ICT and Human Rights

Rikke Frank Jørgensen, Anja Møller Pedersen, Wolfgang Benedek and Reinmar Nindler

30 November 2015

Large-Scale FP7 Collaborative Project
GA No. 320000
1 May 2013-30 April 2017

Case Study on ICT and Human Rights

(Policies of EU)

Work Package No. 2 – Deliverable No. 3

Due date	**30 November 2015**
Submission date	**30 November 2015**
Dissemination level	**PU**
Lead Beneficiary	**Danish Institute for Human Rights**
Authors	**Rikke Frank Jørgensen, Anja Møller Pedersen, Wolfgang Benedek and Reinmar Nindler**

http://www.fp7-frame.eu

Executive Summary

This case-study undertaken by the Danish Institute of Human Rights in Copenhagen and the European Training and Research Centre for Human Rights and Democracy in Graz is part of the FP7 project Fostering Human Rights among European Policies (FRAME), and a follow-up to the report (D 2.1) on 'factors which enable or hinder the protection of human rights'. The first report assesses a wide range of factors – historical, political, legal, economic, social, cultural, religious, ethnic and technological – and their impact on the protection of human rights in EU internal and external policies. The purpose of this case-study is to zoom in on the technological factors and to examine some of the challenges that were identified in the first report.

The first part of the study focuses on the EU's internal policies in the field of online content regulation. Drawing on case-studies of three EU directives – Directive 2000/31/EC on e-commerce, Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography and Directive 2004/48/EC on intellectual property rights enforcement – the study seeks to illustrate how dealing with alleged illegal content through blocking, filtering and take-down of content within co- and self-regulatory frameworks shaped around 'Internet intermediaries' challenge freedom of expression and information. The directives presuppose, accept or encourage self-regulation and, combined with schemes of limited liability, subject the intermediaries to an increasing pressure to implement public policy in the online domain. However, these practices and their limitations to freedom of expression are rarely framed as human rights issues, nor do they have the required safeguards. Based on analysis of the EU directives, the study explores the weaknesses – seen from a human rights perspective – of the European approach towards tackling illegal content on the Internet.

The study provides a number of suggestions to ensure that the EU addresses the human rights implications of co- and self-regulation, including the strengthening of safeguards and guidance for Member States and intermediaries to implement the said EU policy. Also, the study calls for a comprehensive EU freedom of expression and information framework, covering both its internal and external policy. In line with this, the EU should consider the freedom of expression and information implications of current and new policies when reviewing them according to the Digital Single Market Strategy.

The second part addresses the external policies of the EU with a focus on the protection and support of Human Rights Defenders using digital means ('Digital Defenders'). For this purpose, EU policies and instruments of relevance for Digital Defenders are analysed, including the implementation of the Internet Freedom Strategy and the No Disconnect Strategy. The programmes under the European Instrument for Democracy and Human Rights are reviewed with respect to their relevance for human rights activities online, taking into account the recent EU Guidelines on Freedom of Expression Online and Offline. This part of the study also explores the related issues of the safety of journalists (which are often citizen journalists), export control of surveillance technology by the EU Member States and the cooperation with other international organisations active in the field of online rights. Proposals are offered on how to improve the general environment for Digital Defenders and their right to freedom of

expression and information, and how to improve the coherence of EU action in this field. The newly created Human Rights Defenders Mechanism can play a pivotal role in this regard, as could updated EU Guidelines on human rights defenders.

List of abbreviations

AAP	EIDHR's Annual Action Programme
ACHPR	African Commission on Human and Peoples' Rights
Action Plan	EU Action Plan on Human Rights and Democracy
AFET	European Parliament's Committee on Foreign Affairs
AU	African Union
CFREU	Charter of Fundamental Rights of the European Union
CIRCAMP	Cospol Internet Related Child Abusive Material Project
CJEU	Court of Justice of the European Union
CoE	Council of Europe
COHOM	European Council's Working Group on Human Rights
CSR	Corporate Social Responsibility
DD(s)	Digital Defender(s)
DDP	Digital Defenders Partnership
DROI	European Parliament's Committee on Human Rights
ECHR	European Convention on Human Rights and Fundamental Freedoms
ECNP	Electronic Communications Network Provider
ECtHR	European Court of Human Rights
EDRI	European Digital Rights
EEAS	European External Action Service
EIDHR	European Instrument for Democracy and Human Rights
EP	European Parliament
EU	European Union
EuroISPA	European Internet Service Providers Association
EUSR	European Union Special Representative for Human Rights

FIDH	International Federation for Human Rights
FOC	Freedom Online Coalition
GIPO	Global Internet Policy Observatory
GISWatch	Global Information Society Watch
Guidelines	EU Guidelines on Freedom of Expression online and offline
HRC	United Nations Human Rights Council
HRD(s)	Human Rights Defender(s)
HRDM	Human Rights Defenders Mechanism
HRIA	Human Rights Impact Assessment
IAP	Internet Access Provider
ICT	Information and Communication Technology
ICCPR	International Covenant on Civil and Political Rights
IGF	Internet Governance Forum
IHRB	Institute for Human Rights and Business
IIG	Internet Information Gatekeeper
IPR	Intellectual Property Rights
ISP	Internet Service Providers
ISPA	Internet Service Providers Association
ISSP	Information Society Service Provider
IWF	Internet Watch Foundation
MENA	Middle East and North Africa Region
MRF	Netherlands National Human Rights Fund
NAP(s)	National Action Plan(s)
NCA-CEOP	A National Crime Agency Command – Child Exploitation and Online Protection Centre
NGO(s)	Non-Governmental Organisation(s)
OAS	Organisation of American States

OECD	Organisation for Economic Co-operation and Development
OHCHR	Office of the United Nations High Commissioner for Human Rights
OIC	Organization of Islamic Cooperation
OMCT	World Organization against Torture
OSCE	Organisation for Security and Cooperation in Europe
OSP	Online Service Provider
RSF	Reporters without Borders
Strategic Framework	EU Strategic Framework on Human Rights and Democracy
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
UN	United Nations
UNESCO	United Nations Educational, Scientific and Cultural Organization
US	United States
WSIS	World Summit on the Information Society

Table of Contents

Acknowledgement

The research leading to these results has received funding from the European Commission's Seventh Framework Programme (FP7/2007-2013) under the Grant Agreement FRAME (project n° 320000).

Special thanks to Joe McNamee, Executive Director, European Digital Rights (EDRI) and Mathias Vermeulen, policy advisor to Member of the European Parliament Marietje Schaake, for their participation in the session on Technological Factors at the FRAME Milestone Workshop in Brussels on 12 June 2015.

Special thanks to Tariq Desai for language assistance with Chapter II and Pia Niederdorfer and Manuela Rusz for their assistance with Chapter III and the finalisation of the document.

I. Introduction and Methodology

Human rights and fundamental freedoms are applicable both to offline and online environments.

At the global level, the awareness of the human rights implications of the Internet and other types of information and communication technology has risen steadily over the past years, and has resulted in a number of Internet-related resolutions adopted by the UN General Assembly and the UN Human Rights Council (United Nations Human Rights Council, 5 July 2012, United Nations Human Rights Council, 14 July 2014, United Nations General Assembly, 21 January 2015, United Nations General Assembly, 18 December 2013, United Nations General Assembly, 18 December 2014). Internet related potentials and challenges have also increasingly been addressed by UN special procedures such as the UN special rapporteur on the promotion and protection of the right to freedom of opinion and expression (Kaye, 2015, La Rue, 2013, La Rue, 2011).

At the EU level, a large amount of directives, policies and guidelines relate to technological factors (e.g. data protection, e-commerce, intellectual property rights, combating child sexual abuse and child pornography, cyber security, Internet governance, code of online rights, universal service, etc.) but not necessarily in ways that address the issues from a human rights perspective and ensure a coherent and forward looking approach to the protection of human rights online.

A strategic approach to the way technological developments may positively or negatively impact on human rights may guide the EU through areas where different interests conflict, and be used to ensure that the EU has robust and coherent strategies and positions to promote and advance human rights in its internal as well as external policies.

The authors hope that the current case-study will serve as a useful means in that direction.

With regard to its methodology, this case-study is a follow up to the Report on factors which enable or hinder the protection of human rights, specifically chapter IX on Technological Factors (Lassen, 2014). The chapter identified a number of challenges, whereof the authors have chosen to focus on two specific cases: 'Freedom of expression and self-regulation' (EU internal policy); as well as 'Protecting Internet freedoms' (EU External policy).

Besides desk research and literature review, the study has been informed by interviews as well as a number of conversations as mentioned specifically in relation to each case.

In terms of terminology, technological factors are understood as issues related to the use of information and communication technology (ICT) that have an impact on the way individuals are able to enjoy their human rights. Information and communication technology is a broad and not clearly defined term that refers to any communication device or application, encompassing: radio, television, cellular phones, computer and network hardware and software, satellite systems and so on, as well as the various services and applications associated with them (SearchCIO, 2011). In the following, emphasis is on

human rights issues related to the use of the Internet,[1] reflecting the attention, which the Internet has received in the policy debate pertaining to human rights and ICT, globally as well as within Europe.

The case-study is structured as follows: Study (1) Self-regulation and freedom of expression (EU internal policy) and Study (2) Review of EU-Policies on Digital Defenders with a focus on freedom of expression (EU external policy), and (3) Common Recommendations.

* The authors of this chapter are Rikke Frank Jørgensen, Senior Researcher, the Danish Institute for Human Rights and Anja Møller Pedersen, Legal Advisor, the Danish Institute for Human Rights.

[1] The term Internet refers to a global information and communication system that is linked together via the TCP/IP protocol FEDERAL NETWORKING COUNCIL (FNC) RESOLUTION. 24 October 1995. Definition of "Internet" 10/24/95 [Online]. Available: http://www.nitrd.gov/fnc/Internet_res.html [Accessed 10 July 2011].

II. Self-regulation and Freedom of Expression and Information – Case study on potential human rights implications of the EU's internal policies*

A. Introduction

In recent years, the EU has placed strong emphasis on privacy and data protection in the development of ICT related policy and legislation, whereas measures that constitute interferences with freedom of expression have not received similar attention and have often not even been framed as human rights issues. In seeking to remedy this gap, the authors have chosen to focus on the right to freedom of expression and the challenges that arise in relation to this right vis-à-vis co- and self-regulation. While excluding the related discussion on privacy and data protection, the authors wish to emphasise the close and mutual relationship that exists between freedom of expression and the right to privacy and protection of personal data, as illustrated by, for example, La Rue (La Rue, 2013).

The issues discussed are influenced by several factors related to the global infrastructure of the Internet, the role played by private actors, and the nature of human rights law vis-à-vis regional (EU) and/or national regulation. These factors are largely interrelated, and the analysis will seek to identify their mutual relationship and the specific policy challenges each of them raises.

Regarding the *infrastructure*, the Internet, unlike any other medium, enables individuals to seek, receive and impart information and ideas of all kind instantaneously and inexpensively across national borders (La Rue, 2011, para. 19). The global, decentral and inexpensive nature of the Internet infrastructure provides individuals with new means of realising freedom of expression, and at the same time confronts states with obstacles when they seek to sanction illegal expressions online. For example, speakers are numerous and often abroad and new technical means of circumventing censorship continue to evolve. Also, in contrast to the usual free expression scenario (speakers and listeners), the Internet is not dyadic (Kreimer, 2006, p. 1) but triadic with third parties (companies) in control of the communication.

Regarding *actors*, the online sphere is largely ruled by private companies who control the infrastructure and services available to the Internet users. In order to access the Internet, to communicate, debate, find and share information, tweet, associate etc. individuals engage with 'Internet intermediaries'[2] such as Internet service providers (ISPs),[3] search engines and social network platforms that mediate

[2] This study uses the legally neutral term 'Internet intermediary' to describe all services that constitute and operate on the Internet, such as Internet service providers, website operators, portals, platforms and search engines, OLSTER, J. 2013. Liability of Internet Intermediaries for Defamatory Speech – An Inquiry into the Concepts of 'Publication' and 'Innocent Dissemination. The Society of Legal Scholars Edinburgh Conference 2013, ibid. See also MACKINNON, R., UNITED NATIONAL EDUCATIONAL, SCIENTIFIC, AND CULTURAL, ORGANIZATION. 2014. Fostering Freedom Online: The Role of Internet Intermediaries. (Paris: UNESCO 2014), Available from http://unesdoc.unesco.org/images/0023/002311/231162e.pdf.> accessed 10 November 2015. P. 21.

[3] Within the EU, the term 'Internet service provider' is defined broadly as: (1) any public or private entity that provides to users of this service the ability to communicate by means of a computer system; and (2) any other entity that processes or stores computer data on behalf of such communication service EUROPEAN COMMISSION. 2011. Draft Recommendations for Public Private Cooperation to Counter the Dissemination of Illegal Content within the European Union [Online]. Brussels: EC. Available: https://edri.org/files/Draft_Recommendations.pdf

communication and various forms of online expressions. Internet users rely on these companies in order to participate online, thus depending on privately owned technologies, where the owners decide on the terms of use and on what information is allowed/not allowed. In this sense, the Internet intermediaries have become 'gatekeepers' of the online sphere (Laidlaw, 2012, p. 28, Zittrain, 2006).[4] In consequence, states increasingly enlist Internet intermediaries in frameworks of self-regulation and co-regulation[5] to prevent illegal online content such as alleged copyright infringements, child sexual abuse content and hate-speech.[6]

Regarding the *legal framework*, most, if not all, Internet intermediaries are private actors (private companies) with no direct obligations under international human rights law, yet they are expected to subscribe to soft law standards such as the UN Guiding Principles on Business and Human Rights. These companies often operate across a variety of jurisdictions and are expected to comply with national legislation that may conflict with international human rights norms, such as notice and take-down procedures or regulation mandating blocking and filtering of specific categories of content. In some cases, governments are shaping schemes of liability for third-party content around the intermediaries, thereby providing them with strong incentives to remove content upon notification to avoid liability.

B. Methodology and Structure

As mentioned, the study focuses on the right to freedom of expression and the challenges that arise in relation to this right vis-à-vis co- and self-regulation.

In terms of literature, the study draws on scholarly literature and recent studies related to Internet regulation, private actors, and freedom of expression (Jørgensen, 2013, Benedek and Kettemann, 2014, Hoboken, 2012, Brown and Korff, 2012, Balkin, 2014, Brousseau et al., 2012, Brown, 2010, EDRI, 2013, Kuczerawy, 2015, Korff, 2014, Tambini et al., 2008). It also includes standard-setting documents in this field from the UN, Council of Europe, and the EU. The literature review has been supplemented with

[Accessed September 11 2015. Both in Europe and the US, the term 'ISP' is used more frequently than the legally specific terms for access, content and service providers. In Europe, a provider of Internet access is an Electronic Communications Network Provider (ECNP), whereas a provider of content and services is termed an Information Society Service Provider (ISSP) under the E-commerce directive. In the US, an access provider is an Internet Access Provider (IAP), whereas a service provider is an Online Service Provider (OSP), SAVIN, A. & TRZASKOWSKI, J. 2014. Research handbook on EU Internet law. In the context of this study, the term ISP will be used in a non-legal sense, while the term 'Internet intermediaries' will be used covering both ECNPs and ISSPs (Savin and Trzakowski, 2014, p. 37).

[4] As of July 2015, Laidlaw's PhD thesis has been published under the title *Regulating Speech in Cyberspace, by Cambridge University Press*.

[5] Co-regulation refers to a legal model for public authorities based on voluntary delegation of all or some part of implementation and enforcement of norms to private actors. Co-regulation can also be referred to as 'privatised law enforcement'. Self-regulation, in contrast, refers to practices whereby private actors define, implement and enforce norms without public intervention FRYDMAN, B., HENNEBEL, L. & LEWKOWICZ, G. 2008. Public Strategies for Internet Co-Regulation in the United States, Europe and China. Working Papers du Centre Perelman de philosophie de droit, No. 2007/6. p. 133-134.

[6] The study focuses on content regulation as a means to combat alleged 'illegal content'. The notions of ´harmful´ and ´illegal´ are sometimes used together, yet the authors wish to emphasize the crucial distinction between content that is indeed illegal, and content that may be harmful or undesirable to certain audiences, yet legal under national law.

interviews and a number of conversations with representatives from civil society, the technology sector, and European policy makers, notably at the regional Internet Governance Forum in Lisbon in June 2013 as well as the global Internet Governance Forum held in Istanbul in 2014. Finally, a FRAME Milestone workshop was held in Brussels in June 2015, with invited speakers from European Digital Rights and the European Parliament. The workshop gave valuable input to the case study, as well as examples of Internet-related EU internal policy that is seen as problematic from a human rights perspective.

First, in **section C**, the study looks into the right to freedom of expression and information in an online context. In particular, it examines the extent to which restrictions of the freedom are permitted under international human rights law. Drawing on case law of the European Court of Human Rights (ECtHR) and the Court of Justice of the European Union (CJEU), it furthermore illustrates how content regulatory measures such as filtering and blocking may constitute violations of freedom of expression and information.

Second, in **section D**, the E-commerce directive, the directive on combating the sexual abuse and sexual exploitation of children and child pornography and the IPR enforcement directive, are briefly presented, including the human rights and rule of law challenges each of them pose.

Third, **section E** analyses online limitations of freedom of expression and information by private actors, exemplified by the EU directives. The analysis will include both the vertical human rights conflicts (co-regulation) and the horizontal human rights conflict (self-regulation) involved: liability schemes; the UN Guiding Principles on Business and Human Rights; and recent 'gatekeeper' theory, according to which the human rights responsibility of Internet intermediaries increases with their capacity to impact democratic participation. The study will argue that the measures of co- and self-regulation mandated in the EU directives de facto lead to a situation where EU Member States circumvent the obligations they have under international human rights law. As such, the mentioned EU directives constitute examples of limitations of freedom of expression and information without the required human rights safeguards.

Finally, **section F** summarises the conclusions made through the study and outlines further recommendations to relevant policy makers.

C. The Human Rights Standards at Stake

'A growing amount of self-regulation, particularly in the European Union, is implemented as an alternative to traditional regulatory action. Some governments actively encourage or even place pressure on private business to self-regulate as an alternative to formal legislation or regulation which is inherently less flexible and usually more blunt than private arrangements' (MacKinnon et al., 2014, p. 56).

In the online sphere, individuals engage with intermediaries in order to exercise their right to freedom of expression and information. This has given these private companies unprecedented control over online content, and at the same time weakened states´ possibilities of direct interference with online speakers and listeners. In response to this challenge, the EU has for the past two decades enlisted Internet companies in frameworks of self- and co-regulation to assist Member States in preventing online illegal content. While these policies clearly have an impact on end-users' freedom of expression

and information, they have largely been formulated and implemented without an explicit recognition of the fundamental rights issues they raise. In contrast to privacy and data protection, there is no common EU regulation related to online freedom of expression, besides the overall reference in Article 6 of the Treaty of the European Union (TEU) that refers to the Charter of Fundamental Rights of the European Union (CFREU) and the European Convention on Human Rights (ECHR) as general principles of EU-law. In other words, whereas privacy and data protection is protected under article 7 and 8 of the CFREU, in Article 16 of the Treaty of the Functioning of the European Union (TFEU) and in secondary EU-law, such as e.g. the Data Protection Directive (Directive 95/46/EF) (European Parliament and Council of the European Union, 1995) and the E-privacy Directive (2002/58/EC) (European Parliament and Council of the European Union, 2002), freedom of expression is only protected in Article 11 of the CFREU.

The EU has acknowledged the importance of freedom of expression in the recent EU Human Rights Guidelines on Freedom of Expression Online and Offline (see also Section III.D.1.c.), according to which the EU is committed to respecting, protecting and promoting freedom of opinion and expression within its borders. It should be noted, however, that the guidelines focus primarily on the external policy of the EU (Council of the European Union, 2014, para. 7).

In order to understand the human rights challenges that arise from this line of policy, the section offers an introduction to the right to freedom of expression and information generally as well as online, including standards for legitimate restrictions to the right. Moreover, it explains the implications of measures such as blocking and filtering on freedom of expression and information.

1. Freedom of Expression and Information Online

The right to freedom of expression and information is protected both at the international level in the Universal Declaration of Human Rights (Article 19) and International Covenant on Civil and Political Rights (ICCPR) (Article 19) and at the regional European level in the European Convention on Human Rights and Fundamental Freedoms (ECHR) (Article 10) and the Charter of Fundamental Rights of the European Union (CFREU) (Article 11).

As the study has its outset in a European context, the authors primarily refer to European standards and case-law. However, a number of UN documents are also included since online freedom of expression and information has been addressed extensively by the UN Human Rights Council (HRC) and UN Special Rapporteurs.

According to Article 10 of the ECHR, everyone has the right to freedom of expression, including freedom to hold opinions and to receive and impart information and ideas without state interference. The right entails two sets of freedoms: (1) to hold opinions and impart information (freedom of expression); and (2) to receive information that others wish to impart (freedom of information). In the following, 'freedom of expression and information´ will be used to cover both aspects of the right.

Article 11(2) of the CFREU also specifically protects the 'freedom and pluralism of the media'.

The ECtHR has established that freedom of expression 'constitutes one of the essential foundations of a democratic society, one of the basic conditions for its progress and for the development of every man'

(*Handyside v. The United Kingdom*, 1976, para. 48). Freedom of expression is essential for the fulfilment and enjoyment of a wide range of other human rights, including freedom of association and assembly, freedom of thought, religion or belief, the right to education, the right to take part in cultural life, the right to participate in public affairs, etc. In other words, democracy cannot exist without freedom of expression (Council of the European Union, 2014, para. I.A.2.).

Freedom of expression includes all forms of expression, without any distinction to content and through any medium (White et. al, 2010, p. 426). The European Court of Human Rights (ECtHR) has established that Article 10 applies fully to the Internet (*Perrin v. the United Kingdom*, 2005). Likewise, in the first UN HRC resolution on human rights on the Internet from 2012, the HRC has confirmed that human rights apply online as offline (United Nations Human Rights Council, 2012).

Arguably, the Internet expands the ways in which individuals may enjoy their right to freedom of opinion and expression by allowing individuals to seek, receive and impart information instantaneously and inexpensively across borders. It serves as an enabler of other human rights and its use and incorporation into virtually every aspect of modern human life is unprecedented. The Internet has thus become one of the most powerful instruments of the 21st century for increasing transparency in access to information and for facilitating active citizen participation in building democratic societies (La Rue, 2011, para. 2).

The Internet has a 'profound value for freedom of opinion and expression, as it magnifies the voice and multiplies the information within the reach of everyone who has access to it. Within a brief period, it has become the central global public forum' (Kaye, 2015, para. 11). By increasing the information that is available to us through new tools to receive information and circulate, comment or even modify that information, the Internet contributes to democratic culture (Laidlaw, 2012, p. 30). At many occasions, this has also been recognised by the ECtHR (*Ahmet Yıldırım v. Turkey*, 2012, para. 48).[7]

In recognition of this potential, the all states should prioritise to facilitate access to the Internet for all individuals, with as little restriction to online content as possible. Access to the Internet has two dimensions: (1) Availability of the necessary infrastructure and ICT and (2) access to online content without any other restrictions than those permitted under international human rights law (La Rue, 2011, para. 2-3). In the current study, focus is primarily on the latter, access to online content.

With a view to provide the Internet users with a tool to learn about their online human rights, including access to remedies, the Council of Europe (CoE) has produced a 'Guide to human rights for Internet users' (Council of Europe, 2014c) accompanied by an explanatory memorandum (Council of Europe, 2014d). The guide builds on existing rights in the ECHR and other CoE conventions and does not establish any new rights (Council of Europe, 2014c, Introduction, para. 1-3).

As mentioned, the right to freedom of expression and information involves all types of information, including information that offends, shocks or disturbs (*Handyside v. The United Kingdom*, 1976, para.

[7] For an overview of freedom of expression in an online and European context, including recent case-law, see BENEDEK, W. & KETTEMANN, M. 2014. Freedom of Expression and the Internet, Strasbourg, Council of Europe. COUNCIL OF EUROPE June 2015. Factsheet – New technologies. Strasbourg: Council of Europe.

