocking or review procedure (or even a judicial assessment of legality) that would be consistent with human rights.[429]

Three cases in particular stand out. In December 2008 IWF blacklisted the image of a naked child on the 1976 album by the German band Scorpions. As a result of the inclusion of the address on the blacklist the majority of UK Internet users were no longer able to access the content and, more seriously, were no longer able to edit Wikipedia pages without logging in. Wikipedia representatives complained that "[due] to censorship by the UK self-regulatory agency the Internet Watch Foundation (IWF), most UK residents can no longer edit the volunteer-written encyclopedia, nor can they access an article in it describing

425. See more generally 5.1, *supra*, on Internet content regulation and freedom of expression.
426. Juilliard P. (AFP) (24 January 2013), *French court says Twitter must identify racist tweeters.*
427. Cf. RT.com (24 September 2012), *Twitter hands over Occupy protester's tweets to NY judge*, http://rt.com/usa/twitter-occupy-last-harris-153.
428. Ibid.
429. Nunziato D. C. (2013), "Procedural protections for Internet expression", *International Review of Law, Computers, and Technology* (forthcoming), www.osce.org/fom/99458.

a 32-year-old album by German rock group the Scorpions".[430] The IWF Board, after a request by the Wikimedia Foundation, reviewed the image, confirmed its finding of "potential illegality" but in light of the "contextual issues involved in this specific case and, in light of the length of time the image has existed and its wide availability" removed the URL from the blacklist.[431]

In 2009, UK users were also unable to access pages in the Internet Archive Wayback machine because the archive contained a number of blocked URLs. In 2011, customers of ISP Virgin Media were unable to access the cloud-based file-hosting service Fileserve because certain URLs stored in the archive had been blacklisted.[432]

These examples show that, while the overall goal of IWF and similar hotlines is important, the practical denial of procedural protections of freedom of expression can lead to serious negative consequences. As we wrote in Chapter 5, it is essential for hotlines to respect human rights (of all) in their quest to protect human rights (of minors).

6.5. Powerful Internet companies and national laws: who wins the battle for freedom of expression?

Getting international search engine and social network service providers to accept national and European laws, especially in the fields of data protection, privacy and freedom of expression, is sometimes difficult. As of April 2013, Google faced legal action from the data-protection authorities from six different states (Germany, France, the Netherlands, Spain, Italy and Britain) for a failure to change its privacy policy after concerns about the harmonisation of privacy policies between different Google services.[433] Another example, for social networks, is the Austrian initiative "Europe versus Facebook",[434] which has raised a number of privacy issues in Facebook's terms of service with the Irish Data Protection Commissioner. The Irish Data Protection Commissioner's report, and the Austrian initiative's actions, have succeeded in altering some parts of Facebook's policy, but other regional examples show the influence that decentralised norm-making can have – for better and worse.

430. BBC (12 August 2008), *Scorpions censored*, www.bbc.co.uk/6music/news/20081208_scorpians.shtml.
431. Internet Watch Foundation (9 December 2008), *IWF statement regarding Wikipedia webpage*, www.iwf.org.uk/about-iwf/news/post/251-iwf-statement-regarding-wikipedia-webpage.
432. Cf. Nunziato D. C. (2013), "Procedural protections for Internet expression", *International Review of Law, Computers, and Technology* (forthcoming), www.osce.org/fom/99458.
433. Arthur C., Google facing legal threat from six European countries over privacy, *The Guardian*, 2 April 2013, www.guardian.co.uk/technology/2013/apr/02/google-privacy-policy-legal-threat-europe.
434. Europe versus Facebook, www.europe-v-facebook.org.

6.5.1. Germany: regional approaches to ensuring pseudonymity

A regional initiative to safeguard freedom of expression online was started by the regional data-protection office of the German state of Schleswig-Holstein, which ordered Facebook to change its real-name policy and allow the use of pseudonyms.[435] The office based its arguments on paragraph 13 (6) of the German *Telemediengesetz* (TMG; Telemedia Act), which obliges online service providers "to enable the anonymous or pseudonymous use of telecommunications media …, as far as technically possible and reasonable". According to the office, the German legislation complies with European law and serves to protect "in particular the fundamental right to freedom of expression on the Internet". Identity theft and abuse of social networks are a problem, but the real-name obligation does not prevent them effectively. Therefore, the office concluded, "[t]o ensure the data subjects' rights and data-protection law in general, the real-name obligation must be immediately abandoned by Facebook".[436]

This decision raises the larger issue of how international Internet companies should react to different standards in national and regional decisions and legislation. It is important to say clearly that certain standards have to be met and that international human rights commitments, especially the commitment to freedom of expression online, must be respected. The decision also raises the question how to ensure that an authoritative standard of interpretation of freedom of expression, as developed by the Judges in Strasbourg, can be translated for local and regional offices and judiciaries.

The decision also touches on the issue of the role of data-protection offices in the context of a state's judicial system. Only two months after the decisions by the Data Protection Office, the Upper Administrative Court of the German state of Schleswig-Holstein agreed to suspend the ruling of the office on the grounds that German data-protection law was not applicable as the relevant collection of data takes place in Ireland (where Facebook Ltd is incorporated).[437] The office appealed and the court case continues.[438]

---

435. BBC News (18 December 2012), *Germany orders changes to Facebook real name policy*, www.bbc.co.uk/news/technology-20766682.
436. Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (Office of the Data Protection Commissioner for Schleswig-Holstein) (17 December 2012), *ULD issues orders against Facebook because of mandatory real names*, www.datenschutzzentrum.de/presse/20121217-facebook-real-names.htm.
437. Schleswig-Holsteinisches Oberverwaltungsgericht (SHO), Decisions Az.: 8 B 60/12 and 8 B 61/12 (14 February 2013). See SHO (15 February 2013), *Verwaltungsgericht gibt Eilanträgen von Facebook statt*, www.schleswig-holstein.de/OVG/DE/Service/Presse/Pressemitteilungen/15022013VG_facebook_anonym.html.
438. Unabhängiges Landeszentrum für Datenschutz, *Verwaltungsgericht Schleswig erteilt Facebook Freifahrtschein*, www.datenschutzzentrum.de/presse/20130215-verwaltungsgericht-facebook.htm. Cf. Tech Crunch, *Facebook wins court challenge in Germany against its real names policy*.

6.5.2. Google Italy: personalising (criminal) liability for online content

In September 2006 a video was posted on Google videos that showed the taunting of a disabled child by other children. The video was online for three months before being removed by Google after a complaint by the Italian Postal Service. The authors of the video were prosecuted (after Google provided identifying information), but so were four executives of Google for "defamation and violation of data-protection rules" by "co-participation" and by illicitly processing personal and health data for profit.[439]

The Tribunale di Milano in 2010 (case No. 1972/2010) passed suspended prison sentences on three of the executives for the data-protection violations.[440] The tribunal did not find any guilt in co-participation in defamation as the current Italian legislation did not provide for Internet service providers' liability for negligence in delayed removal of postings. After outspoken criticism of the decision, an appeals court, in 2012, reversed the convictions and acquitted the three men.[441] It argued, *inter alia*, that:

> [t]he possibility must be ruled out that a service provider which offers active hosting can carry out effective, pre-emptive checks of the entire content uploaded by its users. … An obligation for the Internet company to prevent the defamatory event would impose on the same company a pre-emptive filter on all the data uploaded on the network, which would alter its own functionality.[442]

Such a pre-emptive filtering system would not only alter the network's functionality but also violate freedom of expression, at least if such a system was imposed by a state, as the European Court of Justice ruled in *SABAM*.[443] However, the Italian prosecutors decided to appeal in the case to the nation's Supreme Court arguing, *inter alia*, that "platforms like YouTube should be responsible for prescreening user-uploaded content and obtaining the consent of people shown in user-uploaded videos".[444] Such a prescreening process

439. Sartor G. and Viola de Azevedo Cunha M. (2010): "The Italian Google-case: privacy, freedom of speech and responsibility of providers for user-generated contents", *I. J. Law and Information Technology* 18(4), pp. 356-78.

440. Tribunale Ordinario di Milano (16 April 2010), penal section, case 1972/2010, pp. 102 et seq.

441. Corte d'Appello di Milano (21 December 2011), Sezione Prima Penale, case 8611/12, www.leggioggi.it/wp-content/uploads/2013/02/20130301111013944.pdf. Cf. Reuters (21 December 2012), *Google executives acquitted in Milan autism video case*, http://www.reuters.com/article/2012/12/21/google-italy-privacy-idUSL5E8NL6RR20121221.

442. The Court's ruling, as quoted by Reuters (27 February 2013), *Google not expected to check every upload says Italian court*, www.reuters.com/article/2013/02/27/net-us-google-italy-privacy-idUSBRE91Q0TP20130227.

443. *SABAM v. Netlog NV* (16 February 2012), ECJ C-360/10.

444. Peter Fleischer, *The saga continues … now to the Italian Supreme Court*, 17 April 2013, http://peterfleischer.blogspot.fr/2013/04/the-saga-continuesnow-to-italian.html.

would amount to an obligation of "prior constraint" censorship for Internet intermediaries – an approach that violates human rights, especially freedom of expression online, and is at odds with the Court's and the Court of Justice of the European Union's jurisprudence and well-established principles for freedom of expression online.[445]

6.5.3. UK: publisher's liability for Google confirmed

This does not mean, however, that the issues are clear. On 14 February 2013, the Court of Appeal of England and Wales ruled that Google can be held liable for comments published on Blogger, its online blogging platform, unless it reacts immediately to a complaint.[446] The appeals judgment reversed a 2012 ruling[447] which had considered, in line with international jurisprudence, that an Internet platform should not be treated as a publisher. Google had received complaints regarding certain comments on a blog post and had forwarded them to the blogger who waited five weeks to delete them. The British NGO Article 19 considered the judgment to be a "serious step back for free speech online".[448]

The judgment means, in effect, that the notice and takedown system is strengthened. This system encourages content hosts, such as Google (but also individual bloggers who have activated their commentary function) to immediately delete even potentially defamatory material immediately after having been notified, even if the material is not illegal at all. According to Article 19, this creates a "worrying chilling effect on freedom of expression, as intermediaries might censor perfectly legitimate speech".[449]

While the British judgment had an obvious connection to content, recent developments have evidenced a tendency to strengthen Google's liability also with regard to its technical role. A German businessman had sued Google because searches for his name were auto-completed by the algorithm with the words "scientology" and "fraud". Although Google argued in the case that this only reflected search preferences by users, Google had previously changed auto-completions, which suggests the search engine

445. See *supra*, especially Chapters 2 and 3.
446. Court of Appeal (14 February 2013), *Payam Tamiz v. Google Inc.*, [2013] EWCA Civ 68, www.bailii.org/ew/cases/EWCA/Civ/2013/68.html.
447. High Court (2 March 2012), *Payam Tamiz v. Google Inc. and Google UK Limited*, [2012] EWHC 449 (QB), www.bailii.org/ew/cases/EWHC/QB/2012/449.html.
448. EDRi-gram newsletter (27 February 2013), *UK Court: Google liable for comments posted on its blogger platform*, www.edri.org/edrigram/number11.4/google-liable-comment-blogger-uk.
449. Press Release on Article 19 (15 February 2013), *United Kingdom: ruling on Google's liability is bad news for free speech online*, www.article19.org/resources.php/resource/3611/en/united-kingdom:-ruling-on-google%E2%80%99s-liability-is-bad-news-for-free-speech-online#sthash.u4O9LisK.dpuf.

company is aware of the harmful dimension of auto-complete. The case of Bettina Wulff, Germany's former First Lady, raises related issues.[450] In the case of the German businessman, the *Bundesgerichtshof* (Germany's highest civil court) ruled that the plaintiff's privacy rights were affected as the auto-completion suggested a relationship between him and the two words with negative connotations. If that connection was untrue, his rights would be violated.[451]

6.5.4. UK, Germany and the Council of Europe: whistle-blowing as a human right

When WikiLeaks, an online whistle-blowing site, released classified US cables in 2010, the issue arose of whether publishing secret or classified information can be a human right. Similarly, during the financial crisis, prosecutors started to rely more heavily on insiders to provide them with information on crimes and wrongdoing. Unlike most Council of Europe member states, the United Kingdom (and globally the United States) have legislation protecting whistle-blowers.[452]

The Council of Europe seeks to provide general rules and guidelines. In its Resolution 1729 (2010) the Council of Europe's Parliamentary Assembly reaffirmed the importance of protecting whistle-blowers in light of the "right of everyone to disclose information of public concern which corresponds to the right of the public to be informed under Article 10 of the Convention".[453] Though everyone has a right to disclose publicly relevant information, the usual limits of section 2 of Article 10 apply. Publishing classified information can be legitimately criminalised if this is prescribed by law and "necessary in a democratic society, in the interests of national security, … public safety, for the prevention of disorder or crime, … 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".

The Parliamentary Assembly's resolution underlines the importance of whistle-blowers who can, through their actions, "provide an opportunity to strengthen accountability and bolster the fight against corruption and

450. Lischka K., *Blaming the algorithm: defamation case highlights Google's double standard*, www.spiegel.de/international/germany/defamation-case-by-bettina-wulff-highlights-double-standard-at-google-a-854914.html.

451. BGH, VI ZR 269/12. See Matussek K., *Google loses German case over autocomplete function*, 3 June 2012, www.bloomberg.com/news/2013-05-14/google-loses-german-case-over-autocomplete-function.html.

452. Cf, on whistle-blowing as a human rights more generally, 2.1.10, *supra*.

453. Council of Europe, Parliamentary Assembly (2010), Resolution 1729 on the Protection of "whistle-blowers", http://assembly.coe.int/main.asp?link = /documents/adoptedtext/ta10/eres1729.htm.

mismanagement, both in the public and private sectors".[454] National laws need to be comprehensive and encompass employment law, criminal law and procedure, and media law to focus on "providing a safe alternative to silence".[455]

In 2011, the European Court of Human Rights demonstrated both national shortcomings in balancing the interests of whistle-blowers and of keeping the secrets of one's employer and the importance of whistle-blowing for the public debate. In *Heinisch v. Germany*[456] the Court found a violation by Germany in that the courts did not protect a geriatric nurse who had been fired after publicising wrongdoing at her workplace.

The Court recalled that as a general rule public-sector employees who publicise illegal conduct or wrongdoing in the workplace "should, in certain circumstances, enjoy protection", especially when the employee is one of the few people who are aware of what is happening and thus "best placed to act in the public interest".[457] However, in light of each employee's duty "of loyalty and discretion", disclosure should be first made to their superior or to other competent authorities. Only when this is "clearly impracticable" should the information "as a last resort, be disclosed to the public".[458] When testing restrictions, the Court therefore will analyse whether the whistle-blower "had any other effective means of remedying the wrongdoing which he or she intended to uncover". Another factor is "the public interest involved in the disclosed information"[459] especially in light of the importance of the strict limits on restrictions on debate on questions of public interest. This approach is also relevant for online cases.

Council of Europe members and their courts therefore have to make sure they strike a fair balance between two countervailing objectives: "the need to protect the employer's reputation and rights on the one hand and the need to protect the applicant's right to freedom of expression on the other."[460] In the US, whistle-blowing is much more of an issue of public interest and protection of whistle-blowing has been institutionalised. The US Securities and Exchange Commission (SEC) even has its own Office of the Whistle-blower.[461] The SEC is authorised to provide "monetary award" to individuals with information leading to enforcement action in which fines over $1 million are ordered. The range of the individual awards is between 10% and 30% of the money collected.[462] In 2012, the office received some 3 000 tips from whistle-blowers in the USA and 49 other

454. Ibid., 1.
455. Ibid., 6.2.
456. *Heinisch v. Germany* (21 July 2011), application No. 28274/08.
457. Ibid., at 63.
458. Ibid., at 65.
459. Ibid., at 66.
460. Ibid., at 94.
461. SEC, Office of the Whistle-blower, www.sec.gov/whistleblower.
462. Cf. ibid.

countries.[463] However, the positive approach to whistle-blowing with regard to some aspects of US law and society did not prevent the US authorities from taking all possible action against WikiLeaks, which sees itself as a whistle-blowing platform but was considered by the US authorities as a threat to national security.[464]

6.6. Business and freedom of expression online

6.6.1. Tajikistan: no complicity of companies in censorship

After violence in the Tajik province of Gorno-Badakshan, a subsidiary of the Swedish-Finnish telecom company Telia Sonera blocked access to a number of websites, including YouTube, the Russian news agency RIA Novosti and BBC News.[465] The blocking was done at the behest of the government,[466] but this raises the issue of whether local subsidiaries of international ICTs should try to emulate the human rights commitments of international companies, as in the Global Network Initiative, or rather subject themselves to national laws. It can be argued that national laws are, of course, important and should be respected as long as they do not violate international commitments to human rights. Companies – especially parent companies, which are less prone to be pressured into submitting to demands to violate the rights of their users – have a special responsibility to support their subsidiaries. But there are also companies that are not only complicit in human rights abuses but provide the technology that governments use in violating human rights, including freedom of expression online.

TeliaSonera responded to the criticism by involving itself more strongly in industry initiatives to support human rights. Together with key telecommunication companies including Alcatel-Lucent, France Telecom-Orange, Nokia Siemens Networks, Telefonica and Vodafone, the company co-founded

463. U.S. Securities and Exchange Commission (Fiscal Year 2012), *Annual report on the Dodd-Frank whistleblower program*, www.sec.gov/about/offices/owb/annual-report-2012.pdf, p. 4.

464. Cf. Goldsmith J. (10 December 2010) *Seven thoughts on WikiLeaks*, www.lawfareblog.com/2010/12/seven-thoughts-on-wikileaks. This is not the only contradiction in US policy on Internet freedom. In her speech introducing the US Internet freedom policy, "Secretary Clinton complained about cyberattacks seven paragraphs before she boasted of her support for hacktivism".

465. PEN International, *PEN Declaration on Digital Freedom*, Case Studies, Tajikistan: Business and Human Rights, www.pen-international.org/wp-content/uploads/2012/11/PEN-declaration-Case-Studies_PDF4.pdf.

466. Global Network Initiative (1 August 2012), *Ensure the free flow of information in Tajikistan*, www.globalnetworkinitiative.org/news/ensure-free-flow-information-tajikistan.

the *Telecommunication Industry Dialogue.* In 2013, the companies published *Guiding Principles on Telecommunication and Freedom of Expression and Privacy* and announced co-operation with the Global Network Initiative (GNI). Their aim is to "advance freedom of expression and privacy rights in the Information and Communication Technology (ICT) sector more effectively".[467] Referring to the Ruggie Principles, the Guiding Principles[468] seek to find a balance between the duty of governments to protect human rights and the corporate responsibility of telecommunications companies to respect human rights.

6.6.2. EU: does the export of censorship and surveillance technology violate human rights?

While the EU is committed to protecting human rights online, a number of European companies such as Nokia Siemens Networks, Gamma, Trovicor, Hacking Team and Bull/Amesys continue to export surveillance equipment and censorship software which is used against citizen activists in countries such as Bahrain, Iran, Syria and Tunisia.[469] Exports of surveillance technology to some countries, such as Libya and Iran, have been restricted, but the EU still does not have a general human rights-sensitive system of export controls.[470] This is unfortunate because the protection of citizens, citizen journalists, and journalists against technologically advanced spyware is an important human rights issue and a declared objective of EU human rights policy, which even finances circumvention tools for digital defenders.[471]

NGOs have been active in demanding accountability from companies for producing software that can be used for violations of freedom of expression by restrictive regimes. In February 2013, Privacy International, Reporters Without Borders and other NGOs filed a complaint[472] with the OECD alleging that two software companies, UK-based Gamma Group and Germany's Trovicor

467. TeliaSonera, *Key telecommunication players sign principles on Freedom of Expression and Privacy and announce collaboration with GNI*, 14 March 2013, www.teliasonera.com/en/newsroom/press-releases/2013/3/key-telecommunication-players-sign-principles-on-freedom-of-expression-and-privacy-and-announce-collaboration-with-gni.
468. Telecommunications Industry Dialogue on Freedom of Expression and Privacy, *Guiding principles* (2013), www.teliasonera.com/Documents/Public % 20policy % 20documents/Telecoms_Industry_Dialogue_Principles_Version_1_-_ENGLISH.pdf.
469. European Digital Rights, EDRi-gram newsletter (19 December 2012), *Export controls for digital weapons*, www.edri.org/edrigram/number10.24/export-controls-digital-weapons.
470. Wagner B., *Export censorship and surveillance technology* (2012), www.hivos.nl/content/download/72343/618288/file/Exporting % 20Censorship % 20And % 20Surveillance % 20Technology % 20by % 20Ben % 20Wagner.pdf.
471. Cf., on the positive role companies can take in promoting freedom of expression online, 4.3.2.
472. Bloomberg (5 February 2013), *Rights groups file OECD complaint against surveillance firms*, www.bloomberg.com/news/2013-02-04/rights-groups-file-oecd-complaint-against-surveillance-firms.html.