49). However, by virtue of Article 17 of the ECHR (prohibition of abuse of rights), the ECtHR has announced, that expressions constituting hate speech or negate the fundamental values of the ECHR fall outside the scope of protection of Article 10 (*Delfi AS v. Estonia*, 2015, para. 136). The ECtHR has also reiterated that such defamatory and other types of clearly unlawful speech, including hate speech, can be disseminated like never before, be globally accessible in a few seconds, and sometimes remain persistently online (*Delfi AS v. Estonia*, 2015, para. 110).

Furthermore, freedom of expression is not an absolute right and can be subject to restrictions. However, any restriction must comply with the criteria laid down in Article 10(2) of the ECHR (or Article 52 of CFREU as regards interferences with Article 11 of the CFREU).

First, any restriction must be prescribed by law; it must be accessible, clear and sufficiently precise in order for individuals to regulate their behaviour accordingly (and avoid state interference) and it should provide for sufficient safeguards against abusive restrictive measures, including effective control by a court or other independent adjudicatory body. *Second*, it must follow one of the legitimate aims exhaustively listed in Article 10(2) of the ECHR; national security, territorial integrity or public safety, the prevention of disorder or crime, the protection of health or morals, the protection of the reputation or rights of others, preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary. *Finally*, the restriction must be necessary in a democratic society, meaning proportionate. Notably it should be proven that the restriction is a result of a pressing social need and that it is the least restrictive means for achieving the legitimate aim of the measure (*Handyside v. the United Kingdom,* 1986, para. 48; *Observer and Guardian v. the United Kingdom*, 1991, para. 59).

Any restriction must be in accordance with the 'rule of law':

> 'The rule of law is a principle of governance by which all persons, institutions and entities, public and private, including the state itself, are accountable to laws that are publicly promulgated, equally enforced, independently adjudicated and consistent with international human rights norms and standards. It entails adherence to the principles of supremacy of law, equality before the law, accountability to the law, fairness in applying the law, separation of powers, participation in decision making, legal certainty, avoidance of arbitrariness and procedural and legal transparency' (Korff, 2014, p. 10).

The three-step test in Article 10(2) is also part of other international human rights law pertaining to freedom of expression such as Article 19 of the International Covenant on Civil and Political Rights (ICCPR).

As stated explicitly in Article 10 of the ECHR, the protection comprises only interferences by *public authorities.*[8] Any limitation of the right introduced by *private actors* therefore does not constitute an 'interference', in a strict legal sense, of Article 10.

It follows that states must abstain from interference with individuals' freedom of expression and information that does not meet the criteria laid down in Article 10(2) of the ECHR (*negative human rights obligations*).

However, Article 10 also places *positive human rights obligations* on the state. Thus, the effective exercise of freedom of expression may require positive state measures in order to secure an effective human rights protection between private parties. A such, state responsibility for human rights violations may be invoked in cases where the state has failed to enact appropriate domestic legislation to ensure human rights protection in the realm of private actors (*VgT Verein Gegen Tierfabriken v. Switzerland*, 2001, para. 45). It is here decisive, whether the state has struck a fair balance between concurring rights e.g. between the private actor's right to conduct a business and the right to freedom of expression and information of the end-user (*Delfi AS v. Estonia*, 2015, para. 138ff.). The scope of this obligation will inevitably vary, having regard to the diversity of situations in states, the difficulties involved in policing modern societies and the necessary choices in terms of priorities and resources. Moreover, the obligation must not be interpreted in such a way as to impose an impossible or disproportionate burden on authorities (*Rees v. the United Kingdom*, 1986, paras. 35-37). Regard must also be taken to the kind of expressions at stake; their capability to contribute to public debates, the nature and scope of the restrictions, the ability of alternative venues for expression and the weight of countervailing rights of others or the public (*Appleby and Others v. the United Kingdom*, 2003, paras. 42-43 and 47-49).[9]

We will return to the Delfi ruling in section E.2. below, including some of the challenges and contradictions it entails. First, however, an examination of some of the measures and standards related to online limitations of freedom of expression.

2. Online Limitations to Freedom of Expression and Information

Limitations to online content can take various forms, from technical measures that prevent access to certain content, such as blocking and filtering, to inadequate guarantees of the right to privacy and the protection of personal data, which inhibit the dissemination of opinions and information (La Rue, 2011, para. 28). Content regulation is a complex field:

> 'Today the disabling of access to and the removal of illegal content by providers of hosting services can be slow and complicated, while content that is actually legal can be taken down erroneously. 52.7% of stakeholders say that action against illegal

[8] This is contrary to Article 19 of the ICCPR, which does not explicitly mention ´public authorities´. For an account of the drafting history of Article 19 and a discussion of whether private actors may (in a soft law sense) ´interfere´ with freedom of expression see LAND, M. 2013. Toward an International Law of the Internet. *Harvard International Law Journal,* 54.

[9] For further elaboration, see also COUNCIL OF EUROPE & EUROPEAN COURT OF HUMAN RIGHTS 2011. Positive obligations on member States under Article 10 to protect journalists and prevent impunity.

content is often ineffective and lacks transparency' (European Commission, 2015, para. 3.3.2)

As mentioned, this study focuses on restrictions in individuals' right to freedom of expression and information caused by measures that either remove the content (take-down), or disable end-users' ability to access it (blocking and filtering). The terms are often used interchangeably and without any precise definition. In the following, 'blocking' refers to technical measures taken to prevent users from accessing specific websites, IP addresses, and domain name extensions. 'Filtering' refers to technical measures used to exclude pages containing certain keywords or other specific content from appearing when the end-user searches for information. 'Take-down' refers to situations where content is removed from webpages at the request of the owner of the content, a victim hereof, or public authorities on behalf of such, such as e.g. the notice-and-take-down procedure described in the Delfi-case (*Delfi AS v. Estonia*, 2015, para. 13).[10]

Generally speaking, filters are used to limit end-users' access to certain material and websites based on the content of the site, while blocking denies access based on the website's URL. Whereas take-down in principle may be applied to target a specific piece of information, blocking and filtering are generally less targeted due to their automated nature. The study will not deal with the technical specifics of these different measures, but will focus on the limitations to freedom of expression and information that arise from their use.[11]

While self-regulation is frequently praised as an effective tool to redress illegal or harmful speech on the Internet, for instance, by the four rapporteurs on freedom of expression from the UN, OSCE, Organization of American States (OAS) and the African Commission on Human and Peoples' Rights (ACHPR) (United Nations Special Rapporteur on Freedom of Opinion and Expression et al., 2011), it entails a number of human rights and rule of law challenges.

Scholars have repeatedly warned against the many practical as well as principal problems related to blocking, filtering and take-down of content (Kuczerawy, 2015, Callahan et al., 2009, Tambini et al., 2008, McIntyre, 2010). As summarised by Korff, blocking is inherently likely to produce (unintentional) false positives (blocking sites with no prohibited material) and false negatives (when sites with

[10] Take-down procedures (often referred to as ´Notice-and-take down´ or the broader term ´Notice-and-action´) derives from Article 14 of the E-commerce directive. Despite several attempts, no common EU standards for these procedures exist. In January 2012, the European Commission announced an initiative on 'notice-and-action' procedures in the Communication on e-commerce and other online services (COM(2011) 942 final). Up till now, the consultation has not led to any tangible results. See KUCZERAWY, A. 2015. Intermediary liability & freedom of expression: Recent developments in the EU notice & action initiative. *Computer Law & Security Review: The International Journal of Technology,* 31, 46-56.

[11] For further elaboration on these technologies see for example 'Beyond Denial, Introducing Next-Generation Information Access Control' in DEIBERT, R., PALFREY, J., ROHOZINSKI, R., ZITTRAIN, J. & OPENNET, I. 2010. *Access controlled: the shaping of power, rights, and rule in cyberspace,* Cambridge, Mass., MIT Press, DEIBERT, R. J., PALFREY, J., ROHOZINSKI, R. & ZITTRAIN, J. (eds.) 2008. *Access Denied : the practice and policy of global Internet filtering*, Cambridge, Mass.: MIT Press, p. 57, TAMBINI, D., LEONARDI, D. & MARSDEN, C. T. 2008. *Codifying Cyberspace : communications self-regulation in the age of internet governance,* London; New York, Routlegde. P. 120ff., the OpenNet Initiative (ONI), https://opennet.net/ and Herdict, www.herdict.org/.

prohibited material slip through a filter); the criteria for blocking certain websites, but not others, and the lists of blocked websites, are often secret; appeals processes may be onerous, little known or non-existent, especially if the decision on what to block or not block is – deliberately – left to private entities; blocking measures are easy to bypass, even for not very technically skilled people; and particularly in relation to child pornography, blocking fails to address the actual issue: the abuse of the children in question (Korff, 2014, p. 13).

The ECtHR has recently ruled that blocking may violate freedom of expression and information. The case of *Yildirim v. Turkey* concerned blocking of access to all websites hosted by Google Sites from Turkey in order to block a site that was regarded as disrespectful of Kemal Atatürk. The court found that the blocking measure had produced arbitrary effects, since it resulted in the wholescale blocking of all sites hosted by Google Sites. Moreover, domestic law did not provide for any safeguards to ensure that a blocking order related to a specific site was not used as a means of blocking access in general. The Court therefore pronounced on a violation of Article 10 of the ECHR (*Ahmet Yıldırım v. Turkey*, 2012).

Also, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has cautioned against the human rights implications of such measures and instructed that 'any requests submitted to intermediaries to prevent access to certain content, or to disclose private information for strictly limited purposes such as administration of criminal justice, should be done through an order issued by a court or a competent body which is independent of any political, commercial or other unwarranted influences' (La Rue, 2011, para. 75).[12]

As argued by Balkin, a significant feature of the digital age is that the infrastructure of free expression is merging with the infrastructure of content regulation and the infrastructure of public and private surveillance. The infrastructure and technologies that people rely on to communicate is thus the same used by states for speech (content) regulation and surveillance (Balkin, 2014). In the pre-digital age, speech regulation was exercised through fines, criminal penalties and injunctions, but due to the specifics of the online environment, new techniques and tools now supplement the old ones. As opposed to 'old-school' speech regulation and censorship exercised by the press, these 'new-school' techniques do not work separately from the source of expression/information, but are built into the communication infrastructure (Balkin, 2014, p. 2). Such techniques are getting increasingly more sophisticated, with multi-layered controls that are hidden from the public and work automatically – or even 'timed' to prevent access to or dissemination of information at key political moments (La Rue, 2011, paras. 29-30).

[12] Whereas in the US, the absolute speech protection of the first amendment provides a counter mechanism to blocking, notice and take-down of content, a similar protection of free speech is not found within the EU, where freedom of expression standards are qualified by state rights. TAMBINI, D., LEONARDI, D. & MARSDEN, C. T. 2008. Codifying cyberspace: communications self-regulation in the age of Internet convergence, London; New York, Routledge, p. 8.

As private companies control the digital infrastructure and its core services, the introduction of measures that limit the information flow requires either cooperation from the intermediaries or coercion exercised upon them. As a result:

> 'Low salience and use of private parties can help governments preserve legitimacy even as their policies block, limit, or spy on expression. This is the big story about the freedoms of speech, press, and association in the digital age' (Balkin, 2014, p. 3)

These 'new-school' techniques have three features in common: (1) *collateral censorship*, meaning that the state regulates one party (the Internet intermediary) in order to control another, the speaker, (2) *public/private cooperation and co-optation*, as the infrastructure is owned by private companies, the government needs to either coerce or co-opt the intermediaries into speech (content) regulation, and (3), new forms of *digital prior restraints* (Balkin, 2014, p. 4).

In relation to content regulation within the EU, it is important to distinguish between two different situations: mandatory (law-based) and voluntary (non-law-based), as the implications on freedom of expression and information vary accordingly. Arguably, it is legitimate to remove or block access to clearly identified illegal content. However, the aim of the measure, and the means used to carry it out remain crucial to determining whether the measure is in fact proportional and therefore lawful. Also, voluntary measures may evoke the positive state responsibility under human rights law, in particular if the state de facto encouraged these measures (Korff, 2014, p. 13), as further addressed in section C.2.b. below.

a) Mandatory Measures

'Mandatory' measures include filtering, blocking and take-down schemes introduced and applied directly by public authorities and measures initiated by public authorities, but applied by intermediaries through co-regulatory schemes.

Mandatory blocking and filtering carried out by intermediaries, such as general 'blacklisting' of certain content, deprives the speakers (providers of the alleged illegal content) that are being blocked from reaching end-users. In the CoE Recommendation on Freedom of Expression and Information and Internet Filters, mandatory filtering is considered a restriction to freedom of expression and information which must meet the criteria laid down in Article 10(2) of the ECHR (Council of Europe, 2008).

Both the intermediary and the speaker would be able to assert the protection in Article 10 of the ECHR. Firstly, on behalf of its end-users, the intermediary may contest the validity of blocking sources that would not be judged illegal by a proper authority, and secondly, on behalf of itself or the speaker, it may argue that mandatory filtering causes it to block information that would otherwise be accessible. If the intermediary does not contest the mandatory filtering, the speaker may assert its right to freedom of expression, but can also do this irrespectively of the action of the intermediary (Hoboken, 2012, p.

146).[13] Likewise, the end-users to whom the speaker is deprived access can no longer access all information freely. The measures thus limit their freedom of information (Hoboken, 2012, p. 149).

Since mandatory measures constitute an interference with the right to freedom of expression and information protected under Article 10 of the ECHR, it must meet the three criteria laid down in Article 10(2), i.e. that any inference must be (1) prescribed by law; (2) have a legitimate aim and; (3) be necessary in a democratic society, i.e. proportional. First, it must be prescribed by law. Blocking, filtering and take-down procedures introduced and applied directly by an EU Member State will most likely have a legal basis. However, the legal basis needs to be sufficiently clear, precise and foreseeable, which is often difficult to meet, as the 'blacklists' or 'blocking-lists' are generally not made public. Moreover, the outcome of the first criteria regarding the legal basis of the restriction is influenced by the outcome of the proportionality assessment under the third criteria (and vice-versa). Secondly, the measures must pursue a legitimate aim. In principle, this should be easily assessed, if the measure is prescribed by law. However, as the blocking criteria are not made public, it is often difficult to assess whether blocking in reality follows a legitimate aim. As a result, the outcome of the proportionality assessment becomes decisive for the legality of the measure. Guidance for this assessment can be found in the CoE Recommendation on respect for freedom of expression and information with regard to Internet filters:

> 'Such action by the state should only be taken if the filtering concerns specific and clearly identifiable content, a competent authority has taken a decision on its illegality and the decision can be reviewed by an independent and impartial tribunal or regulatory body, in accordance with the requirements of Article 6 of the European Convention on Human Rights' (Council of Europe, 2008, Section III(ii)).

Arguably, mandatory and general blocking and filtering introduced/ordered by public authorities constitute prior restraints to the information that is blocked. Prior restraints resemble classical censorship, and although Article 10 does not prohibit prior restraints, the ECtHR has reiterated that, due to the dangers inherent in such prior restraints, they call for the most careful scrutiny of the Court (*Ahmet Yıldırım v. Turkey*, 2012, para. 47). Furthermore, generalised filtering tends to be insufficiently targeted, and as a result, content is made inaccessible beyond what is deemed necessary/illegal. Lack of proper targeting is highly problematic when taking into account that content is frequently blocked without any intervention or possibility for judicial or independent review (La Rue, 2011, para. 31). States and intermediaries are therefore encouraged to assess and review the effectiveness and proportionality of the filters on a regular basis (Council of Europe, 2008, Section III). In line with this, states should ensure that all filters are assessed both before and during their implementation to ensure that their effects are proportionate to the purpose of the restriction and thus necessary in a democratic society, in order to avoid unjustified blocking of content (Council of Europe, 2014d, para. 49). Judicial review should weigh-up the competing interests at stake, strike a balance between them and determine whether a less far-reaching measure could be taken to block access to specific Internet content (*Ahmet Yıldırım v. Turkey*, 2012, para. 64-66).

[13] Hoboken operates with access providers, information providers and end-users, while the study uses the term 'intermediaries' (that includes 'access providers'), and the term 'speaker' (instead of 'information providers').

The Court of Justice of the European Union (CJEU) has delivered two rulings on the imposition of generalised mandatory filtering on ISPs and social media platforms.

On 24 November 2011, the CJEU ruled, that generalised, mandatory Internet filtering may violate both freedom of expression and information and the protection of personal data as safeguarded in Articles 11 and 8 of the CFREU (Case C-70/10 *SABAM v. Scarlet Extended*, 24 November 2011). The ruling concerned whether EU Member States are allowed – through injunctions ordered by national courts – to order an ISP to install a preventive system for filtering all electronic communications passing via its services in order to identify electronic files of which the applicant claims to hold (intellectual property) rights, with a view to block the transfer of files. The CJEU ruled, that such an obligation would *de facto* require the ISP to carry out general monitoring, prohibited in Article 15(1) of the E-commerce directive (Case C-70/10 *SABAM v. Scarlet Extended*, 24 November 2011, para. 40).

However, in order to assess whether the injunction was in conformity with EU law, the requirements stemming from the protection of the applicable fundamental rights also has to be taken into account. A fair balance thus had to be struck between the fundamental right to (intellectual) property of the copyright holders, cf. Article 17(2) of the CFREU, and the freedom to conduct a business of the ISP (forced to install a generalised filter), cf. Article 16 of the CFREU. The court found that the Member State in question had failed to strike such a fair balance. Furthermore, the injunction could also infringe the rights of the ISP's customers, in particular their right to protection of personal data and their freedom of expression and information. Since generalised filtering may not adequately distinguish between lawful and unlawful content, the Member State had also failed to strike a fair balance towards these rights (Case C-70/10 *SABAM v. Scarlet Extended*, 24 November 2011, paras. 44-53).

On similar grounds and with reference to the previously mentioned ruling from 2011, on 16 February 2012, the CJEU ruled that social network platforms cannot be required to install a general filtering system, covering all users, in order to prevent unlawful use of musical and audio-visual work (Case C-360/10 *SABAM v. Netlog NV*, 16 February 2012).

In sum, in the case of mandatory blocking and filtering where the measures are introduced and applied directly by the state, the human rights conflict remains a *vertical conflict* between the state and the intermediary, the speaker or the end-users. The potential violation of freedom of expression or information is thus clearly attributable ('attribution' meaning responsibility for human rights violations) to the state. To a certain extent, this is also the case when the measures are clearly initiated by the state. At some point, however – in the zone between co- and self-regulatory frameworks – potential human rights violations may no longer be attributed directly to the state but rather indirectly through its positive human rights obligations. These cases of horizontal human rights conflicts (positive obligations), however, are not as clear-cut as the vertical ones (negative obligations). This will be further elaborated below in relation to voluntary measures of content-regulation.

b) Voluntary Measures

Voluntary measures are more complicated than their mandatory counterpart, since they cause a *horizontal conflict* between the intermediary who imposes the measure and the speaker or the end-user.

For instance, if an intermediary blocks access to certain content based on codes of conduct, it interferes (in a non-legal sense) with the freedom of expression of the author of that content or the freedom of information of the end-user the content was trying to reach. This interference must be resolved under the positive human rights obligations of the state. Accordingly, what determines the outcome is whether the state has struck a fair balance between the freedom of the intermediary to conduct a business (provide Internet services) and the right to freedom of expression and information of the speaker or end-user.

The state normally holds a wide margin of appreciation with regard to how it chooses to balance the rights of one individual against the rights of another. The protection of interests of the speaker against limitation by an intermediary is generally considered to lie within the margin of appreciation of the state. Positive obligations to protect speakers from being blocked/filtered will only arise when individuals are prevented from effectively exercising their right to freedom of expression and information or when pluralism of the information environment would be clearly at stake. Accordingly, a clear example of a strict positive obligation arises where blocking or filtering by intermediaries deprives an online speaker from reaching an audience completely – or deprives an end-user completely from accessing certain content (Hoboken, 2012, p. 148f.). For instance (and quite simplified), if a speaker is being blocked by a social media platform, but he/she may 'publish' the content on another social media platform, that speaker is not deprived from reaching an audience completely, and likewise, the end-user is not completely deprived from accessing the content. As a result, the positive obligations of the state are not triggered.

Hence, as positive human rights obligations are not easily established, there is a risk that the rights of the speakers and end-users are not properly protected in cases of blocking and filtering. However, as argued by some scholars:

> The fact that Article 10 of the ECHR only refers to interferences with this right 'by public authorities' does not mean that the state can simply wash its hands of measures by private entities that have such effect – especially not if the state de facto strongly encouraged those measures. In such circumstances, the state is responsible for not placing such a system on a legislative basis: without such a basis, the restrictions are not based on 'law' (Korff, 2014, p. 14).

We will return to this point in section E.1., when we discuss the human rights challenges raised by the EU directives. In sum, the distinction between mandatory and voluntary measures is far from clear-cut, but contains several grey zones. Generally, in co- and self-regulatory cases states seek to regulate a domain outside their direct sphere of control, and by different means – formally or informally – they encourage intermediaries to introduce measures that remove or disable access to content. As such,

states leave it to the intermediaries to impose measures that would have constituted 'interferences' under Article 10 of the ECHR had they been applied by public authorities.

Similar to mandatory schemes, limitations to freedom of expression and information within voluntary schemes may lack proportionality due to insufficiently targeting. Additionally – and importantly – voluntary schemes lack a clear legal mandate and uncertainty persists as to when (at which level of gravity) these practices fall under the state's positive human rights obligation. This directs attention to the human rights compliance that may be expected from private actors, in particular those who exercise powers or take on roles that have a substantial impact on the way individuals may exercise fundamental rights. In section E.3. below, recent standard-setting on the human rights responsibility of private actors will be included when discussing the said examples of EU policy pertaining to online content regulation.

D. Selected EU Directives with Implications on Freedom of Expression and Information

Although the protection of human rights now is a well-established part of EU-law, cf. Article 6 of the TEU, secondary EU-law entails freedom of expression implications that are not addressed within the framework of Article 10 of the ECHR and Article 11 of the CFREU. The directives discussed below all encourage or obligate Member States to take on action that may interfere with freedom of expression and information, but without referencing Article 10 of the ECHR and Article 11 of the CFREU.

The EU approach towards self-regulation has been subject to several studies over the past years. In a comprehensive European Commission funded study conducted in 2001-2004, researchers looked at self-regulatory practices in the then-15 EU Member States across a variety of media sectors. In conclusion, the study warned of the negative impact that self-regulatory practices may have on the fundamental rights to privacy and freedom of expression (Tambini et al., 2008). The conflict between self- and co-regulatory measures and freedom of expression has also been emphasised by Frydman and Rorive (Frydman and Rorive, 2002, Frydman et al., 2008), and by Callahan et. al. (Callahan et al., 2009), specifically in relation to blocking carried out by Internet intermediaries. Moreover, European Digital Rights (EDRI) has repeatedly commented on the human rights implications of self-regulation.[14]

The EU policy in this area should be seen on the backdrop of political pressure to tackle illegal content on the Internet, not least related to child pornography; lack of direct control over the online domain; and the seemingly effectiveness of technical solutions to filter and block unwanted content.

For an elaboration of the EU policy environment and historical context leading to the present co- and self-regulatory regime codified in the three directives, please refer to Tambini (Tambini et al., 2008, p. 2-9).

Below follows an introduction to the EU directives on E-commerce, on combating the sexual abuse and sexual exploitation of children and child pornography and on IPR enforcement. The background, aim and relevant provisions of each directive is briefly introduced, followed by an introduction to the freedom of expression and rule of law challenges that the directive causes.

1. Directive 2001/31/EC on E-commerce

The E-commerce directive sets up an Internal Market framework for electronic commerce (European Parliament and Council of the European Union, 2000). It 'seeks to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between the Member States (European Parliament and Council of the European Union, 2000, Article 1(1)).

The directive does not use the notion of 'Internet intermediaries', but pursuant to Article 2(a), 'information society services' is to be understood in accordance with directive 1998/34/EC (as amended by directive 1998/48/EC), which according to recital 18 comprises a wide range of on-line economic activities such as services offering on-line information or commercial communications, tools for search,

[14] See e.g. EDRI 2013. Human Rights and privatised law enforcement. Brussels: EDRI. MCNAMEE, J., FIEDLER, K. & EDRI. 2013. *Copyright: challenges of the digital age*. Brussels: EDRI.

access and retrieval of data, services consisting of the transmission of information via a communication network or providing access to a communication network or hosting Internet user-generated information (European Parliament and Council of the European Union, 2000). In other words, the directive is applicable to the services provided by intermediaries such as ISPs, search engines and social media platforms.

Within the context of the directive, the service providers are subject to limited liability for the third-party content they carry, while the third-party itself is directly liable for her/his own communication. Section 4 'Liability of Internet service providers' of the directive stipulates, in Articles 12-14, the conditions under which, information society service providers cannot be held liable for Internet user-generated content, so-called – 'safe harbours'. The framework consists of three liability exemptions based on three types of activities: 'mere conduit',[15] 'caching'[16] and 'hosting'[17]. In other words, the directive protects information society services acting as intermediaries for these activities. Furthermore, Article 15 prevents – to a certain extent – Member States from imposing general monitoring obligations on the service providers involved with the above activities.

The directive harmonises only some aspects of the internal market of electronic communications services. In 2010, during the public consultation on the future of e-commerce within the internal market and the implementation of the directive, it became apparent that although promoting the development of information society services in the EU, the directive gave rise to various challenges, such as fragmentation of the law in question. For instance, problems arose in areas outside the competence of the directive or related to its derogations (European Commission, 2010b). These challenges will be further addressed in section E.2. below.

In January 2012, the European Commission announced a new initiative on 'Notice-and-Action' procedures with a goal to set up a horizontal European framework to combat illegality on the Internet, and to ensure the transparency, effectiveness, and proportionality of the employed procedures, as well as compliance with fundamental rights (European Commission, 2012b). In April 2013, the European Commission launched a follow up on the communication and earlier EU initiatives towards a digital single market with the aim to encourage the EU institutions to fast-track all key legislative acts and adopt them as a priority by Spring 2014 (European Commission, 2013a).[18]

Most recently, steps have been taken towards greater harmonisation in the EU Strategy on the Digital Single Market, launched by the European Commission in May 2015 (European Commission, 2015). The strategy proposes, among others things, to improve cross-border e-commerce and to look into the how to best tackle illegal content on the Internet 'with due regard to the impact on the fundamental right to freedom of expression and information' (European Commission, 2015, paras. 2.1. and 3.3.2.). At the

[15] 'Mere conduit' includes the automatic, intermediate and transient storage of information necessary for carrying out a transmission, such as e.g an Internet intermediary connecting an end-user to the Internet.

[16] The automatic, intermediate and temporary storage of information for the purpose of making its onward transmission more efficient.

[17] The storage of information provided by a user of the service in question.

[18] For further discussion on these developments, please see SPANGENBERG, J. 3 February 2015. The EU Notice & Action Initiative: Recent Developments [Accessed 11 September 2015].

same time, the analysis will also include 'whether to require intermediaries to exercise greater responsibility and due diligence in the way they manage their networks and systems – a duty of care' (Ibid.).

In an open letter of 27 April 2015 to Vice-President of the European Commission, Andrus Ansip, several civil society organisations – such as e.g. European Digital Rights (EDRI), Article 19 and Digitaleurope – welcomed greater harmonisation and transparency in the implementation of the directive, yet they encouraged the European Commission – as a minimum – to reaffirm and preserve the basic principle underpinning the E-commerce directive of a strong protection of the intermediaries from liability for third party content. Also, they strongly opposed any new duty of care requirements for intermediaries to proactively monitor, judge or remove potentially illegal third party content on networks and hosting platforms (EDRI and others, 2015).

Although the above organisations seem in favour of the limited liability 'principle' underpinning the directive, the analysis below will illustrate, that the liability provisions and their scope of application are not as clear cut as they might seem. This is clearly illustrated by the recent Delfi-case, in which the ECtHR – despite the principles of the directive – seems to expand the duty of care responsibilities of the service providers (*Delfi AS v. Estonia*, 2015). Such ambiguities may lead to over-blocking of content with a negative impact on freedom of expression, as the service providers might prefer to take down or block content rather than – potentially – face liability charges.

2. Directive 2011/93/EU on Combating the Sexual Exploitation and Sexual Abuse of Children and Child Pornography

Blocking of online content related to the sexual abuse and exploitation of children has been high on the EU's Internet policy agenda since the mid-nineties when the European Commission adopted a *Communication on Illegal and Harmful Content on the Internet* (European Commission, 1996a) and a *Green Paper on the Protection of Minors and Human Dignity in Audio-Visual and Information Services* (European Commission, 1996b). While the early approach left control of illegal content to Member States and self-regulation by the industry, from 2006 onwards the approach prevailed towards co-regulation, specifically the imposition of blocking (Tambini, 2008, p. 28, McIntyre, 2010, p. 210ff.) Moreover, in the same period, several self-regulatory regimes were established in the Member States, notably the UK and the Nordic countries. A brief introduction follows below.[19] For an elaboration of the origins of online child protection, see e.g. Villeuve (Villeuve, 2010).

The UK was one of the first EU Member States to establish a self-regulatory model that has since inspired many other countries. In 1996, the Metropolitan Police notified the Internet Service Providers Association (ISPA) that newsgroup content hosted by UK ISPs contained indecent images of children,

[19] For a further elaboration of the origins of child protection, reference is made to VILLENEUVE, N. 2010. Barriers to Cooperation: An Analysis of the Origins of International Efforts to Protect Children Online. *In:* DEIBERT, R., PALFREY, J., ROHOZINSKI, R. & ZITTRAIN, J. (eds.) *Accessed Controlled: The Shaping of Power, Rights, and Rule in Cyberspace,* Cambridge, Mass. & London, United Kingdom: MIT Press. 55-70.

which the Police believed constituted a publication offence by the ISPs under British law.[20] The Police threatened to seize British ISPs' servers if these groups were not blocked (Brown, 2010, p. 3). In response, the ISPs set up the Internet Watch Foundation (IWF) to operate a telephone hotline to receive reports from those who had come across illegal abuse images online. The IWF assesses the legality of the content according to UK law and passes on reports on illegal content to UK ISPs who remove it from their servers. As regards overseas ISPs, reports are sent to foreign police via the Child Exploitation and Online Protection Centre.[21] Following heavy government pressure, most UK consumer ISPs block customer access to web pages blacklisted by the IWF (Brown, 2010, p. 4).[22]

The UK self-regulatory model has been widely followed around the world, although the lists of illegal content are often maintained by law enforcement (co-regulation), rather than independent organisations. In Denmark, for instance, the National Police, Save the Children Denmark *(Red Barnet)* and the Danish Telecommunications sector has collaborated since 2005, and is part of the Danish Safer Internet Centre (Insafe Network).[23] According to the Danish model, alleged child pornography may be reported to a hotline organised by Save the Children Denmark who perform a legality assessment. On that basis Save the Children Denmark forwards the information to the national police (Centre for Cyber Crime) or similar hotlines abroad. The police may also be contacted directly. If the police find that the content is illegal under the Danish Criminal Code, the ISPs will block access to the concerned website according to a voluntary agreement between the involved parties[24] In consequence, no court or independent administrative authority assess the legality/illegality of the content, and due to the voluntary agreement no authority can be held responsible for the blocking in question.

Since 1999, the European Commission has funded the Norwegian CIRCAMP law enforcement network (Cospol Internet Related Child Abusive Material Project), which has developed a blocking system for ISPs called the Child Sexual Abuse Anti Distribution Filter (Brown, 2010, p. 4).

Scholars and activists have continuously warned that automatic blocking without judicial intervention based on secret blacklists may cause freedom of expression violations (McNamee and EDRI, 2010, Korff, 2014). The leak of a number of countries' blacklists reveals that concern is justified, as they contain not only illegal, but also legal content that have been mistaken for being illegal (Brown, 2010, p. 4). Furthermore, the blocking systems seem to have little impact on the sharing of child abuse images, since end-users as well as criminals can easily circumvent blocking criminals (McNamee and EDRI, 2010, p. 6). As a result, blocking does not prevent file sharing and sexual abuse of children. Nevertheless, in 2010, the European Commission suggested to extend mandatory blocking systems across Europe. The original

[20] For further elaboration, please see Internet Watch Foundation, Available from <www.iwf.org.uk/about-iwf/iwf-history> accessed 10 November 2015.

[21] Now a National Crime Agency Command Child Exploitation and Online Protection Centre (NCA-CEOP).

[22] For specific cases, see also BENEDEK, W. & KETTEMANN, M. 2014. *Freedom of Expression and the Internet,* Strasbourg, Council of Europe, p. 119.

[23] For information on the Danish Safer Internet Centre, see http://www.saferinternet.org/denmark.

[24] For further information, please see the Danish National Police: www.politi.dk/da/borgerservice/boernepornofilter/om_blokering.htm, RED BARNET 2015. *Hvor slemt ka' det være – En antologi om it-relaterede seksuelle overgreb på børn og unge*. and http://stopdigitaleovergreb.nu/redbarnet/ressourcer/antologi-om-digitale-overgreb.

proposal to what became directive 2011/93/EC on combating child exploitation, suggested to make blocking mandatory (European Commission, 2010a, Article 21). Throughout the legislative process, it remained unclear whether the European Commission was seeking to prevent deliberate access to illegal content, or accidental access to the content.[25] No evidence was produced – for example, from countries that currently use blocking – to show that one or other legitimate aim, or both aims (or a different aim) would be achieved to any appreciable extent (Korff, 2014, p. 71). The proposal to make blocking mandatory was, however, discarded in the end (Jørgensen, 2013, p. 115).

The directive on combating the sexual abuse and sexual exploitation of children and child pornography (child pornography directive) was adopted on 13 December 2011 and replaced an earlier framework decision (The European Parliament and the Council of the European Union, 2011). It seeks to establish minimum rules concerning the definition of criminal offences and sanctions within sexual abuse and exploitation of children and introduces provisions to strengthen the prevention of such crimes and the protection of the victims, cf. Article 1.

Pursuant to Article 25, Member States shall take all necessary measures to ensure the prompt removal of web pages containing or disseminating child pornography hosted in their territory, but also endeavour to obtain the removal of such pages hosted outside their territory. Under certain conditions, Member States also have the possibility to block access to webpages containing or disseminating child pornography towards Internet users within their territory. It is also worth noting that, on 11 March 2015, the European Parliament adopted a resolution on online child abuse (The European Parliament, 2015) which reiterates that any illicit content must be promptly removed and reported to the authorities.

According to recital 47 of the directive, Member States can use legislative, non-legislative, judicial or other measures in order to comply with their obligations under the directive and it is without prejudice to voluntary action by the industry. Yet, blocking is not framed as a freedom of expression issue, although recital 47 requires that account is taken to the rights of the end-users (the rights of the intermediaries are not mentioned) and that Article 25 requires that such measures provide adequate safeguards, such as proportionality, as well as user information regarding the reason for the restriction and the possibility for redress. In this context, it should be noted that the former UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has stressed that child pornography is one clear exception where blocking measures can be justified, provided that the national law is sufficiently precise, and there are effective safeguards against abuse or misuse, including oversight and review by an independent and impartial tribunal or regulatory body. However, concern is also raised that states tend to rely on these blocking measures, rather than focusing on those responsible for the production and dissemination of the material (La Rue, 2011, para. 32)

[25] The question is whether accidental access to illegal content is a major problem worth spending resources on compared to preventing deliberate access to the content concerned or to punish the crimes that led to the file sharing. This is also elaborated on in MCNAMEE, J. & EDRI. 2010. *Internet Blocking: Crimes should be punished and not hidden*. EDRI, Brussels.

It might prove difficult to ensure proper safeguards if blocking is introduced through self-regulation such as voluntary codes of conduct, in particular as the directive offers no guidance on the matter. Furthermore, as the trend moves towards invisible and unaccountable censorship (McIntyre, 2010, p. 219), which is built into the communication infrastructure (Balkin, 2014), the proportionality assessment that human rights law requires might also prove difficult from a technical point of view. Illegal content related to sexual abuse of children is a legitimate target for content take-down or blocking, yet the measures taken must still comply with the three-step test of Article 10(2) of the ECHR. The above factors may thus have a severe impact on freedom of expression.

3. Directive 2004/48/EC on IPR Enforcement

For more than a decade, the music and film industries have searched for solutions to fight alleged copyright infringements e.g. through online file sharing in peer-to-peer networks. In the beginning, the industries tried to solve the problem through lawsuits against file sharers but increasingly, the industries try to find ways to disconnect users and websites accused of infringements. The industries now encourage Internet intermediaries to filter the Internet access of their users, block access to peer-to-peer software and introduce 'three strikes' schemes in which users are cut off after three unverified allegations of copyright infringements based on codes of conduct. However, such mandatory self-regulatory schemes have had mixed success (Brown, 2010, p. 3). See also (McNamee, Fiedler and EDRI, 2013, EDRI 2013)

To prevent intellectual property rights (IPR) infringements, the EU has adopted Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society (copyright directive) (European Parliament and Council of the European Union, 2001) and Directive 2004/48/EC on IPR enforcement (European Parliament and Council of the European Union, 2004). The latter concerns the measures, procedures and remedies necessary to ensure IPR enforcement, cf. Article 1. It imposes on Member States an obligation to ensure that judicial authorities may issue provisional and precautionary measures, corrective measures, such as e.g. destruction or recall from commercial channels, injunctions, pecuniary compensation and damages (Articles 9-13), and allows Member States to apply other appropriate sanctions in cases of IPR infringements (Article 16).

The directive is without prejudice to the liability exemptions and the prohibition against a general monitoring obligation pursuant to Articles 12-15 of the E-commerce directive. Consequently, national authorities are prohibited from adopting measures which would require an intermediary to carry out general monitoring of the information that it transmits on its networks (Case C-70/10 *SABAM v. Scarlet Extended*, 24 November 2011, para. 34). Pursuant to Article 17 and recital 29, the directive, however, imposes on Member States an obligation to encourage the industry to take an active part in the fight against piracy and counterfeiting and to develop codes of conduct.

Hence, the directive poses various challenges. Firstly, although recital 32 recognises the respect for fundamental rights, it focuses mainly on IPR protection. However, to the extent that alternative measures imposed by Member States or intermediaries involve blocking and filtering, interferences with freedom of expression are likely to occur. Yet, the directive does not offer any guidance on how to resolve them. Secondly, the directive encourages the industry to play an active role in the fight against

IPR infringements, in particular through the development of codes of conduct and thereby through self-regulation.

Besides lack of compliance with the rule of law and the three-step test in Article 10(2) of the ECHR, this may lead to massive blocking of legitimate file exchanges as the intermediaries are not necessarily in a position to assess whether a specific use of IPR protected work is legitimate or to perform a proper balancing of rights as required when a conflict of rights occur. Furthermore, although Member States must refrain from imposing general monitoring obligations on the intermediaries, according to the E-commerce directive, they are not prevented from encouraging the intermediaries to impose it on themselves.

During the public consultation on the review of the EU copyright rules, the role of the internet intermediaries was debated, including whether their obligations should be increased or not. The collective management organisations across the creative sectors stressed that the intermediaries should be more actively involved in addressing copyright infringements. They argued, that the problem lay within the safe harbour regime of the E-commerce-directive – as the intermediaries had no liability under the safe harbour regime, they could afford not to provide information about the original copyright infringer (European Commission, 2014, p. 85), while others, including some intermediaries, found the current legal framework (the IPR enforcement directive combined with the E-commerce directive) sufficient (European Commission, 2014, p. 88). EDRI, for instance, underlined the importance of the limited liability scheme to prevent the risk of censorship and restrictions to freedom of expression and information (EDRI, 2014 p. 39)

In sum, the three directives pose a number of human rights ambiguities and concerns, whereof only those with an impact on freedom of expression and the rule of law are addressed in this study. With regard to the E-commerce directive, the focus is on the potential negative impact of the liability and safe harbour provisions (Articles 12-14) as well as the provision related to the prohibition of general monitoring (Article 15). Regarding the child pornography directive, particularly the provision on removal or blocking of web pages (Article 25) in the context of recital 47, according to which Member States can use both legislative, non-legislative, judicial or other measures, including voluntary action by the industry, to comply with the directive. Finally, in relation to the directive on IPR enforcement, focus is on the provisions that not only accept, but encourage the industry to play an active role in fighting copyright infringements and to develop codes of conduct (Article 17 and recital 29).

E. Human Rights Challenges Related to Co- and Self-Regulation in the Field of EU Content Regulation

The examples of EU regulation in section D above show that content regulation in the online sphere has either tended towards self-regulation, such as the EU's approach in the mid-1990s when dealing with online distribution of child pornography, or towards co-regulation, such as the underpinning principle of the limited liability scheme in the E-commerce directive. The EU approach is based on the intermediaries playing an active role in implementing public policy or in some cases even developing the norms and enforcement mechanisms themselves.

As described in section C.2., the situations where the state itself applies filters or blocks content are rather straight-forward, at least from a human rights perspective. Although likely to constitute severe human rights violations, the legal basis is accessible and restrictions to freedom of expression and information of the intermediaries, speakers and end-users is accordingly more foreseeable and last, but not least, attributable to the state. In contrast, when the role of the state becomes less formal or indirect as it is in the case of voluntary filtering regimes, several concerns arise.

As mentioned, the debate on co- and self-regulation in an EU context is not new, yet with the new Digital Single Market Strategy and recent Internet-related ECHR and CJEU case law, the related human rights challenges are more relevant than ever.

1. Vertical and Horizontal Human Rights Conflicts

As illustrated by the EU directives addressed in section D, EU Member States are obligated to take action in order to combat alleged child sexual abuse material, copyright infringements, and illegal content more generally. Moreover, the directives either accept or suggest that such action is taken through co- or self-regulatory frameworks. Internet intermediaries are thus encouraged or forced to assist Member States in dealing with alleged illegal content. However, as the practices of the intermediaries are established through co- or self-regulatory frameworks, they often have no legal basis, and although such schemes seem more flexible than traditional regulatory schemes, they tend to lack transparency, procedural fairness and protection of fundamental rights. Moreover, the decisions to sanction users are taken administratively rather than judicially. As argued by some scholars, current practices imply that intermediaries are *de facto* being used to implement public policy with limited oversight:

> 'Internet Service Providers are commercial profit-making entities who are increasingly being asked to implement social policy without appropriate oversight or accountability. They operate in a very confusing situation with regards to competing and sometimes contradictory legal requirements. For example between providing high levels of quality of access to the Internet, on the one hand, and blocking access to services, on the other' (Callahan et al., 2009, p. 35).

Before getting deeper into these challenges, some preliminary definitions need to be established on co- and self-regulation.

As mentioned, the concept of 'co-regulation' is a legal model in which the drafting, implementation and enforcement of norms is not under the sole authority of the state, but spread, voluntarily or not, between both public and private players. In a more rigorous sense, 'co-regulation' embraces a new form of governance for public authorities based on voluntary delegation or transfer of all or some part of drafting, implementation and enforcement of norms (Frydman et al., 2008, p. 1). 'Co-regulation' can also be referred to as 'privatised law enforcement' (Korff, 2014, p. 85), and may either be restricted to cover regulation that contains a legally formalised role of public authorities (Hoboken, 2012, p. 140), or include state participation in a broader sense:

> 'A regulatory regime involving private regulation that is actively encouraged or even supported by the state through legislation, funding or other means of state support or

> institutional participation, has come to be known as 'co-regulation'' (MacKinnon et al., 2014, p. 56).

'Co-regulation' differs from a 'command and control' model, in which drafting, implementation and enforcement is solely on the hands of public authorities, but also from a 'self-regulation' model, in which private actors make the rules and enforce them, often defined and enacted via codes of conduct (Schulz and Held, 2001, p. A-2), without any public intervention. The UK model for countering online distribution of child pornography, for instance, as described in section D.2., falls within the notion of self-regulation.

Pressure on private entities can be more or less formal and be imposed, for example, by indicating, that liability schemes will be introduced or that the activities of the intermediaries will be seized in the absence of self-regulation ('raised eyebrow technique'). The latter approach was used in the UK in the mid-nineties to 'encourage' blocking of content related to child pornography as described in section D.2. (Brown, 2010, p. 3).

The directives do not themselves provide for common EU procedures for dealing with alleged illegal content, but set up some limits and provide suggestions for possible national means to obtain the goals enlisted in the three directives. Articles 12-14 of the E-commerce directive, for instance, do not provide for a liability scheme to be implemented in the Member States. Instead, as described in section D.1., they provide for 'safe harbours', meaning situations in which Member States cannot impose liability on the intermediaries for third party content. This is most likely linked to the procedural freedom of the Member States, but as a result, the liability schemes vary from Member State to Member State, making the online landscape harder for the intermediaries to navigate in. Consequently, when Member States are free to decide on and deal with such complex matters, they need guidance. The public consultation on the E-commerce directive in 2010 showed great fragmentation with respect to implementation (European Commission, 2010b) and the Commission received several critical comments from civil society organisations (EDRI, 2010, Article 19, 2010) as further addressed in the Commission Staff Working Document on a coherent framework to boost confidence in the Digital Single Market of e-commerce and other online services (European Commission, 2012a). Also, in relation to the launch of the Digital Single Market Strategy, civil society organisations have encouraged further harmonisation in this area (EDRI and others, 2015).

As mentioned, the European system of co-regulation was set up by the E-commerce directive, according to which the intermediaries are protected from liability, if they take down alleged illegal content expeditiously upon notification (Articles 12-14) and thereby implement public policy. However, due to increasing pressure on intermediaries, co-regulation can easily lead to self-regulation, in particular as voluntary action is either accepted or encouraged. This is the case, for instance, with the child pornography directive. From Article 25 of the directive, it follows that the Member States shall take all necessary measures to ensure the prompt removal of websites containing or disseminating child pornography (para. 1), and that Member States may take measures to block such webpages (para. 2). Recital 47 supplements (to Article 25) that 'all necessary measures' may include voluntary action taken by the Internet industry. Although the directive does not encourage self-regulation, it clearly accepts it. The IPR directive goes even further on this account, as it follows from Article 17 and recital 29 of the

directive that the industry should play an active part in the fight against piracy and counterfeiting by developing codes of conduct, and that Member States should encourage such voluntary action. In this sense, the IPR directive not only accepts self-regulation, but actively supports it.

The directives thus shift from self-regulation being presupposed as a more or less accidental result of a co-regulatory framework (the E-commerce directive) towards self-regulation as an accepted means to obtain EU-law compliance (the child pornography directive) to impose on Member States to encourage self-regulation (IPR enforcement directive).

As described above in section C.2., in the case of mandatory blocking and filtering, the human rights conflict remains a *vertical conflict* between the state and the intermediary, the speaker or the end-users. In contrast, content regulation in a pure self-regulatory scheme remains a *horizontal conflict* between the intermediary who imposes content restrictions and the speaker who is subject to it.

However, in practice, these issues are extremely complex. For example, does active coercion of intermediaries to 'voluntarily' filter or block content, in the absence of a legal duty to do so, comply with Article 10(2) of the ECHR (or are even covered by the provision as a human rights issues), according to which such restrictions must be prescribed by law?; and at what stage is state attribution reasonably triggered, when freedom of expression violations occur on the basis of 'voluntary' measures taken by the intermediaries following state encouragement to do so?

The more informal the role of public authorities, the more difficult it is to argue that limitations to freedom of expression derive from public authorities and thus constitute 'interferences' (in a legal sense) with freedom of expression and information. Likewise, it is often difficult to argue that they fall within the positive obligations of the state (as discussed in Section C.2.b.) unless individuals are prevented from effectively exercising their right to freedom of expression and information, or when pluralism of the information environment would be clearly at stake (Hoboken, 2012, p. 148f.). In other words, as mentioned in section C.1., the ECtHR puts weight on the nature and scope of restrictions on expression rights and the ability of alternative venues for expression. Furthermore, account must also be taken of the capability of the rights at stake to contribute to public debates (*Appleby and Others v. the United Kingdom*, 2003, paras. 42-43 and 47-49). As a result, limitations of content with no or little public interest, is less severe from a human rights perspective than limitations of content of public interest. This must be kept in mind when assessing whether the positive obligations of states can be evoked.