GmbH, violated the OECD's Guidelines for Multinational Enterprises.[473] Similarly, Reporters Without Borders, for the first time, published a list of five "corporate enemies of the Internet"[474] – Gamma, Trovicor, Hacking Team, Amesys and Blue Coat – describing these companies as "digital era mercenaries" that "sell products that are liable to be used by governments to violate human rights and freedom of information".[475]

Some European states such as Germany show two different faces when it comes to fighting online violations of freedom of expression. Not only have they in the past stopped the development of comprehensive export controls, but they also use spyware in domestic settings. In January 2013 a classified document of the German Ministry of Interior was leaked that confirmed that the German Federal Police had purchased the commercial Spyware toolkit FinFisher from the Eleman/Gamma Group for use in telecommunication surveillance.[476]

A positive approach towards stopping the use of European software to target citizen activists abroad has been evidenced by the Digital Freedom Strategy in EU Foreign Policy adopted by the European Parliament in December 2012.[477] The Strategy:

> deplores the fact that EU-made technologies and services are sometimes used in third countries to violate human rights through censorship of information, mass surveillance, monitoring, and the tracing and tracking of citizens and their activities on (mobile) telephone networks and the internet[478]

and it urges the Commission to stop this "digital arms trade". This should be ensured through a ban on exports of repressive technology and services to authoritarian regimes. In order to ensure a comprehensive approach the European Parliament also argues that technology exports-related sanctions should be monitored more effectively.

The national practice we have discussed in this chapter has been, necessarily, selective. But it aptly illustrates just how varied the challenges to freedom of expression can be. States alone cannot hope to cope with them. Therefore, the co-operation of all stakeholders is important throughout the process of setting standards, monitoring and promoting freedom of expression online. Monitoring and promotion of freedom of expression will be the focus of the following two chapters, 7 and 8.

---

473. OECD, *Guidelines for multinational enterprises*, www.oecd.org/daf/inv/mne.
474. Reporters Without Borders (2013), *Enemies of the Internet 2013*, http://surveillance.rsf.org/en.
475. Ibid.
476. Netzpolitik.org (16 January 2013), *Secret government document reveals: German Federal Police plans to use Gamma FinFisher spyware*, http://netzpolitik.org/2013/secret-government-document-reveals-german-federal-police-plans-to-use-gamma-finfisher-spyware.
477. European Parliament (11 December 2012), Resolution on a digital freedom strategy in EU foreign policy, 2012/2094(INI).
478. Ibid., p. 22.

7. European monitoring mechanisms

The goal of protecting freedom of expression can be reached through a number of ways: via universal treaties, regional treaties, national laws, regulation via soft law and promotion of good practice. National laws, such as prohibition of Holocaust denial online, are implemented by the national executive with subsequent control by national courts. International agreements are usually monitored by the states themselves or, in some treaties, by a quasi-judicial body. Very often, however, courts and quasi-judicial bodies are not the only actors in the promotion and protection of freedom of expression on the Internet. A central role is taken by other institutions that monitor freedom of expression and identify both best practice and violations.

In Chapters 2, 3 and 4 we described the legal side of the protection of freedom of expression and the standard-setting function of the Council of Europe and non-state actors. In Chapters 5 and 6 we looked at national and international examples of the challenges faced by freedom of expression. In this chapter we consider the role of (mainly) European monitoring mechanisms. We first analyse the role and impact of Council of Europe monitoring bodies, including its main political bodies (the Committee of Ministers, the Parliamentary Assembly, the General Secretary, the Commissioner for Human Rights), the European Court of Human Rights and the Council of Europe's relevant expert bodies: the European Committee on Social Rights, Advisory Committee under the Framework Convention for the Protection of National Minorities and European Commission against Racism and Intolerance (ECRI). Then we briefly touch on monitoring activities by other European organisations, such as the OSCE and the EU, before looking at the role of private hotlines and civil society watchdogs.

7.1. Council of Europe Internet governance strategy

According to the Council of Europe's Internet Governance Strategy the goal of all Council of Europe activities regarding online freedom of expression is "[m]aximising the rights of, and freedoms for, Internet users".[479] The Internet

479. Council of Europe, Committee of Ministers, Internet Governance (15 March 2012), *Council of Europe Strategy 2012-2015*, CM(2011)175 final, para. 5.

governance strategy includes a broad variety of commitments and activities for Council of Europe bodies, which inform the monitoring mechanisms. Though they concern all human rights online, the following aspects are particularly relevant for monitoring freedom of expression on the Internet.

In its Internet governance strategy, the Council of Europe has committed to ensuring effective recourse in cases of violations of rights and raising public awareness of human rights on the Internet. Further, the Council commits to developing human rights-based guidelines and best-practice models, most of which we discuss in this book. These guidelines are important in monitoring and inform the activities of both states and private Internet actors, such as social engine services and search engine providers.

The strategy also calls for further exploration of "the possibilities for positive use of information and communication technologies … in fighting human rights abuses, such as alerting public authorities of incidents of domestic violence or threats to 'whistleblowers'".[480]

7.2. Monitoring by Council of Europe bodies

7.2.1. The Committee of Ministers

This is responsible for supervising the execution of judgments by the European Court of Human Rights. Progress is regularly assessed during four key human rights meetings per year,[481] in which the Committee of Ministers discusses the progress made by states and can pass interim resolutions and, once implementation is achieved, final resolutions.

As the European Court of Human Rights is an important actor in the process of protecting freedom of expression online and its jurisprudence is key for establishing a European standard of protection, the role of the Committee of Ministers in monitoring implementation of its judgments is essential for the protection of expression online. The Committee of Ministers is also in a unique position to recognise emerging problems and, supported by the work of its expert committees, can develop and pass resolutions and declarations on all aspects of human rights protection in Europe, notably freedom of expression.

Specifically with regard to freedom of expression the Committee of Ministers has passed a Declaration on libel tourism and its impact on freedom of

480. Ibid., para. 5, lit. h.

481. Cf. Council of Europe, Committee of Ministers, Supervision of execution of judgments of the European Court of Human Rights, www.coe.int/t/cm/humanRights_en.asp.

expression (2012)[482] and two recommendations on measures to promote respect for freedom of expression and information with regard to Internet filters (2008)[483] and on promoting freedom of expression and information on the Internet (2007).[484] Though these documents are more properly described as part of the standard-setting endeavours of the Council of Europe, they provide guidance for the monitoring role of the highest Council of Europe body.

7.2.2. The Parliamentary Assembly

The Assembly can use three different procedures to influence human rights policies.[485] It can adopt recommendations to the Committee of Ministers on policies to be implemented by member states, it can pass resolutions containing decisions and expressing points of view, and it can express opinions on questions posed by other bodies. Through these three approaches the Parliamentary Assembly has exercised a quasi-monitoring function. Documents adopted by the Parliamentary Assembly include a general resolution[486] and a recommendation[487] on the protection of freedom of expression and information on the Internet and online media, a resolution[488] and recommendation[489] on fighting "child abuse images" through committed, transversal and internationally co-ordinated action, and a recommendation[490] and resolution[491] on the protection of privacy and personal data on the Internet and online media. In 2009, the Parliamentary Assembly had already passed a recommendation on the promotion of Internet and online media services appropriate for minors.[492]

482. Council of Europe, Committee of Ministers (4 July 2012), Declaration on the desirability of international standards dealing with forum shopping in respect of defamation, "libel tourism" to ensure freedom of expression.
483. Council of Europe, Committee of Ministers (26 March 2008), Recommendation CM/Rec(2008)6 to member states on measures to promote the respect for freedom of expression and information with regard to Internet filters.
484. Council of Europe, Committee of Ministers (26 September 2007), Recommendation CM/Rec(2007)11 on promoting freedom of expression and information in the new information and communications environment.
485. Council of Europe, Parliamentary Assembly, Assembly procedure, http://assembly.coe.int/Main.asp?Link = /AboutUs/APCE_Procedure.htm, accessed 9 March 2013.
486. Council of Europe, Parliamentary Assembly, Resolution 1877 (2012), The protection of freedom of expression and information on the Internet and online media.
487. Council of Europe, Parliamentary Assembly, Recommendation 1998 (2012), The protection of freedom of expression and information on the Internet and online media.
488. Council of Europe, Parliamentary Assembly, Resolution 1834 (2011), Combating "child abuse images" through committed, transversal and internationally co-ordinated action.
489. Council of Europe, Parliamentary Assembly, Recommendation 1980 (2011), Combating "child abuse images" through committed, transversal and internationally co-ordinated action.
490. Council of Europe, Parliamentary Assembly, Recommendation 1984 (2011), The protection of privacy and personal data on the Internet and online media.
491. Council of Europe, Parliamentary Assembly, Resolution 1843 (2011), The protection of privacy and personal data on the Internet and online media.
492. Council of Europe, Parliamentary Assembly, Recommendation 1882 (2009), The promotion of Internet and online media services appropriate for minors.

In its Recommendation 1897 (2010), Respect for media freedom,[493] the Parliamentary Assembly also recalled the 2007 commitment to establishing a specific monitoring mechanism "for identifying and analysing attacks on the lives and freedom of expression of journalists" and welcomed the appointment of a rapporteur on media freedom in its Committee on Culture, Science and Education. The recommendation repeatedly calls for review of national legislation in light of European human rights commitments and identifies Council of Europe member states that have violated media-related human rights standards.

7.2.3. The Secretary General

Within the Council of Europe, two individuals have an institutional responsibility to monitor human rights developments. Overall responsibility for strategic management of the Council of Europe falls upon the Secretary General,[494] currently Thorbjørn Jagland. His office has engaged with various issues of freedom of expression online by, for example, focusing on the role of hate speech on the Internet. As the Secretary General said in a 2012 speech in Budapest, the challenge of ensuring human rights on the Internet is central to Council of Europe activities and "lies at the heart of the Council of Europe's Internet Governance Strategy". Jagland continued: "Human rights, freedom of expression, privacy rights: this is the bread and butter of our Organisation. Online and offline." In the fight against cybercrime and the support of rule of law all across Europe it must remain a priority of the Council of Europe to maximise rights and freedoms. The key challenge for ensuring freedom of expression in light of the technological revolution was, according to Jagland:

> Successfully synchronising technology and our core values involves using the tools – such as our Internet Government Strategy – at our disposal and taking into account the specific features of the internet. We must avoid unnecessary restrictions that can smother innovation and hinder the free flow of information and knowledge. We need an open, inclusive and safe environment.[495]

7.2.4. The Commissioner for Human Rights

The Council of Europe's Commissioner for Human Rights,[496] currently Nils Muižnieks, is a non-judicial institution charged with promoting human

493. Council of Europe, Parliamentary Assembly, Recommendation 1897 (2010), Respect for media freedom.
494. Council of Europe, Secretary General, www.coe.int/web/secretary-general.
495. Council of Europe, Secretary General (27 November 2012), *Tackling hate speech: living together online*, Budapest, www.coe.int/web/secretary-general/-/%E2%80%9Ctackling-hate-speech-living-together-onlin-1.
496. Commissioner for Human Rights of the Council of Europe, www.coe.int/t/commissioner/default_en.asp.

rights in Council of Europe member states and monitoring cases of human rights violations. He fulfils this role by issuing, for example, opinions critical of legislative developments in member states[497] or by defending the rights of journalists.[498] His predecessor, Thomas Hammarberg, in 2011 commissioned several studies on the future of human rights protection in the changing media landscape.[499] Two of these are of direct relevance to the protection of freedom of expression online.

The study on social media and human rights[500] emphasises that, if made enforceable, the emerging Internet governance principles could exercise a positive role on freedom of expression online as they also encompass the responsibilities of private actors. For that, the rules on intermediary liability would have to be adapted.[501] The study reiterates the key elements necessary for restrictions of freedom of expression online to be legal and legitimate (as explained in more detail in Chapter 3) and refines them for the Internet age. Restrictions need to be based on clear, specific and accessible rules. All delegations of authority to private actors need to be transparent and must cover the means and mechanisms of Internet blocking, including due process guarantees and judicial procedures to check blocking decisions. The authors conclude that "[f]reedom of expression on the Internet is a fundamental freedom of our age. Together with Internet privacy, it is vital to our freedoms to communicate and associate, and to collectively determine how our societies should be run".

The second study on public service media and human rights[502] stresses that the Internet economy and the more informal, participatory and democratic communication environment challenge the current model of public service media. Therefore, the authors suggest developing indicators for a human rights-based approach to public service media, advocating a stronger role for

497. Cf. Opinion of the Commissioner for Human Rights on Hungary's media legislation in light of Council of Europe standards on freedom of the media (25 February 2011), CommDH(2011)10.
498. Cf. Continued attacks in Europe: journalists need protection from violence (5 June 2012), http://humanrightscomment.org/2012/06/05/continued-attacks-in-europe-journalists-need-protection-from-violence.
499. Council of Europe (2011), *Human rights and a changing media landscape*, Council of Europe, Strasbourg, www.coe.int/t/commissioner/Activities/themes/MediaFreedom/MediaLandscape2011.pdf.
500. Korff D. and Brown I. (February 2012), Commissioner for Human Rights of the Council of Europe, *Social media and human rights: issue discussion paper*, CommDH (2012)8, http://wcd.coe.int/ViewDoc.jsp?id = 1904319.
501. For challenges regarding the regime of intermediary liability, cf. the cases discussed in 6.3-4.
502. Boev B. and Bukovska B. (6 December 2011), Commissioner for Human Rights of the Council of Europe, *Public service media and human rights: issue discussion paper*, CommDH 2011/41, http://wcd.coe.int/ViewDoc.jsp?id = 1881537.

human rights in public service media and encouraging regulators to supervise and enforce human rights aspects of public service media.

7.2.5. The European Court of Human Rights

The Judges in Strasbourg exercise a central role in ensuring freedom of expression on the Internet throughout the Council of Europe member states. The Court's judgments on the protection and the limits of expression on the Internet are discussed in Chapters 2, 3 and 5. The Court has a central judicial monitoring function and anyone under the jurisdiction of a Council of Europe member state who believes their rights have been violated can submit their case to the Court, respecting the usual admissibility criteria.

Due to the substantial backlog of cases before the Court, Internet-related cases have taken some time to reach the benches. But even as they have, the Court's decisions on Internet and human rights have led only to incremental rather than fundamental changes to case law, though some refinement has proved necessary. Though staying true to its principles – namely that freedom of expression is of fundamental importance in a democratic society – a study has identified four factors related to the character of the Internet that have led to adaptations of the Court's jurisprudence. These are the stronger impact of information posted on the Internet than of information published offline, the global nature of the Internet (with consequences for the accessibility of information and jurisdictional boundaries), and the durability, asychronicity and repeated accessibility of information.[503]

7.2.6. The Council of Europe's other monitoring bodies

Just as the European Court of Human Rights oversees the European Convention on Human Rights, four other monitoring bodies within the Council of Europe system have an influence on the development of human rights. They conduct, as the broad study by Renate Kicker and Markus Möstl found in 2012, "standard-setting through monitoring".[504]

The European Committee on the Prevention of Torture (CPT) oversees implementation of the European Convention for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment (ECPT). The European Social Charter (ESC) is monitored by the European Committee on Social Rights (ECSR). Monitoring the implementation of the Framework Convention for the Protection of National Minorities (FCNM) is the role of the Advisory

503. Vajic N. and Voyatzis P., "The Internet and freedom of expression: a 'brave new world' and the ECtHR's evolving case law", in *Freedom of expression: essays in honour of Nicolas Bratza*, pp. 391-408.

504. Kicker R. and Möstl M. (2012), *Standard-setting through monitoring? The role of Council of Europe expert bodies in the development of human rights*, Strasbourg: Council of Europe.

Committee under the FCNM. Finally, the European Commission against Racism and Intolerance (ECRI) oversees the fight against racism and intolerance on the basis of the European Convention on Human Rights and state commitments.

The monitoring functions of the European Committee on Social Rights, the European Commission against Racism and Intolerance and the Advisory Committee under the Framework Convention for the Protection of National Minorities (FCNM) are relevant for the development of freedom of expression online.

7.2.7. The European Committee on Social Rights

The ECSR was established by the European Social Charter,[505] which came into force in 1965. The Charter guarantees 19 fundamental social and economic rights. An Additional Protocol to the European Social Charter[506] came into force in 1992. Monitoring systems were established by the ESC and further developed by that Additional Protocol, and by the Additional Protocol to the European Social Charter providing for a system of collective complaints[507] that came into force on 1 July 1998. A Revised European Social Charter (RevESC)[508] was adopted on 3 May 1996 and came into force on 1 July 1999.[509] The RevESC takes into account new rights such as the protection against poverty and social exclusion, the right to protection against sexual harassment in the workplace and the rights of workers with family responsibilities to equal opportunities and equal treatment.

The work of the ECSR relies on a reporting procedure and a system of collective complaints. The ECSR evaluates the reports of states on their implementation of the ESC/RevESC in law and in practice and, after completing a cycle of analysis, adopts conclusions in the framework of the reporting procedure and decisions under the collective complaints procedure. Conclusions of non-compliance are then considered by a governmental committee, which comprises representatives of both states and European social partners and can recommend the Committee of Ministers to address a recommendation to the state violating an ESC/RevESC provision.

A number of economic, social and cultural rights are connected to freedom of expression on the Internet. Indeed, freedom of expression is an important enabler of economic, social and cultural rights, including the right to health, food and education. Up to now, however, freedom of expression on the Internet

505. ETS No. 35.
506. ETS No. 128.
507. ETS No. 158.
508. ETS No. 163.
509. The high number of states not having ratified the revision notwithstanding, the RevESC will replace the ESC and the Additional Protocols.

has not played a substantial role in the work of the ESCR. The Committee should devote more attention to the potential of ICTs.

7.2.8. The Framework Convention for the Protection of National Minorities (FCNM)

The FCNM came into force in 1998.[510] Pursuant to Article 24 (1) and 26 (1) FCNM, the Committee of Ministers monitors implementation of the Convention, assisted by an Advisory Committee. Being the first legally binding multilateral instrument providing for the protection of national minorities, the FCNM seeks to "protect the existence of national minorities within the respective territories of the Parties", to ensure their "full and effective equality" and to "[enable] them to preserve and develop their culture and to retain their identity". On the basis of state reports the Advisory Committee evaluates the adequacy of implementation, prepares an opinion on the measures taken by the reporting state and forwards it to the Committee of Ministers, who may then come to certain conclusions as to the adequacy of the measures taken by the state. If appropriate, the Committee of Ministers may adopt recommendations in respect of the state party concerned, which are then made public.

National minorities often suffer from discrimination because of their ethnic background, affiliation or minority status. This discrimination results in reduced levels of ICT usage, which again make it more difficult for minorities to ensure their human rights. In order to increase the presence of national minorities on the Internet, and their freedom of expression, the Advisory Committee counselled, in its Thematic Commentary No. 3 of 2012, to take into account electronic media as they play a growing role "in the circulation of information in minority languages". The Committee identified the "need for professional and financial support for the maintenance of websites and increased training of journalists working for minority language electronic media".

The "special needs and interests of minority communities" must always be taken into account when states introduce new media regulation, as "[t]echnical and technological developments in the media field, including social media, ... can also become obstacles in accessing media in minority languages". The Committee also recognised the potential of ICTs to facilitate the reception of programmes in minority languages from neighbouring countries, as encouraged by Article 17 of the Framework Convention. Still, this does not absolve states from supporting nationally produced content.[511]

510. See www.conventions.coe.int/Treaty/en/Summaries/Html/157.htm.

511. Advisory Committee of the Framework Convention on the Protection of National Minorities (5 July 2012), *Thematic Commentary No. 3, The language rights of persons belonging to national minorities under the Framework Convention*, ACFC/44DOC(2012)001 rev, www.coe.int/t/dghl/monitoring/minorities/3_FCNMdocs/PDF_CommentaryLanguage_en.pdf, at 48-49.

7.2.9. The European Commission against Racism and Intolerance (ECRI)

The ECRI was established as an expert body in the context of the Vienna Declaration on Human Rights of 1993, when Council of Europe member states undertook to combat racism, xenophobia, anti-Semitism and intolerance. It is not a convention-based body but, since the European Conference against Racism in Strasbourg of 2002, has a statutory basis.[512]

Pursuant to Article 1 of its Statute, the ECRI is entrusted with the task of combating racism, racial discrimination, xenophobia, anti-Semitism and intolerance in greater Europe from the perspective of the protection of human rights, in the light of the ECHR. Its mandate includes, *inter alia*, reviewing member states' legislation to combat the aforementioned phenomena and formulating policy recommendations. It follows a trilateral approach: country-by-country analysis, general thematic work and capacity-building programmes with partners in civil society. In addition to its reports, ECRI formulates general policy recommendations, which can be seen as general guidelines on certain aspects of its mandate, and publishes examples of good practice in member states.

In 2006 the ECRI pointed to the complexities of fighting discrimination over a variety of media, including the Internet.[513] But it has taken on the challenge. In its country reports, it takes the role of the Internet into account. In its report on Austria, for example, the Committee explicitly studied neo-Nazi behaviour online, commending the state for applying offline law to online offences and for having a multi-player private and public-sector-based monitoring system.[514] The ECRI also highlighted the importance of Internet access for advisers of asylum seekers.[515]

In its recommendations to Austria, the ECRI pointed to its General Policy Recommendation No. 6 on combating the dissemination of racist, xenophobic and anti-Semitic material via the Internet, which bears on the limits of freedom of expression online.[516] Recognising that the Internet can make a positive contribution to promoting tolerance and fighting racism, the ECRI nevertheless was concerned by the use of the Internet "for disseminating rac-

512. Council of Europe, Appendix to the Committee of Ministers Res. 2002 (8).
513. Proceedings of the 2006 ECRI Expert Seminar (July 2007), *Combating racism while respecting freedom of expression*, www.coe.int/t/dghl/monitoring/ecri/activities/22-Freedom_of_expression_Seminar_2006/NSBR2006_proceedings_en.pdf.
514. ECRI (2 March 2010), Report on Austria, Fourth Monitoring Cycle, CRI(2010)2, www.coe.int/t/dghl/monitoring/ecri/country-by-country/austria/AUT-CbC-IV-2010-002-ENG.pdf, 86-87. See also para. 132 (anti-semitism).
515. Ibid., para. 129.
516. ECRI General Policy Recommendation No. 6 (15 December 2000), *Combating the dissemination of racist, xenophobic and antisemitic materiel via the internet*, www.coe.int/t/dghl/monitoring/ecri/activities/gpr/en/recommendation_n6/Rec%206%20en.pdf.

ist, xenophobic and anti-Semitic material … aiming to incite to intolerance or racial and ethnic hatred". It recommended that states ensure that their national legislation against hate speech extended to the Internet and strengthen their international co-operation and assistance in enforcing laws against hate speech. This was premised on training of law-enforcement authorities and supporting self-regulation by Internet intermediaries, including content and access providers.[517]

7.2.10. Capacity building

Apart from adjudication and monitoring, the Council of Europe also has an important (legal) monitoring and capacity-building programme,[518] which we look at in more depth in Chapter 8. It seeks to increase the effectiveness of national human rights structures, administers training for judicial personnel and implements reforms to increase the efficiency of the justice sector. In all of these activities the challenges connected to ensuring freedom of expression on the Internet need to be taken into account. In planning and implementing capacity-building programmes Council of Europe bodies need to mainstream the protection of human rights online.

7.3. Monitoring by the OSCE and the EU

7.3.1. The OSCE

In 1997, the OSCE's Office of the Representative on Freedom of the Media[519] was established to ensure that OSCE participating states comply with commitments they made regarding freedom of the media. Observing national legislation on media freedom is also the main function of the Representative who functions as an early warning institution in cases of violations. The Representative also assists states in advocating and implementing legislation that fully complies with their commitments on media freedom. The office can further function as a rapid non-judicial response institution for cases of serious non-compliance with OSCE principles and commitment by participating states.[520]

Apart from international co-operation with other monitoring bodies, namely the UN Special Rapporteur on Freedom of Opinion and Expression, the OAS Special Rapporteur on Freedom of Expression and the ACHPR Special Rapporteur on

517. On legitimate restrictions in fighting online hate speech, see 3.2 and 5.6.
518. Council of Europe, Human rights and legal affairs capacity-building, www.coe.int/t/dghl/cooperation/capacitybuilding/default_en.asp.
519. OSCE Representative on Freedom of the Media, www.osce.org/fom.
520. Cf. OSCE, Office of the OSCE Representative on Freedom of the Media, *Mandate*, www.osce.org/fom/43207 (accessed 9 March 2013).

Freedom of Expression and Access to Information, the OSCE Representative on Freedom of the Media – currently Dunja Mijatović – is committed to applying the commitments to media freedom to the Internet. "Any attempt at Internet policy must be discussed openly", she stated at the OSCE's Internet 2013 conference, "with the broadest possible involvement, and must be examined for its implications for the free flow of information around the globe".[521]

Among the issues the Representative identified as particularly relevant for future monitoring was the "underlying fundamental principle that offline and online content are subject to the same protection under freedom of expression and freedom of the media standards".[522]

7.3.2. The EU

Within the European Union freedom of expression (and freedom of the media more broadly) is protected by Article 11 of the Charter of Fundamental Rights, which echoes the similar provision of Article 10 of the ECHR. Freedom of expression is one of the "essential foundations of the European Union".[523] Three recent initiatives of European Commission Vice-President Neelie Kroes can be seen as part of the EU's interest in monitoring freedom of expression online and in promoting the EU's digital future.

The High Level Group on Media Freedom and Pluralism, established in 2011, was charged with advising and providing recommendations on how best to respect, protect, support and promote media freedom and pluralism in Europe. In its final report, published in 2013,[524] the High Level Group argued that the link between freedom of expression and democracy justified a more extensive competency for the EU and that further harmonisation of EU legislation would be important. Regarding the Internet, the group found that effective monitoring of the changing media environment was necessary to be able to adapt the regulatory framework. The group recommended, *inter alia*, that journalist and media organisations should adapt their codes of conduct to the changing media environment. In light of the growing role of the Internet as a source of information, users have to be informed about the "application of any filtering, selecting or hierarchical ordering of the information they

521. OSCE, Office of the OSCE Representative on Freedom of the Media (14 February 2013), *OSCE media freedom representative calls for inclusive dialogue at Internet freedom conference in Vienna*, www.osce.org/fom/99582.

522. Office of the OSCE Representative on Freedom of the Media (15 February 2013), "Closing remarks", *Internet 2013: Shaping policies to advance media freedom*, Vienna, www.osce.org/fom/99727.

523. Cf. European Commission, Information society, freedom and pluralism of the media, http://ec.europa.eu/digital-agenda/en/european-journalism-study.

524. Report of the High Level Group on Media Freedom and Pluralism (January 2013), *A free and pluralistic media to sustain European democracy*, http://ec.europa.eu/information_society/media_taskforce/doc/pluralism/hlg/hlg_final_report.pdf.

receive" and should have the right "to object to the automatic application of such filtering algorithms". To that end the group also recommended that the channels through which information is conveyed to the users should be "entirely neutral" and therefore, net neutrality and the end-to-end principle "should be enshrined within EU law".[525]

The Commission has also recognised that media freedom, EU competencies and the Internet are closely related. Commissioner Kroes charged the Centre for Media Pluralism and Media Freedom (CMPF) within the Robert Schuman School of the European University Institute to report on European Union competencies in respect of media pluralism and media freedom. The report highlighted the impact of the Internet on the development of media freedom and pluralism, and advised further monitoring.[526]

Furthermore, European Commission Vice-President Neelie Kroes established in 2011 the EU Media Futures Forum, which was charged with developing and identifying trends for EU digital policy. In its June 2012 report,[527] the Forum recommended increased access to and use of legal content and services from anywhere in the EU on any device for all citizens in the EU. That they called "on industry to commit to these principles"[528] shows the interlinkages between human rights and growth in the digital economy, between the role of states and international organisations and the responsibility of the IT industry.

The European Parliament has also been very active in monitoring freedom of expression online and in monitoring violations. In 2011, for instance, the Parliament overwhelmingly adopted a resolution on the open Internet and net neutrality in Europe.[529] An example of the *de facto* monitoring function of the European Parliament is the 2012 resolution on "freedom of expression in Belarus: in particular the case of Andrzej Poczobut",[530] in which the European Parliament strongly criticised the Belarus Government for using Internet filtering and Internet controls in violation of human rights commitments. Since then, the European Parliament has called for EU-wide monitoring of media laws and measures to ensure freedom of expression and freedom of the media, which it saw endangered by state violations (through coercive measures) and

525. Ibid., at 5.
526. European University Institute RSCAS, *European Union competencies in respect of media pluralism and media freedom*, CMPF Policy Report 2013, http://cmpf.eui.eu/Projects/cmpf/Documents/CMPFPolicyReport2013.pdf.
527. EU Media Futures Forum (September 2012), *Final Report*, http://ec.europa.eu/information_society/media_taskforce/doc/pluralism/forum/report.pdf.
528. Ibid., at 7.
529. European Parliament Resolution on the open internet and net neutrality in Europe (7 November 2011), www.europarl.europa.eu/sides/getDoc.do?type = MOTION&reference = B7-2011-0572&language = EN.
530. European Parliament (3 July 2012), Motion for a resolution on Freedom of expression in Belarus: in particular the case of Andrzej Poczobut, Doc. 2012/2702(RSP), www.europarl.europa.eu/sides/getDoc.do?type = MOTION&reference = B7-2012-0403&language = EN.

violations by companies themselves through media concentration.[531] States therefore have to refrain from violating Internet-related media rights and positively provide for a legal framework that is conducive to the fulfilment of freedom of expression online.

7.4. European hotlines

Hotlines play an important role as monitors of (allegedly) illegal Internet content.[532] Most of these hotlines focus on images of sexual exploitation of children, but also accept notices of other allegedly illegal contents, like (where applicable) Holocaust denial and Nazi propaganda.[533] According to a survey of hotlines in OSCE participating states, hotlines existed in 66 % of states while 15 % of states replied negatively.[534] The biggest organisation of hotlines is INHOPE, the International Association of Internet Hotlines with 43 hotlines from 37 countries.[535]

Though they fulfil an important self-regulatory role, hotlines often lack both the transparency and the legitimacy of official bodies and, if private, are not subject to formal public controls, unlike governmental agencies, which are by law accountable to the public. Since Internet service providers usually prefer to err on the side of caution, blocking on the basis of blacklists provided by hotlines can violate freedom of expression. At the same time, however, decreased availability of commercial child abuse websites can be traced back to disruptions caused by, *inter alia*, private hotlines and international efforts, such as the European Commission's Safer Internet programme.[536]

Hotlines have recognised the importance of transparency and accountability. Among its values, INHOPE expressly mentions "freedom of the Internet" and the Articles of Association call for associations seeking membership to provide "effective transparent procedures for dealing with complaints" and to have "the support of government, industry, law enforcement, and Internet users in the countries of operation".[537]

531. European Parliament (21 February 2013), *Media freedom: MEPs call for annual EU monitoring of member states' media laws*, www.europarl.europa.eu/news/en/pressroom/content/20130218IPR05922/html/Media-freedom-MEPs-call-for-annual-EU-monitoring-of-member-states%E2%80%99-media-laws.
532. On the importance of protecting children online, see 3.1 and 5.8.
533. Cf. Stopline.at, a characteristic Internet hotline where users can directly and unbureaucratically use an online form to identify illegal content.
534. OSCE Office of the Representative on Freedom of the Media, Mijatovic D., "Freedom of expression on the Internet: a 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", *Report*, www.osce.org/fom/80723, 209.
535. INHOPE, *About INHOPE*, www.inhope.org/gns/about-us/about-inhope.aspx.
536. OSCE, "Freedom of expression on the Internet" (2010), 146.
537. INHOPE, Articles of Association (17 January 2011), Article 5 (b) and (c), www.inhope.org/Libraries/Documents_Homepage/2011_INHOPE_Articles_of_Association_EN.sflb.ashx.

In order to avoid over-reporting, hotlines need to establish clear procedures on how to deal with reported websites and how to ensure that these websites are, in fact, violating national laws that embody international commitments. Before including websites on blacklists and communicating them to law-enforcement authorities and Internet service providers, hotlines should conduct a substantive, transparent and accountable internal check.

At Stopline.at, the Austrian Internet hotline, for example, Stopline.at employees analyse whether or not the incriminated site is indeed illegal under national law. In that case, the relevant Austrian law-enforcement agency will be contacted as will the Austrian provider of the website containing the illegal material. If the material is not hosted on an Austrian site, the foreign partner hotline in the framework of INHOPE will be contacted to ensure quick removal of the website.[538]

At the UK Internet Watch Foundation (IWF), the British hotline, users can anonymously report "Child sexual abuse images hosted anywhere in the world; [n]on-photographic images of child sexual abuse hosted in the UK; [c]riminally obscene adult content hosted in the UK".[539] The IWF and the Association of Chief Police Officers (ACPO) have concluded a "Service Level Agreement"[540] that regulates the processes for managing criminal Internet content hosted in the UK. On receipt of a report to the IWF, the content is first traced and its legality assessed. If the content is traced to a UK server and the IWF assesses it as potentially criminal under UK law, the foundation will refer the content to the police services. The IWF will also issue an "evidential preservation request and Notice and Take Down (NTD) to the Service Provider" that hosts the contents, with an immediate phone call to follow up. The IWF will also advise and assist the ISP in preserving the content securely before an investigating officer takes physical control of the content. The IWF will then continue to monitor the website to ensure that content is "removed [or] disabled expeditiously in line with the requirements of the Electronic Commerce (EC Directive) Regulations 2002".[541]

Thus the assessment of content before deciding on a notice to remove or inclusion of a URL on the Internet Watch Foundation's Child Sexual Abuse Images and Content URL List (the 'black list') is, in effect, based on the judgment of an employee of the hotline and not that of an independent judge reached in a fair procedure. The inclusion of an URL on the blacklist, which is updated twice daily, amounts to a *de facto* denial of access to that website as 98.6 % of UK ISPs use the blacklist to block access to the listed

538. Stopline.at, www.stopline.at.

539. UK Internet Watch Foundation, www.iwf.org.uk/hotline.

540. Service Level Agreement between the Association of Chief Police Officers (ACPO) and the Internet Watch Foundation (IWF) (5 October 2010), www.iwf.org.uk/assets/media/hotline/SLA%20ACPO%20IWF%20FINAL%20OCT%202010.pdf.

541. Ibid., at i-vi.

URLs.[542] It is even more problematic that most users do not receive any indication that the site they tried to access has been blacklisted. Most ISPs will return the generic "404 Not Found" status code.[543]

The approach taken by the Internet Watch Foundation, and most hotlines globally, namely the blacklisting and immediate URL blocking by the ISPs, is problematic in light of fundamental procedural human rights guarantees of freedom of expression. This includes the ability to challenge decisions to filter/block content and (not) to give notice to affected users.[544]

Currently, the Internet Watch Foundation's internal Content assessment appeal process falls short of both of these human rights-based requirements. An appeal against the assessment of content as potentially illegal can be made by emailing an IWF address and citing the reasons for appealing. In theory any "party with a legitimate association … with the content or a potential victim or the victim's representative, hosting company, publisher or internet consumer who believes they are being prevented from accessing legal content may appeal against the accuracy of an assessment".[545] This sounds broad enough, but in practice most users will never realise that the content has been blocked because they are never told.

The internal review process is also opaque. When an appeal is lodged "[t]he content is re-assessed … by a suitably trained IWF manager not involved in the original assessment decision".[546] If that manager decides not to allow the appeal and the appellant wishes to continue their appeal "then the content is referred to the relevant lead police agency for assessment". This means that a non-judicial actor (the police agency) reviews the decision by a non-judicial actor (the IWF manager) regarding an appeal against a decision by a non-judicial actor (the IWF employee). From a human rights viewpoint, this approach does not amount to a fair procedure in line with Article 6 and with the procedural protections inherent to Article 10 ECHR.

Yet there is no lack in human rights-consistent approaches to filtering. In *Yildirim v. Turkey*,[547] the separate opinion of Judge Pinto sheds some light on how filtering decisions can be made in a human rights-consistent way. He espouses certain "minimum criteria" for laws on blocking Internet access. Some of his points can be taken as a guide to hotline providers to ensure

542. Wei W. (2011), *Online child sexual abuse content: the development of a comprehensive, transferable international Internet notice and takedown system*, www.iwf.org.uk/assets/media/resources/IWF%20Research%20Report_%20Development%20of%20an%20international%20internet%20notice%20and%20takedown%20system.pdf, p. 28.

543. Nunziato D. C. (2013), "Procedural protections for Internet expression", *International Review of Law, Computers, and Technology* (forthcoming).

544. Cf. ibid.

545. *Content Assessment Appeal Process*, www.iwf.org.uk/accountability/complaints/content-assessment-appeal-process.

546. Ibid.

547. *Yildirim v. Turkey* (18 December 2012), application No. 3111/10.

legitimate blocking recommendations. Judge Pinto recommends (legislators to include in their laws allowing Internet blocking) a clear definition of who can be blocked (users, hyperlink providers, hosts), what will be blocked and what the reach of the blocking measure will be (regional, national, international); a time limit on the blocking order; a review whether the interests pursued by the blocking fall under those protected in Article 10 (2) ECHR, and whether the proportionality and necessity requirements are met; a review whether competent authorities have passed the blocking order and whether such blocking order is the result of a "fair trial", that is, a procedure where all interested parties can be heard (if this is possible and does not hurt the interests sought to be protected by the blocking order); a reasoned notification of the blocking order; and a recourse procedure against such a blocking order.

As a first step, hotlines can take inspiration from these suggestions and provide, at the very least, for an open and fair internal review process, and a reasoned notification (of the website host containing the allegedly illegal content whose blocking is proposed) sent to the national executives and the host providers. Though monitoring by non-governmental organisations makes an essential contribution to safeguarding freedom of expression online, some activities of European hotlines are deeply problematic, especially the lack of respect for the procedural protections inherent in Article 10 ECHR and the private standard-setting function that is inherent in any decisions of "probable illegality" by a hotline employee, including the internal appeals system without any judicial involvement.

7.5. Civil society watchdogs

There is a growing number of civil society watchdogs that monitor online freedom of expression.[548] These include privately funded foundations, universities and non-governmental organisations. Some of these are co-ordinated by IFEX, the global network defending and promoting freedom of expression,[549] and have a long pedigree of fighting for offline freedom of expression. In this context, however, we will focus on selected NGOs that have contributed to protecting freedom of expression online and, though focusing on Europe, we will also include NGOs with a global reach.

Two of the most important NGOs monitoring freedom of expression online are Freedom House and Reporters Without Borders. *Freedom on the Net 2012*, a report by Freedom House, covers developments in 47 countries from January 2011 to May 2012.[550] It found that the transformative effect of the

548. On the standard-setting function of civil society organisations with regard to freedom of expression online, see 4.3.
549. IFEX, *Our network*, www.ifex.org/our_network.
550. Freedom House, *Freedom on the net 2012*, www.freedomhouse.org/report/freedom-net/freedom-net-2012.