Scholars have suggested, that states could be held accountable (through positive human rights obligations) for failing to ensure that private actors do not violate human rights (Lagoutte, 2014 p. 9). Also, they have an obligation to ensure that general terms and conditions of private companies that are not in accordance with international human rights law must be held null and void (Korff, p. 16 and 63). In terms of international human rights law, states are responsible if, within their jurisdiction, there are systems in place that *effectively* restrict freedom of opinion, expression and information. As a result, although Article 10 of the ECHR only refers to interferences by public authorities, states cannot simply disown measures (blocking, filtering etc.) by private entities that have such effects – especially not if the state de facto strongly encouraged those measures. In such circumstances, the state is responsible for

not placing such a system on a legislative basis: without such a basis, the restrictions are not based on law (Korff, 2014, p. 73) and do not meet the three-step rule of law test:

> 'There are serious doubts as to whether a blocking system that effectively imposes a restriction on most ordinary people's access to online information will ever be in accordance with the rule of law when it is chosen and operated by private parties, in the absence of public scrutiny, in the absence of a democratic debate, in the absence of a predictable legal framework, in the absence of clear goals or targets, in the absence of evidence of effectiveness, necessity and proportionality, and in the absence, either before or after the system is launched, of any assessment of possible counter-productive effects.' (Korff, 2014, p. 72)

However, as discussed in section C.2.b., it is quite complex to establish 'when' an individual is effectively prevented from exercising his/her right to freedom of expression and information and thus, when the positive human rights obligations of the state are triggered.

Despite these challenges, the three EU directives either accept or require blocking, filtering or take down of content, yet none of them frames such measures as limitations of/interference with freedom of expression. This might explain why self-regulation continues to be widely promoted by EU regulators, although it – from a rule of law perspective – is inherently imperfect, as it will always lack the legal basis required to comply with Article 10(2) of the ECHR. Moreover, it seems self-contradictory that the EU claims, in the EU Human Rights Guidelines on Freedom of Expression Online and Offline (in relation to its external policies), that the EU will work against any attempts to block, jam, filter, censor or close down communications networks or any kind of other interference that is a violation of international law (Council of the European Union, 2014, para. 33).[26] Clearly, such a principle must apply externally as well as internally.

Furthermore, even where the EU has intended certain safeguards, this might prove difficult to the state to ensure when the measures are introduced through voluntary action, and particularly when the directive offers no guidance to the matter. This is the case, for instance, with the child pornography directive, which requires, e.g. that account is taken of the rights of the end users, and that the measures imposed provide for adequate safeguards, cf. Article 25(2) and recital 47 of the directive. In recital 47, reference is made to the general human rights obligations of the ECHR and the CFREU, but without specific reference to the relevant provisions, such as e.g. Article 10 of the ECHR and Article 11 of the CFREU.

Another critical aspect of self-regulation is that the Internet intermediaries to whom regulatory or judicial power is delegated are not the best placed to assess whether an allegation of illegal content is well founded. For example, the intermediaries are not necessarily equipped to assess whether a specific use of an IPR protected work is illegal, or whether content believed to be child pornography is in fact so, for instance, are the persons involved minors, is it pornographic etc. The intermediaries are therefore likely to rely on a request to block or take-down content without challenging it, in particular when the

[26] The EU Human Rights Guidelines on Freedom of Expression Online and Offline is further elaborated on in Chapter III, Section D.

notice and take-down scheme in place contains liability provisions for illegal third-party content. As a result, if the intermediaries are encouraged or coerced to disable access to content which is in fact legal, the measure does not follow a legitimate aim. Or if the content is illegal, the measure might result in over-blocking (lack of targeting), in which case it does not meet the strict criteria of proportionality required by Article 10(2) of the ECHR.[27]

Furthermore, measures with an impact on fundamental rights, specifically blocking and filtering of Internet sites, cannot be said to be 'necessary' and 'proportionate' to a 'legitimate aim' in a 'democratic society' if they are unsuited to achieve the intended aim, excessive in their effect and lacking in procedural safeguards. For example, blocking of content related to sexual exploitation of children: (i) does not stop either sexual abuse of children or the sharing of images of such abuse; (ii) does stop access to legal sites; (iii) is based on secret criteria or lists that do not have the quality of a 'law' in the ECHR sense; and (iv) is not subject to adequate and appropriate systems of appeal and remedy. This harms the rights to freedom of expression and information for both those whose sites are wrongly blocked and for those who are effectively missing out on what may well be relevant, or even important, information (for instance, on sexual or gender problems or sexual health) (Korff, 2014, p. 74, McNamee and EDRI, 2010).[28]

In sum, the examples indicate that within the EU, focus seems to be more on the (perceived) effectiveness that such schemes provide for in the fight against IPR infringements and distribution of child pornography (as well as other forms of alleged illegal content), than the human rights conflicts and rule of law concerns raised by such self-regulatory practices.

2. Intermediary Liability

As described above, intermediaries are under an increasing pressure to intervene with respect to alleged illegal content. Such pressure can also occur through schemes of intermediary liability. Generally speaking, provisions on intermediary liability codify government expectations for how an intermediary must handle 'third-party' content or communications. Within the EU, the E-commerce directive stipulates the conditions under which information society service providers cannot be held liable. However, the liability scheme of the E-commerce directive causes various challenges:

> 'As the amount of digital content available on the Internet grows, current arrangements are likely to be increasingly tested. It is not always easy to define the limits on what intermediaries can do with the content that they transmit, store or host before losing the possibility to benefit from the exemptions from liability set out in the e-Commerce Directive' (European Commission 2015, p. 12).

As we will illustrate below, the lack of clearly defined liability provisions in the directive put pressure on the intermediaries to act as 'gatekeepers' of the online sphere. Concerns have been raised that

[27] Presupposed that these limitation can be attributed to states in such a manner that it constitutes 'interferences' by public authorities and fall under the protection of Article 10 of the ECHR.

[28] See also LUMEN (BERKMAN CENTER FOR INTERNET AND SOCIETY, HARVARD UNIVERSITY), Available at: <https://cyber.law.harvard.edu/research/chillingeffects> accessed 18 November 2015.

intermediaries are being used to implement public policy with limited oversight and accountability, with severe implications on the right to freedom of expression and information (Callahan et al., 2009, p. 35).

At a general level, 'gatekeepers' are entities that decide what shall or shall not pass through a gate (Laidlaw, 2012, p. 44). Within regulatory studies, gatekeepers are non-state actors with the capacity to alter the behaviour of others in circumstances where the state has limited capacity to do the same. When regulation no longer has its centre or origin within the state, this is referred to as 'decentralised regulation' (Morgan and Yeung, 2007, p. 280). What makes gatekeepers unique is that they usually do not benefit from the misconduct they facilitate although they are in a position to prevent it. Therefore, it can prove more effective to shape a liability regime around gatekeepers as opposed to those breaking the rules (Laidlaw, 2010, p. 264).

Hence, gatekeeping theory has been used to describe the tort doctrine of vicarious liability, such as e.g. liability for accountants and lawyers for their clients. One of the areas in which the concept has been developed the most is the area of mass media, in particular the role of journalists and press institutions as gatekeepers of information (Laidlaw, 2010, p. 264). Most recently, vicarious liability has been imposed on Internet intermediaries to target e.g. peer-to-peer providers such as Napster and Pirate Bay for copyright infringements caused by illegal downloading by their users and in relation to the notice and takedown provisions of the E-commerce directive, which will be discussed below.

Traditionally, in the EU Member States – as in many other countries – intermediaries are protected from liability for user-generated content, also in relation to hosting webpages, as long as they take down alleged illegal material upon notice. The European approach consists of a limited liability scheme, which primarily creates 'safe harbours' of conditional exemptions from liability. In contrast to the US approach, the E-commerce directive does not differ liabilities at a criminal or civil level, and whereas the US favours a *vertical* approach regulating legal issues related to the infringement of a specific right, the directive follows a *horizontal* approach defining one set of general rules applicable to any content; child pornography, IPR infringements etc. (Frydman et al., 2008, p. 6). During the 2012 public consultation on a Clean and Open Internet, concern was raised by civil society organisations, such as EDRI and Netzpolitik, about the 'one size fits all' approach towards civil and criminal liability as it will lead to some content being handled in a disproportionate manner. Intermediaries cannot be expected to judge if material is potentially in breach of civil law or criminal law, and differentiate between criminal law systems of all Member States (Kuczerawy, 2015, p. 52, EDRI, 2012, Netzpolitik, 2012). When facing liability, in case illegal content is not removed or access to it disabled expeditiously, an intermediary may be tempted to rely on a notification and block rather too much than too little.[29]

[29] See also EUROPEAN COMMISSION 2012b. Commisssion Communication to the European Parliament, the Council, The Economic and Social Committee and the Committee of the Regions. A coherent framework for building trust in the Digital Single Market for e-commerce and online services. Brussels: European Commission. EUROPEAN COMMISSION 2012a. Commission Staff Working Socument. Communication from the Commission to the European Parliament, the Council, the European Economic ans Social Committee of the Regions. A coherent framework to bost confidence in the Digital Single Market of e-commerce and other online services (SEC(2011) 1641 final). Brussels.

Pursuant to Article 12 of the E-commerce directive, an intermediary acting as mere conduit, is protected from liability if it does not *initiate* or *actively interfere* with the transmission. Under Articles 13 and 14 of the directive, both 'caching' and 'hosting' is exempted from liability under certain conditions. For caching, the intermediary is protected from liability, if it does not actively interfere with the transmission and acts expeditiously to remove or disable access to information, upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, access to it has been disabled or that a court or administrative authority has ordered such removal or disablement. For 'hosting', the intermediary is not liable for information stored on the request of a user, if it does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent, and if the intermediary, upon obtaining such knowledge or awareness, acts expeditiously to remove it or disable access to it.

Furthermore, Article 15 of the E-commerce directive prevents Member States from imposing obligations on the intermediaries to generally monitor the information that they transmit or store, or to actively seek facts or circumstances indicating illegal activity. Nevertheless, Member States may compel the intermediaries to promptly inform the competent public authorities of alleged illegal activities or information provided by their users, or to communicate to the competent authorities, at their request, information enabling the identification of users with whom they have storage agreements (European Parliament and Council of the European Union, 2000).

However, the European approach to liability as stipulated in the directive entails various challenges.

First, as discussed extensively by e.g. Hoboken (Hoboken, 2012), the liability distinctions of the directive are not clearly defined. In order to benefit from a safe harbour, the intermediary has to act 'expeditiously' to remove or to disable access to the information concerned, upon obtaining 'actual knowledge' of the illegality (as regards criminal liability) or 'awareness of facts or circumstances´ from which the illegal activities or information is apparent (as regards civil liability) (Articles 13 and 14). The meaning of these terms remain, however, unclear,[30] and thus, the limits of the safe harbours, as also stressed in the Digital Single Market Strategy (European Commission, 2015, para. 3.3.2). Furthermore, the interpretation of these conditions often differs across borders, leading to legal fragmentation (European Commission, 2012a, p. 32ff.). Such unclear conditions for liability exemptions create strong incentives for over-compliance.

Second, the safe harbours of the directive concern only liability, but do not protect the intermediaries from litigation aimed at injunctions, including actions such as the removal or disabling access to information, cf. Articles 12(3), 13(2) and 14(3). As a result, they do not prevent Member States from forcing the intermediaries to play an active role in law enforcement, or prevent Member States from introducing procedures to disable or remove content. Furthermore, an order to disconnect a specific

[30] As regards the differences between the degree of knowledge in relation to civil and criminal liability, see also KUCZERAWY, A. 2015. Intermediary liability & freedom of expression: Recent developments in the EU notice & action initiative. *Computer Law & Security Review: The International Journal of Technology,* 31**,** 46-56. p. 48.

user or to block access to specific information is not necessarily accompanied by guidance on how to ensure that the measure complies with the principle of proportionality and Article 10(2) of the ECHR.[31]

Third, Articles 12-15 concern intermediary liability with respect to illegal content, yet the question of what counts as 'illegal' content is determined by the national law of the Member States. In relation to caching, it is required that the intermediary does not 'actively interfere' with the transmission, cf. Article 13 of the E-commerce directive. However, if an intermediary, due to government pressure, introduces filters e.g. aiming at restricting access to child pornography according to Article 25 of the child pornography directive or the national implementation of that provision, they might run the risk of increased liability, as they then actively interfere with the transmission. The intermediary is thus cut off from the same safe harbour it is trying to reach.

This paradox related to active interference by the intermediary does not seem to be envisaged by the directive, but has become even more present with the recent *Delfi AS v. Estonia judgment* (*Delfi AS v. Estonia*, 2015). Delfi is the first case, in which the ECtHR examined a complaint related to liability for user-generated content, specifically whether a news portal can be held liable for offensive comments posted on its website by anonymous third parties. The ECtHR agreed with the decision of the national court and found that the news portal could in fact be held liable. The case thus illustrates some important aspects of the limited liability scheme of the E-commerce directive, and seems to increase the responsibilities of the intermediaries. The ECtHR, however, stressed that the findings could not be transferred to discussion forums or social media platforms (Ibid, para. 116)

Delfi AS is the owner of one of the largest Internet news portals in Estonia. Following the online publication of an article on a ferry company, comments, including personal threats and offensive language against the ferry company (of which the majority constituted hate speech) were posted on the website. The comments were taken down upon notification, six weeks after publication, yet defamation proceedings were launched against Delfi for publishing the comments.

Based on the national transposition of the E-commerce directive, Delfi claimed to fall within the safe harbours of the directive. The Government, however, claimed, that Delfi acted – not as an intermediary – but as a media publisher (due to their degree of editorial control). This was approved by the ECtHR, and as a media publisher Delfi could not benefit from the safe harbours of the directive. As a result, one of the key question became whether Delfi had been obliged to remove the comments *before* notification, which depended on three aspects: the context of the comments, the alternative liability of the authors of the comments and the consequences of the domestic proceedings.

The Court referred to the facts: that Delfi was professionally managed on a commercial basis (and actively called for comments to generate revenue from advertisements); that its 'rules of comments' stated that it was prohibited to post such comments (they could be removed and the author restricted from posting further comments); and once posted, the authors could no longer modify or delete them. On these grounds, the Court considered, that Delfi exercised a substantial degree of control over the

[31] See also HOBOKEN, J. V. 2012. *Search engine freedom: on the implications of the right to freedom of expression for the legal governance of web search engines.* Kluwer Law International, p. 129.

comments – an involvement which went beyond that of a purely *passive* service provider (the Court distinguishes between *active* and *passive* intermediaries). Also, as the majority of the authors were anonymous (the Court reiterated the need hereof), the liability could not be placed elsewhere, and the proceedings did not have any severe consequences for Delfi, as Delfi had not, as a result of the judgment, been forced to change its business model or disallow anonymous comments. Moreover, the compensation Delfi had been obliged to pay did not aim at obtaining huge or punitive awards, but was in fact negligible (Ibid, paras. 144-151).

Furthermore, the Court interpreted national legislation in such a way that Delfi had not been obliged to prevent the uploading of comments, in order to avoid liability. It would have sufficed to remove the comments without delay after publication. Combined with the fact that Delfi exercised a substantial degree of control over the comments posted on its portal, the Court considered that the interference with Delfi´s freedom of expression was not disproportionate. The pertinent issue was then whether the national court's finding that liability was justified, based on relevant and sufficient grounds, as the applicant had not removed the comments without delay after publication, . Account was first taken as to whether Delfi had installed filters capable of blocking comments amounting to hate speech. Such filters were installed and the portal had an automatic deletion of certain vulgar words and a notice-and-take down system. Sometimes, the administrators even removed inappropriate comments on their own initiative. Therefore, Delfi had not wholly neglected its duty to avoid causing harm to third parties. The filters, however, had failed to filter the comments in question even though they did not include sophisticated metaphors, hidden meanings or subtle threats. In consequence, the clearly unlawful comments remained online for six weeks (Ibid: Paras. 154-156).

Having regard to the fact that there are ample possibilities for anyone to make his or her voice heard on the Internet, the Court considered that a large news portal's obligation to take effective measures to limit the dissemination of hate speech and speech inciting violence – the issue in the present case – could not be equated with private censorship:

> 'In cases where an individual victim exists, he or she may be prevented from notifying an Internet service provider of the alleged violation of his or her rights. The Court attached weight to the consideration that the ability of a potential victim of hate speech to continuously monitor the Internet is more limited than the ability of a large commercial Internet news portal to prevent or rapidly remove such comments.' (Ibid: Paras. 157-158)

Finally, Delfi had argued that the Court should have due regard to the notice-and-takedown system it had introduced. The Court found that, if such system were accompanied by effective procedures allowing for rapid response, the system could be an appropriate tool for balancing the rights and interests of all those involved in many cases. However, in cases such as the present one, where third-party comments were in the form of hate speech and constituted direct threats to the physical integrity of individuals, the Court considered that the rights and interests of others and of society as a whole would entitle Member States to impose liability on Internet news portals, if they fail to take action to

remove clearly unlawful comments without delay, even without notice from the alleged victim or from third parties (para. 159), without contravening Article 10 of the ECHR.

Several judges had concurring or dissenting opinions reflecting their sincere concerns about the implications of the judgment. Some judges claimed that it approved a liability system that imposes a requirement of constructive knowledge on *active* Internet intermediaries (hosts who provide their own content and open their intermediary services for third parties to comment on that content):

> 'We find the potential consequences of this standing troubling. The consequences are easy to foresee. For the sake of preventing defamation of all kinds, and perhaps all 'illegal' activities, all comments will have to be monitored from the moment they are posted. As a consequence, active intermediaries and blog operators will have considerable incentives to discontinue offering a comments feature, and their fear of liability may lead to additional self-censorship by operators. This is an invitation to self-censorship at its worst.' (*Delfi AS v. Estonia*, 2015, Joint Dissenting Opinion of Judges Sajó and Tsotsoria, para. 1).

With a direct reference to Jack Balkin, mentioned in section C.2., these judges stressed, that although governments do not directly intend to censor expressions, by putting pressure and imposing liability on the intermediaries who control the communication infrastructure, they are actually creating an environment in which 'collateral' or private-party censorship is the inevitable result.[32] When an intermediary is liable for content generated by its users, it has strong incentives to self-censor, limit access and deny users access to communicate via the platform in order to avoid liability. As a result, the fear of liability may cause the intermediary to impose prior restraints on its users' expressions/information. Also, the practices entail limited procedural safeguards as action is taken not by a court, but private parties (*Delfi AS v. Estonia*, 2015, Joint Dissenting Opinion of Judges Sajó and Tsotsoria, para. 3).

By confirming that Delfi should have *prevented* or rapidly removed the comments, the ECtHR seems to accept both pre- and post-publication liability. A duty to remove offensive comments without actual knowledge of their existence, immediately after publication, in fact imposes on active intermediaries (as news portals or blogs) an obligation to monitor all comments. Such obligation does not differ from imposing prior restraints (*Delfi AS v. Estonia*, 2015, Joint Dissenting Opinion of Judges Sajó and Tsotsoria, paras. 34-35). The Court found that the filtering mechanisms were insufficient, but it did not define the appropriate level relevant for the case, which could have served as future guidance.

Some judges argued that the strict liability imposed on the news portal is closely linked to the clear defamatory and illegal nature of the content (*Delfi AS v. Estonia*, 2015, Concurring Opinion of the Dissenting Judges Raimondi, Karakas, De Gaetano and Kjølbro). The intermediaries, however, are still required to monitor all content in order to prevent manifestly illegal content from being published or to

[32] Collateral censorship 'occurs when the state holds one private party A liable for the speech of another private party B, and A has the power to block, censor or otherwise control access to B's speech' BALKIN, J. M. 2014. Old-School/New-School Speech Regulation. *HARVARD LAW REVIEW,* 127**,** 2296-2342.

be able to take it down immediately. To impose such an obligation on the intermediaries is prohibited by Article 15 of the E-commerce directive.

To sum up, the legal uncertainty around the E-commerce directive may lead to the intermediaries blocking and filtering rather too much than too little in fear of facing liability for third-party content. In consequence of the unclear provisions of the directive, and their transposition to the national level, intermediaries may choose over-compliance, and in effect prevent end-users from accessing lawful materials. Such 'over-compliance' implies insufficient targeting, which means that interferences with freedom of expression and information are likely to be disproportionate. The intermediaries are thus motivated to impose restrictions on freedom of expression and information that have not been tested for effectiveness or proportionality and which do not have the predictability of 'law'. Moreover, legal uncertainty can lead to extra-legal pressure on intermediaries to self-regulate by blocking or filtering without challenging requests from public authorities or others to block or take down certain content. As the speakers or end-users who are being blocked or whose content is taken down might not have the resources to challenge the measures, content may be blocked or removed without any – administrative or judicial – review.

Furthermore, if the 'victim' of blocking, filtering or take-down wishes to challenge the decision, these co- or self-regulatory frameworks do not necessarily provide for access to effective remedies, as required by Article 13 of the ECHR. As explained in the CoE Guide to human rights for Internet users, there should be a national authority tasked with deciding on allegations of violations of the rights guaranteed in the ECHR. It may not necessarily be a judicial authority, as long as it presents guarantees of independence and impartiality. Effective remedies can also be obtained directly from the intermediaries, although they may not enjoy sufficient independence to be compatible with Article 13 of the ECHR. Therefore, according to the CoE guide, states should, as part of their positive obligations to protect individuals against violations of human rights by private actors, take appropriate steps to ensure that when such violations occur those affected have access to judicial and non-judicial mechanisms (Council of Europe, 2014d, para. 101ff.). However, if the state accepts or even encourages self-regulation, as described above, it might prove difficult to ensure that such mechanisms are in place.

Without proper control or review mechanisms and with no challenge of the decisions to block or take down content, nothing prevents potential human rights violations. Although recital 9 of the E-commerce directive ties the free movement of information society services to Article 10 of the ECHR (freedom of expression and information), and Recital 46 stipulates that with regards to 'the removal or disabling of access to the information concerned; the removal or disabling of access has to be undertaken in the observance of the principle of freedom of expression and of procedures established for this purpose at national level' (European Parliament and Council of the European Union, 2000), it is not sufficient to protect freedom of expression. Particularly not, when the directive has to be transposed into national law without proper guidance, as exemplified with the recent Delfi-case.

3. Human Rights Violations of Private Actors

As explained above in section C, only limitations to freedom of expression imposed by a *public authority* constitute interferences in a legal sense. While limitations to freedom of expression in *vertical* conflicts

constitute 'interferences' that are rather easily attributed to the state (all dependent on how formalised the role of the state is) under its *negative* obligations, *horizontal* conflicts may only be attributed to the state when they fall under the *positive* human rights obligations of the state. States cannot simply escape their positive human right obligations by delegating the responsibility to private parties, but it is not clear when the positive obligations are triggered, as discussed in section E.1. By initiating co- and self-regulatory frameworks for dealing with alleged illegal content, states rely on the Internet intermediaries, while not providing them with proper guidance on the matter. Moreover, and adding to the complexity, there is an increasing focus on the internet companies' own human rights responsibilities, which puts pressure on these private actors to both implement public policy and respect human rights.

The key standard-setting document in this regard is the United Nations (UN) 'Guiding Principles on Business and Human Rights' (UNGPs), drafted by the UN Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, John Ruggie (United Nations Human Rights Council, 2011a).[33] The Human Rights Council (HRC) endorsed the Guiding Principles in Resolution 17/4 (United Nations Human Rights Council, 2011b) in which it also established the UN Working Group on business and human rights.[34] Based on three pillars, ´Protect´, ´Respect´, and ´Remedy´, the principles unpack the distinction between the *state duty to protect human rights* and the *corporate responsibility to respect human rights.*

The first pillar concerns the *state duty to* protect against human rights abuses by third parties, including private companies, which requires that states take appropriate steps to prevent, investigate, punish and redress human rights violations committed by private actors within their jurisdiction through effective policies, legislation and regulations and adjudications (United Nations Human Rights Council, 2011a, paras. 1-10). The UNGPs' state duty to protect is two-fold: (1) a reminder of the international human rights obligations undertaken by states through previous international and regional treaties and conventions; and (2) a set of recommendations to take action in specific ways and matters. It thus consists of both hard-law and soft-law commitments (Lagoutte, 2014, p. 8f.).

The second pillar is the *corporate responsibility to respect human rights*, which implies that private companies should publish a policy commitment to respect human rights and act with due diligence in order to avoid infringing the human rights of others (United Nations Human Rights Council, 2011a, paras. 11-24). Due diligence is envisaged to comprise four steps, taking the form of a continuous improvement cycle (United Nations Human Rights Council, 2011a, paras. 17-20). First, the company must access the actual and potential impacts of business activities on human rights (human rights impact assessment); second, remediate the findings of this assessment into company policies and practices; third, track how effective the company is in preventing adverse human rights impacts; and fourth, communicate publicly about the due diligence process and its results. Companies are expected to address all their human rights impacts, though they may prioritise their actions. The general

[33] The UN Guiding Principles are also discussed in the context of the EU's external policies in Chapter III, Section D and E.

[34] For further information, please see www.ohchr.org/EN/Issues/Business/Pages/WGHRandtransnationalcorporationsandotherbusiness.aspx.

principles recommend that companies first seek to prevent and mitigate their severest impacts, or those where a delay in response would make consequences irremediable (United Nations Human Rights Council, 2011a, para. 24).

The third pillar is on *remedy*, which addresses the need for greater access by victims of human rights infringements to effective – both judicial and non-judicial – remedy (United Nations Human Rights Council, 2011a, paras. 25-31).

The principles do not create new international law obligations, nor do they limit or undermine legal obligations of states under international human rights law (United Nations Human Rights Council, 2011a, General Principles). Rather they elaborate on the implications of *existing* standards and practices for states and businesses in order to provide for a coherent framework that may help bring human rights and business challenges to an end (United Nations Human Rights Council, 2011a, Introduction, paras. 13-14). As such, the principles maintain the primary (hard law) obligation of states to protect against human rights violations. At the same time, however, they give explicit recognition to the (soft law) responsibility of businesses to respect human rights (O'Brien and Dhanarajan, 2015, p. 3).

As only limitations with human rights imposed by a *public authority* constitute 'interferences', cf. section C.1. above, in a strict legal sense, businesses do not 'violate' human rights. They breach environmental law, labour law, criminal law etc. that might be human rights related, as they might occur within the sphere of the state's positive obligations to protect human rights, but they do not violate human rights (Lagoutte, 2014, p. 13). However, they may breach their due diligence responsibilities under the Guiding Principles (United Nations Human Rights Council, 2011a, paras. 11-24).

The HRC has stressed that a company's responsibility to respect human rights is a global standard which 'exists independently of states' abilities and/or willingness to fulfil their own human rights obligations, and does not diminish those obligations' (United Nations Human Rights Council, 2011a, para. 11). This was also reiterated by the former UN High Commissioner for Human Rights, Navi Pillay, in her report on 'The right to privacy in a digital age' to the UN General Assembly:

> 'The responsibility to respect human rights applies throughout a company's global operations regardless of where its users are located, and exists independently of whether the state meets its own human rights obligations' (The Office of the United Nations High Commissioner for Human Rights, 2014, para. 43).

Accordingly, private business enterprises cannot escape their responsibility to respect human rights based on the states' lack of doing so, and states cannot escape their human rights obligations, by delegating powers to private entities or by claiming that these private entities should, but do not, comply with human rights. Although Internet intermediaries have a *responsibility* to assess the human rights impact of their activities in order to minimise their negative human rights impact, states are not 'lifted' from their human rights *obligations*. For instance, if an intermediary implements a filter with a view to block online content related to child pornography, as suggested in the directive on combating child pornography, the company has a responsibility to make a human rights impact assessment (HRIA) of that activity. If the HRIA shows that the filter results in the blocking of perfectly legitimate content,

such activity has a negative human rights impact on the freedom of expression of the speaker or freedom of information of the end-users and should be minimised accordingly. However, the obligation to ensure freedom of expression and information on the state's territory remain with the state, and under certain conditions the state may be held liable for the potential human rights violations caused by the filter.

The effectiveness of the UN Guiding Principles has been widely questioned, yet, they have raised important awareness among businesses to incorporate respect for human rights in their corporations (O'Brien and Dhanarajan, 2015, p. 3). In co- and self-regulatory frameworks dealing with alleged illegal content, intermediaries are entrusted with powers that have a direct impact on users' ability to enjoy freedom of expression and information. However, it is paramount, that states do not use self-regulation by intermediaries as a lever to escape their own – hard law – human rights obligations, nor should they rely on the soft law responsibilities of businesses. During the FRAME milestone workshop in Brussels on 12 June 2015, it stressed, that the UN Guiding Principles are actually very profitable for states, as they move the focus from the state obligations to the (moral) responsibilities of businesses. From a human rights perspective, such a shift in attention from hard law *obligations* to soft law *recommendations*, is obviously a dangerous path, but close to the EU policies described in this study.

In 2013, the European Commission launched an ICT Sector Guide on how companies in the ICT sector could implement the UN Guiding Principles (European Commission, 2013b). The ICT Sector Guide takes into account the state duty to protect human rights and the rule of law and underlines that the states' obligations and the companies' responsibilities are independent of each other. However, if governments are unwilling *or unable* to meet their own human rights obligations, it becomes more challenging for ICT companies to avoid being involved in harm to individuals' human rights. For instance, when Internet intermediaries operate in domestic legal contexts where governments impose restrictions on rights that are not compatible with international human rights law, or where governments request the companies to provide information about users or to block access to specific content or ICT infrastructure for law enforcement purposes (European Commission, 2013b, p. 5 and p. 12f.).

As the intermediaries largely control the online domain, such requests may be necessary in order for the state to meet its *obligation to protect* human rights, for example, in order to counter the distribution of child pornography. However, whenever such request is unlawful, because it lacks a legal basis, is disproportionate etc., this constitutes a direct threat to an intermediary's ability to meet its *responsibility to respect* human rights. In these situations, if the intermediary merely obeys domestic law – or in absence of domestic law – orders of national authorities, this is unlikely to be sufficient in order to demonstrate respect for human rights (European Commission, 2013b, p. 10).[35]

The CoE has also taken steps towards recognising the UN Guiding Principles. In a declaration from April 2014, the Committee of Ministers recognised the responsibility of business to respect human rights and stressed that the effective implementation by both states and business enterprises is essential to respect human rights in the business context (Council of Europe, 2014a). Furthermore, a drafting Group

[35] For similar initiatives, see Global Network Initiative, https://globalnetworkinitiative.org/ and Telecommunications Industry Dialogue, www.telecomindustrydialogue.org/.

for Human Rights and Business is currently elaborating a draft recommendation of the Committee of Ministers on human rights and business (its work is expected to be finalised by the end of 2015) (Council of Europe, 2015, para. 29).[36] Also in acknowledgement of the potential human rights impact of intermediaries, and specifically in relation to ISPs, the CoE, in cooperation with the European Internet Services Providers Association (EuroISPA), has developed guidelines that provide human rights benchmarks for intermediaries (Council of Europe in co-operation with the European Internet Service Providers Association (EuroISPA), 2008).

In sum, there is a clear distinction between the state *duty* to protect and the business *responsibility* to respect human rights. Although intermediaries have a responsibility to assess the human rights impact of their practices, services and products in order to minimise their negative impact on end-users (and others within their sphere of influence), the obligation to protect human rights remains with the state. As such, the UN Guiding Principles have arguably contributed to preserving the legitimacy of human rights through a 're-orientation' of human rights norms. However, as already mentioned, doubts do persist as regards their effectiveness due to their voluntary approach to business responsibilities (O'Brien and Dhanarajan, 2015, p. 3).

Recent scholarship suggests that neither a corporate social responsibility (CSR) model, according to which businesses are responsible for human rights breaches within their sphere of influence, nor the UN Guiding Principles are sufficient to describe the human rights responsibilities of intermediaries in the online sphere. This is due to the intermediaries' role as gatekeepers for a number of practices essential to democratic participation (searching information, expressing opinions, participating in public debate, etc.). As such, individuals have no choice but to engage with intermediaries in order to benefit from the Internet's democratic potential (Laidlaw, 2012, p. 11).

As briefly introduced above in section E.2., gatekeepers are non-state actors with the capacity to alter the behaviour of others in circumstances where the state has limited capacity to do the same, yet they usually do not benefit from the misconduct they facilitate although they are in a position to prevent it.

There is a distinction between Internet gatekeepers, who control the flow of information, and Internet information gatekeepers (IIGs), who as a result of this control, impact participation and deliberation in democratic culture (Laidlaw, 2010, p. 266). Not all 'Internet gatekeepers' can qualify as IIGs, but only those entities, which due to their role, their type of business or technology, or a combination of all of these, have the capacity to impact democracy in a way traditionally reserved for public institutions. When private actors take on roles traditionally reserved for public actors, concern may rise regarding accountability and the protection of human rights. Gatekeepers that have the capacity to impact democratic life are expected to serve the public interest, however IIGs are not imbued with the norms and requirements normally accompanying the exercise of public power. Moreover, they remain relatively isolated from legislative, executive and judicial oversight (Laidlaw, 2012, p. 46).

[36] Furthermore, it should be noted that the Committee of Ministers has also adopted a recommendation on the Council of Europe Charter on shared social responsibilities COUNCIL OF EUROPE COMMITTEE OF MINISTERS 2014b. Recommendation CM/Rec(2014)1 of the Committee of Ministers to member States on the Council of Europe Charter on shared social responsibilities.

To counter this challenge, Laidlaw suggests that the human rights obligations of IIGs should increase according to the extent that their activities facilitate or impact democratic culture. A distinction is made between micro-gatekeepers (certain content moderators), authority gatekeepers (Facebook, Wikipedia, portals), and macro-gatekeepers (ISPs, search engines). Macro-gatekeepers have the greatest democratic impact and thus the strongest human rights obligations (Laidlaw, 2012, p. 60ff.). They are distinguished from the other levels, because users must inevitably pass through them to use the Internet. As such, they engage all aspects of freedom of expression and information. Moreover, a shift from voluntary to more binding obligations is suggested (Laidlaw, 2012, p. 241).

Within the UN system, attempts towards more legally binding norms have been taken – and although an earlier attempt to introduce legally binding human rights obligations for businesses failed – the discussion on establishing such legally binding norms has continued. (Lagoutte, 2014, p. 8). In June 2014, the HRC adopted a resolution representing steps towards a legally binding instrument on human rights and business and decided to establish an intergovernmental working group to elaborate such an instrument on transnational corporations and other business enterprises with respect to human rights (United Nations Human Rights Council, 2014a). The author of the UN Guiding Principles, however, has stated that the elaboration and adoption of a legally binding instrument will entail 'monumental challenges' in relation to institutions, enforcement etc. (Ruggie, 2014, p. 3). It should also be noted, that the final vote of the resolution consisted of 20 in favour, 14 against and 13 abstentions, while the non-legally binding UN Guiding Principles were endorsed by consensus.[37]

In sum, states are obliged to prevent human rights violations by private actors, and private actors have a (moral – not legal) duty to respect human rights. States must ensure human rights compliant business practices via appropriate regulation, and each company has a responsibility to assess their actual human rights impact. In the case of Internet intermediaries, there is an extended ´sphere of influence´, compared to most companies. Not only does the intermediary have responsibilities in relation to its employees and community, its practices also may affect directly or indirectly billions of Internet users.

The increasing focus on the human rights responsibilities of private actors adds to the complexity of the situation of the intermediaries. Aside from the state pressure to implement public policy, the intermediaries are also under an increasing pressure from states and the international community to respect human rights as elaborated in the UN Guiding Principles. However, by implementing public policy with implications on freedom of expression and information, the intermediaries may limit the human rights, they are expected to respect according to the UN Guiding Principles.

Hence, it might prove difficult to meet these contradictory expectations, in particular when the implementation of the said directives happens in co- or self-regulatory frameworks that offer guidance

[37] As regards the EU's position on the work towards a legally binding instrument, the EU has had reservations about the development and voted against the resolution, arguing that more efforts should be made by all States to implement the agreed framework of the UN Guiding Principles instead of polarising the debate and embarking on an ill-defined drafting process on a legally binding instrument. Despite its reservations, the EU is actively taking part in the process, European perspectives on Business and Human Rights (19/03/2015), (2015), Available from: <http://eeas.europa.eu/delegations/un_geneva/press_corner/all_news/news/2015/20150323_bus_and_hr_en.htm> accessed 19 November 2015.

on how to obtain such human rights compliance, and which - due to their nature - lack compliance with the rule of law, cf. section E.1.

An intermediary in good faith, who intends to comply with both public policy with a view to protect e.g. children against exploitation and copyright holders against infringements, may easily interfere with freedom of expression and information of Internet users. This is a complex landscape for the intermediaries to operate in, and with limited or no guidance from the EU regulator or Member State, it may result in a severe negative impact on freedom of expression and information e.g. when measures are not sufficiently targeted.

F. Conclusions and Recommendations

The study has pointed to a number of human rights challenges that occur at the junction of the EU policies for combating illegal content on the Internet, self-regulation, and intermediary (limited) liability schemes.

As illustrated, Internet intermediaries are increasingly being enlisted to impose – in a mix of mandatory and state-encouraged 'voluntary' schemes – restrictions on freedom of expression and information without being subject to the human rights law constraints that apply to state interference with the right to freedom of expression. The UN Guiding Principles on Business and Human Rights have indicated the importance of addressing private actors' responsibility to respect international human rights law, yet they do not solve the fundamental challenge raised by this study. In the current regulatory environment related to the digital domain, interference with EU citizens' online freedom of expression and information largely occurs in a legal grey-zone with limited means of transparency and accountability.

Arguably, Internet intermediaries have a significant impact on users' ability to enjoy freedom of expression and information online. Yet, the EU regulation that these actors are subjected to does not maximise their adherence with international human rights standards, but creates ambiguity around liability and encourages schemes of self-regulation. Also, importantly the measures deployed by the intermediaries are not subjected to the rule of law test developed by the ECtHR in its case law on Article 10(2) of the ECHR. While the EU has had an increasing focus on freedom of expression in its external policy (as addressed in the following study), its internal policy and regulation related to blocking, filtering and take-down of content have neither been framed nor assessed for its impact on freedom of expression – despite the obligation to respect this fundamental right according to Article 11 of the EU Charter.

The study has highlighted how the EU´s policy related to intermediary liability, IPR enforcement, and combating the sexual abuse and sexual exploitation of children and child pornography, may influence negatively on users' right to freedom of expression online. As illustrated in section E, the regulation in this area places the intermediaries in a legal grey zone with different and often conflicting expectations related to their role vis-à-vis content regulation. In practice, the intermediaries are expected to navigate between: (1) liability schemes that expect them to expediently remove alleged illegal content but also *not* to interfere with the transmission in order to benefit from safe harbours, (2) expectations of self-regulation (e.g. blocking of content) that might cut them off from the safe harbours, and (3)

expectations of conducting human rights impact assessments to mitigate negative human rights impacts, as stipulated in the UN Guiding Principles on Business and Human Rights and the related EU ICT Sector Guide.

This zone of unclear expectations, norms and liability provisions is partly due to the character of the digital domain. With private actors in control of the digital infrastructure and services it is no surprise that EU regulators and Member States have turned to these actors to regulate content that is outside their own zone of control. Looking through the prism of the right to freedom of expression, however, this practice is problematic and calls for guidance and standards from EU regulators to ensure that the rule of law standards of Article 10(2) of the ECHR is protected when regulatory action is delegated to private actors. In the absence of such standards and guidance, the legal grey-zone presented by the directives is transposed to Member States, and the intermediaries are left with self-devised codes of conduct while carrying out practices that affect users' fundamental rights. Also, as discussed in section C.2. and E.1., it remains unclear to which extent these practices may be addressed under the positive state obligation in relation to Article 10 of the ECHR.

As described, EU policy tends to thrive towards a common and comprehensive EU approach when dealing with alleged illegal content, but fails to take into account some of the related concerns about freedom of expression and the rule of law. Arguably, there is a fundamental difference between the weight that is attributed to freedom of expression in the online environment from an economic free movement perspective as opposed to a human rights perspective. Until recently, the underlying motivations and rationales for addressing human rights issues at the EU level, have been economic in nature, and human rights issues, which are by nature non-economic, have been addressed as auxiliaries to the establishment of an Internal Market.[38] As a result, important policy concerns from the perspective of human rights end up being addressed indirectly, inefficiently and incompletely or are not addressed at all.[39]

Despite the goal, set out by the EU Human Rights Guidelines on Freedom of Expression Online and Offline, according to which the EU is committed to respecting, protecting and promoting the freedom of opinion and expression within its borders (Council of the European Union, 2014, para. 7), this has not yet been implemented in secondary EU law (such as the three above mentioned directives. In consequence, the overall EU policy related to online freedom of expression appears contradictory and incoherent. Moreover, it may weaken the impact and credibility of the external policy, if the EU in its internal policies actively promotes policies with a negative impact on freedom of expression and information.

[38] See for instance directive 95/46/EC on data protection. It follows from the Preamble, that the establishment and functioning of an internal market require that personal data should be able to flow freely from one Member State to another (Recital 3), and that the difference in levels of protection of the rights and freedoms of individuals, notably the right to privacy, with regard to the processing of personal data afforded in the Member States may prevent the transmission of such data from the territory of one Member State to that of another Member State (Recital 7). Consequently, data protection must be ensured. This is an example of data protection not being promoted from a human rights perspective, but as a means for obtaining an internal market.

[39] This point has also been raised by Hoboken (2014) in relation to privacy and data protection. See HOBOKEN, J. August 15, 2014. The European Approach to Privacy *2014 TPRC Conference Paper.*

Furthermore, the EU needs to strengthen its focus on the implications on freedom of expression caused by EU content regulation imposing on Member States and intermediaries to take down content or disable access to it, including the rule of law challenges related to the use of self-regulation. Up until now, the debate on co-regulation and self-regulation within the EU has shown limited attention to the freedom of expression issues evoked by such arrangements. In contrast, the Council of Europe has developed a number of standards pertaining to the use of Internet filters, online freedom of expression, rule of law, etc. over the past ten years, cf. section C.1. Also, a number of UN reports and resolutions adopted on freedom of expression on the Internet since 2011 set standards in this field, cf. section C.1. The

With the entry into force of the Lisbon Treaty, fundamental rights play a more important role than ever within EU-law, cf. article 6 of the TEU. Yet, while the right to privacy and data protection has received considerable attention over the past decade, EU standards and guidance for the protection and promotion of freedom of expression in the online domain are still lacking, particularly as it relates to the EU's internal policies. The recently launched Digital Single Market Strategy for Europe envisages among others an analysis of the need for new measures to tackle illegal content on the Internet 'with due regard to the impact on the fundamental right to freedom of expression and information' (European Commission, 2015, para. 3.3.2.). The ongoing debate following the adoption of the Strategy is a unique opportunity to ensure that the fundamental rights that the EU subscribes to are firmly situated as the baseline of the EU's vision in this field.

In the remaining part of this chapter, the authors suggest a number of concrete actions that may help to remedy the current situation and provide stronger freedom of expression protection in relation to co- and self-regulation. The list below is not exhaustive but suggests a number of actions that aim to improve respect for freedom of expression in relation to current practices of blocking, filtering and take-down of content. While some of the suggested actions may have a broader positive impact, the main focus has been the identified challenges related to the three directives addressed in this study.

1. While the European Council in 2014 adopted Human Rights Guidelines on Freedom of Expression online and offline, in relations to the EU's *external human rights policy*, a similar policy is lacking in relation to the EU's internal policies. Informed by the Guidelines, and drawing on current challenges highlighted in this study, the EU should develop an EU Policy on freedom of expression targeting internal EU policy, coherent with the external policy, and covering issues such as to (the list below is merely illustrative, drawing on existing standard-setting in this field):

- Reaffirm the importance of the Internet to the full enjoyment of human rights and, in this context, in particular the right to freedom of expression and information.
- Recognise the role played by Internet intermediaries and their potential impact on freedom of expression and information in the online domain.
- Recall relevant international standards in this field.
- Stress that Member States should foster and encourage access for all to Internet communication and information services on a non-discriminatory basis at an affordable price.

- Reaffirm that rule of law obligations flowing from Article 10 of the ECHR may not be circumvented through ad hoc arrangements with Internet intermediaries.
- Reaffirm the need for intermediary liability protections.
- Reaffirm that public authorities should not, through general blocking or filtering measures, deny access by the public to information and other communication on the Internet.
- Call upon Member States to ensure that service providers are not held liable for content on the Internet when their function is limited, as defined by national law, to transmitting information or providing access to the Internet.
- Stress that Member States should not impose on service providers a general obligation to monitor content on the Internet, nor that of actively seeking facts or circumstances indicating illegal activity, cf. the principle in Article 15 of the E-commerce directive.
- Reiterate that when Member States define under national law the obligations of service providers, due care must be taken to respect the freedom of expression of the speakers, as well as the corresponding right of the end-users to the information.
- Stress that where Member States deploy measures to remove clearly identifiable illegal Internet content or, alternatively, block access to it, they must respect the safeguards provided in Article 10(2) of the ECHR. Such action by the state should only be taken if a competent national authority has taken a decision on its illegality and the decision can be reviewed by an independent and impartial tribunal or regulatory body, in accordance with the requirements of Article 6 of the ECHR.
- Stress that Member States should regularly review and update the criteria and process for disabling or removing Internet content in order to secure its effectiveness, proportionality and legitimacy in relation to the intended purpose.
- Stress that Member States must ensure that effective remedies for affected users exist, including the possibility of appeal through the procedures provided by the intermediary.[40]

2. Action: Conduct a review of Member States' implementation of the three directives focusing in particular on: (1) how the deployed filtering, blocking and take-down measures impact on freedom of expression and information in the online domain; and (2) their compliance with Article 10(2) of the ECHR. The authors suggest to start with Member States that have a long and established tradition of self-regulatory regimes such as the UK, and the Nordic countries.

3. Action: Develop best practice Guidance to Member States based on the review, including adequate standards for Article 10(2) compliance, transparency and accountability in the – both mandatory and voluntary – regimes for content regulation. Member States should ensure that any restrictions on access to Internet content affecting users under their jurisdiction are based on a strict and predictable legal framework regulating the scope of any such restrictions and affording the guarantee of judicial or administrative oversight to prevent possible abuses.

[40] The need for effective remedies is stressed in LA RUE, F. 2011. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, A/HRC/17/27. United Nations General Assembly, Human Rights Council. as well as COUNCIL OF EUROPE 2014c. Recommendation CM/Rec(2014)6 of the Committeee of Ministers to member States on aguide to human rights for Internet users.

4. Action: Introduce more specific provisions on the measures allowed by intermediaries across Member States to counter alleged illegal content, in particular harmonised safeguards related to rule of law and compliance with Article 10(2) of the ECHR. As part of this, standards and guidance should be provided on counter-notice procedures for end-users to challenge wrongful blocking and take-down requests.

5. Action: Develop guidance to Member States on their positive human rights obligations related to freedom of expression. This should include instructions on the level of state involvement in filtering, blocking and take-down of content that is necessary for state responsibility to be engaged and on the obligations of the state to ensure that the practices of private companies are not at variance with human rights standards.[41]

6. Action: Develop guidance on the responsibilities of Internet intermediaries when they engage in activities that have an impact on end-users' freedom of expression or information, in particular related to self-regulatory measures such as blocking, filtering or take-down of content. The Guidance should build on the UN 'Guiding Principles on Business and Human Rights' and the EU ICT Sector Guide.

7. Action: Ensure that the Digital Single Market Strategy explicitly addresses freedom of expression and information as a fundamental right (and value) underpinning the European vision of the digital domain – as it does with privacy and data protection. This further implies that the current regime – as well as any new measures introduced – for tackling illegal content on the Internet have to be in full compliance with Article 10(2) of the ECHR.

8. Action: Follow-up on previous work towards a harmonised European approach in the field of ´notice-and-action´ procedures, in particular addressing the current legal uncertainty on key notions in the E-commerce directive (e.g. ´notice´, ´actual knowledge´, ´expeditiously´) as well as the scope of the definition of intermediaries. The on-going development of the initiatives under the Digital Single Market Strategy in relation to dealing with alleged illegal content is an excellent opportunity for improvements in this area. As part of this, experiences with 'counter-notice' provisions from EU Member States should be included. Also, the current uniform approach to alleged breaches of civil law and criminal law respectively should be critically examined, in order to provide for a more tailored and proportionate regime for combating illegal content.

G. Bibliography

1. Legal and Policy Instruments

a) Council of Europe

Council of Europe (2008), 'Recommendation CM/Rec(2008)6 of the Committee of Ministers to member states on Measures to promote the respect for freedom of expression and information with regard to Internet filters'.

[41] A similar suggestion is made in the recent Council of Europe Issue paper, p. 23. See KORFF. 2014. The rule of law on the Internet and in the wider digital world - Issue Paper.

Council of Europe (2014a), 'Declaration by the Committee of Ministers on the UN Guiding Principles on Business and Human Rights'.

Council of Europe (2014b), 'Recommendation CM/Rec(2014)1 of the Committee of Ministers to member States on the Council of Europe Charter on shared social responsibilities'.