Internet has led authoritarian regimes to take extreme measures to censor and obstruct online free speech. Of the 47 countries studied in 2012, 20 have experienced a decline in online freedom (with Bahrain, Pakistan and Ethiopia showing the biggest declines). Most of the declines were due to intensified censorship, arrests and violence against bloggers, threats of violence from organised crime (Mexico) or serious sentences for allegedly blasphemous speech (Pakistan). At the same time, 14 countries under review experienced a positive development. This was due either to democratic change (Tunisia, Libya, Burma) or growing diversity and diminishing censorship (Georgia, Kenya, Indonesia).[551]

The report noted that an increasing number of states were turning to proactive manipulation of web content through pro-government bloggers. But Freedom House also found that there had been an increase in citizen participation in online policy-making, especially through highly publicised campaigns against legislation such as ACTA, SOPA and PIPA.[552]

Among the key future trends identified are the emergence of new laws that restrict freedom of expression online, more stringent enforcement of existing ones, leading to more Internet users being imprisoned, the use of paid commenters and misinformation through governmentally organised online campaigns, an increase in physical attacks on bloggers and Internet activists and the increased use of surveillance technologies without clear checks on their abuse.[553]

Reporters without Borders (RWB), an NGO committed to furthering freedom of information, publishes the *Enemies of the Internet Report*. In its 2012 edition, the report[554] found (similarly to Freedom House) that authoritarian states are increasingly imposing tougher measures on online activists who wished to use the dynamics of the Arab Spring of 2011 to effect political and social change within their countries. The report criticises democratic countries for giving in to the temptation of adopting security and anti-terrorism measures that may violate human rights and by adopting "disproportionate" measures to protect copyright. The 2012 report names Bahrain, Belarus, Burma, China, Cuba, Iran, North Korea, Saudi Arabia, Syria, Turkmenistan, Uzbekistan and Vietnam as "enemies of the Internet" and has the following countries "under surveillance": Australia, Egypt, Eritrea, France, India, Kazakhstan, Malaysia, Russia, South Korea, Sri Lanka, Thailand, Tunisia, Turkey and the United Arab Emirates.

551. Kelly S. and Cook S. (24 September 2012), "Evolving tactics of Internet control and the push for greater freedom", in Kelly S., Cook S. and Truong M. (eds), *Freedom on the Net 2012: a global assessment of Internet and digital media*, Freedom House, pp. 1-18 (2).
552. Ibid., pp. 4-5.
553. Ibid., pp. 6 et seq.
554. Reporters Without Borders (2012), *Enemies of the Internet*, http://en.rsf.org/beset-by-online-surveillance-and-13-03-2012,42061.html, accessed 22 February 2013.

RWB identifies as positive the development of microblogs and opinion aggregators, and the use of mobile phones to freely disseminate information across traditional technological boundaries. Negative developments in 2011 and 2012 included the use of Internet shutdowns (e.g. Egypt, Kazakhstan, Tibet, China's Xinjiang Province) and SMS blockings (DRC, Cameroon) during actual or anticipated unrest. RWB also reports that surveillance of online activists has become more intrusive and effective: "The security services no longer interrogate and torture a prisoner for the names of his accomplices. Now they want his Facebook, Skype and Vkontakte passwords."[555]

In its 2013 report, focusing on online surveillance, RWB sees the dawn of the era of "digital mercenaries". It focuses on five "State Enemies of the Internet", countries that employ "active, intrusive surveillance of news providers, resulting in grave violations of freedom of information and human rights". The governments it names (and shames) are those of Syria, China, Iran, Bahrain and Vietnam. The report also, for the first time, names five "corporate enemies of the Internet": Gamma, Trovicor, Hacking Team, Amesys and Blue Coat, and criticises them for "sell[ing] products that are liable to be used by governments to violate human rights and freedom of information".

Reporters Without Borders called for new controls on the export of surveillance software and hardware to countries with poor human rights records. "The private sector", RWB argued, "cannot be expected to police itself. Legislators must intervene". Existing international treaties on export controls, such as the Wassenaar Agreement, could be extended to include surveillance technology, but states have not yet managed to find an enforceable compromise. RWB warned democratic countries not to "yield to the siren song of the need for surveillance and cyber-security at any cost" because of the negative effect on other countries: "If governments that traditionally respected human rights adopt this kind of repressive legislation, it will provide the leaders of authoritarian countries with arguments to use against the critics of their own legislative arsenals."[556]

Three other notable NGOs that work on monitoring freedom of expression on the Internet are Article 19, European Digital Rights and PEN International. Established in 1987, Article 19[557] is registered as a UK charity and has been active in the promotion of freedom of expression and the protection of journalists online. European Digital Rights (EDRi)[558] was founded in 2002 and unites 32 privacy and civil rights organisations based in 20 different countries in Europe. Their work focuses on privacy, data protection, copyright law reform and freedom of speech online.

555. Ibid.
556. Ibid.
557. Article 19, *History and achievements*, at www.article19.org/pages/en/history-achievements.html.
558. European Digital Rights (EDRi), www.edri.org.

Founded in 1921, PEN International has a long pedigree of fighting for the rights of poets, novelists and essayists and promoting freedom of expression. With 20,000 members in 100 countries, PEN International aims to further the "unhampered transmission of thought within each nation and between all nations".[559] In 2012, PEN International passed the *PEN Declaration on Digital Freedom*[560] which is premised upon the promise of digital media to fulfil freedom of expression. PEN reiterates the right of all persons to freedom of expression and the right to seek and receive information through digital media. Governments must refrain from prosecuting individuals who use the Internet to convey information and must actively protect freedom of expression online. Limitations should only be introduced in line with international standards. PEN also declared that everybody needs to be free from government surveillance of digital media and that the private sector, just like governments, is bound by human rights obligations of freedom of expression.

559. PEN International, *Who we are*, http://pen-international.org/who-we-are.

560. PEN International (September 2012), *PEN Declaration on Digital Freedom*, http://pen-international.org/pen-declaration-on-digital-freedom.

8. Promotion of freedom of expression online

In Chapters 4 and 7 we showed how standards are set for freedom of expression online and how the right is monitored. But this is not enough. In light of the catalytic function of the Internet for all human rights, the promotion of Internet-based speech is of fundamental importance. A broad variety of international actors, including the most influential international organisations, have made important contributions to the promotion of freedom of expression on the Internet. This chapter presents an overview of selected international promotion activities. It looks first at the role of the Council of Europe and the European Union, considers the impact of the OSCE, UNESCO and the UN Special Rapporteur on Freedom of Opinion and Expression, and concludes with examples of the promotion of freedom of expression through the initiatives of individual states.

8.1. The Council of Europe

The Council of Europe has had a leading role in promoting freedom of expression online, both in the field of standard-setting and by undertaking or participating in numerous activities explaining the relevance of freedom of expression online. With regard to standard-setting, the Council of Europe did not aim at developing new standards, but at translating the existing standards of freedom of expression to the online world. According to the existing division of labour, the European Court of Human Rights interprets Article 10 in the context of cases related to the Internet, which have already been analysed in previous chapters. While the Court plays its role in law enforcement, other bodies of the Council of Europe have been active in monitoring and promotion, by highlighting the relevance of freedom of expression to the Internet in various ways, in particular by adopting pertinent resolutions, declarations or guidelines explaining the meaning of freedom of expression in various online contexts as shown in Chapter 4 and, in light of specific issues, Chapter 5. In this way, they also contribute to preventing human rights violations in this field.

In particular, the Council of Europe has become the main international organisation active in promoting freedom of expression online in Europe and worldwide by regularly contributing to the annual Internet Governance Forum (IGF) since Athens in 2006, except for Hyderabad in 2008 when the terrorist acts in Mumbai prevented attendance. The Council of Europe is a major stakeholder in Internet Governance debates, to which it contributes

in various fields with a focus on human rights, in particular the protection of freedom of expression and information as well as personal data protection and privacy, the protection of children (while encouraging their participation in the Internet) and prevention of cybercrime.

The Council of Europe was instrumental in setting up the first European Dialogue on Internet Governance (EuroDIG) which took place in Strasbourg in 2008 and, since the 2009 EuroDIG in Geneva, Switzerland, has provided its umbrella for the yearly EuroDIG meetings, held in co-operation with a local host – the Swedish Government in Stockholm 2012 and the Portuguese Government in Lisbon 2013. These meetings are important in raising awareness and in preparing for subsequent IGF meetings. Unlike the IGF, EuroDIGs manage to produce "messages", which reflect the progress made in discussions.[561]

In addition, the Council of Europe organises particular conferences like the 2011 conference in Vienna on the Council of Europe Strategy on Internet Governance 2012-2015.[562] This strategy aims at addressing some of the problems that prevent full exercise of the rights and freedoms of Internet users, *inter alia*, by raising public awareness of rights and freedoms on the Internet and by focusing on the development of a "compendium of existing human rights for Internet users".[563]

For this purpose, a Committee of Experts on Rights of Internet Users was established, with the task of drafting such a compendium before the end of 2013.[564] The challenge is to render human rights like the freedom of expression more accessible and operational for the common user. The user should be aware of the content of the right and the available remedies in the context of the Internet. In this way, the various declarations and recommendations on the protection of freedom of expression and information on the Internet should be complemented by empowering Internet users to use their rights more fully.

One important issue in this regard is that human rights like freedom of expression need to be respected also in private contracts, for example, with Internet service providers; this may be an issue for regulation by government, self-regulation by the private sector or co-regulation.

In 2011, the Committee of Ministers of the Council of Europe adopted the Declaration on measures to promote the respect of Article 10 of ECHR.[565] In

561. Cf. EuroDIG, www.eurodig.org.
562. Council of Europe and Federal Ministry for European and International Affairs of Austria (24-25 November 2011), *Our Internet – our rights, our freedoms: towards the Council of Europe strategy on Internet governance 2012-2015*, Vienna.
563. Cf. Council of Europe, Internet Governance: Council of Europe Strategy 2012-2015, adopted by the Committee of Ministers (14 March 2012), Strasbourg 2012.
564. Committee of experts on rights of Internet users (MSI-DUI), www.coe.int/t/dghl/standardsetting/media/MSI-DUI/default_en.asp.
565. Declaration on measures to promote the respect of Article 10 of ECHR (13 January 2011).

this declaration, the Council of Europe directly focused on the promotion of freedom of expression, but it failed to mention freedom of expression online, which can be considered as a lost opportunity for highlighting the relevance of freedom of expression for the Internet.[566] However, the Committee of Ministers has addressed freedom of expression online in a number of other resolutions and declarations as explained in Chapter 4.

The Parliamentary Assembly of the Council of Europe has adopted several pertinent recommendations, already referred to in Chapter 4. In particular, in its Resolution and Recommendation on the protection of freedom of expression and freedom of information on the Internet and online media (2012),[567] the Parliamentary Assembly is concerned about the possible misuse of market power by Internet access and service providers and that such intermediaries "might unduly restrict the access to, and dissemination of, information for commercial and other reasons without informing their users and in breach of user rights". To protect freedom of expression and information on the Internet and in online media, the Assembly calls on member states to encourage intermediaries of ICT-based media to set up self-regulatory codes of conduct for the respect of the rights of their users to freedom of expression and information and to seek to ensure that intermediaries can be held accountable for violation of their user rights to freedom of expression and information, including establishing the jurisdiction of domestic courts.[568]

For the same purpose, the recommendation calls on the Committee of Ministers to strengthen the responsibility of intermediaries for the functioning of the Internet and online media by developing guidelines on domestic jurisdiction over such companies. Furthermore, a common application of Article 10 ECHR and Article 11 of the Charter of Fundamental Rights of the EU with regard to freedom of expression and information should be ensured in co-operation with pertinent EU bodies.[569]

Finally, the role of the European Commissioner for Human Rights, already referred to in Chapter 7, should also be noted in the context of promoting freedom of expression online, as can be seen from the pertinent publication he issued dealing with Internet freedoms.[570]

---

566. Kettemann M. C., "Ensuring human rights online: an appraisal of selected Council of Europe initiatives in the information society sector in 2010", in Benedek, Benoit-Rohmer, Karl and Nowak (eds), *European Yearbook on Human Rights 2011*, pp. 461ff., at 464.
567. Cf. Council of Europe, Parliamentary Assembly (25 April 2012), Resolution 1877 (2012) on the protection of freedom of expression and freedom of information on the Internet and online media; and Recommendation 1998 (2012) on the same topic.
568. Resolution 1877 (2012), ibid., paras. 9, 10 and 11.
569. Recommendation 1998 (2012) on the protection of freedom of expression and freedom of information on the Internet and online media, para. 2.
570. Cf. Hammarberg T. et al (2011), *Human rights and a changing media landscape*, Council of Europe; see also Chapter 4.

The Council of Europe has produced a wealth of promotional materials on the information society and human rights. The fact sheet on protecting freedom of expression and freedom of information in particular lists all relevant activities.[571]

8.2. The European Union

The activities of the European Union (EU) regarding freedom of expression on the Internet are related to its main competencies and responsibilities. Freedom of expression and human rights in general are primarily a political concern in the context of EU Internet governance policies. In its Communication on Internet Governance (2009), the Commission links the security and stability of the global Internet with respect for human rights, freedom of expression, privacy, data protection and cultural and linguistic diversity.[572] The European Parliament has taken a keen interest in the relationship of ICT and human rights.[573] The European Commission in 2011 announced a "No disconnect strategy" including the development and distribution of tools to Internet activists to bypass restrictions of their freedom to communicate on the Internet while avoiding indiscriminate surveillance.[574] Certainly, the fact that European companies are still allowed to sell surveillance technology to oppressive regimes raises a problem of coherence with the trade policy of the EU.[575]

Members of the European Commission and the European Parliament have participated in the annual IGF and stood up for freedom of expression even in countries like Azerbaijan, which hosted the IGF in 2012. The commissioner in charge of the digital agenda, Neelie Kroes, clearly denounced the repression of bloggers and of freedom of expression in this country in her speeches there.[576] Several members of the European Parliament spoke out at various human rights-related events at the IGF in Baku in 2012. Soon after, in December 2012, the European Parliament adopted a Digital Freedom Strategy in EU Foreign Policy, including uncensored access to the Internet. It calls for

571. Cf. The Council of Europe and the Internet, Fact Sheets, Protecting freedom of expression and freedom of information, www.coe.int/t/dghl/standardsetting/media.

572. Communication from the Commission to the European Parliament and the Council (18 June 2009), Internet Governance: the next steps, COM (2009) 277 final, para. 7.

573. See Horner L., Hawtin D. and Puddephatt A. (2010), Information and communication technologies and human rights: study for the Subcommittee on Human Rights of the European Parliament, Directorate-General for External Policies of the Union, EXPO/B/DROIT/2009/24.

574. See Press Conference of Commissioner Neelie Kroes, Using technology to support freedom, No disconnect strategy of 12 December 2011, Speech/11/873.

575. On export controls for surveillance technology and pertinent monitoring, see 6.5 and 7.5.

576. Joint statement of the EU Delegation to the 7th Internet Governance Forum (IGF) in Baku (9 November 2012), http://europa.eu/rapid/press-release_MEMO-12-852_en.htm. Blog of Neelie Kroes, http://blogs.ec.europa.eu/neelie-kroes/malala-day-power-Internet/ of 12 November 2012.

"recognition by the EU of digital freedoms as fundamental rights and as indispensable prerequisites for enjoying universal human rights such as privacy, freedom of expression, freedom of assembly and access to information".[577]

The rapporteur of the European Parliament Committee on Foreign Affairs, Marietje Schaake, resorted to the Internet itself by employing the methodology of crowd-sourcing to collect views from NGOs, business, governments and Internet users in general on the topic of her report.[578] The European Parliament also commissioned a study on human rights and the Internet in European foreign policy after the Arab Spring,[579] which has opened the eyes of the European Union to the relevance of the Internet and its users for democratisation.

The Commission in 2010 adopted a Digital Agenda for Europe as one of seven European flagship projects for the Europe 2020 strategy; its main purpose is to strengthen the European economy by maximising the social and economic potential of ICT, but it also includes the promotion of digital literacy and inclusion of still absent potential users among disadvantaged groups like the elderly or disabled, who in this way could be empowered in their freedom of expression and information.[580]

In order to protect users of online networks and services better, the European Commission published, in 2012, a Code of EU Online Rights, compiling rights and principles enshrined in EU law to protect citizens when they access and use online networks and services. Of basic importance is the "universal service principle", according to which everyone in the EU must have access to a minimum of electronic services at an affordable price. Fundamental rights and freedoms need to be respected. Regulatory authorities have to uphold the principle of Internet neutrality. Incitement to hatred is forbidden. Privacy and data protection are dealt with in some detail, whereas freedom of expression is only promoted indirectly.[581]

8.3. The Organization for Security and Co-operation in Europe (OSCE)

The Organization for Security and Co-operation in Europe with its 57 members (in 2013) covers a significantly larger membership than the Council of Europe, reaching farther to the east, but also west to include the United

577. European Parliament, Resolution on a digital freedom strategy in EU foreign policy (11 December 2012), 2012/2094 (INI).
578. Cf. Schaake M. (15 November 2012), Report, EP-doc. P7_TA (2012)0470.
579. Cf. Wagner B. (2012), *After the Arab spring: new paths for human rights and the Internet in European foreign policy*, European Parliament, Sub-Committee on Human Rights, EXPO/B/DROIT/2011/28.
580. Communication on a Digital Agenda for Europe (19 May 2010), COM 2010 245 final.
581. European Commission (2012), *Code of EU online rights*, European Union.

States and Canada. In some of its member states major problems in freedom of expression online still persist. In 1997, the OSCE created a specific institution for the promotion of freedom of expression in the form of the Special Representative for the Freedom of the Media (RFoM), based in Vienna.[582] This institution has the mandate "to observe relevant media developments" in all OSCE states and "to promote full compliance with OSCE principles and commitments regarding freedom of expression and free media".[583] It has an early warning function and addresses serious problems impeding the activities of the media and journalists, which can involve rapid responses in cases of serious non-compliance. As an autonomous institution within the OSCE, the RFoM assesses situations that threaten the freedom of the media, it addresses questions, recommendations or warnings to OSCE participating states and regularly goes public to denounce non-compliance with a state's commitments and its own recommendations.[584]

For example, the OSCE RFoM, Dunja Mijatović, has publicly expressed her concern about the arrest of social media activists in Belarus and welcomed the release of journalists in Azerbaijan.[585] In its activities, the RFoM co-operates with other institutions inside OSCE, like the Office for Democratic Institutions and Human Rights (ODIHR), and outside, like the Council of Europe or the United Nations. Given the fact that the Council of Europe does not have a special mandate-bearer who is fully devoted to promoting freedom of expression online, the role of this OSCE mandate is also important for the Council of Europe area.

Since about 2003, the OSCE Representative on Freedom of the Media has become increasingly involved in matters of freedom of expression online.[586] For this purpose, the Representative has issued several pertinent publications and participated in declarations on freedom of the media on the Internet.[587] Of particular relevance is the study on *Freedom of Expression on the Internet*, commissioned by the Representative on Freedom of the Media and published in 2011. It contains an overview of the legal provisions and practices of OSCE participating states on freedom of expression, free flow of information and

582. This function is presently assumed by Dunja Mijatović from Bosnia-Herzegovina.

583. Permanent Council (5 November 1997), Decision No. 193, www.osce.org/pc/40131.

584. Mujic Ž., "The OSCE Representative on Freedom of the Media – an inter-governmental watchdog: an oxymoron?", in Benedek, Benoît-Rohmer, Karl and Nowak (eds), *European yearbook on human rights 2010*, pp. 309-319, at 312. See also Chapter 6 on monitoring activities of the RFoM.

585. Cf. Press Release (4 September 2012), www.osce.org/FOM/93345, and Press Release (18 December 2012), www.osce.org/FoM/98422 (both accessed 9 March 2013).

586. Möller C. (2008), "The future of media freedom on the Internet", in *OSCE, the Representative on Freedom of the Media, ten years for media freedom, an OSCE anniversary, current and forthcoming challenges*, Vienna, pp. 139-48.