Council of Europe (2014c), 'Recommendation CM/Rec(2014)6 of the Committeee of Ministers to member States on aguide to human rights for Internet users'.

Council of Europe (2014d), 'Recommendation CM/Rec(2014)6 of the Committeee of Ministers to Member States on aguide to human rights for Internet users - Explanatory Memorandum'.

Council of Europe in co-operation with the European Internet Service Providers Association (EuroISPA) (2008), 'Human rights guidelines for Internet service providers'.

Council of Europe Steering Committee on Media and Information Society (2015), 'Internet Governance Strategy 2012-2015 - Oversight of implementation (CDMSI(2015)009Rev)'.

b) European Union

Council of the European Union (2014), 'EU Human Rights Guidelines on Freedom of Expression Online and Offline'.

European Commission (1996a), 'Communication from the Commission on Illegal and Harmful Content on the Internet (COM(1996) 487 final)'.

European Commission (1996b), 'Green Paper on the Protection of Minors and Human Dignity in Audio-Visual and Information Services (COM (1996) 483 final)'.

European Commission (2010a), 'Proposal for a directive of the European Parliament and of the Council on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA (COM(2010)94 final)', in European Union (ed.).

European Commission (2010b), 'Summary of the results of the Public Consultation on the future of electronic commerce in the Internal Market and the implementation of the Directive on electronic commerce (2000/31/EC)'.

European Commission (2012a), 'Commisssion Communication to the European Parliament, the Council, The Economic and Social Committee and the Committee of the Regions. A coherent framework for building trust in the Digital Single Market for e-commerce and online services'.

European Commission (2012b), 'Commission Staff Working Socument. Communication from the Commission to the European Parliament, the Council, the European Economic ans Social Committee of the Regions. A coherent framework to bost confidence in the Digital Single Market of e-commerce and other online services (SEC(2011) 1641 final)'.

European Commission (2013a), 'ICT Sector Guide on Implementering the UN Guiding Principles on Business and Human Rights'.

European Commission (2013b), 'Commission Staff Working Document. E-commerce Action plan 2012-2015. State of play 2013 (SWD(2013) 153 final)'.

European Commission (2014), 'Report on the responses to the Public Consultation on the Review of the EU Copyright Rules', (July 2014), Available from: <http://ec.europa.eu/internal_market/consultations/2013/copyright-rules/docs/contributions/consultation-report_en.pdf> accessed 11 November 2015.

European Commission (2015), 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Commitee and the Committee of Regions (COM(2015) 192 final). A Digital Single Market Strategy for Europe'.

European Parliament (2015), 'Resolution on child sexual abuse online (2015/2564/(RSP))'.

European Parliament and Council of the European Union (1995), 'Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data'.

European Parliament and Council of the European Union (2000), 'EU directive on E-Commerce (2000/31/EC)'.

European Parliament and Council of the European Union (2001), 'Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society'.

European Parliament and Council of the European Union (2002), 'Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)'.

European Parliament and Council of the European Union (2004), 'Directive 2004/48/EC on the enforcement of intellectual property rights'.

European Parliament and the Council of the European Union (2011), 'Directive 2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography'.

c) UN

Kaye, David (2015), 'Report of the Special rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, A/HRC/29/32', (United Nations General Assembly, Human Rights Council).

La Rue, Frank (2011), 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, A/HRC/17/27', (United Nations General Assembly, Human Rights Council).

La Rue, Frank (2013), 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La', (United Nations General Assembly, Human Rights Council).

The Office of the United Nations High Commissioner for Human Rights (2014), 'The Right to Privacy in the Digital Age. Report of the Office of the United Nations High Commissioner for Human Rights, A/HRC/27/37*'.

United Nations General Assembly (2013), 'Resolution adopted 68/167 by the General Assembly. The Right to Privacy in the Digital Age', (December 18, 2013).

United Nations General Assembly (2014), 'Resolution 69/166 adopted by the General Assembly. The Right to Privacy in the Digital Age', (December 18, 2014)

United Nations General Assembly (2015), 'Resolution 69/204, Information and communications technologies for development, A/RES/69/204 ', (January 21, 2015).

United Nations Human Rights Council (2011a), 'Report of the Special Representative John Ruggie. Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework'.

United Nations Human Rights Council (2011b), 'Resolution 17/4 adopted by the Human Rights Council. Human rights and transnational corporations and other business enterprises. '.

United Nations Human Rights Council (2012), 'Resolution 20/8. The promotion, protection and enjoyment of human rights on the internet. A/HRC/20/L.13', (July 5, 2012).

United Nations Human Rights Council (2014a), 'Resolution 26/9 Elaboration of an international legally binding instrument on transnational corporations and other business enterprises with respect to human rights. A/HRC/26/L.22/Rev.1'.

United Nations Human Rights Council (2014b), 'Resolution 26/13, The promotion, protection and enjoyment of human rights on the Internet, A/HRC/RES/26/13', (July 14, 2014).

United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, et al. (2011), 'Joint Declaration on Freedom of Expression on the Internet', (June 1, 2011).

2. Case-law

a) Court of Justice of the European Union

Case C-360/10 *SABAM v. Netlog NV* (CJEU 16 February 2012).

Case C-70/10 *SABAM v. Scarlet Extended* (CJEU 24 November 2011).

b) European Court of Human Rights

*Ahmet Yıldırım v. Tur*key App. No. 3111/10 (ECtHR 18 December 2012).

Appleby and Others v. the United Kingdom App. No. 44306/98 (ECtHR 6 May 2003).

Delfi AS v. Estonia App. No. 64569/09 (ECtHR 16 June 2015).

Handyside v. The United Kingdom App. No. 5493/72 (ECtHR 7 December 1976).

Observer and Guardian v. the United Kingdom App. No. 13585/88 (ECtHR 26 November 1991)

Perrin v. the United Kingdom App. No. 5446/03 (ECtHR 18 October 2005).

Rees v. the United Kingdom App. No. 9532/81 (ECtHR 17 October 1986).

VgT Verein Gegen Tierfabriken v. Switzerland App. No. 24699/94 (ECtHR 28 June 2001).

3. Literature

a) Books

Benedek, W. and Kettemann, M., *Freedom of Expression and the Internet* (Strasbourg: Council of Europe 2014).

Brousseau, E., Marzouki, M. and Méadel, C., *Governance, regulations and powers on the Internet* (Cambridge; New York: Cambridge University Press 2012).

Deibert, R., et al., *Access controlled : the shaping of power, rights, and rule in cyberspace* (Cambridge, Mass.: MIT Press 2010).

Deibert, R., et al., *Access denied : the practice and policy of global Internet filtering* (Cambridge, Mass.: MIT Press 2008).

Hoboken, J. van, *Search engine freedom : on the implications of the right to freedom of expression for the legal governance of web search engines*, (Kluwer Law International 2012).

Jørgensen, R. F., *Framing the Net – The Internet and Human Rights* (Cheltenham: Edward Elgar Publishing 2013).

Laidlaw, E. B., *Internet Gatekeepers, Human Rights, and Corporate Social Responsibility*, (London School of Economics and Political Science 2012).

Morgan, B. and Yeung, K., *An introduction to law and regulation : text and materials* (Cambridge, UK; New York: Cambridge University Press 2007).

Savin, A. and Trzaskowski, J., *Research handbook on EU Internet law* (Cheltenham, UK: Edward Elgar 2014).

Tambini, D., Leonardi, D., and Marsden, C. T., *Codifying cyberspace: communications self-regulation in the age of Internet convergence* (London; New York: Routledge 2008).

White, R.C.A., Ovey, C., Jacobs, F. G., *Jacobs, White and Ovey: The European Convention on Human Rights* (Oxford; New York: Oxford University Press 2010).

b) Book Chapters

Villeuve, N. (2010), 'Barriers to Cooperation: An analysis of the Origins of International Efforts to Protect Children Online' in Deibert, Ronald, et al. (2010), *Access controlled : the shaping of power, rights, and rule in cyberspace* (Cambridge, Mass.: MIT Press) 55-70.

Deibert, R. and Rohozinski, R. (2010), 'Beyond Denial, Introducing Next-Generation Information Access Control' in Deibert, R., et al. (2010), *Access controlled : the shaping of power, rights, and rule in cyberspace* (Cambridge, Mass.: MIT Press) 3, 15.

c) Journal Articles

Balkin, J. M., 'Old-School/New-School Speech Regulation' (2014) Harvard Law Review, 127 (8), 2296, 342.

Brown, I., 'Internet self-regulation and fundamental rights' (2010) Index on Censorship, 1, 98, 106.

Frydman and Rorive, 'Regulating Internet Content through Intermediaries in Europe and in the USA' (2002) Zeitschrift für Rechtssoziologie, 23 (2002), Heft 1, 41, 59.

Frydman, B., Hennebel, L., and Lewkowicz, G., 'Public Stategies for Internet Co-Regulation in the United States, Europe and China' (2008) Working Papers du Centre Perelman de philosophie de droit, No 2007/6.

Hoboken, J., 'The European Approach to Privacy ' (August 15, 2014) 2014 TPRC Conference Paper, Available from: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2418636> accessed 10 November 2015.

Kreimer, S. F., 'Censorship by Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link' (2006) univpennlawrevi University of Pennsylvania Law Review, 155 (1), 11, 101.

Kuczerawy, A., 'Intermediary liability & freedom of expression: Recent developments in the EU notice & action initiative' (2015), Computer Law & Security Review: The International Journal of Technology, 31 (1), 46, 56.

Laidlaw, E. B., 'A framework for identifying Internet information gatekeepers' (2010) International Review of Law, Computers & Technology, 24 (3), 263, 276.

Land, M., 'Toward an International Law of the Internet' (2013) Harvard International Law Journal, 54 (2).

McIntyre, T. J., 'Blocking child pornography on the Internet: European Union developments' (2010) International Review of Law, Computers & Technology, 24 (3), 209, 221.

O'Brien, C. M. and Dhanarajan, S., 'The Corporate Responsibility to Respect Human Rights: A Status Review' (2015) NUS Law Working Paper Series, 2015/005.

Olster, J., 'Liability of Internet Intermediaries for Defamatory Speech – An Inquiry into the Concepts of 'Publication' and 'Innocent Dissemination' (2013) The Society of Legal Scholars Edinburgh Conference 2013.

Ruggie, J. G., 'A UN Business and Human Rights Treaty? An Issues Brief by John G. Ruggie' (2014) HARVARD Kennedy School (28 January 2014), Available from <www.hks.harvard.edu/m-rcbg/CSRI/UNBusinessandHumanRightsTreaty.pdf> accessed 10 November 2015.

Zittrain, J., 'A History of Online Gatekeeping' (2006) Harvard journal of law & technology, 19 (2), 253-98.

4. Policy and Other Reports

Article 19, 'European Commission: Freedom of Expression Needs Better Protection in Digital Communications' (Article 19, London 2010), Available from: < www.article19.org/data/files/pdfs/press/european-commission-freedom-of-expression-needs-better-protection-in-digital.pdf> accessed on 11 November 2015.

Brown, I. and Korff, D., 'Digital Freedoms in International Law - Practical Steps to Protect Human Rights Online', (Global Network Initiative (2012)), (14 June 2012).

Callahan, C., et al., 'Internet blocking. Balancing cybercrime responses in democratic societies', (2009), (Report prepared within the framework of Open Society Institute funding).

Cave, J., et al., 'Options for and Effectiveness of Internet Self- and Co-Regulation', (RAND, Report prepared for the European Union 2008).

Council of Europe, 'Factsheet - New technologies', (Council of Europe June 2015).

Council of Europe and European Court of Human Rights, 'Positive obligations on member States under Article 10 to protect journalists and prevent impunity' (Research Report 2011).

EDRI, 'EDRI response to the consultation on the E-commerce directive' (EDRI, Brussels 2010) Available from <https://edri.org/files/EDRi_ecommerceresponse_101105.pdf> accessed 11 November 2015.

EDRI, 'A clean and open Internet: Public consultation on procedures for notifying and acting on illegal content hosted by online intermediaries' (EDRI, Brussels 2012) Available from: < https://edri.org/files/057862048281124912Submission_EDRi_NoticeAction.pdf> accessed 13 November 2015.

EDRI, 'Human Rights and privatised law enforcement' (EDRI, Brussels, 2013) Available from https://edri.org/wp-content/uploads/2014/02/EDRi_HumanRights_and_PrivLaw_web.pdf accessed 10 November 2015.

EDRI, 'EDRI's answer to the EC consultation of the review of EU copyright rules' (EDRI, Brussels 2014) Available from: <https://edri.org/wp-content/uploads/2014/03/EDRi-answer-copyright-consultation-2014_web.pdf> accessed 11 November 2015.

EDRI and others, 'Open letter on intermediary liability protections in the digital single market to Vice-President of the European Commission Andrus Ansip' (2015).

Federal Networking Council (FNC) Resolution 'Definition of "Internet" 10/24/95', <http://www.nitrd.gov/fnc/Internet_res.html> accessed 10 July 2011.

Korff, D., 'The rule of law on the Internet and in the wider digital world - Issue Paper' (2014).

Lagoutte, S., 'The State Duty to Respect Against Business-Related Human Rights Abuses. Unpacking Pillar 1 and 3 of the UN Guiding Principles on Human Rights and Business.' (2014) *Matters of Concern - Human Rights' Research Papers Series,* 2014/1.

Lassen, E. M. et. al., 'Report on factors which enable or hinder the protection of human rights', (Danish Institute for Human Rights 2014), Available from www.fp7-frame.eu/report-on-factors-which-enable-or-hinder-the-protection-of-human-rights/ accessed 10 November 2015.

MacKinnon, R. et al., United Nations Educational, Scientific, and Cultural, Organization, 'Fostering Freedom Online: The Role of Internet Intermediaries', (Paris: UNESCO 2014), Available from http://unesdoc.unesco.org/images/0023/002311/231162e.pdf.> accessed 10 November 2015.

McNamee, J. and EDRI, 'Internet Blocking: Crimes should be punished and not hidden', (EDRI, Brussels, 2010), Available from: <https://edri.org/files/blocking_booklet.pdf> accessed 11 November 2015.

McNamee, J. et al., 'Copyright: challenges of the digital age', (EDRI, Brussels, 2013), Available from <https://edri.org/files/paper07_copyright.pdf> accessed 11 November 2015.

Netzpolitik, 'A clean and open Internet: Public consultation on procedures for notifying and acting on illegal content hosted by online intermediaries' (2012) Available from: <https://netzpolitik.org/wp-upload/N_a_T_answers_digiges.pdf> accessed 15 November 2015.

Red Barnet, 'Hvor slemt ka' det være - En antologi om it-relaterede seksuelle overgreb på børn og unge' (Copenhagen: Red Barnet 2015), Available from <http://stopdigitaleovergreb.nu/redbarnet/ressourcer/antologi-om-digitale-overgreb/> accessed 10 November 2015.

Schulz, W. and Held, T., 'Regulated Self-Regulation as a form of modern Government' (2001) Study Commissioned by the German Federal Commissioner for Cultural and Media Affairs, Interim Report (Hamburg: Germany).

SearchCIO 'ICT (information and communications technology – or technologies)' Available from: <http://searchcio-midmarket.techtarget.com/definition/ICT>, accessed July 10, 2011.

Spangenberg, J., 'The EU Notice & Action Initiative: Recent Developments' (2015) Available from <http://revealproject.eu/> accessed 10 November 2015).

5. Electronic Sources

European perspectives on Business and Human Rights (19/03/2015), (2015), Available from: <http://eeas.europa.eu/delegations/un_geneva/press_corner/all_news/news/2015/20150323_bus_and_hr_en.htm> accessed 19 November 2015.

Herdict (Berkman Center for Internet and Society, Harvard University), Available from <www.herdict.org/> accessed 10 November 2015.

Internet Watch Foundation (IWF), Available from <www.iwf.org.uk/about-iwf/iwf-history> accessed 10 November 2015.

Lumen (Berkman Center for Internet and Society, Harvard University), Available from < https://cyber.law.harvard.edu/research/chillingeffects> accessed 18 November 2015.

OpenNet Initiative (ONI) (Collaborative partnership between Citizen Lab, Munk School of Global Affairs, University of Toronto; the Berkman Center for Internet and Society, Harvard University and the SecDev Group (Ottawa), Available from <https://opennet.net/> accessed 10 November 2015.

III. Review on EU policies on Digital Defenders with a focus on freedom of expression – Case study on human rights implications of the EU's external policies*

A. Introduction and Focus of Research

This case study concerns the external dimension of the human rights policies of the European Union (EU) with regard to challenges posed by the use of Information and Communications Technology (ICT). As the United Nations (UN) Human Rights Council confirmed in its fundamental Resolution of 2012 (Human Rights Council, 2012), Human rights apply online and offline. This was confirmed by the EU Guidelines on Freedom of Expression Online and Offline of 2014 (Council, 2014a).[42] The EU has developed policies for the online dimension of human rights in order to support their application globally. This relates in particular to freedom of expression and information as it does to freedom of association. In the Arab spring of 2011 the Internet played a major role. It was used by the democracy movements to share their views and organise conventions, as well as to circumvent the censored print and electronic media. This has been an impressive example of the potential of new technologies in the service of democracy and human rights, although their importance should also not be overestimated (See Allagui and Kuebler, 2011; Axford, 2011; Osman and Samei, 2012). In a similar way, the protests in Turkey, like the Gezi park protests of 2013 led to a temporary closure of Twitter by the Turkish government, and the Russian amendments to its information law of 2014 aim at a better control of bloggers (Russian Federal Republic, 2014).[43] The main social media used are Facebook and Twitter (Salem and Mourtada, 2011).

Accordingly, the Internet and the social services offered on its many platforms have opened new opportunities for freedom of expression and other human rights, but also brought new threats of restrictions and the surveillance of users, like bloggers and users of social media, which created new challenges for EU policies in favour of freedom of expression and other human rights online, like the right to privacy and data protection (Benedek and Kettemann, 2013; Frank Joergensen, 2013). According to Freedom House, out of 65 countries assessed for the 'Freedom on the Net'-report showed a negative development since May 2013.[44]

A particular focus of this case study is on Human Rights Defenders (HRDs) using digital services. Among them there are those who act mainly by digital means, like bloggers, who use the Internet and the social platforms available to share their views or to get information on human rights and democracy (right to information). In a wider sense, any human rights defender using digital means in pursuit of her or his human rights can be in the situation of a digital Human Rights Defender, for example by being subject to

* The authors of this chapter are Prof. Dr. Wolfgang Benedek and Mag. Reinmar Nindler, European Training and Research Centre for Human Rights and Democracy, Graz, Austria.

[42] See also Wolfgang Benedek, 'EU Human and Fundamental Rights Action in 2014' in Wolfgang Benedek, Florence Benoit-Rohmer, Matthias C. Kettemann, Benjamin Kneihs and Manfred Nowak (eds), *European Yearbook on Human Rights 2015* (NWV/Intersentia 2015) 79-103, 101.

[43] See also Olga Khazan, 'These Charts show how crucial Twitter is for Turkish protesters' (The Atlantic, 12 June 2013) <www.theatlantic.com/international/archive/2013/06/these-charts-show-how-crucial-twitter-is-for-the-turkey-protesters/276798/> accessed 14 October 2015.

[44] Freedom House, 'Freedom on the Net 2014' <https://freedomhouse.org/report/freedom-net/freedom-net-2014#.Vh5HWk0gmUk> accessed 14 October 2015.

censorship or surveillance. These 'Digital Defenders' (DDs) and their activities and needs of protection and support are a particular focus of this case study, which also seeks to analyse how the EU has reacted or should react to this new challenge. More specifically, the case study investigates what support schemes are available for DDs, whether they are aware of those and which intermediary structures exist to provide them with access to those opportunities. This leads to the question whether or not the existing support schemes are sufficient or what improvements could be suggested to make them more effective. In this context, specific attention is given to the European Instrument on Democracy and Human Rights (EIDHR) and its specific actions, in particular the relevance of the new Human Rights Defenders Mechanism (HRDM) for Digital Defenders.

Furthermore, a mapping of EU policies regarding the external dimension of ICT and human rights also requires to look into the issue of safety of online journalists, the issue of export controls of surveillance technologies and the cooperation between the EU and other international organisations like the Council of Europe (CoE), the Organisation for Security and Cooperation in Europe (OSCE), the United Nations Educational, Scientific and Cultural Organization (UNESCO) and the UN at large, to protect DDs and users of ICT for human rights purposes. In this respect their freedom of expression and access to information is the main focus, while also other, related human rights like freedom of association, privacy and data protection are being addressed. The case study aims to offer a better understanding of the opportunities and threats related to the use of ICT, the new vulnerabilities created and the need for new means of protection.

The findings of this case study allow us to provide a set of conclusions and to formulate recommendations on how the EU can make its policies more coherent and effective.

B. Methodology and Structure

The methodological approach of the second case study is based on desk research and interviews of representatives of Non-governmental Organizations (NGOs) working with ICT tools for human rights and democracy or supporting Digital Defenders as well as EU staff members working in this area. For this purpose the occasion of the Internet Governance Forum in Istanbul in September 2014 was used as was the EU-NGO-Forum on Human Rights in Brussels in December 2014, which had a focus on the EU Guidelines on Freedom of Expression Online and Offline (Guidelines), and other pertinent workshops and events. It was, however, not possible to speak to a significant number of EU focal points. For lack of availability of EU human rights country strategies these documents could not be analysed.

The presentation of the case study is structured in three parts: first, the background and driving forces of EU engagement are to set the stage and explain the main considerations for engaging with this study. In order to focus the issues at stake, a particular concept of digital defenders is introduced, while it is clear that many Human Rights Defenders do use digital means and are therefore also subject to similar experiences and problems. As such, this report considers them as Digital Defenders as well.

Second, EU policies and instruments to protect and support Digital Defenders are analysed, covering both the general policies on the external dimension of Freedom of Expression and Privacy/Data Protection, crystallised in the 'No Disconnect Strategy', as well as how digital vulnerabilities and emergencies have been addressed in practice. Particular attention is devoted to the European Instrument for Democracy and Human Rights, which funds crucial support programmes in this respect.

Third, the study looks at the relationship between the protection of Digital Defenders and the safety of journalists, the relationship of Freedom of Expression and Privacy/Data Protection to export controls of surveillance technology, the relationship between EU action and measures by member states to protect and support digital defenders and the cooperation with other international organisations active in this field like the CoE, OSCE, UNESCO and the UN. Finally, it also looks at the role of private business for the protection of Digital Defenders before ending with conclusions and proposals to strengthen EU action in form of general and specific recommendations.

C. Background and Driving Forces of EU Engagement

Since the Arab Spring began in December 2010, with the Jasmine Revolution in Tunisia, the debate on the importance and role of the Internet in the context of pro-democratic movements in the Arab region has increased. While some authors already saw the Internet as a 'playground for political liberalisation in the Arab world' and underlined, that in the states, which 'exercise the most heavy-handed control of Internet traffic in the region [...] the net has proven to be a vital factor in opening windows and expanding the realm of what can be said in public' (Hofheinz, 2005, p. 80) even well before the Arab Spring, others warned not to overestimate the importance and influence of the Internet in this context (Wagner, 2012a).

For the EU, 'the Arab Spring demonstrated the importance of Internet access in a startling manner'. 'Calls to gather for peaceful protests and against human rights abuses' were 'relayed with extreme rapidity thanks to social networking during the revolutions of 2011' (Commission, 2011a, p. 14). For example, the European Parliament (EP) recognised in its 2012 resolution on 'A digital freedom strategy in EU foreign policy' that 'uncensored access to the open Internet, mobile phones and ICTs have impacted on human rights and fundamental freedoms, exerting an enabling effect, by expanding the scope of freedom of expression, access to information, the right to privacy and freedom of assembly across the world' (European Parliament, 2012a, para. 1). The use of digital technologies has radically changed human rights advocacy as they provide new opportunities for engagement and (virtual) community building (Dutt and Rasul, 2014).

In the context of the Internet blackout in Egypt in 2011, when the government used the so-called 'kill switch' during protests, the term 'digital emergencies' was coined. It has also been employed for the recently increased crack-down on bloggers, journalists and others who use the Internet for critical expression globally. These developments are documented in the 2014 report of the Global Information Society Watch (GISWatch) entitled 'From digital threat to digital emergency' (Jansen, 2014).

The ability to effectively react to digital emergencies must be viewed as a crucial part of an effective policy on DDs. The EU's reactions to digital emergencies should in any case be as complementary as possible with thematically connected bilateral and multilateral activities by the EU Member States,[45] to avoid duplication and use synergies.

Following evidence of disruption or attempted disruption of communication technology 'by authoritarian governments during the Arab Spring uprising', the EU committed itself to develop tools to

[45] See subchapter II.D.3 'Relationship with Member States activities to protect and support DDs'.

counter such actions.[46] Those tools should 'allow the EU, in appropriate cases, to assist civil society organisations or individual citizens to circumvent such arbitrary disruptions' (Commission, 2011b, p. 11). Consequently, the EU made assistance to digital defenders a core concern in promoting human rights and democracy.

While the term 'Digital Defenders' is not used by the EU in its relevant policy documents, the notion itself is established in the human rights discourse and used by actors working in the field of the protection and promotion of human rights online. For example the Digital Defenders Partnership (DDP) bears the notion in its name.[47]

There exists no universally accepted definition of the term 'Digital Defenders' within the academic community. However, it is possible to identify some indispensable core elements of the term's meaning. Firstly, DDs are individuals or groups of individuals, secondly, they work towards the defence, support, fostering, or promotion of human rights and thirdly, their work is conducted, at least partly, online. For the purpose of this case study, the term Digital Defender will be used in this (broad) sense.

Since Digital Defenders are Human Rights Defenders, who conduct their work with the help of Information and Communication Technology, for example as bloggers or on social media, the EU's policies to protect and support DDs must therefore be viewed within the larger context of both the EU's engagement in the field of ICT and Human Rights and the EU's engagement with HRDs.[48] This study will also look into the support DDs receive directly from EU institutions or indirectly through specialized NGOs.

While the possibilities offered by ICT can have an influence on the enjoyment and promotion of numerous human rights, this chapter will focus on a selection of human rights and ICT related phenomena, notably freedom of expression, free access to information, freedom of assembly, privacy, data protection and (ICT related) surveillance. These are the areas that are widely considered to be the most influenced by positive and/or negative human rights impacts of the use of ICT.

When the uprising against the Ben Ali regime in Tunisia began by the end of 2010 and led to the fall of president Ben Ali's regime in early 2011[49] it was the beginning of a series of protests, uprisings and revolutions across the MENA region, generally referred to as the 'Arab spring'. Egypt, Libya and finally Syria became the theater of revolutions in which the use of ICT played a major role regarding the

[46] European Commission, 'Digital Agenda: Karl-Theodor zu Guttenberg invited by Kroes to promote internet freedom globally' (12 December 2011) <http://europa.eu/rapid/press-release_IP-11-1525_en.htm> accessed 17 May 2015.

[47] The DDP is a grant making mechanism in support of DDs, funded by several EU Member States as well as the United States and managed by an NGO, i.e. Hivos. See for the webpage <https://digitaldefenders.org/> accessed 1 October 2015.

[48] For a more in-depth analysis of the EU's engagement with HRDs, see: Wolfgang Benedek, Mary Footer, Jeffrey Kenner, Maija Mustaniemi-Laakso, Reinmar Nindler, Aoife Nolan and Stuart Wallace, 'Report on enhancing the contribution of EU institutions and Member States, NGOs, IFIs and Human Rights Defenders, to more effective engagement with, and monitoring of, the activities of Non-State Actors' (FRAME D7.2 2015) chapter VI.

[49] Al Jazeera, 'Timeline: Tunisia's uprising' (23 January 2011) <www.aljazeera.com/indepth/spotlight/tunisia/2011/01/201114142223827361.html> accessed 17 August 2015.

uprisings. Accordingly, the world became aware of the power of the Internet, though so did authoritarian states, which increased their efforts to restrict access or censor the Internet or to use it for their own surveillance purposes. This raised the need to better protect and support Digital Defenders as those employing the Internet as a public sphere (Joergensen, 2013, p. 89) to make use of their human rights of freedom of expression, information and association in particular.

At the same time, the rights to privacy and data protection of DDs are of core importance for their ability to act. In particular, ICT tools are successfully used for monitoring of human rights and documentation of human rights violations (Dankwa and Pahnecke, 2014). ICTs can be employed to secure the right to life, when they are used to document or monitor human rights violations as indicated in a recent report of the UN Special Rapporteur on extrajudical, summary and arbitrary executions (Human Rights Council, 2015b). More generally, the Internet can be used to protect or promote most human rights,[50] a fact that can only be noted here.

Problems of Digital Human Rights Defenders are manifold and range from limitations of the right to freedom of expression, including the right to blog, but also of the right to information to being subjected to defamation and hate speech. Sometimes, DDs are subject to harassment or made liable for third party content. They may be denied protection as a journalist or be subject of censorship and surveillance and have to face impunity of the perpetrators.[51]

D. EU Policies to Protect/Support Digital Defenders

The EU's policies to protect and support and thus empower DDs are not to be found in a single, unified legal or policy document, but rather can be derived from several thematic documents, which each contain certain aspects relevant for the EU's overall policy towards the protection and support of DDs.

While at the core of their work DDs are HRDs and therefore the protection and support for DDs is based also on the general tools and instruments provided for the protection of HRDs, certain aspects of the work of DDs' require a more tailored approach.

1. EU policies to strengthen freedom of expression and privacy/data protection for DDs

This section will focus on those EU policies that are either explicitly aimed at the strengthening of freedom of expression and privacy/data protection for DDs, or do at least have a significant effect in this regard. The EU Guidelines on Human Rights Defenders and on Freedom of Expression online and offline are analysed as well as the European Commission's 'No Disconnect Strategy' and the EP's 'Digital

[50] See Internet Rights and Principles Coalition, 'The Charter of human rights and principles for the internet' (UN Internet Governance Forum 2014) <http://internetrightsandprinciples.org/site/wp-content/uploads/2014/06/IRPC_booklet_3rded_English.pdf> accessed 14 October 2015, which shows that practically all rights of the Universal Declaration of Human Rights do have an online dimension. See also CoE Committee of Ministers, 'Recommendation of the Committee of Ministers to Member States on a Guide to Human Rights for Internet Users' (16 April 2014) CM/Rec (2014) 6; and the explanatory memorandum thereto.

[51] See Article 19, 'The Right to Blog' (Policy Brief, 2013) <www.article19.org/data/files/medialibrary/3733/Right-to-Blog-EN-WEB.pdf> accessed 14 October 2014.

Freedom Strategy in EU Foreign Policy'. Furthermore, the EU Strategic Framework on Human Rights and Democracy as well as the EU Action Plan on Human Rights and Democracy (Commission, 2015a) are examined, with a view to their contribution to the overall EU policy framework regarding the strengthening of freedom of expression and privacy/data protection for DDs. Also the new approach of a Global Internet Policy Observatory (GIPO), supported by the EU, is introduced. Lastly, the activities of selected EU key institutions with regard to the matter at hand will be taken into consideration.

a) The 'No Disconnect Strategy' by the European Commission

The European Commission introduced the 'No Disconnect Strategy' in 2011, to support movements, which protested for democracy and against human rights abuses during the Arab Spring (Commission, 2011a, p. 14). This can be viewed as the 'EU's first major attempt to address digital rights in its external work' or the 'EU's digital human rights response to the Arab Spring'.[52] The strategy was created with the goal of 'providing on-going support to activists, political dissidents, bloggers, journalists and citizens living and operating under non-democratic regimes to help them organise, mobilise and exercise their rights through a variety of tools to circumvent arbitrary censorship and fight indiscriminate surveillance' (Council, 2014b, p. 85).

The strategy is based on four pillars. The first one, which is also the most relevant one in relation to DDs, is 'developing and providing technological tools to enhance privacy and security of people living in non-democratic regimes when using ICT'. The second pillar, which also bears relevance for DDs, is 'educating and raising awareness of activists about the opportunities and risks of ICT'. The other two pillars concern the collection of high quality intelligence about censorship and surveillance and the building of cross-regional cooperation to protect human rights (Wagner, 2012a, p. 14).

Three of the most important actions of the 'No Disconnect Strategy' are particularly important for the support and protection of DDs. One of them is the dissemination of so-called 'Internet-survival-packs' to activists, which are 'easy-to-use software/hardware packages helping people to bypass censorship and counter surveillance' (Leichtfried, 2012, p. 17). This action undertaken with the help of specialised NGOs, arguably has the most direct impact on DDs on the ground. The second action is 'stimulating EU companies to develop self-regulatory approaches (or join existing ones, such as the Global Network Initiative) so they stop selling despots their ICT tools of repression' (Ibid: p. 18). Preventing repressive governments from gaining access to tools which can be used to restrict access to the Internet or to censor it allows more space for the work of DDs. Lastly, hosting support, which means to 'help prohibited content reach its audience' and 'support for anonymous usage of the Internet' is part of the most important actions of the strategy (Ibid.).

The Strategy can also be seen as an important first step 'to build a European body of knowledge on communications technologies and how they may enable or harm human rights' (Wagner, 2012a, p. 14).

[52] Index on Censorship, 'Index policy paper: Is the EU heading in the right direction on digital freedom?' (20 June 2013) <www.indexoncensorship.org/2013/06/is-the-eu-heading-in-the-right-direction-on-digital-freedom/>, accessed 17 May 2015.

While the focus of the Strategy is external, it may also be of relevance for the internal sphere, for example, with regard to the human rights responsibilities of private actors.[53]

b) The 'Digital Freedom Strategy' of the European Parliament

The EP adopted the 'Digital Freedom Strategy in EU Foreign Policy' in December 2012, largely in reaction to the Arab spring. It was prepared by the European Parliament's Committee on Foreign Affairs (European Parliament, 2012a). The report explains, that 'the struggle for human rights has moved online' and explicitly refers to human rights violations by Iran, China and furthermore stresses that 'the Ben Ali government of Tunisia was, and the Al Assad regime in Syria is, well known for their sophisticated use of technologies against citizens' (European Parliament, 2012b, p. 16). The Rapporteur, Member of European Parliament Marietje Schaake, used crowd-sourcing in order to support the writing of the report, by putting a discussion paper online, so that various stakeholders could provide their input.[54] The Rapporteur also expressed her view that the European Instrument for Democracy and Human Rights and the No Disconnect Strategy were 'initial policy steps', but not ambitious enough.[55] The Strategy acknowledges the importance of uncensored access to ICT with regard to human rights and also refers to HRDs (European Parliament, 2012a, paras. 6-7 and 62), a term which encompasses DDs. The EP, *inter alia* calls on the Commission and the Council to 'support, train and empower' HRDs ' to use ICT in their activities and to assert the related fundamental rights of privacy, freedom of expression, freedom of assembly and freedom of association online (Ibid: para. 62). The Strategy also suggests that the restriction of digital freedoms should be taken 'into full consideration in the EU's relations with third countries' and that conditionality clauses regarding digital freedoms should be included in negotiations and dialogues with third countries (Ibid: paras. 65-66), which, however, does not seem to have been implemented in practice. Finally, the EP has also worked towards the inclusion of Internet freedom funds into the EIDHR (European Parliament Budget Adoption, 2014, Chapter 19 04 01, Remarks; see also Wagner, 2012a, p. 14).

In 2015, the European Parliament decided to give its annual Sakharov prize for freedom of thought to the Saudi Arabian blogger and human rights activist Ralf Badawi, who was sentenced to a draconic punishment for running an online platform for political and religious debate and thus can be considered a Digital Defender.

c) EU Guidelines on Human Rights Defenders and on Freedom of Expression online and offline

In order to provide guidance in this important field of EU action, the Council of the EU in 2004 adopted the EU Guidelines on Human Rights Defenders, which should contribute to the implementation of the UN Declaration on Human Rights Defenders of 1998. They were revised only four years later and now provide a solid basis for the EU action in this regard.[56] However, there would be need for an update

[53] See subchapter II.E.3 'Human rights responsibilities of private actors'.
[54] marietjeschaake.eu, 'European Parliament endorses first ever Digital Freedom Strategy' (10 December 2012) <http://www.marietjeschaake.eu/2012/12/european-parliament-endorses-first-ever-digital-freedom-strategy/> accessed 16 August 2015.
[55] Ibid.
[56] See FRAME D7.2 2015 (n 48) 139 et seq.

again as important developments in EU human rights policies are not yet reflected in the Guidelines, like the role of human rights focal points and liaison officers or the Human Rights Defenders Mechanism. However, as shown by a recent study, they also need to be more systematically disseminated and implemented (Bennet, 2015).

The Guidelines on HRD of 2008 do not include the needs of digital defenders. They were adopted before the significance of online applications for Freedom of Expression and other Human Rights was fully recognised (Council, 2008). In May 2014, the Council adopted the EU Guidelines on Freedom of Expression Online and Offline, which deal with support to freedom of opinion and expression. The EU emphasizes that these rights need to be protected online as well.[57] Within the so-called 'Priority Areas of Action' of the Guidelines, there are some areas of specific relevance to DDs. First and foremost, the EU commits itself to combat 'violence, persecution, harassment and intimidation of individuals, including journalists and other media actors, because of their exercise of the right to freedom of expression online and offline, and combating impunity for such crimes' (Council, 2014a, B.1.).

The 'Operational Guidelines' as part of the document refer several times to HRDs working online, therefore including DDs within the scope of the actions set forth in the 'Operational Guidelines'. For example, according to the document, the EU will '[...] continue to provide [...] human rights defenders [...] with the technical tools and support they need in order to exercise their right to freedom of expression online [...]' (Ibid: para. 31 h.). Promotion of, and respect for, 'human rights in cyberspace and other information and communication technologies' (Ibid: para. 33) is another goal of the Guidelines. This encompasses 'advocating for the application of all human rights, including the right to freedom of opinion and expression, both offline and online' (Ibid: para. 33 a.), and to work 'against any attempts to block, jam, filter, censor or close down communication networks or any kind of other interference that is in violation of international law' (Ibid: para. 33 d.), as well as to provide 'technical support to individuals on the ground to help counter such attempts, when necessary' (Ibid: para. 33 e.).

Also, representatives of the EU and the EU Member States should, when visiting third countries, be 'fully briefed on the situation of freedom of opinion and expression, both online and offline' and meet with 'journalists, human rights defenders and media actors' (Ibid: para. 40). Some of the actions viewed by the EU as examples of violation or undermining of the right to freedom of opinion and expression are threats to DDs, such as 'attacks on a person because of his or her exercise of the freedom of expression', 'Internet restrictions by operators' or 'restrictions on the right of privacy and data protection' (Ibid: Annex I). Consequently, the needs of DDs for protection and support have been identified and the EU Guidelines on Freedom of Expression Online and Offline suggest concrete steps on how to address them. Different from the EU Guidelines on Human Rights Defenders they cover the online dimension of threats to human rights on an equal basis and suggest specific actions to counter them.

[57] Council of the European Union, 'The Council adopts the Guidelines on Freedom of Expression online-offline' (12 May 2014) <http://eeas.europa.eu/delegations/documents/the_council_adopts_the_guidelines_on_freedom_of_expression_online-offline_12_may_2014_en.pdf> accessed 17 May 2015.

The EU Guidelines on Freedom of Expression Online and Offline also comprise a short section on implementation and evaluation, which *inter alia* tasks the European Council's Working Group on Human Rights (COHOM) to support the implementation of the Guidelines, to 'develop additional guidance for action by EU missions, in particular regarding systemic issues and individual cases' and to 'adopt 'lines to take' documents on key questions and topical issues when necessary' (Ibid: para. 70). This seems to be an appropriate opportunity to explicitly include protection and support of DDs in guidance and 'lines to take' documents for EU missions and other EU institutions.[58] This would ensure that the importance of special support to DDs with regard to the implementation of the Guidelines, as well as the implementation of thematically related EU Human Rights Guidelines, such as the EU Guidelines on Human Rights Defenders, is brought to the attention of the EU institutions responsible for impementing the EU's human rights framework on the ground. However, COHOM has not, as yet, developed the 'additional guidance', while the 'lines to take' do exist, but are not available to the public. The relevance of other EU human rights guidelines can only be highlighted without going into detail. For example, the recent Guidelines on Promotion and Protection of Freedom of Religion and Belief, or the Guidelines to Promote and Protect the Enjoyment of All Human Rights by LGBTI Persons, are also of importance for DDs in this fields.

d) EU Strategic Framework and Action Plan on Human Rights and Democracy

In June 2012, the EU adopted a 'Human Rights package', comprising the EU Strategic Framework on Human Rights and Democracy (Strategic Framework), the Action Plan on Human Rights and Democracy (Action Plan) and the appointment of the EU Special Representative on Human Rights.[59] The Strategic Framework adopted on 25 June 2012 (Council, 2012, Annex II) sets out 'the principles, objectives and priorities of EU policy'[60] in the field of human rights and democracy. The Action Plan contains concrete objectives, in order to implement the provisions of the Strategic Framework. The Action Plan (2012-2014) expired at the end of 2014. According to the European External Action Service (EEAS), the Action Plan (2012-2014) was successful, with 'about 90% of actions completed by the end of 2014'.[61] A new EU Action Plan on Human Rights and Democracy for the period from 2015 to 2019 was proposed by the end of April 2015 and adopted in July 2015 by the Council (Council, 2015b).[62]

[58] See for example Delegation of the European Union to Turkey, 'European Union Local Strategy to Support and Defend Human Rights Defenders in Turkey' <http://avrupa.info.tr/fileadmin/Content/Files/File/EIDHR/EU_local_strategy_on_HRD_draft_07012011_L-EN.pdf> accessed 12 November 2015.

[59] See also European Commission, 'EU proposes new Joint Action Plan on Human Rights and Democracy' (29 April 2015) <http://europa.eu/rapid/press-release_IP-15-4893_en.htm> accessed 22 May 2015.

[60] Cristina Churruca Muguruza, Felipe Gómez Isa, Daniel García San José, Pablo Antonio Fernández Sánchez, Carmen Márquez Carrasco, Ester Muñoz Nogal, María Nagore Casas and Alexandra Timmer, 'Report mapping legal and policy instruments of the EU for human rights and democracy support' (FRAME D12.1 2014) 5.

[61] Anna-Luise Chané, Nicolas Hachez, Brecht Lein, Karolina Podstawa and Jan Wouters, 'The Post-2014 EU Action Plan on Human Rights and Democracy. A Policy Brief' (FRAME) 3 <http://www.fp7-frame.eu//wp-content/materiale/policy_brief/02-FRAME%20Policy%20Brief%20No%202%20--Post%202014%20SFAP%20Policy%20Brief.pdf> accessed 17 November 2015.

[62] See also European Commission, 'EU proposes new Joint Action Plan on Human Rights and Democracy' (n 59).

As DDs are HRDs, mechanisms and actions which are aimed at or contribute to the support and protection of HRDs, are also relevant for DDs.[63] The Action Plan (2015-2019) contains a set of 34 objectives, each of them encompassing two or more concrete actions aimed at implementing the objective. While the Action Plan (2015-2019)[64] does not explicitly refer to DDs, several of its objectives are highly relevant for the support and protection of DDs, for example objectives such as 'Invigorating support to Human Rights Defenders (HRDs), including in international and regional fora' (Council, 2015b, Annex Objective 9) and 'Addressing threats to civil society space' (Ibid: Objective 10). The latter objective should be reached by the following actions:

a. 'Promote and support legislation, policies and mechanisms designed to protect HRDs; in particular, strengthen the implementation of the relevant EU Guidelines and the EU HRD Mechanism launched under the EIDHR'

b. 'Oppose through public or non-public messaging unjustified restrictions to freedom of peaceful assembly and association, confinement of civil society's space and attempts to hinder the work of civil society, including HRDs, such as the criminalisation of HRDs, ensuring these issues are regularly raised in bilateral meetings, human rights dialogues, and UN and regional fora' (Ibid: Objective 10).

The objective 'Protecting and promoting freedom of expression online and off line' (Ibid: Objective 11a) is also of particular relevance to the work of DDs as it commits the EU to take 'active steps to prevent and respond to violence against […] bloggers, enabling them to work in safety and security […] without fear of harassment, political pressure, censorship and persecution […]'.

The action plan emphasises the role of HRDs working to uphold economic, social and cultural rights, like, in particular, labour rights or to counter 'land grabbing' (Council, 2015b, Objective 17, Action c). Indeed, HRDs have complained that human rights focal points or EU embassies at EU delegations are less responsive regarding concerns related to economic, social or cultural rights.

Furthermore, DDs are a subgroup of HRDs whose work can be strongly affected by the actions and business practices of private businesses.[65] Therefore, the objective 'Advancing on Business and Human Rights', which encompasses development and implementation of 'National Action Plans (NAPs) on the implementation of the UN Guiding principles' (Ibid: Objective 18, Action c), could also have a positive impact on the protection of DDs if properly taken into account. Unfortunately, only few NAPs have been elaborated so far (Pearson, 2015, 140; Commission, 2015d, p. 7).[66]

[63] For an analysis of the Strategic Framework and the Action Plan (2012-2014) with a focus on its contribution to the protection of HRDs, see: FRAME D7.2 2015, (n 48) chapter VI.
[64] See for a first analysis Wolfgang Benedek, 'EU Human and Fundamental Rights Action in 2014' (n 42) 82.
[65] See Section IV.B., 'Relationship to export controls of surveillance technology' and section IV.E. 'Role of private business with regard to protection of DDs'.
[66] See also subchapter II.E.3 'Human rights responsibilities of private actors'.

e) Global Internet Observatory

Of potential relevance for the topic of ICT and human rights is the new GIPO. It is an initiative by the European Commission, announced already in 2013,[67] which should serve as an open-access tool for stakeholders to better understand 'internet-policy regulatory and technological developments around the world'.[68] Its goal is to 'make it easier for stakeholders with limited resources to follow, understand and engage with internet governance and policy' (Commission, 2014a, p. 7). This should also include human rights policies as part of Internet governance. An increasing understanding about Internet-related policy and technological developments will also contribute to a better understanding of the influence of these developments on human rights in general and the work of DDs in particular. Since the GIPO was announced, a tender for the GIPO online platform was launched and on 17 December 2014, a contract for the technical development of the online platform was signed with the winning consortium, consisting of three companies.[69] The overall idea of GIPO is to provide 'an online platform to automatically collect, analyse and visualize real-time information on Internet policy developments and decisions across the world'.[70] In order to achieve this, the concept of GIPO foresees to apply new IT technologies, like data mining, semantic analysis and data visualisation tools on the available data, such as articles, papers and websites in order to 'overcome information overload, fragmentation and complexity'.[71] Some of the core design principles of the GIPO online platform are the use of existing free and open source software solutions, a modular design and a focus on core functions.[72] Regarding the timeframe for the operationalization of the online platform, a step-by-step implementation of the necessary elements is planned until December 2016.[73]

f) Activities of selected EU key institutions

In order to get the full picture of the EU's policies towards DDs, it is important to examine the activities of EU key institutions in this field. Therefore, this section will look at the activities of the EEAS, COHOM, the European Union Special Representative for Human Rights (EUSR) and the relevant EP committees.

[67] European Commission, 'Commission plans guide through global internet policy labyrinth' (13 May 2013) <http://ec.europa.eu/digital-agenda/en/news/commission-plans-guide-through-global-internet-policy-labyrinth> accessed 17 May 2015.

[68] European Commission, 'The Global Internet Policy Observatory (GIPO)' (last updated on 22 April 2015) <https://ec.europa.eu/digital-agenda/en/global-internet-policy-observatory-gipo> accessed 7 August 2015.

[69] Ibid.

[70] Cristina Monti and Maciej Tomaszewski, 'Building GIPO the Global Internet Policy Observatory', 9 <www.giponet.org/sites/default/files/1.%20Building%20GIPO%20%20the%20Global%20Internet%20Policy%20Observatory.pdf> accessed 7 August 2015.

[71] Ibid 10.

[72] Ibid 11.

[73] Luis Meijueiro, 'Technical Development of the Online Platform for the Global Internet Policy Observatory – SMART 2014/0026' (April 2015) <www.giponet.org/sites/default/files/3.%20GIPO%20Technical%20Platform%20proposal.pdf> accessed 7 August 2015.