587. See OSCE Representative on Freedom of the Media (2003), *Spreading the word on the Internet,* www.osce.org/fom/13871 based on the OSCE's *Media Freedom Internet Freedom Cookbook* (2004), www.osce.org/fom/13836.

media pluralism on the Internet, mainly collected with the help of a survey. For this purpose, it focuses on Internet access, Internet content regulation, blocking, content removal and filtering, as well as licensing and liability. The results are alarming, as they show an increasing trend towards governmental control of the Internet.[588]

With regard to standards for freedom of expression online, the OSCE Representative on Freedom of the Media bases itself on established human rights, but also contributes to the interpretation of freedom of expression on the Internet. In the Amsterdam Recommendations of 14 June 2003 on Freedom of the Media and the Internet, access to the Internet and freedom of expression online were of top importance. The principle that any means of censorship unacceptable for the classical media must not be used for online media already appears there.[589] Together with Reporters Without Borders, the RFoM in 2005 issued a declaration on guaranteeing media freedom on the Internet.[590] It is also worth mentioning that the Permanent Council of the OSCE in 2004 adopted a decision on the promotion of tolerance and media freedom on the Internet,[591] while the OSCE Ministerial Council in Brussels in 2006 adopted a decision on countering the use of the Internet for terrorist purposes.[592]

The OSCE Parliamentary Assembly has also contributed to the clarification of standards: at its session in Belgrade in 2011 as part of a wider declaration, it adopted a Resolution on freedom of movement of information and knowledge, which underlines the fundamental importance of freedom of expression and the enormous potential of the Internet as a tool for realising this right. It "stresses the need for free access to information, especially through an Internet network easily accessible to all population groups" and invites the OSCE to enable the Representative on Freedom of the Media and the Office for Democratic Institutions and Human Rights (ODIHR) to be more active in the field of promoting free movement of information and knowledge and its free access.[593]

The Representative on the Freedom of the Media also participates in the annual joint statements of the four international special mechanisms for promoting freedom of expression, in particular the Joint Declaration on Freedom

588. Akdeniz Y. (2012), *Freedom of expression on the Internet*, Office of the OSCE Representative on Freedom of the Media; see also at www.osce.org/fom/80723.
589. See OSCE Representative on Freedom of the Media (2003), *Spreading the word on the Internet,* www.osce.org/fom/13871, p. 211 et seq., at 213.
590. See Representative on Freedom of the Media, Guaranteeing media freedom on the Internet, www.rsf.org/IMG/pdf/declaration_anglais.pdf.
591. OSCE, Permanent Council (2004), Decision No. 633, Promoting tolerance and media freedom on the Internet.
592. Cf. Ministerial Council of Brussels (2006), Decision No. 13/06 on countering the use of the Internet for terrorist purposes.
593. Cf. OSCE, 20th Parliamentary Assembly in Belgrade, Belgrade Declaration (10 July 2011), www.oscepa.org/meetings/annual-sessions.

of Expression and the Internet of July 2011.[594] Thus, the voice of the RFoM in Internet government debates is important in highlighting the relevance of human rights, in particular freedom of expression, in Internet governance. Working closely with governments, media and civil society, the RFoM also supports the multi-stakeholder approach as it is practised in the annual Internet Governance Forum.[595]

Besides participating in numerous pertinent conferences and workshops to promote freedom of expression, including the IGFs and EuroDIGs, the Representative on Freedom of the Media also organises major conferences for that purpose. The first such conference was held in Amsterdam in 2003 on freedom of the media and the Internet; another major conference, in 2013 in Vienna, was devoted to "Internet 2013 – shaping policies to advance media freedom". Whereas the earlier one can be considered as exploratory in nature, the later one aimed to identify operational approaches in dealing with problems of media freedom on the Internet. In this context, issues of filtering and blocking were discussed, as was media freedom in social media. At this occasion, the 2013 Social Media Guidebook was presented, and this contains a set of Guidelines for social media compiled by the RFoM.[596] One focus was on self-regulation of online media, the topic of a new OSCE Guidebook, also presented there.[597] An important awareness-raising function can be expected from conferences organised by the Representative on the Freedom of the Media on Internet issues in the Caucasus and Central Asia, which also produced pertinent declarations, dealing with different aspects of freedom of expression.[598]

Particular attention is devoted by the Representative on the Freedom of the Media to the safety of journalists. For this purpose specific recommendations have been adopted[599] and a guidebook on the safety of journalists has been issued.[600]

---

594. See International mechanisms for promoting freedom of expression, Joint Declaration on Freedom of Expression and the Internet, at www.osce.org/fom/78309.
595. Cf. Moeller C., "Internet governance in the OSCE region: media freedom, human security and the multi-stakeholder approach", in Benedek, Bauer and Kettemann (eds) (2008), *Internet governance and the information society, global perspectives and European dimensions*, Eleven, pp. 95-106. See also Moeller C. and Amouroux A. (eds) (2007), *Governing the Internet: freedom and regulation in the OSCE region*, OSCE, Representative for the Freedom of the Media, Vienna.
596. OSCE, The Representative on Freedom of the Media (2013), *Social media guidebook, Vienna.*
597. OSCE, The Representative on Freedom of the Media (2013), *The online media self-regulation guidebook,* Vienna.
598. Cf., e.g. OSCE, The Representative on Freedom of the Media (2010), *Access to information and new technologies,* Tbilisi, Georgia 11-12 November 2010, Vienna. OSCE, The Representative on Freedom of the Media (2012), *Pluralism and Internet governance,* Dushanbe, Tajikistan, 29-30 November 2011, Vienna.
599. In particular, *Vilnius recommendations on the safety of journalists* (June 2011), www.osce.org/cio/78522.
600. Cf. OSCE, The Representative on the Freedom of the Media (2012), *Safety of journalists: guidebook*, Vienna. See also 2.1.3.

8.4. The United Nations Educational, Scientific and Cultural Organization (UNESCO)

Among United Nations bodies, UNESCO was the first to recognise the relevance of freedom of expression online. Together with the International Telecommunication Union (ITU), UNESCO had a major role in the World Summit on the Information Society (WSIS) and, due to this involvement, increasingly promoted major human rights concerns like freedom of expression, privacy and diversity. For example, the work of UNESCO on the free flow of ideas by word and image and on multilingualism on the Internet was crucial for the right to freedom of expression and information for all those people without access to Internet content in their own language. Accordingly, the General Conference of UNESCO in 2003 adopted a recommendation on the promotion and use of multilingualism and universal access to cyberspace.[601]

UNESCO also uses the annual IGFs to promote freedom of expression online, for example by inviting bloggers to share their experiences. In its regional activities, it organises pertinent events worldwide, either within regional IGFs or separately. For example, the UNESCO Conference on Freedom of Expression and the Internet in Marrakesh, Morocco, in February 2013 promoted an enabling environment for freedom of expression in Arab countries.[602]

UNESCO is also the publisher of several important reports and publications on freedom of expression online, such as the report on *Freedom of connection, freedom of expression: the changing legal and regulatory ecology shaping the Internet*, which found empirical evidence for the increased use of Internet filtering based on legal and regulatory trends constraining freedom of expression online.[603] Another pertinent report is the *Global survey on Internet privacy and freedom of expression*, published for the IGF 2012.[604] This publication focuses on developments in privacy on the Internet and the intersection between privacy and freedom of expression. Protection of privacy can create the trust necessary for freedom of expression, but it can also limit freedom of expression and information. In such cases, the public interest test is proposed for the necessary

601. Cf. UNESCO (15 October 2003), *General Conference Recommendation Concerning the Promotion and Use of Multi-Lingualism and Universal Access to Cyberspace.*
602. Freedom of Expression on the Internet: UNESCO conference, Marrakesh, www.unesco.org/new/en/media-services/single-view/news/freedom_of_expression_on_the_Internet_unesco_conference_in_marrakech.
603. Cf. Dutton W. H., Depatka A., Law G. and Nash V. (2011), *Freedom of connection, freedom of expression: the changing legal and regulatory ecology shaping the Internet,* UNESCO.
604. Mendl T., Puddephatt A., Wagner B., Hawkin D. and Torres N. (2012), *Global survey on Internet privacy and freedom of expression,* UNESCO.

balancing with reference to *Mosley v. UK*.[605] All in all, UNESCO pursues concerns in the field of freedom of expression similar to those of the Council of Europe and the Representative on Freedom of the Media, but globally.

8.5. The UN Special Rapporteur on Freedom of Opinion and Expression

The United Nations human rights bodies have been surprisingly absent in the area of freedom of expression online. Although WSIS and the follow-up IGFs were organised in the framework of the United Nations, and the Office of the High Commissioner for Human Rights was involved in the pertinent workshop on human rights and the information society in 2003,[606] neither the office nor the UN Human Rights Bodies took part in the IGF meetings, though human rights issues constantly gained in importance there.[607] Nonetheless, in their first Joint Declaration of 2005, the year of the WSIS in Tunis, the (then three) rapporteurs on Freedom of Expression of the UN, the OAS and OSCE did have a focus on Internet governance and human rights[608] and in his report of 2006, the former Special Rapporteur on Freedom of Opinion and Expression, for the first time, included a substantive section on Internet governance and human rights in his annual report.[609]

Not until the fourth IGF at Sharm El Sheikh in 2009 did the UN Special Rapporteur on Freedom of Opinion and Expression, now Frank La Rue, participate for the first time. He immediately realised the potential of the event for his mandate and in 2011 focused his annual report to the Human Rights Council on the topic of freedom of opinion and expression and the Internet.[610] This report had been prepared after a number of regional meetings worldwide with the support of the Swedish Government.[611] It got a positive welcome from

605. *Mosley v. the United Kingdom* (10 May 2011), application No. 48009/08.
606. Cf. Chapter 4, note 169.
607. Benedek W., "Internet governance and human rights", in Benedek, Bauer and Kettemann (eds), *Internet governance and the information society, global perspectives and European dimensions*, pp. 31-50, at 41 et seq.
608. Joint Declaration (21 December 2005), www.OSCE.org/FoM/27455.
609. Ligabo A. (27 March 2006), *Report of the Special Rapporteur on the Promotion and Protection of Freedom of Opinion and Expression*, UN Doc. E/CN.4/2006/55.
610. The Special Rapporteur actually submitted two reports, the first of a more general nature and the second with a focus on access and content-related issues: La Rue F. (16 May 2011), *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, UN Doc. A/HRC/17/27 (an earlier version is of 24 April 2011). La Rue F. (10 August 2011), UN Doc. A/66/290.
611. See the comprehensive background report: Horner L., *Freedom of expression and the Internet: report from regional consultation meetings convened by Demos, Global Partner and Associates*, www.mediapolicy.org/Demos-FoE-Internet.

civil society, which saw it as confirming some of its major concerns.[612] Since then the Special Rapporteur has had a crucial role in promoting freedom of expression online by appearing in various conferences and meetings.

In 2011 the four International Mechanisms for Promoting Freedom of Expression – the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media, the OAS Special Rapporteur on Freedom of Expression and the ACHPR Special Rapporteur on Freedom of Expression and Access to Information – issued a joint declaration of key principles for freedom of expression online.[613] These include the principle that freedom of expression online should be protected just as freedom of expression online and that restrictions should only be allowed under international law's well-established three-part test. Further, the four experts posited that any restriction on freedom of expression on the Internet must always be proportionate in light of both the positive potential of the Internet and the rights of others. The regulatory environment of the Internet demands a unique approach and existing approaches to technology orientation cannot just be transferred online. In tailoring approaches to the needs of the Internet, self-regulation can be an effective tool. Overall, however, awareness raising and educational efforts are essential and Internet literacy needs to be fostered.

The Human Rights Council adopted its first crucial Resolution on promoting, protecting and enjoyment of human rights on the Internet in July 2012.[614] However, the Office of the High Commissioner on Human Rights still has no structure for follow-up on this important issue for human rights, apart from the Special Rapporteur on the right to freedom of opinion and expression.

8.6. Initiatives by individual states

Besides the promotional activities of international organisations and bodies, individual states have taken important initiatives that can be considered as examples of good practice.

We must highlight the support of Sweden for the work of the Special Rapporteur on the right to freedom of opinion and expression when drafting his fundamental reports of 2011. Sweden also supports other international activities like the Conference on Freedom of Expression of UNESCO in

612. APC, *Internet rights are human rights*, written statement prepared by Association for Progressive Communications (APC), a non-governmental organisation in general consultation status to the Human Rights Council, www.apc.org/en/node/12371.

613. International Mechanisms for Promoting Freedom of Expression (1 June 2011), *Joint Declaration on Freedom of Expression and the Internet*, www.osce.org/fom/78309.

614. Human Rights Council (5 July 2012), *The Promotion, Protection and Enjoyment of Human Rights on the Internet*, UN Doc. A/HRC/20/8.

Marrakesh in 2013 and, since 2012, it has organised a yearly international Internet Forum in Stockholm bringing together stakeholders from around the world, in particular also from the South.[615]

The Netherlands, in 2011, initiated an international coalition of countries who stand up for freedom of expression on the Internet. The first conference of this Freedom Online Coalition took place in The Hague; subsequent conferences were hosted by Kenya in 2012 and Tunisia in 2013. The Netherlands also announced it would spend €6 million on freedom of expression on the Internet, with initiatives to support bloggers or cyber activists operating under repression.[616] In this way they contribute to a "digital defenders partnership". The Freedom Online Coalition by 2013 counted 18 members from around the world, including the United States.[617]

Austria was the main sponsor of a resolution of the UN Human Rights Council on the safety of journalists, adopted in 2012. It hosted a preparatory meeting in Vienna, supported a UNESCO study on specific threats to women journalists and successfully lobbied for the resolution, which finally found 67 sponsors and was adopted by consensus.[618]

615. Internet Freedom for Global Development, www.stockholminternetforum.se.
616. See Government of Netherlands, Coalition of countries for free internet, www.government.nl/news/2011/12/14/coalition-of-countries-for-free-internet.html.
617. See U.S. Department of State, Fact Sheet: Freedom Online Coalition, www.humanrights.gov/2012/11/20/fact-sheet-freedom-online-coalition.
618. Human Rights Council (27 September 2012), *Resolution on the Safety of Journalists*; see also International Press Institute, *UN Human Rights Council passes resolution in favour of journalists safety, Austria pushed for protection of media workers*, www.freemedia.at/home/singleview/article/un-human-rights-council-passes-resolution-in-favor-of-journalist-safety.html.

9. Conclusions

The Tunis Commitment of 2005 clearly commits states to a "people-centred, inclusive and development-oriented Information Society" that is "premised on the purposes and principles of the Charter of the United Nations, international law and multilateralism" and respects fully and upholds the Universal Declaration of Human Rights. States confirm the "universality, indivisibility, interdependence and interrelation of all human rights and fundamental freedoms, including the right to development, as enshrined in the Vienna Declaration".[619]

The Internet has become "the public space of the 21st century – the world's town square, classroom, marketplace, coffeehouse, and nightclub".[620] As a room where opinions are shaped and articulated, the Internet therefore needs to be protected. This protection for communicator and recipient and for the content of the communication is provided by human rights law, Article 19 of the UDHR and the ICCPR and, in the Council of Europe area, Article 10 ECHR.

As this book has shown, the explosion of human activity online has resulted in a regulatory backlash, with a number of states seeing Internet freedom as something to fear and online expression as a destabilising force. This book has set out to analyse how freedom of expression is protected online by human rights law, in state practice and through the case law of, especially, the European Court of Human Rights. It is the aim of this book to shed light on the manifold challenges to freedom of expression on the Internet.

9.1. Freedom of expression as the key right of the Internet age

The analysis of the content of freedom of expression online in Chapter 2 has shown that, while the principle of "what applies offline also applies online" is largely followed by the European Court of Human Rights, by applying its rich practice also to cases involving the Internet, it also takes the specificities of the new media into account. Although only a limited number of judgments exist, they do allow conclusions on the key principles and lines of action of

619. World Summit on the Information Society (18 November 2005), Tunis Commitment, WSIS-05/TUNIS/DOC/7-E, paras. 2 and 3.

620. Secretary of State Clinton H. R. (15 February 2011), *Internet rights and wrong: choices and challenges in a networked world*, George Washington University, Washington DC, www.state.gov/secretary/rm/2011/02/156619.htm.

the Court. The Court is well aware of the opportunities and threats that the Internet brings to freedom of expression *(Editorial Board)*. Although the case law on freedom of expression on the Internet is still limited, the Court has recognised the importance of the Internet for freedom of information *(Times Newspapers)* and its amplifying effect *(Mouvement Raëlien)* and it demands from states both a legal framework ensuring the effective prosecution of crimes on the Internet (*K.U.*) and a framework for how the media can use information obtained from the Internet *(Editorial Board)*.

In *Yildirim*, the Court clarified the right to freedom of expression, indicating that it also covers the means of diffusion and the right of the public to receive the information, i.e. the right to information. It further affirmed an obligation of states to assure the accessibility of the Internet in this case. Journalistic freedom and better protection of journalists, including "citizen journalists" using the Internet, has been found to be a priority concern of a broad range of international actors and has been addressed by several new initiatives.

While freedom of expression online also includes scientific and artistic expression, conflicts can occur that are difficult to solve. These can be conflicts with other rights like freedom of religion on a global level, as exemplified by the debate about Islamic reactions on presenting the Prophet Mohammed in the media. Within freedom of cultural expression, multilingualism on the Internet as a crucial element of cultural diversity was found to be a major challenge.

Freedom of expression on the Internet is not a new freedom, but an extension of an existing human right to the new media. Accordingly, the rights of anonymity and whistle-blowing are extended to the Internet. This is also true for related rights like freedom of assembly and association and the right to education as related to the Internet. Conflicts, which have emerged between intellectual property rights and the right of access to knowledge, can only be resolved by a careful balancing of those rights. Other rights like the right to property may also play a role in the context of freedom of expression online, for example when the licence of an Internet Service Provider is withdrawn by the authorities in a decision that does not meet the proportionality requirement *(Megadat.com)* or when a monopolistic service provider invokes the right to property to exclude users from its services.

Chapter 3 showed that freedom of expression online can be restricted for the same reasons as freedom of expression offline. However, the problem of different standards in different jurisdictions becomes even more relevant in the context of the Internet. The magnifying effect of the Internet is a new challenge to respect for private life *(K.U.)* and to the protection of minors in general *(Pérrin, Ovchinnikov)* or the immigrant community *(Féret)*. It is also disputed whether the character of the Internet deserves a wider or narrower margin of appreciation *(Mouvement Raëlien)*, which in practice will depend on the context of the case. The same applies to cases of privacy where the information has already appeared on the Internet (*Editions Plon*). When making

use of their freedom of the press and the media, journalists and media have a special responsibility when publishing information on the Internet *(Stoll, Fatullayev, Times Newspapers)*. The same holds true for politicians *(Féret)*.

So far, the challenges have only partly been addressed by the Court, while other responsible bodies like the Committee of Ministers of the Council of Europe have gone further and systematically addressed the new challenges. Accordingly, the Court has taken guidance from the declarations, resolutions or guidelines of the Council of Europe and other regional institutions like the OSCE or the legal acts of the European Union *(Editorial Board*, *Yildirim)*. Guidance can also be derived from the universal level, for example, from the reports of the UN Special Rapporteur on Freedom of Opinion and Expression or the UN Human Rights Council, which are also noted by the Court *(Editorial Board)*. Chapter 4 provides an overview of these "soft law" texts, some of which the Court has repeatedly taken into account.

9.2. Setting standards for free speech online: the impact of the Council of Europe

In Chapter 4 on standard-setting by the Council of Europe and non-state actors, we showed that the Council of Europe plays a leading role in standard-setting by way of its declarations, recommendations and guidelines. They inform not only the jurisprudence of the Court, but also other institutions and legal actors worldwide. In the ten years following its declaration of freedom of communication on the Internet of 2003, Council of Europe bodies successfully responded to the major challenges posed by the Internet, in particular by guidance like the Recommendation on measures to promote the public service value of the Internet of 2007 and the Recommendation on the new notion of media in 2011.

The Council of Europe also successfully engaged in co-regulation by involving private actors (in business) in the drafting of human rights guidelines for certain business sectors. The recommendations on human rights protection with regard to search engines and social networking services again urge member states to regulate the relevant actors in conformity with human rights. The user perspective is given particular attention in the Internet Governance Strategy 2012-2015, which envisages the drafting of a Compendium of User Rights by a Committee of Experts. In all this work, the protection of freedom of expression under the conditions of the Internet is the main concern, next to privacy and data protection.

The Council of Europe has committed itself to a multi-stakeholder approach, working also with NGOs. In this context, some pertinent activities of non-state actors – like the Charter of Human Rights and Principles for the Internet, issued by the Internet Rights and Principles Coalition – have led to closer

co-operation. The work of the Global Network Initiative is an example of good practice coming mainly from private stakeholders. Finally, we note the role of transparency in state requests to businesses to take down websites or provide information on their owners because these may have a chilling effect on freedom of expression online.