(1) The EEAS and the EU Missions

While the EEAS and the EU diplomatic missions[74] already became a 'cornerstone of the EU's engagement with HRDs in general',[75] this subsection analyses the EEAS and EU missions' activities which are especially relevant for the strengthening of freedom of expression, freedom of association and privacy/data protection for DDs. Indeed, the EEAS plays an important role in the EU's policy framework in those thematic areas. Within both the Action Plan (2012-2014) and the new Action Plan (2015-2019), the EEAS is responsible for the implementation of several objectives and actions relevant for DDs. The EEAS also led in the elaboration of the EU Guidelines on Freedom of Expression Online and Offline (Council, 2014b, p. 86) and has been assigned various tasks within the Guidelines in order to implement and to promote its goals. For example, the EEAS should, in cooperation with the Commission services, 'build on existing actions such as the 'No Disconnect Strategy', aiming to uphold the EU's commitment to ensure that the Internet and other information and communication technologies remain a driver of political freedom, democratic development and economic growth' (Council, 2014a, para. 48). Other relevant EEAS tasks within the Guidelines are *inter alia* connected to information sharing regarding projects on freedom of expression in third countries (Ibid: para. 51), active engagement 'in debates at the Internet Governance Forum (IGF) and the World Summit on the Information Society (WSIS) Forum with a view to promoting a human rights perspective and a multi-stakeholder model and to foster awareness on freedom of opinion and expression issues in co-operation with civil society' (Ibid: para. 56) and to monitor and to offer guidance 'on persisting media freedom issues, offline as well as online' in the context of the EU's enlargement policy (Ibid: para. 60).

In the context of consultations with civil society regarding improvements in the engagement with, and protection of, journalists and bloggers, an online public consultation was launched in June 2013 by the EEAS (Council, 2014b, p. 86).

EU delegations have a particular role to play when it comes to the protection and support of HRDs in general and DD in particular. Human Rights Focal Points within the EU delegations are expected to follow repressive measures, report on it and take action. This includes formulating demarches, trial monitoring or empowering HRDs by inviting them to civil society meetings with the delegations and providing public support. The practice appears to differ depending on how committed the focal points and also the heads of delegation are in supporting HRDs. There are examples of good practice, but also of lack of interest. There are sometimes limits to the capacity of the delegations, which means that HRDs outside the capitals receive significantly less attention, a problem also addressed by the Action Plan 2015-2019.[76]

Some of the embassies of EU Member States have particular activities in this field, like the Netherlands. As a member of the Freedom Online Coalition (FOC), the Netherlands are committed to support freedom of expression of DDs, which is partly done with the help of specialized NGOs. In this respect,

[74] The term 'EU diplomatic missions' covers both the EU delegations and EU Member States' embassies.
[75] For an analysis of the EEAS in the EU's engagement with HRDs, see: FRAME D7.2 2015 (n 48) chapter VI.
[76] This finding is based on interviews. See Council, 2015b, para. 9 b. See also FRAME D7.2 2015 (n 48).

the actions of the Netherlands for the support of DDs are an example for unilateral Member States activities contributing to the realisation of the EU's policy goals.

(2) Activities of COHOM

The Working Group on Human Rights of the Council of the European Union plays a crucial role within the EU's policy framework regarding the thematic areas of freedom of expression and privacy/data protection in connection with DDs. Not only does COHOM play 'an important role under the operational part' of the European Union Guidelines on HRDs,[77] it also has its role in the implementation and evaluation of the EU Guidelines on Freedom of Expression. COHOM and its task force on freedom of expression support the implementation of the Guidelines and are supposed to 'develop additional guidance for action for EU missions, in particular regarding systemic issues and individual cases' (Council, 2014a, para. 70). Additionally, COHOM is to undertake an evaluation of the implementation of the Guidelines after three years, in consultation with civil society and other actors, in which, *inter alia*, HRDs should be involved (Ibid: para. 71).

(3) Activities of the EU Special Representative on Human Rights

Since the appointment of Mr. Stavros Lambrinidis as the first thematic EU Special Representative on Human Rights in 2012 (Council Decision, 2012) and the extension of his mandate until 2017 (Council Decision, 2015), he is supposed to thematically focus on 'protecting NGOs and human rights defenders and expanding the space in which they operate' (Council, 2014b, p. 14). The EP has encouraged the EUSR to make digital freedoms as well as the 'No Disconnect Strategy' part of his key priorities (European Parliament, 2012c, para. 12). As there are no publicly available reports on the EUSR's activities, little is known about his concrete actions with regard to DDs. Sometimes, he has been criticised for not being active enough on HRDs, but this might also be due to the lack of reporting on his activities.

(4) Activities of the European Parliament's Committees

Among the EP's committees, the Committee on Foreign Affairs (AFET) has taken a lead on issues relevant for DDs as can be seen from its report on a digital freedom strategy in EU Foreign Policy, adopted by the EP in December 2012. A recent report on 'Human rights and technology: the impact of intrusion and surveillance systems on human rights in third countries' was prepared with the EP Sub-Committee on Human Rights (DROI), and adopted by the plenary EP in September 2015 (European Parliament, 2015b and 2015c).

DROI is actively engaged with HRDs in general and also engages with topics such as ICT and human rights. For example, already in 2010 DROI commissioned a study on 'Information and Communication Technologies and Human Rights' (Horner, Hawtin and Puddephatt, 2010), which identified the major implications of ICT on human rights, both with regard to new opportunities and threats. A briefing paper entitled 'After The Arab Spring: New Paths For Human Rights and the internet in European Foreign Policy' (Wagner, 2012a) provided the first analysis on the topic. The DROI Sub-Committee has a practice of hearings of prominent HRDs, which could include DDs, thereby giving them

[77] For COHOM's role with regard to the EU Guidelines on HRDs, see FRAME D7.2 2015 (n 48) chapter VI.

more support. In its regular resolution on the Annual Report on Human Rights and Democracy in the World of the EU Council the EP calls for increased support for media freedom, protection of bloggers and uncensored access to the Internet (digital freedom) (European Parliament, 2015a). The EP also adopts specific resolutions on the persecution of HRDs, like in the case of Azerbaijan (Council, 2015a, 153). All these activities help creating awareness on the situation and needs of DDs, which need to be followed up by concrete action like support from the EU's financial instruments.

2. Role of the European Instrument for Democracy and Human Rights

The EIDHR serves as the EU's main instrument for the support of 'the promotion of democracy and human rights in non-EU countries'. With a budget of 1.104 billion Euro for its initial 2007-2013 period[78] and an increased financial envelope of 1.332 billion Euro for the subsequent 2014-2020 period (European Parliament and Council Regulation, 2014, Art. 10), it is by far the largest funding instrument for human rights world-wide. As the EIDHR plays an important role with regard to the EU's engagement with HRDs,[79] this subsection will analyse the EIDHRs role in protection and support for DDs as a subgroup of HRDs, including actions which already have been carried out, as well as options for further actions under the EIDHR legal framework, including actions under the future EU HRDM.

The initial EIDHR (2007-2013) programme explicitly referred to support and solidarity for HRDs in its objectives (European Parliament and Council Regulation, 2006, Art. 1 para. 2 a.), and to the promotion of freedom of association and assembly, freedom of opinion and expression as well as 'unimpeded access to information, and measures to combat administrative obstacles to the exercise of these freedoms, including the fight against censorship' in its scope (Ibid: Art. 2 para. 1 a. i.). While there is no explicit reference made to DDs, there is no question that DDs and their work are implicitly encompassed in the objectives and scope of the initial EIDHR legal framework. Internet access was one of the 'thematic points that the instrument chose to focus on in its 2011-2013 Strategy Paper' and the EIDHR 2012 global call for proposals includes 'projects to fight cyber-censorship and protect confidentiality of activists' (Commission, 2011a, p. 15). An EIDHR report explains how, through the NGO Front Line Defenders, hundreds of organisations were supported in protecting their ICT infrastructure.[80] In a more recent legal framework for the EIDHR (2014-2020) period, the thematic field of human rights online is addressed even more specifically than in its predecessor. While there is still no explicit reference to DDs or HRDs working online, the scope of the EU assistance under the EIDHR encompasses the promotion of 'freedom of association and assembly, [...] freedom of opinion and expression, [...] unimpeded access to information, a free press and independent pluralistic media, both traditional and ICT-based and internet freedom and measures to combat administrative obstacles to the exercise of these freedoms, including the fight against censorship' (European Parliament and Council Regulation, 2014, Art. 2). In addition, also within the set of 'Specific objectives and priorities of the EIDHR', the 'Objective 3 - Support to democracy' refers to freedom of expression online and offline (Ibid: Annex Para. 3). This fact, combined

[78] European Commission, 'Democracy and Human Rights, Small Grants' <www.eidhr.eu/whatis-eidhr> accessed 3 June 2015.

[79] For the EIDHR's role with regard to the EU's engagement with HRDs, see FRAME D7.2 2015 (n 48) chapter VI.

[80] European Commission, 'Delivering on Human Rights Defenders' (Highlights of the Semester January-June 2012) 10 <www.eidhr.eu/files/dmfile/EIDHR_DeliveringonHumanRightsDefenders_Report.pdf> accessed 14 October 2015.

with the continued focus of the EIDHR on the effective support to HRDs (Ibid: Annex Para. 1) makes the current EIDHR a suitable instrument for the support and protection of DDs.

The increased engagement of the EU with the thematic areas of the exercise of human rights online and the work of HRDs online is also reflected in the 2015 Annual Action Programme (AAP) for the EIDHR. Of the nine actions outlined in the Annual Action Programme's Annexes, three are thematically relevant for DDs, notably 'Supporting Human Rights and their Defenders where they are the most at risk – EIDHR facility', 'Supporting Democracy - Media and freedom of expression in the framework of the pilot exercise for democracy' and 'Supporting Human Rights priorities – EIDHR global call 2015' (Commission, 2015b, Art. 1). While the actions dealing with HRD-support are broad and ambitious in scope, they do not refer to DDs or the work of HRDs online. Interestingly, freedom of expression (online and offline) is not mentioned as a cross-cutting issue for the implementation of the action, while other issues, such as indigenous peoples' rights, the rights minorities and persons with disabilities, the rights of people affected by caste based discrimination' are listed (Ibid: Annex 2, p. 4). The action dealing with media and freedom of expression mainly concerns engagement with journalists and media actors.

According to the AAP, 'governments have woken up to the risk of allowing their citizens new possibilities to exercise freedom of expression'. They are 'introducing new measures to control new media such as increasing the liability of intermediaries[81] for the material stored on or moving across their networks, introducing filtering and blocking mechanisms, and criminalising expression' (Ibid: Annex 2, p. 3). This, combined with the fact that the activities in the framework of this action could cover *inter alia* free, pluralistic and investigative reporting, innovative news production across a diversity of platforms (on-line and offline) and the constructive use of publicly available data as well as the use of 'ICTs to promote freedom of expression, taking into account privacy and personal data protection', makes the AAP's action on media and freedom of expression a potential tool to support the work of DDs (Ibid: Annex 2, p. 7). Lastly, also the action 'Supporting Human Rights priorities – EIDHR global call 2015' has a component relevant for DDs as one out of five target objectives.is 'Supporting Human Rights and their Defenders where they are the most at risk' (Ibid: Annex 1, p. 3). As DDs are not explicitly mentioned as one of the 'categories of HRDs at risk' (Ibid: Annex 2, p. 6) it is suggested to foresee an online component of the supported categories of HRDs, which would strengthen support for DDs as well.

In conclusion, the EIDHR offers an important instrument with regard to fields directly related to the support of DDs. These fields include support and protection for HRDs and the promotion of freedom of expression online. However, the EIDHR does not focus on DDs as a specific subgroup of HRDs and the specific needs of HRDs using digital means are not sufficiently taken into account, thus falling short of the commitments made under the No Disconnect and Digital Freedom Strategies outlined above.

a) Small grants programme to HRDs in need of urgent support

Since its initial establishment, the EIDHR has included the possibility to carry out 'Ad hoc Measures' in the form of allocation of 'small grants on an ad hoc basis to human rights defenders responding to urgent protection needs' (European Parliament and Council Regulation, 2006, Art. 9 para. 1). Since 2010

[81] See also Subchapter II.E.2. of this case study 'Intermediary liability' on the issue of liability of intermediaries inside the EU.

'more than 400 HRDs and organisations in over 30 countries have received this type of direct support', which encompassed *inter alia* 'coverage of legal fees, medical expenses including rehabilitation of torture victims, operational survival for local organizations, or urgent relocation of HRDs at risk' (Commission, 2014b, p. 3). However, there is no specific information available on whether or not the small grants programme included support to DDs, which, however, would be fully possible.

b) Temporary relocation system

The initiative to provide temporary shelter to HRDs, which was undertaken under the Czech EU Presidency in 2009,[82] has been another initiative within the framework of the EIDHR relevant to the protection of DDs. A study on existing shelter programs, which was published by the Commission in 2012, does not deal with DDs as a distinct group, but analysed shelter for HRDs in general.[83] However, it is clear that DDs are eligible for temporary relocation under the temporary shelter initiative by the mere fact that they are HRDs as well.

c) EU HRDs Mechanism

The EU HRDs Mechanism[84] is presented as a 'comprehensive human rights defenders mechanism addressing the most difficult situations faced by human rights defenders in the world and providing support to the local actors who strive to promote and defend them'[85] and will include a broad range of measures with regard to support and protection of HRDs.[86] As for DDs, the mechanism will encompass measures not only for physical protection of DDs, but also include 'digital protection' under its 'Priority 2: Providing urgent, medium and long term support to HRDs'.[87] The consortium of 12 international NGOs to establish and run the HRDM will be under the lead of 'Front Line Defenders', a very experienced NGO based in Ireland and supporting HRDs in about 80 countries worldwide. The board consists of Frontline Defenders, Reporters without Borders (RSF), World Organization against Torture (OMCT) and International Federation for Human Rights (FIDH). The Secretariat of the HRDM has been established in Brussels, where it started work on 1 October 2015 for an initial period of three years.[88]

---

[82] FRAME D12.1 2014 (n 60) 128.

[83] GHK Consulting Ltd/ HTSPE, 'Mapping of temporary shelter initiatives for Human Rights Defenders in danger in and outside the EU, Final Report' (February 2012) <www.europarl.europa.eu/meetdocs/2009_2014/documents/droi/dv/504_mapping_/504_mapping_en.pdf> accessed 27 June 2015.

[84] EIDHR 'Human Rights Defenders Mechanism', to be established in accordance with European Parliament and Council Regulation (EU) 235/2014 of 11 March 2014 establishing a financing instrument for democracy and human rights worldwide [2014] OJ L 77/85.

[85] European Commission, 'Establishing a European Union Human Rights Defenders Mechanism, Open Call for Proposals 2014, Guidelines for grant applicants' (DG DEVCO, 3 December 2014) 4 <https://webgate.ec.europa.eu/europeaid/online-services/index.cfm?ADSSChck=1425290260269&do=publi.getDoc&documentId=145307&pubID=136316> accessed 27 June 2015.

[86] For a more detailed overall analysis of the mechanism, see: FRAME D7.2 2015 (n 48) chapter VI.

[87] European Commission, 'Establishing a European Union Human Rights Defenders Mechanism' (n 85) 6.

[88] See Front Line Defenders, 'Human Rights Defenders Mechanism' <www.frontlinedefenders.org/EUHRD Mechanism> accessed 14 October 2015.

While other measures foreseen under the mechanism such as a 'permanent helpline for HRDs (24h/7)', legal support or urgent relocation can be relevant for the protection and support for DDs as well, digital protection is the only measure in the future EU HRDM which explicitly aims to protect the digital security of HRDs. The details of this action were under development at the time of writing.

d) Concrete EIDHR Actions for the Protection and Support of DDs

While there is no comprehensive list of EIDHR Actions for the protection and support of DDs, some examples for such actions can be provided and included in the overall analysis. One such example is 'financial support to journalists and NGOs working on media independence and freedom of expression', in particular an 'EIDHR funded project run by Reporters Without Borders aiming to fight cyber censorship and develop the free flow of digital information' (Council, 2013, p. 98). One of the main activities of the project had been 'the creation and maintenance of a virtual shelter', which is 'a secured space where independent journalists can work and publish news that would otherwise be censored' (Ibid). Within the 2012 EIDHR call for proposals, a lot was dedicated to actions against cyber censorship and to the promotion of digital freedom. (Ibid).[89]

e) Conclusions with regard to the EIDHRs role in protection and support for DDs

An analysis of the EIDHR's legal framework and the initiatives and mechanisms funded by the EIDHR makes clear that the EIDHR plays a crucial role in the EU's overall policy framework on the protection and support for DDs. While support for HRDs and the promotion of freedom of association and assembly, as well as freedom of opinion and expression, are amongst the objectives of the instrument, explicit references to DDs as a distinct group cannot be found. Nonetheless, the overall aims of the EIDHR and several of its concrete actions are highly relevant for the protection and support of DDs, especially with a view to the topics of freedom of expression, freedom of assembly and privacy, data protection and surveillance. The fact that DDs are not explicitly mentioned in the EIDHR legal framework as a distinct subgroup of HRDs is understandable in view of the aspects of simplicity and effectiveness of the EIDHR's normative framework. However, it also conceals the different and special needs of DDs with regard to support and protection. While other subgroups of HRDs, e.g. 'activists' and 'journalists' - are specifically mentioned in documents connected to the EIDHR's actions, e.g. with regard to thematic areas such as 'fighting cyber censorship' and the promotion of 'digital freedom and security', DDs do not get the same level of attention within the framework of the EIDHR. This may be due to the fact that the use of digital means has become quite common for HRDs in general. However, this would also mean that specific action is needed to protect human rights work online.

Bearing in mind the ever-growing importance of the Internet as a tool for the promotion and exercise of human rights, it seems reasonable to adjust the future focus of the EIDHR in a way that will increasingly focus on the use of ICT by HRDs. This could include recognition of DDs as a distinct group of HRDs with

[89] 'Actions aiming at fighting cyber censorship and promoting digital freedom and security supporting projects to counter violations of human rights through Information and Communication Technologies and to safeguard privacy and freedom of expression in those regions where activists, journalists and human rights defenders are most at risk' (Council, 2013, p. 98).

special needs, and would lead to a more tailored and effective support for their work towards the protection and promotion of human rights in cyberspace.

E. Related Issues

There are several thematic fields and issues that are strongly interlinked with the topic of the support of DDs. The protection of DDs and the protection of journalists are overlapping thematic areas, which is reflected by the fact that journalists who promote and protect human rights online by means of journalistic work, have a double role as DDs and as journalists.

Export controls for surveillance technology constitute another related issue. Sophisticated surveillance technology can massively hinder the work of DDs and expose them to repressions of authoritarian governments. As such, the EU's policy towards export controls for these technologies strongly influences the situation of DDs.

Some important multilateral activities of some EU member states, namely the Freedom Online Coalition and the Digital Defenders Partnership, are analysed with a view to their contribution to the realisation of the EU's policies towards DDs. Furthermore, the EU's cooperation with other international organizations like the CoE, OSCE, UNESCO and the United Nations when it comes to an effective promotion of the EU's DD policy at international fora and the role of the private sector with regard to the protection of DDs will be analysed.

1. Relationship of protecting DDs and Safety of Journalists' agenda

It is a fact that the EU sees the protection of journalists and the protection of HRDs (including DDs) as strongly interlinked. This is also apparent by the formulations used in the EU Guidelines on Freedom of Expression Online and Offline. Accordingly, the EU Member States' 'efforts to protect journalists should not be limited to those formally recognised as such, but should also cover support staff and others, such as 'citizen journalists', bloggers, social media activists and human rights defenders' (Council, 2014a, para. 5). Congruently, the EIDHR AAP 2015 confirms that 'ensuring the safety of journalists and a free and accessible online information exchange is therefore vital for democracy' (Commission, 2015b, Annex 4, p. 3).

2. Relationship to export controls of surveillance technology

The export of surveillance technology relates closely to the protection of DDs. Indeed, 'governments and businesses across the world are using ICTs to monitor the behaviour of citizens in increasingly sophisticated and hidden ways'. This is a development boosted by the so-called war on terror, which encouraged governments to develop and use enhanced surveillance technology to increase public security (Horner, Hawtin and Puddephatt, 2010, p. 9). The same technology, however, is often used to monitor the activities of citizens, particularly journalists or online activists (Human Rights Council,

2013b, paras. 52-53).[90] According to the OpenNet Initiative (ONI), information controls are increasing rapidly and widely around the world.[91]

While 'some of the most sophisticated censorship systems have been developed by Western companies, this technology is 'in many instances' [...] 'sold directly to authoritarian regimes'. There are 'various ways in which companies in democratic countries can assist with, or contribute to, illegal censorship and surveillance systems in other countries' (Horner, Hawtin and Puddephatt, 2010, p. 32). The EP is concerned about the problem as well. The report of its Committee on Foreign Affairs on 'Human rights and technology: the impact of intrusion and surveillance systems on human rights in third countries' finds that 'EU-based companies have an important share of the global market in ICTs, in particular when it comes to exporting surveillance, tracking, intrusion and monitoring technology' (European Parliament, 2015c, para. T). In this context, it 'recalls the still very incomplete nature of the EU dual-use regime, namely the EU dual-use regulation, when it comes to the effective and systematic export control of harmful ICT technologies to non-democratic countries' (Ibid: para. 35). The report also contains concrete suggestions for measures in order to prevent or at least diminish the negative effects of the export of surveillance technology. Also the Parliamentary Assembly of the Council of Europe has adopted a resolution on the problems of mass surveillance practices and urges the Council of Europe Members and Observer States 'to refrain from exporting advanced surveillance technology to authoritarian regimes' (Council of Europe, 2015, para. 19.6).

With regard to the export of such technology it is important to note that such 'typical censorship and surveillance technologies are sold as systems and are not typically used for multiple overlapping purposes', which means that they are not 'dual use' but 'single use' in the sense that they are 'typically built and maintained for one specific purpose: limiting individual human rights' and 'so fundamentally designed to invade basic human rights that it becomes difficult to ascertain 'legitimate' or 'lawful' purposes, within which such technologies might be used' (Wagner, 2012b, p. 7).[92] Accordingly, appropriate regulation has been requested to prevent abuses of human rights by exporting such surveillance technologies (European Parliament, 2015c).[93]

Some new export controls including Internet surveillance and intrusion software were introduced by amendments to Council Regulation (EC) No. 428/2009 in 2014, but implementation depends on the

[90] See also Reporters without Borders, 'Enemies of the Internet. 2013 Report – Special Edition: Surveillance' (12 March 2013) 3-5 <http://surveillance.rsf.org/en/wp-content/uploads/sites/2/2013/03/enemies-of-the-internet_2013.pdf> accessed 9 October 2015.

[91] See the publications of the OpenNet Initiative, 'Access Denied' (2008), 'Access Controlled' (2010) and 'Access Contested' (2011), available at OpenNet Initiative, 'ONI Access: Denied Controlled Contested' <http://access.opennet.net> accessed 14 October 2015.

[92] See also Tim Maurer, Edin Omanovic, Ben Wagner, 'Uncontrolled Global Surveillance. Updating Export Controls to the Digital Age' (March 2014) <https://digitalegesellschaft.de/wp-content/uploads/2014/03/Uncontrolled-Surveillance_March-2014_final.pdf> accessed 9 October 2015; Freedom Online Coalition, 'Statement on the Use and Export of Surveillance Technology' <www.freedomonlinecoalition.com/wp-content/uploads/2014/10/2-FOC-Joint-Statement-on-the-USe-and-Export-of-Surveillance-Technology-October-2014.pdf> accessed 9 October 2015.

[93] See also FIDH, 'Surveillance technologies "Made in Europe": Regulation needed to prevent human rights abuses' (Position Paper, 1 December 2014) <www.fidh.org/IMG/pdf/surveillance_technologies_made_in_europe.pdf> accessed 9 October 2015.

goodwill of the EU Member States. The first report on the implementation of this regulation after the amendments only informs about the setting up of a 'surveillance technology expert group' (Commission, 2015c).

3. Relationship with Member States' activities to protect and support DDs

The activities of EU MS in the field of protection and support for DDs have to be analysed and put in the context of the EU's policy framework on HRDs and freedom of expression, in order to explore options for potential use of synergies and the avoidance of duplication of mechanisms and structures and thus increase effectiveness. Therefore, this subchapter will analyse the two most important multilateral actions in this field, in which EU member states play an important role, as well as the actions of the Netherlands as an example of good practice of a single EU member state to strengthen support and protection for DDs.

a) Freedom Online Coalition

The FOC