9.3. Protecting Internet-based freedom of expression: a daily challenge

The challenges of regulating Internet content in a human rights-consistent way are substantial. Indeed, libertarian states would argue that Internet content regulation as such is already a violation of freedom of expression. A human rights-oriented point of view, however, leads instead to the conclusion that states are under an obligation to respect, protect and ensure human rights online, just as they do offline. This means that states need to adopt the necessary laws (or adapt their legalisation in judicial practice) that enable them to safeguard freedom of expression online. We analysed the practical implications of this, and selected practical issues that states are faced with, in Chapter 5.

These issues include the important precondition to exercising freedom of expression online (and, as free speech is an enabling right, also a variety of other human rights): the right of access to the Internet. Internet access in both its dimensions, infrastructure and content, is a human right. Another key issue is technological neutrality. This means that Internet service providers are not allowed to treat transmitted data packets differently because of the content contained therein. States need to provide for legislation ensuring network neutrality, as one of the key foundational principles of the Internet.

Fighting online hate speech is particularly difficult in light of the characteristics of freedom of expression online, including the self-moderated nature of free speech, the possibility of self-publishing and universal access to opinions. States with divergent historical experiences or religious and cultural values are faced with striking the right balance between the right of individuals to voice opinions that "offend, shock or disturb", as the European Court of Human Rights ruled in 1976 in *Handyside*, and the rights of others not to be subjected to messages of hate.

Children are in special need of protection from online dangers. The Court's jurisprudence makes clear that states need to protect children as part of their right to private life and therefore interfere legitimately with the right to freedom of expression, as confirmed in *Perrin.* Children are especially vulnerable in social networks, and Internet companies therefore have an important regulatory function.

Limiting the *ex ante* content-moderation obligations of Internet intermediaries is essential for keeping the flow of ideas on the Internet open. Navigating

between state laws and their own content-moderation rules is often difficult for international Internet intermediaries, and especially social networking sites, who are faced with conflicting demands and threats by states to disallow access altogether if they do not remove impugned information.

Social networks have emerged as central spaces for Internet users to congregate, aggregate opinions and articulate them. Freedom of expression can be endangered in social networks by terms of service indifferent to human rights, especially when these are opaque and provide no accountability and human rights-based safeguards around processes of exclusion of users or censorship of content. A further major issue is the lack of privacy-friendly default settings and a lack of transparency about the purposes and duration of data collection and processing. Social networks urgently need to re-establish the primacy of human rights within their systems, especially as they grow in importance and become quasi-public spheres. While there is no gold standard of mixing self-regulation and state regulation, a higher level of human rights sensibility on the part of social networking services and higher levels of willingness to commit to, and implement, standards of corporate social responsibility, are essential. Publishing transparency reports showing requests for user data by states and suppression of content (or refusal thereof) on behalf of states would be a good step. Google and Twitter are already publishing such reports, and Microsoft has been asked to follow suit.

The importance of social networks as the new public spaces cannot be overestimated. In social networks, private citizens progressively "speak truth to power". Such networks (and also search engines and other hosting companies) therefore have an important role to further the communicative potential of civil society, whistle-blowers and human rights defenders.

9.4. The corrective function of the European Court of Human Rights

In the absence of a universal human rights court that adjudicates on the legality of interferences with freedom of expression, we have to rely on national and regional bodies to fulfil this role. In the cases we examined in Chapter 6, three key themes emerge: national courts are the first ports of call for questions of freedom of expression online as they are most closely connected to realities on the ground. At the same time pursuing a freedom-of-expression case in front of a court may not always be the best solution. What is most certainly problematic is when a company sued in one country decides to try its luck in another country with the result of two different judgments (as in one phase of the French/US *Yahoo!* cases). Often it will be up to Internet companies to shape their policies in a way that is both respectful of human rights and in keeping with host state laws. This is a difficult endeavour. What

is considered a legitimate interference with freedom of expression in one state (e.g. Holocaust denial) may not be criminalised in another state. Yet few Internet companies will be faced with protests when they prohibit speech that may be legal in certain countries but violates clear international freedom of speech commitments and international best practice.

The cases are also evidence of the corrective function of appeals courts in reviewing lower court judgments that have misapplied human rights protection guarantees in freedom-of-expression contexts. Both the British *Twitter* and the Italian *Google* cases were corrected on appeal. This does not mean that lower courts should be free to decide what they want but rather that we can expect fewer lower court decisions to go awry now that appeals courts are taking on more and more freedom-of-expression online cases.

We also find that the European Court of Human Rights plays a very important role in protecting human rights in Europe by laying down fundamental principles and reviewing difficult cases. Together with the monitoring and promotion activities of other Council of Europe expert bodies, the Strasbourg system has emerged as a key player making positive contributions to the evolution of Internet freedom of expression.

9.5. Judges outside the courtroom: monitoring freedom of expression

Monitoring, as shown in Chapter 7, can be a very effective and efficient tool for ensuring the protection of freedom of expression on the Internet. It is less cumbersome, quicker and cheaper than judicial proceedings and can lead states and companies to change their law and practices through international naming-and-shaming campaigns. At the same time we have seen that even co-ordinated efforts by European organisations and international NGOs are not enough to stop violations of freedom of expression by authoritarian regimes.

Within the Council of Europe system, the organisation's key bodies and the monitoring bodies under human rights treaties have exercised monitoring functions regarding the Internet and freedom of expression. Just as with the European Court of Human Rights, the Internet has forced other monitoring bodies not so much to apply new principles but rather to gradually refine their analysis and case law, their statements and reports in light of the challenges of information and communication technologies.

Parallel to international organisations and states, private hotlines perform an important monitoring function online, but their legitimacy is based on a system of controls equal to that of a state agency. Though reductions in the availability of commercial child abuse websites can be traced back to disruptions in their 'business' caused, *inter alia*, by private hotlines, these hotlines

still need to meet essential accountability criteria. Currently, the takedown of a website is based on the judgment of a hotline employee and their recommendation to an Internet service provider or host, who will usually not wait for an independent judge to determine whether the content is, in fact, illegal. This *de facto* private standard-setting is an important part of any decision of "probable illegality" by a hotline employee, but it is problematic from a human rights perspective. Hotlines must provide for an open and fair process of internal review and send a reasoned notification to the host of the website that contains the allegedly illegal content that it proposes should be blocked by the national executives and host providers, thereby respecting the procedural protections inherent in Article 10 ECHR. Just as states need to respect certain minimum criteria in drafting any law enabling blocking or online censorship, so private entities like hotlines need to do so as well.

A key monitoring function is also exercised by civil society watchdogs. International NGOs like Freedom House and Reporters Without Borders are essential because of the worldwide reach of their networks and the global nature of their reports. Their monitoring allows them to identify trends in freedom of expression online like the backlash against netizens, increased use of ICTs to combat free expression and the increased export of surveillance technology by private companies headquartered in democratic states, which is then used by autocratic regimes to spy on their citizens. This raises questions of corporate social responsibility and due diligence for the companies involved. The (mostly European) home states of the companies have to face questions – as does the EU – about the seriousness of their commitment to human rights, especially to freedom of expression.

9.6. Taking things one step further: promoting freedom of expression

Having looked at the various monitoring mechanisms for freedom of expression, Chapter 8 provides insights into the promotional work of the main regional and global organisations in support of freedom of expression. Again, the Council of Europe is in the lead, and this is reflected in its role in the annual Internet Governance Forum and EuroDIG. Next to the Committee of Ministers, the work of the Parliamentary Assembly should be noted in this context. EU bodies also have increased their promotional activities, with regard to both foreign policy and the consumer's perspective.

Only the OSCE Representative on Freedom of the Media has a special mandate to monitor and promote freedom of expression. The Representative's office is active in OSCE participating states and closely co-operates with the Council of Europe. On a global level, UNESCO and the UN Special Rapporteur on the right to freedom of opinion and expression contribute to

raising awareness and clarifying a universal standard of freedom of expression online. Finally, the initiatives of states like Sweden, the Netherlands and Austria provide examples of good practice in the promotion of freedom of expression.

Finally, the main challenges to freedom of expression in the future can be seen in the conceptual differences supported by different jurisdictions, but also in technical developments, which provide new opportunities for freedom of expression but also for censorship. Furthermore, the responsibilities of private actors like Internet companies and the rights of the users would both merit further clarification. The challenge is how to identify the public interest and then have it respected and promoted by private actors, regionally and globally. In conclusion, the main responsibility for protecting freedom of expression on the Internet lies with states, but in a multi-stakeholder approach all other actors – international bodies, the private sector and civil society – are also called upon to make their contribution.

9.7. Freedom of expression on the Internet: a catalyst and an enabler of human rights

In the quest to build a people-centred, inclusive and development-orientated information society – respecting fully and upholding the Universal Declaration of Human Rights, as well as the universality, indivisibility, interdependence and interrelation of all human rights and fundamental freedoms – in this quest, freedom of expression plays a fundamental role. Just as the Internet is a catalyst for exercising human rights, so freedom of expression is an enabler of civil and political, economic, social and cultural rights.

In his 1996 *Declaration of the independence of cyberspace*, John P. Barlow declared the "global social space … to be naturally independent of the tyrannies you [states] seek to impose on us".[621] With regard to freedom of expression for the Council of Europe region, however, we have strong international commitments to Article 10 of the European Convention on Human Rights, Article 19 of the Universal Declaration of Human Rights and Article 19 of the International Covenant on Civil and Political Rights. The practice of states and the case law (of the courts and the UN's quasi-judicial bodies, taken together) enable a clear case to be made for only very few, clearly circumscribed exceptions to freedom of expression. Any such exception must meet the three-part test of legality, necessity in the pursuit of legitimate purposes and proportionality. Coupling this with the UN Human Rights Council

621. Barlow J. P. (8 February 1996), *A Declaration of the Independence of Cyberspace*, Davos, www.projects.eff.org/ ~ barlow/Declaration-Final.html.

Resolution 20/8, which provides that all human rights that apply offline also apply online, the technical neutrality of the cited human rights provisions and the numerous commitments by all stakeholders to the special role of the Internet as an enabler for human rights and freedom of expression, and as a catalyst for other human rights, we can come to the conclusion that freedom of expression online enjoys strong protection.

When Barlow discounted states' "moral right to rule us [inhabitants of cyberspace]", he was wrong. A moral right to rule does exist (and even a duty to rule), but only insofar as states aim to safeguard human dignity, human security and human rights.

A story going around in Internet circles illustrates this impressively. At one international conference, an African delegate was asked whether freedom of expression on the Internet was really that important to his country of origin or whether, rather, it was not more essential to ensure, say, the right to food. His answer should be kept in mind whenever freedom of expression online is at stake. "Without the Internet", he said, "I can't tell the world who is stealing my bread".

Executive summary

The development of a people-centred, inclusive and development-orientated information society is premised upon strong protection of freedom of expression on the Internet based on the fact that freedom is a catalyst for other human rights online and an essential human right by itself.

Freedom of expression online, including the freedom to author, pass on, seek and receive information and to be active in social networks, is protected by human rights law, in particular Article 19 of both the UDHR and the ICCPR and, for the Council of Europe area, Article 10 of the ECHR. Conventional and citizen journalists using the Internet need special protection, but also have to observe professional and ethical standards.

In protecting freedom of expression online the basic rule must be: what is permissible offline is permissible online. However, the specificities of the Internet – like its amplifying effect, the ubiquity of the information posted and the impossibility of deleting information once on the Net – need to be taken into account. Restrictions of freedom of expression online are only allowed when they are in keeping with the rules for interference under the ECHR. For that, the three-part test of legality, necessity in the pursuit of a legitimate goal and proportionality has to be applied in the light of the online context.

In addition to the protection of the ECHR, as developed by the Court, the Council of Europe has systematically set important standards for the content and interpretation of freedom of expression online. Its recommendations sometimes include co-regulatory approaches that turn private Internet companies into normative partners of Strasbourg. Other important contributions to the standards applicable to regulating freedom of expression online have been made by non-governmental organisations that focus on Internet policy-making and human rights, such as the Internet Rights and Principles Coalition.

In implementing freedom of expression on the Internet at state level, three themes emerge: national courts are the first ports of call for questions of freedom of expression online as they are most closely connected to realities on the ground; appeal courts have an important corrective function in reviewing lower court judgments that have misapplied human rights protection guarantees in freedom-of-expression contexts; and the European Court of Human Rights plays a key role in protecting human rights in Europe by laying down fundamental principles and reviewing controversial cases.

Monitoring can be as effective a tool for protecting freedom of expression on the Internet as adjudication. Quicker and cheaper and often more effective than judicial proceedings, it has a good track record of influencing states

and Internet companies, but it is not enough to stop violations of freedom of expression by "outliers", especially authoritarian regimes. Some private monitoring bodies are also problematic because they assume a quasi-judicial role in censoring Internet content by the inclusion of websites in blacklists.

Promoting freedom of expression on the Internet is a task actively undertaken by the Council of Europe, other intergovernmental or non-governmental organisations and states. The Council of Europe's policy reaches out to the user and the Internet community at large, which is reflected in its role in the annual Internet Governance Forum and the European Dialogue on Internet Governance (EuroDIG).

All states, and all stakeholders, have an obligation to respect, protect and implement freedom of expression online. In so doing they have to resist any development of new barriers and respect the existing rules, which are also applicable to freedom of expression on the Internet.

Bibliography

Books

Cuceranu Dragos (2012), *Aspects of regulating freedom of expression on the Internet*, Intersentia.

Dutton William H., Depatka Anna, Law Ginette and Nash Victoria (2011), *Freedom of connection, freedom of expression: the changing legal and regulatory ecology shaping the Internet*, UNESCO.

Fisher Desmond and Harms L. S. (eds) (1983), *The right to communicate: a new human right*, Boole Press.

Grabenwarter Christoph and Pabel Katharina (2012), *Europäische Menschenrechtskonvention*, 5th edn, C. H. Beck.

Hammarberg Thomas et al. (2011), *Human rights and a changing media landscape*, Council of Europe.

Harms L. S., Richstad Jim and Kie Kathleen (eds) (1977), *The right to communicate: collected papers*, University of Hawaii Press.

Harris David, O'Boyle Michael and Warbrick Michael (2009), *Law of the European Convention on Human Rights*, Oxford University Press.

Herz Michael and Molnar Peter (eds) (2012), *The content and context of hate speech: rethinking regulation and responses*, Cambridge University Press.

Jørgensen Rikke F. (2013), *Framing the Net. The Internet and Human Rights*, Edward Elgar.

Jørgensen Rikke F. (ed.) (2006), *Human rights in the global information society*, MIT Press.

Karpenstein Ulrich and Mayer Franz C. (2012), *EMRK-Kommentar*, C. H. Beck.

Kettemann Matthias C. (2013), *The future of individuals in international law: lessons from international Internet law*, Eleven International.

Kicker Renate and Möstl Markus (2012), *Standard-setting through monitoring? The role of Council of Europe expert bodies in the development of human rights*, Council of Europe.

Krikorian Gaëlle and Kapczynski Amy (eds) (2010), *Access to knowledge in the age of intellectual property*, MIT Press.

Kulecza Joanna (2012), *International Internet law*, Routledge.

Mares Radu (ed.) (2012), *The UN Guiding Principles on Business and Human Rights: foundation and implementation*, Martinus Nijhoff.

Mendl Toby, Puddephatt Andrew, Wagner Ben, Hawtin Dixie and Torres Natalia (eds) (2012), *Global survey on Internet privacy and freedom of expression*, UNESCO.

Milo Dario (2008), *Defamation and freedom of speech*, Oxford University Press.

Moeller Christian and Amouroux Arnaud (eds) (2007), *Governing the Internet: freedom and regulation in the OSCE region*, OSCE Publishing.

Sakulin Wolfgang (2011), *Trademark protection and freedom of expression*, Wolters Kluwer.

Sunstein Cass R. (2009), *Going to extremes: how like minds unite and divide*, OUP.

Verpeaux Michel (2010), *Freedom of expression*, Council of Europe.

Virgil, *Aeneid*, transl. by A. S. Kline (2002).

Articles

Benedek Wolfgang (2012), "Menschenrechte in der Informationsgesellschaft" in: Schüller-Zwierlein André and Zillien Nicole (eds), *Informationsgerechtigkeit*, De Gruyter, pp. 69-88.

Benedek Wolfgang (2012), "Right to education" in: Benedek Wolfgang (ed.), *Manual on human rights education*, 3rd edn, NWV, pp. 251-301.

Benedek Wolfgang (2008), "Internet governance and human rights" in: Benedek Wolfgang, Bauer Veronika and Kettemann Matthias C. (eds), *Internet governance and the information society: global perspectives and European dimensions*, Eleven International, pp. 31-49.

Benedek Wolfgang and Kettemann Matthias C. (2010), "The Council of Europe and the information society" in: Kicker Renate (ed.), *The Council of Europe, pioneer and guarantor for human rights and democracy*, Council of Europe, pp. 109-115.

Cromie John D. and Jacobus James (2000), "Court stakes a middle ground on free speech in shopping malls", *2000 New Jersey Law Journal*, www.connell-foley. com/content/page/court-stakes-middle-ground-free-speech-shopping-malls.

De Hert Paul and Kloza Dariusz (2012), "Internet (access) as a new fundamental right. Inflating the current rights framework?", *European Journal of Law and Technology*, 3 (2012) 3, http://ejlt.org/article/view/123/268.

Dunstan Allison Hope (2011), *Protecting human rights in the digital age: understanding evolving freedom of expression and privacy risks in the ICT industry*, https://globalnetworkinitiative.org/sites/default/files/files/BSR_ICT_Human_Rights_Report.pdf.

Greenberg Marc H., "A return to Lilliput: the *Licra v. Yahoo!* case and the regulation of online content in the world market", *1192 Berkeley Technology Law Journal*, 18 (2004-05), pp. 1191-1258, www.btlj.org/data/articles/18_04_05.pdf.

Hertig Randall M. (2006), "Commercial speech under the European Convention on Human Rights: subordinate or equal?", *Human Rights Law Review*, 6 (1), pp. 53-86.

Karanasiou Argyro P. (2012), "Respecting context: a new deal for free speech in the digital era", *European Journal of Law and Technology* (3), No. 3, http://ejlt.org/article/ view/144/266.

Kelly Sanja and Cook Sarah (2012), "Evolving tactics of Internet control and the push for greater freedom", Kelly S., Cook S., Truong M. (eds), *Freedom on the net 2012: a global assessment of Internet and digital media,* Freedom House, pp. 1-18.

Kettemann Matthias C. (29 February 2012), "The power of principles: reassessing the Internet Governance principle hype", *Jusletter IT*, http://jusletter-eu.weblaw.ch.

Kettemann Matthias C. (2012), "Das Internet als internationales Schutzgut: Entwicklungsperspektiven des Internetvölkerrechts anlässlich des Arabischen Frühlings" [The Internet as a global object of protection: perspectives on international Internet law in light of the Arab Spring], *Heidelberg Journal of International Law* 72, pp. 469-482.

Kettemann Matthias C. (2012), "The UN Human Rights Council Resolution on Human Rights on the Internet: boost or bust for online human rights protection", *Human Security Perspectives*, pp. 145-169.

Kettemann Matthias C. (2011), "Ensuring human rights online: an appraisal of selected Council of Europe initiatives in the information society sector in 2010" in: Benedek, Benoit-Rohmer, Karl and Nowak (eds), *European yearbook on human rights*, NWV, pp. 461-482.

Kleinwächter Wolfgang (2011), *Internet principle hype: how soft law is used to regulate the Internet, .nxt, internet policy and governance dissected*, www.news.dot-nxt.com/2011/07/27/internet-principle-hype-anon.

Moeller Christian (2008), "The future of media freedom on the Internet" in: OSCE*, Ten years for media freedom, an OSCE anniversary, current and forthcoming challenges*, OSCE, pp. 139-148.

Moeller Christian (2008), "Internet governance in the OSCE region: media freedom, human security and the multi-stakeholder approach" in: Benedek,

Bauer and Kettemann (eds), *Internet governance and the information society: global perspectives and European dimensions*, Eleven International, pp. 95-106.

Mujic Ženet (2010), "The OSCE Representative on Freedom of the Media – an inter-governmental watchdog: an oxymoron?" in: Benedek, Benoît-Rohmer, Karl and Nowak (eds), *European yearbook on human rights*, NWV, pp. 309-319.

Nunziato Dawn C. (2013), "Procedural protections for Internet expression", *International Review of Law, Computers, and Technology*, pp. 1-22, www.osce.org/fom/99458.

O'Flaherty, Michael (2012), "Freedom of expression: Article 19 of the International Covenant on Civil and Political Rights and the Human Rights Committee's General Comment No. 34", *Human Rights Law Review* 12 (2012) 4, pp. 627-654.

Partsch Karl-Josef (1981), "Freedom of conscience and expression, and political freedoms", in Louis Henkin (ed.), *The International Bill of Rights – The Covenant on Civil and Political Rights*, New York: Columbia University Press, pp. 209-245.

Sartor Giovanni and Viola de Azevedo Cunha Mario (2010), "The Italian Google-case: privacy, freedom of speech and responsibility of providers for user-generated contents", *International Journal of Law and Information Technology* 18(4), pp. 356-378.

Schmalenbach Kirsten (2007), "Ein Menschenrecht auf Kommunikation: Erfordernis oder Redundanz?" in: Benedek Wolfgang and Pekari Catrin (eds), *Menschenrechte in der Informationsgesellschaft*, Boorberg, pp. 183-213.

Smet Stijn (2011), "Freedom of expression and the right to reputation: human rights in conflict", *American University International Law Review* 26 (2011) 1, pp. 183-236.

Vajic Nina and Panayotis Voyatzis (2012), "The Internet and freedom of expression: a 'brave new world' and the European Court of Human Rights' evolving case law" in: *Freedom of expression: essays in honour of Nicolas Bratza*, Council of Europe, pp. 391-420.

White Aidan (2013), "Who should follow journalism ethical standards in the digital era?" in: OSCE, *The Representative on the Freedom of the Media: the online media self-regulation guidebook*, pp. 63-69.

Wu Tim (2003), "Network neutrality, broadband discrimination", *Journal of Telecommunications and High Technology Law* 2, pp. 141-179.

Yoo Christopher S. (2005), "Beyond network neutrality", *Harvard Journal of Law and Technology* 19, pp. 1-77.

Reports and documents[622]

Council of Europe

1st Council of Europe Conference of Ministers responsible for Media and New Communication Services, Resolution on Internet Governance and critical Internet resources, Doc. MCM (2009) 011 of 29 May 2009.

Additional Protocol to the Cybercrime Convention concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189) of 28 January 2003.

Advisory Committee of the Framework Convention on the Protection of National Minorities, Thematic Commentary No. 3, The Language Rights of Persons Belonging to National Minorities Under the Framework Convention, ACFC/44DOC(2012)001 rev, 5 July 2012, www.coe.int/t/dghl/monitoring/minorities/3_FCNMdocs/PDF_CommentaryLanguage_en.pdf, 48-49.

Commissioner for Human Rights of the Council of Europe, Public Service Media and Human Rights, Issue Discussion Paper (Boev Boyko and Bukovska Barbora), CommDH (2011)41, 6 December 2011, https://wcd.coe.int/ViewDoc.jsp?id = 1881537.

Commissioner for Human Rights of the Council of Europe, Social Media and Human Rights. Issue Discussion Paper (Korff Douwe and Brown Ian), CommDH (2012)8, February 2012, https://wcd.coe.int/ViewDoc.jsp?id = 1904319.

Commissioner for Human Rights of the Council of Europe, Opinion on Hungary's media legislation in light of Council of Europe standards on freedom of the media, CommDH (2011)10, 25 February 2011.

Committee of experts on rights of Internet users (MSI-DUI), www.coe.int/t/dghl/standardsetting/media/default_en.asp.

Committee of Ministers (4 July 2012), Declaration on the desirability of international standards dealing with forum shopping in respect of defamation, "libel tourism", to ensure freedom of expression.

Committee of Ministers, Recommendation CM/Rec(2012)4 on the protection of human rights with regard to social networking services, http://wcd.coe.int/com.instranet.InstraServlet?Index = no&command = com.instranet.CmdBlobGet&InstranetImage = 2068708&SecMode = 1&DocId = 1878492&Usage = 2.

Committee of Ministers (4 April 2012), Recommendation CM/Rec(2012)3 on the protection of human rights with regard to search engines.

622. All websites were last accessed on 1 May 2013.

Committee of Ministers (4 April 2012), Recommendation CM/Rec(2012)4 on the protection of human rights with regard to social networking services.

Committee of Ministers (7 December 2011), Declaration on the protection of freedom of expression and freedom of assembly and association with regard to privately operated Internet platforms and online service providers, https://wcd.coe.int/ViewDoc.jsp?id = 1883671& Site = CM.

Committee of Ministers (21 September 2011), Recommendation CM/Rec(2011)8 on the protection and promotion of the universality, integrity and openness of the Internet.

Committee of Ministers (21 September 2011), Recommendation CM/Rec(2011)7 on a new notion of media.

Committee of Ministers (21 September 2011), Declaration on Internet governance principles, https://wcd.coe.int/ViewDoc.jsp?id = 1835773.

Committee of Ministers (21 September 2011), Declaration on the protection of freedom of expression and information and freedom of assembly and association with regard to Internet domain names and name strings, https://wcd.coe.int/ViewDoc.jsp?id = 1835805&Site = CM.

Committee of Ministers (13 January 2011), Declaration on measures to promote the respect of Article 10 of ECHR.

Committee of Ministers (29 September 2010), Declaration of the Committee of Ministers on network neutrality, https://wcd.coe.int/ViewDoc.jsp?id = 1678287.

Committee of Ministers (28 and 29 May 2009), Resolution on developments in anti-terrorist legislation in Council of Europe member states and their impact on freedom of expression and information, MCM (2009) 11.

Committee of Ministers (26 March 2008), Recommendation CM/Rec(2008)6 on measures to promote the respect for freedom of expression and information with regard to Internet filters.

Committee of Ministers (20 February 2008), Declaration on protecting the dignity, security and privacy of children on the Internet.

Committee of Ministers (7 November 2007), Recommendation CM/Rec(2007)16 on measures to promote the public service value of the Internet.

Committee of Ministers (26 September 2007), Recommendation CM/Rec(2007)11 on promoting freedom of expression and information in the new information and communication environment.

Committee of Ministers (13 May 2005), Declaration of the Committee of Ministers on human rights and the rule of law in the Information Society, CM(2005) 56 final.

Committee of Ministers (2 March 2005), Declaration on freedom of expression and information in the media in the context of the fight against terrorism.

Committee of Ministers (28 May 2003), Declaration on freedom of communication on the Internet.

Committee of Ministers (30 October 1997), Recommendation No. R 97 (20) on "hate speech".

Committee of Ministers (4 March 2012), Council of Europe Strategy 2012-2015 on Internet Governance.

Council of Europe and Federal Ministry for European and International Affairs of Austria (24-25 November 2011), *Our Internet – our rights, our freedoms: towards the Council of Europe strategy on Internet governance*, 2012-2015, Vienna.

Council of Europe in co-operation with the Interactive Software Federation of Europe, Human rights guidelines for online game providers, Doc. H/Inf (2008).

Council of Europe in co-operation with the European Internet Service Providers Association (Euro. ISPA), human rights guidelines for Internet Service Providers, Doc. H/Inf (2008) 9.

Council of Europe and the Internet, Fact sheets: protecting freedom of expression and freedom of information, www.coe.int/t/dghl/standardsetting/media.

ECRI Report on Austria, Fourth Monitoring Cycle (2 March 2010), CRI(2010)2, www.coe.int/t/dghl/monitoring/ecri/country-by-country/austria/AUT-CbC-IV-2010-002-ENG.pdf.

ECRI, Proceedings of the 2006 ECRI Expert Seminar: Combating racism while respecting freedom of expression, www.coe.int/t/dghl/monitoring/ecri/activities/22-Freedom_of_expression_Seminar_2006/NSBR2006_proceedings_en.pdf.

ECRI (15 December 2000), General Policy Recommendation No. 6: Combating the dissemination of racist, xenophobic and anti-Semitic material via the Internet, www.coe.int/t/dghl/monitoring/ecri/activities/gpr/en/recommendation_n6/Rec%206%20en.pdf.

European Court of Human Rights (June 2012), Press Unit, Factsheet: hate speech, www.echr.coe.int/NR/rdonlyres/D5D909DE-CDAB-4392-A8A0-867A77699169/0/FICHES_Discours_de_haine_EN.pdf.

European Court of Human Rights (2011), Research Division, Internet: Case law of the European Court of Human Rights, Council of Europe.

Parliamentary Assembly, Assembly procedure, http://assembly.coe.int/Main.asp?Link=/AboutUs/APCE_Procedure.htm.

Parliamentary Assembly, Resolution 1877 (2012) on the protection of freedom of expression and freedom of information on the Internet and online media.

Parliamentary Assembly, Resolution 1843 (2011) The protection of privacy and personal data on the Internet and online media.

Parliamentary Assembly, Resolution 1834 (2011), Combating "child abuse images" through committed, transversal and internationally co-ordinated action.

Parliamentary Assembly (25 April 2012), Recommendation 1998 (2012), The protection of freedom of expression and information on the Internet and online media.

Parliamentary Assembly, Recommendation 1984 (2011), The protection of privacy and personal data on the Internet and online media.

Parliamentary Assembly, Recommendation 1980 (2011), Combating "child abuse images" through committed, transversal and internationally co-ordinated action.

Parliamentary Assembly, Recommendation 1897 (2010), Respect for media freedom.

Parliamentary Assembly, Resolution 1729 (2010), Protection of "whistle-blowers", http://assembly.coe.int/main.asp?link = /documents/adoptedtext/ta10/eres1729.htm.

Parliamentary Assembly, Recommendation 1882 (2009), The promotion of Internet and online media services appropriate for minors.

Parliamentary Assembly Recommendation 1814 (2007), Towards decriminalisation of defamation.

Parliamentary Assembly, Recommendation 1805 (2007) on blasphemy, religious insults and hate speech against persons on grounds of their religion.

Secretary General (27 November 2012), *Tackling hate speech: living together online*, Budapest, www.coe.int/web/secretary-general/-/%E2%80%9Ctackling-hate-speech-living-together-onlin-1.

European Union

Communication on a Digital Agenda for Europe, COM 2010 245 final of 19 May 2010.

Communication from the Commission to the European Parliament and the Council (18 June 2009), Internet Governance: the next steps, COM (2009) 277 final.

European Commission (30 November 2010), Antitrust: Commission probes allegations of antitrust violations by Google, Press Release, IP/10/1624.

European Commission (2012), Code of EU Online Rights.

European Commission (5 December 2012), "Commission agrees way forward for modernising copyright in the digital economy", *Press Release*, http://europa.eu/rapid/press-release_MEMO-12-950_en.htm.

European Commission (13 February 2012), *Transparency of ACTA negotiations*, http://trade.ec.europa.eu/doclib/docs/2012/february/tradoc_149103.pdf.

European Commission, *Information society: freedom and pluralism of the media*, http://ec.europa.eu/information_society/media_taskforce/pluralism/index_en.htm.

European Commissioner responsible for the Digital Agenda (12 December 2011), Vice-President Neelie Kroes, Press Conference, Using technology to support freedom: no disconnect strategy, Speech/11/873.

European Union competencies in respect of media pluralism and media freedom (2013), *CMPF Policy Report* 2013, http://cmpf.eui.eu/Projects/cmpf/Documents/CMPFPolicyReport2013.pdf.

EU Media Futures Forum (September 2012), *Final report*, http://ec.europa.eu/information_society/media_taskforce/doc/pluralism/forum/report.pdf.

European Parliament, *Media freedom: MEPs call for annual EU monitoring of member states' media laws*, www.europarl.europa.eu/news/en/pressroom/content/20130218IPR05922/html/Media-freedom-MEPs-call-for-annual-EU-monitoring-of-member-states%E2%80%99-media-laws.

European Parliament (26 March 2009), Recommendation A6-0103/2009 to the Council on strengthening security and fundamental freedoms on the Internet, www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A6-2009-0103&language=EN.

European Parliament (11 December 2012), Resolution on a digital freedom strategy in EU foreign policy, 2012/2094(INI), www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2012-470.

European Parliament (7 November 2011) Resolution on the open internet and net neutrality in Europe, www.europarl.europa.eu/sides/getDoc.do?type=MOTION&reference=B7-2011-0572&language=EN.

European Parliament (3 July 2012), Resolution on freedom of expression in Belarus: in particular the case of Andrzej Poczobut, 2012/2702(RSP), www.europarl.europa.eu/sides/getDoc.do?type=MOTION&reference=B7-2012-0403&language=EN.

Joint statement of the EU Delegation to the 7th Internet Governance Forum (IGF) in Baku (9 November 2012), http://europa.eu/rapid/press-release_MEMO-12-852_en.htm.

Blog of Neelie Kroes (12 November 2012), http://blogs.ec.europa.eu/neelie-kroes/malala-day-power-Internet.

High Level Group on Media Freedom and Pluralism, Report, "A free and pluralistic media to sustain European democracy", http://ec.europa.eu/information_society/media_taskforce/doc/pluralism/hlg/hlg_final_report.pdf.

OSCE

20th Parliamentary Assembly in Belgrade (10 July 2011), Belgrade Declaration, www.oscepa.org/meetings/annual-sessions.

Freedom of Expression on the Internet. A 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, 2011, www.osce.org/fom/80723.

Office of the OSCE Representative on Freedom of the Media (15 February 2013), "Closing remarks", Internet 2013: Shaping policies to advance media freedom, Vienna, www.osce.org/fom/99727.

Office of the OSCE Representative on Freedom of the Media, OSCE media freedom representative calls for inclusive dialogue, Internet freedom conference in Vienna, www.osce.org/fom/99582.

Office of the OSCE Representative on Freedom of the Media, Mandate, www.osce.org/fom/43207.

Permanent Council (2004), Decision No. 633, Promoting tolerance and media freedom on the Internet.

Permanent Council (5 November 1997), Decision No. 193, www.osce.org/pc/ 40131.

Press Releases of 4 September 2012 and of 18 December 2012, www.osce.org/FOM/93345 and www.osce.org/FoM/98422.

The Representative on Freedom of the Media, www.osce.org/fom.

The Representative on Freedom of the Media (2013), The online media self-regulation guidebook, Vienna.

The Representative on Freedom of the Media (2012), Safety of journalists guidebook, Vienna.

The Representative on Freedom of the Media (2012), Pluralism and Internet Governance, Dushanbe, Tajikistan, 29-30 November 2011, Vienna.

The Representative on Freedom of the Media (8 June 2011), Vilnius recommendations on safety of journalists, OSCE-doc. C10. GAL/111/11, www.osce.org/cio/78522.

The Representative on Freedom of the Media (2010), Access to information and new technologies, Tbilisi, Georgia, 11-12 November 2010, Vienna.

The Representative on Freedom of the Media (2004), Internet freedom cookbook, www.osce.org/fom/13836.

The Representative on Freedom of the Media (2003), Spreading the word on the Internet, www.osce.org/fom/13871.

United Nations

Human Rights Council (5 July 2012), Resolution A/HRC/20/8 on the promotion, protection and enjoyment of human rights on the Internet. For an analysis, see Cf. Kettemann M. C. (1/2012), "The UN Human Rights Council Resolution on Human Rights on the Internet: boost or bust for online human rights protection", *Human Security Perspectives*, pp. 145-169.

Human Rights Council (27 September 2012), Resolution on the safety of journalists, application No. 21/12, A/HRC/21/L.6.

Human Rights Council (July 2012), The promotion, protection and enjoyment of human rights on the Internet, UN Doc. A/HRC/20/8.

Human Rights Council (16 June 2011), "Guiding principles on business and human rights: implementing the United Nations 'Protect, respect and remedy' framework", *Annex to the Final Report of the Special Representative to the Human Rights Council*, UNGA-Doc. A/HRC/17/31 and adopted by the Human Rights Council by Resolution 17/4.

Human Rights Council (7 April 2008), Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, John Ruggie, "Protect, respect and remedy: a framework for business and human rights", *Report*, UNGA-Doc. A/HRC/8/5.

Human Rights Committee (12 September 2011), General Comment No. 34 on Article 19: Freedom of opinion and expression of 21 July 2011, UN Doc. CCPR/C/GC/34.

Human Rights Committee (2004), General Comment No. 31: Nature of the general legal obligation imposed on states parties to the Covenant, UN Doc. CCPR/C/21/Rev.1/Add.13.

Human Rights Committee (29 June 1983), General Comment No. 10: Freedom of expression.

ITU-T (November 2012), Recommendation Y.2770 on Requirements for deep packet inspection in next generation networks, www.itu.int/rec/T-REC-Y.2770-201211-P.

OHCHR, *Between free speech and hate speech: the Rabat Plan of Action*, a practical tool to combat incitement to hatred, www.ohchr.org/EN/NewsEvents/Pages/TheRabatPlanofAction.aspx.

OHCHR, Rabat Plan of Action on the prohibition of advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence. Conclusions and recommendations emanating from the four regional expert workshops organised in 2011, and adopted by experts in Rabat, Morocco (5 October 2012), www.ohchr.org/Documents/Issues/Opinion/SeminarRabat/Rabat_draft_outcome.pdf.

UN GA (10 August 2011), Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/66/290.

UNESCO (2012), The International Programme for the Development of Communication.

UNESCO (2005), Convention on the Protection and Promotion of the Diversity of Cultural Expressions, Articles 1 and 4.

UNESCO (15 October 2003), General Conference Recommendation concerning the promotion and use of multi-lingualism and universal access to cyberspace.

UNESCO (11 November 1997), Recommendation concerning the Status of Higher Education Teaching Personnel.

Other sources

Ad hoc Advisory Group on cross-border Internet was established in 2009 and completed its mandate after four meetings in 2011; www.coe.int/t/dghl/standardsetting/media/MC-S-CI/default_en.asp.

Association for Progressive Communications (APC), www.apc.org/en/pubs/briefs/wikleaks-human-rights-whistleblowers-under-attack.

Association for Progressive Communications (APC), A non-governmental organisation in general consultation status to the Human Rights Council, *Internet rights are human rights,* www.apc.org/en/node/12371.

Article 19, History and achievements, www.article19.org/pages/en/history-achievements.html.

Article 19, Intellectual property, www.article_19.org/pages/en/intellectual-property.html.

Article 19, *Balancing the right to freedom of expression and intellectual property protection in the digital age*, Policy brief.

Article 19 (2012), *Prohibiting incitement to discrimination, hostility or violence*, Policy Brief, www.article19.org/data/files/medialibrary/3572/12-12-01-PO-incitement-WEB.pdf.

Article 19, *United Kingdom: Ruling on Google's liability is bad news for free speech online*, www.article19.org/resources.php/resource/3611/en/united-kingdom:-ruling-on-google%E2%80%99s-liability-is-bad-news-for-free-speech-online#sthash.u4O9LisK.dpuf.

Barlow John Perry, *A declaration of the independence of cyberspace*, http://w2.eff.org/Censorship/Internet_censorship_bills/barlow_0296.declaration.

Benedek Wolfgang and Madanmohan Rao (2013), *Background paper*, 12th Informal ASEM Seminar on Human Rights, "Human Rights and Information and Communication Technology" in Seoul 27-29 June 2012, ASEM, Singapore.

Benedek Wolfgang, Gragl Paul, Kettemann Matthias C., Liddicoat Joy and van Eijk Nico (October 2012), "Comments relating to freedom of expression and freedom of association with regard to new generic top level domains", *DG-I*, 2012/4.

Center for Democracy and Technology (28 November 2012), *Adoption of traffic sniffing standard fans WCIT flames*, https://www.cdt.org/blogs/cdt/2811adoption-traffic-sniffing-standard-fans-wcit-flames.

Charter on Human Rights and Principles for the Internet, http://internetrightsandprinciples.org/wpcharter.

Commentary to the Charter on Human Rights and Principles for the Internet (October 2011), www.law-democracy.org/wp-content/uploads/2011/10/Charter-Commentary.pdf.

Commissioner for Human Rights of the Council of Europe, www.coe.int/t/commissioner/default_en.asp.

Cowie James (28 January 2011), *Egypt leaves the Internet*, www.renesys.com/blog/2011/01/egypt-leaves-the-internet.shtml.

De la Chapelle Bertrand and Fehlinger Paul (2012), "Internet and jurisdiction, a global multi-stakeholder dialogue process", *Annual Report*, www.Internetjurisdiction.net/wp-content/uploads/2013/01/Internet-Jurisdiction-Annual-Report-2012.pdf.

EDRI, *Copyright: challenges of the digital era*, www.edri.org/ files/paper07_copyright.pdf.

EDRI (19 December, 2012), "Export controls for digital weapons", *EDri-gram newsletter*, www.edri.org/edrigram/number10.24/export-controls-digital-weapons.

EDRI (27 February 2013), *UK court: Google liable for comments posted on its blogger platform*, www.edri.org/edrigram/number11.4/google-liable-comment-blogger-uk.

Facebook, Community Standards, www.facebook.com/communitystandards.

Facebook, Principles, www.facebook.com/principles.php.

Facebook (11 December 2012), Statement of rights and responsibilities, www.facebook.com/legal/terms.

Freedom House, *Freedom on the Net 2012*, www.freedomhouse.org/report/freedom-net/freedom-net-2012.

Global Network Initiative (2010), "Our Work. Our vision. Our progress", *Inaugural Report*, www.globalnetworkinitiative.org/files_Annual_Report_2010.pdf.

Global Network Initiative, *Protecting and advancing freedom of expression and privacy in information and communications*, www.globalnetworkinitiative.org.

Global Network Initiative (1 August 2012), *Ensure the free flow of information in Tajikistan*, www.globalnetworkinitiative.org/news/ensure-free-flow-information-tajikistan.

Google, Transparency Report, www.google.com/transparencyreport/removals.

Google (Richard Salgado), "Transparency report: what it takes for governments to access personal information", *Google public policy blog*, http://googlepublicpolicy.blogspot.co.at/2013/01/transparency-report-what-it-takes-for.html.

Google Blog, *Google's approach to government requests for user data*, at http://googleblog.blogspot.com/2013/01/googles-approach-to-government-requests.html.

Hamelink Cees J. (2002), *Draft declaration on the right to communicate*, Amsterdam/Geneva, www.article19.org/data/files/pdfs/analysis/hamelink-declaration-the-right-to-communicate.pdf.

IFEX, *Special rapporteurs call for a "crime against freedom of expression"*, www.ifex.org/international/2012/06/27/free_expression_crime.

IFEX, Our Network, www.ifex.org/our_network.

INHOPE, About INHOPE, www.inhope.org/gns/about-us/about-inhope.aspx.

INHOPE (2011), *Articles of Association*, www.inhope.org/Libraries/Documents_Homepage/2011_INHOPE_Articles_of_Association_EN.sflb.ashx.

International Mechanisms for Promoting Freedom of Expression [UN, OSCE, OSA, ACHPR] (1 June 2011), *Joint Declaration on Freedom of Expression and the Internet*, www.osce.org/fom/78309.

Internet Rights and Principles Coalition, *10 Internet rights and principles*, http://internetrightsandprinciples.org.

Internet Watch Foundation, *Content assessment appeal process*, www.iwf.org.uk/accountability/complaints/content-assessment-appeal-process.

Internet Watch Foundation, *Service level agreement between the Association of Chief Police Officers (ACPO) and the Internet Watch Foundation (IWF)*, https://www.iwf.org.uk/assets/media/hotline/SLA%20ACPO%20IWF%20FINAL%20OCT%202010.pdf.

Internet Watch Foundation (9 December 2008), *IWF statement regarding Wikipedia webpage*, www.iwf.org.uk/about-iwf/news/post/251-iwf-statement-regarding-wikipedia-webpage.

Netzpolitik.org (16 January 2013), *Secret government document reveals: German Federal Police plans to use Gamma FinFisher spyware*, https://netzpolitik.org/2013/secret-government-document-reveals-german-federal-police-plans-to-use-gamma-finfisher-spyware.

oDesk (2013), *Abuse Standards 6.2. operation manual for live operators*, http://de.scribd.com/doc/81877124/Abuse-Standards-6-2-Operation-Manual.

Osborne Charlie (17 December 2012), *China reinforces its 'Great Firewall' to prevent encryption*, http://news.cnet.com/8301-1009_3-57559531-83/china-reinforces-its-great-firewall-to-prevent-encryption.

PEN International, Who we are, http://pen-international.org/who-we-are.

PEN International (September 2012), *PEN declaration on digital freedom*, adopted in Gyeongju, South Korea, http://pen-international.org/pen-declaration-on-digital-freedom.

PEN International, *PEN Declaration on Digital Freedom. Case studies, Tajistikan: business and human rights*, www.pen-international.org/wp-content/uploads/2012/11/PEN-declaration-Case-Studies_PDF4.pdf.

Reporters Without Borders (2012), Enemies of the Internet, http://en.rsf.org/beset-by-online-surveillance-and-13-03-2012,42061.html

SEC, Office of the Whistleblower, www.sec.gov/whistleblower.

Secretary of State Hillary Rodham Clinton (15 February 2011), *Internet rights and wrong: choices and challenges in a networked world*, George Washington University, Washington, D.C., www.state.gov/secretary/rm/2011/02/156619.htm.

Siracusa Principles on the Limitation and Derogation of Provisions in the International Covenant on Civil and Political Rights (1984), Annex, UN Doc. E/CN.4/1984/4, www.uio.no/studier/emner/jus/humanrights/HUMR5503/h09/undervisningsmateriale/SiracusaPrinciples.pdf.

Starmer Keir (20 September 2012), Director of Public Prosecutions, Crown Prosecution Service, *DPP statement on Tom Daley case and social media prosecutions*, http://blog.cps.gov.uk/2012/09/dpp-statement-on-tom-daley-case-and-social-media-prosecutions.html.

Statement on human rights, human dignity and the information society, www.pdhre.org/wsis/statement.doc.

TeliaSonera (14 March 2013), *Key telecommunication players sign principles on Freedom of Expression and Privacy and announce collaboration with GNI*, www.teliasonera.com/en/newsroom/press-releases/2013/3/key-telecommunication-players-sign-principles-on-freedom-of-expression-and-privacy-and-announce-collaboration-with-gni.

Telecommunications industry dialogue on freedom of expression and privacy (2013), Guiding Principles, www.teliasonera.com/Documents/Public % 20 policy % 20documents/Telecoms_Industry_Dialogue_Principles_Version_1_-_ENGLISH.pdf.

Twitter, Transparency Report, https://transparency.twitter.com.

Twitter (1 July-1 December 2012), Twitter transparency report, copyright notices, https://transparency.twitter.com/copyright-notices.

Unabhängiges Landeszentrum fuer Datenschutz (ULD, Office of the Data Protection Commissioner) Schleswig-Holstein (17 December 2012), *ULD issues orders against Facebook because of mandatory real names*, https://www.datenschutzzentrum.de/presse/20121217-facebook-real-names.htm.

U.S. Securities and Exchange Commission (Fiscal Year 2012), Annual Report on the Dodd-Frank Whistleblower Program, www.sec.gov/about/offices/owb/annual-report-2012.pdf, 4.

Wagner Ben (2012), *Export censorship and surveillance technology*, www.hivos.nl/content/download/72343/618288/file/Exporting % 20Censorship % 20And % 20Surveillance % 20Technology % 20by % 20Ben % 20Wagner.pdf.

Wagner Ben (2012), *After the Arab Spring: new paths for human rights and the Internet in European foreign policy*, European Parliament, Sub-Committee on Human Rights, EXPO/B/DROIT/2011/28.

Weixiao Wei (2011), *Online child sexual abuse content: the development of a comprehensive, transferable international Internet notice and takedown system*, https://www.iwf.org.uk/assets/media/resources/IWF % 20Research % 20Report_ % 20Development % 20of % 20an % 20international % 20internet % 20notice % 20and % 20takedown % 20system.pdf, 28.

World Summit on the Information Society (WSIS) (12 December 2003), Doc. WSIS-03/GENEVA/DOC/4-E.

WSIS (18 November 2005), Doc. WSIS-04/TUNIS/DOC/7-E.

WSIS (18 November 2005), Tunis Commitment, WSIS-05/TUNIS/DOC/7-E.

WSIS (12 December 2003), Declaration Principles, UN Doc. WSIS-03/GENEVA/DOC/4-E.

York Jillian C. (September 2010), *Policing content in the quasi-public sphere*, OpenNet, https://opennet.net/policing-content-quasi-public-sphere.

Media

AFP (24 January 2013), "French court says Twitter must identify racist tweeters".

Ars Technica Finland (31 October 2012), "Plan for universal 100Mbps service by 2015 on track", http://arstechnica.com/business/2012/10/finland-plan-for-universal-100mbps-service-by-2015-on-track.

BBC (1 July 2010), "Finland makes broadband a 'legal right'", www.bbc.co.uk/news/10461048.

BBC (12 August 2008), "Scorpions censored", www.bbc.co.uk/6music/news/20081208_scorpians.shtml.

BBC News (18 December 2012), "Germany orders changes to Facebook real name policy", www.bbc.co.uk/news/technology-20766682.

Benesch Susan and MacKinnon Rebecca (5 October 2012), "The innocence of YouTube", *Foreign Policy*, www.foreignpolicy.com/articles/2012/10/05/the_innocence_of_youtube.

Bowcott Owen (27 July 2012), "Twitter joke trial: Paul Chambers wins high court appeal against conviction", *The Guardian*, www.guardian.co.uk/law/2012/jul/27/twitter-joke-trial-high-court.

Cerf Vinton (4 January 2012), "Internet access is not a human right", *New York Times*, www.nytimes.com/2012/01/05/opinion/internet-access-is-not-a-human-right.html.

Dynamic coalition on freedom of expression, activities, http://dcexpression.wordpress.com.

Elmer-Dewitt Philip (6 December 1993), "First nation in Cyberspace. Twenty million strong and adding a million new users a month, the Internet is suddenly the place to be", *Time International*, No. 49, www.chemie.fu-berlin.de/outerspace/internet-article.html.

EU-Info.de (18 February 2013), "Europäische Datenschutzbehörden wollen Sanktionen gegen Google", www.eu-info.de/dpa-europaticker/226952.html.

Horner Lisa, Comprehensive background report: freedom of expression and the Internet, report from regional consultation meetings convened by Demos, Global Partner and Associates, www.mediapolicy.org/Demos-FoE-Internet.

Lee Dave (10 December 2012), "Pirate Party threatened with legal action over Pirate Bay proxy", *BBC News*, www.bbc.co.uk/news/technology-20668699.

O'Brien Kevin J. (4 December 2012), "Law students in Austria challenge Facebook privacy policy", *New York Times*, www.nytimes.com/2012/12/05/

technology/austrian-group-plans-court-challenge-to-facebooks-privacy-policies.html?_r = 0.

Reuters (21 December 2012), "Google executives acquitted in Milan autism video case", http://www.reuters.com/article/2012/12/21/google-italy-privacy-idUSL5E8NL6RR20121221.

RT.com (24 September 2012), "Twitter hands over Occupy protester's tweets to NY judge", http://rt.com/usa/twitter-occupy-last-harris-153.

Sabbagh Dan (9 October 2012), "Facebook and Twitter could be asked to increase moderation of networks", *The Guardian*, www.guardian.co.uk/media/2012/oct/09/dpp-criminal-tweets-facebook-posts.

Scola Nancy (13 December 2010), "Ten ways to think about DDoS attacks and 'legitimate civil disobedience'", http://techpresident.com/blog-entry/ten-ways-think-about-ddos-attacks-and-legitimate-civil-disobedience.

The Times of India (17 September 2012), "Anti-Prophet Mohamed film: Pakistan blocks YouTube as two killed in violence".

ZD.net (Protalinski Emil) (15 November 2011), "Facebook name battle: Ahmed Salman Rushdie claims victory", www.zdnet.com/blog/facebook/facebook-name-battle-ahmed-salman-rushdie-claims-victory/5358.

Sales agents for publications of the Council of Europe
Agents de vente des publications du Conseil de l'Europe

BELGIUM/BELGIQUE
La Librairie Européenne -
The European Bookshop
Rue de l'Orme, 1
BE-1040 BRUXELLES
Tel.: +32 (0)2 231 04 35
Fax: +32 (0)2 735 08 60
E-mail: info@libeurop.eu
http://www.libeurop.be

Jean De Lannoy/DL Services
Avenue du Roi 202 Koningslaan
BE-1190 BRUXELLES
Tel.: +32 (0)2 538 43 08
Fax: +32 (0)2 538 08 41
E-mail: jean.de.lannoy@dl-servi.com
http://www.jean-de-lannoy.be

BOSNIA AND HERZEGOVINA/
BOSNIE-HERZÉGOVINE
Robert's Plus d.o.o.
Marka Maruliça 2/V
BA-71000 SARAJEVO
Tel.: + 387 33 640 818
Fax: + 387 33 640 818
E-mail: robertsplus@bih.net.ba

CANADA
Renouf Publishing Co. Ltd.
22-1010 Polytek Street
CDN-OTTAWA, ONT K1J 9J1
Tel.: +1 613 745 2665
Fax: +1 613 745 7660
Toll-Free Tel.: (866) 767-6766
E-mail: order.dept@renoufbooks.com
http://www.renoufbooks.com

CROATIA/CROATIE
Robert's Plus d.o.o.
Marasoviçeva 67
HR-21000 SPLIT
Tel.: + 385 21 315 800, 801, 802, 803
Fax: + 385 21 315 804
E-mail: robertsplus@robertsplus.hr

CZECH REPUBLIC/
RÉPUBLIQUE TCHÈQUE
Suweco CZ, s.r.o.
Klecakova 347
CZ-180 21 PRAHA 9
Tel.: +420 2 424 59 204
Fax: +420 2 848 21 646
E-mail: import@suweco.cz
http://www.suweco.cz

DENMARK/DANEMARK
GAD
Vimmelskaftet 32
DK-1161 KØBENHAVN K
Tel.: +45 77 66 60 00
Fax: +45 77 66 60 01
E-mail: reception@gad.dk
http://www.gad.dk

FINLAND/FINLANDE
Akateeminen Kirjakauppa
PO Box 128
Keskuskatu 1
FI-00100 HELSINKI
Tel.: +358 (0)9 121 4430
Fax: +358 (0)9 121 4242
E-mail: akatilaus@akateeminen.com
http://www.akateeminen.com

FRANCE
Please contact directly /
Merci de contacter directement
Council of Europe Publishing
Editions du Conseil de l'Europe
FR-67075 STRASBOURG cedex
Tel.: +33 (0)3 88 41 25 81
Fax: +33 (0)3 88 41 39 10
E-mail: publishing@coe.int
http://book.coe.int

Librairie Kléber
1 rue des Francs-Bourgeois
FR-67000 STRASBOURG
Tel.: +33 (0)3 88 15 78 88
Fax: +33 (0)3 88 15 78 80
E-mail: librairie-kleber@coe.int
http://www.librairie-kleber.com

GERMANY/ALLEMAGNE
AUSTRIA/AUTRICHE
W. Bertelsmann Verlag Gmbh @ Co KG
Auf dem Esch 4
D-33619 BIELEFELD
Tel.: +49 521 91101 13
Fax: +49 521 91101 19
E-mail: uno-verlag@wbv.de
www.uno-verlag.de

GREECE/GRÈCE
Librairie Kauffmann s.a.
Stadiou 28
GR-105 64 ATHINAI
Tel.: +30 210 32 55 321
Fax.: +30 210 32 30 320
E-mail: ord@otenet.gr
http://www.kauffmann.gr

HUNGARY/HONGRIE
Euro Info Service
Pannónia u. 58.
PF. 1039
HU-1136 BUDAPEST
Tel.: +36 1 329 2170
Fax: +36 1 349 2053
E-mail: euroinfo@euroinfo.hu
http://www.euroinfo.hu

ITALY/ITALIE
Licosa SpA
Via Duca di Calabria, 1/1
IT-50125 FIRENZE
Tel.: +39 0556 483215
Fax: +39 0556 41257
E-mail: licosa@licosa.com
http://www.licosa.com

NORWAY/NORVÈGE
Akademika
Postboks 84 Blindern
NO-0314 OSLO
Tel.: +47 2 218 8100
Fax: +47 2 218 8103
E-mail: support@akademika.no
http://www.akademika.no

POLAND/POLOGNE
Ars Polona JSC
25 Obroncow Street
PL-03-933 WARSZAWA
Tel.: +48 (0)22 509 86 00
Fax: +48 (0)22 509 86 10
E-mail: arspolona@arspolona.com.pl
http://www.arspolona.com.pl

PORTUGAL
Marka Lda
Rua dos Correeiros 61-3
PT-1100-162 LISBOA
Tel: 351 21 3224040
Fax: 351 21 3224044
Web: www.marka.pt
E mail: apoio.clientes@marka.pt

RUSSIAN FEDERATION/
FÉDÉRATION DE RUSSIE
Ves Mir
17b, Butlerova ul. - Office 338
RU-117342 MOSCOW
Tel.: +7 495 739 0971
Fax: +7 495 739 0971
E-mail: orders@vesmirbooks.ru
http://www.vesmirbooks.ru

SWITZERLAND/SUISSE
Planetis Sàrl
16 chemin des Pins
CH-1273 ARZIER
Tel.: +41 22 366 51 77
Fax: +41 22 366 51 78
E-mail: info@planetis.ch

UNITED KINGDOM/ROYAUME-UNI
The Stationery Office Ltd
PO Box 29
GB-NORWICH NR3 1GN
Tel.: +44 (0)870 600 5522
Fax: +44 (0)870 600 5533
E-mail: book.enquiries@tso.co.uk
http://www.tsoshop.co.uk

UNITED STATES and CANADA/
ÉTATS-UNIS et CANADA
Manhattan Publishing Co
670 White Plains Road
USA-10583 SCARSDALE, NY
Tel: + 1 914 472 4650
Fax: +1 914 472 4316
E-mail: coe@manhattanpublishing.com
http://www.manhattanpublishing.com

Council of Europe Publishing/Editions du Conseil de l'Europe
FR-67075 STRASBOURG Cedex
Tel.: +33 (0)3 88 41 25 81 – Fax: +33 (0)3 88 41 39 10 – E-mail: publishing@coe.int – Website: http://book.coe.int

With the rise of the Internet, the opportunities to express oneself have grown exponentially, as have the challenges to freedom of expression. From the Arab Spring to the global Occupy movement, freedom of expression on the Internet has had a profound impact on the debates which shape our future. At the same time, an increasing number of states use the Internet to spy on journalists and citizens, to prosecute and jail bloggers, and to censor online information.

This book sets out to answer essential questions regarding the extent and limits of freedom of expression online. It seeks to shed light on the often obscure landscape of what we are allowed to say online and how our ideas, and the process of imparting and receiving information, are protected.

It shows the large ambit of rights protected by freedom of expression – including freedom of the media and the right to access information via the Internet. It also highlights the importance of the standard-setting, monitoring and promotion activities of international and non-governmental organisations, with a chapter on relevant national practices that illustrates how different states deal with the challenge that the Internet has brought to ensuring freedom of expression for all. As the importance of the Internet in our daily lives grows, readers will find this book to be a valuable resource for understanding the rights and obligations of each actor on the Internet, including states, Internet companies and civil society.

Professor Wolfgang Benedek is Head of the Institute of International Law and International Relations and Director of the European Training and Research Centre for Human Rights and Democracy of the University of Graz. His main research interests are human rights, human security, regulation of the Internet, and international economic law with a focus on global governance and international development law. He is the executive editor of the *European Yearbook on Human Rights*.

Dr Matthias C. Kettemann LL.M. (Harvard) studied international law in Graz, Geneva and at Harvard Law School, and is a lecturer at the Institute of International Law and International Relations of the University of Graz and a post-doctoral fellow at the Cluster of Excellence "Normative Orders" at the University of Frankfurt/Main. He is co-editor of the *European Yearbook on Human Rights*.

Prems 167417

www.coe.int

The Council of Europe is the continent's leading human rights organisation.
It includes 47 member states, 28 of which are members of the European Union.
All Council of Europe member states have signed up to the European Convention on Human Rights, a treaty designed to protect human rights, democracy and the rule of law.
The European Court of Human Rights oversees the implementation of the Convention in the member states.

http://book.coe.int

€29/US$58

ISBN 978-92-871-7702-5

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE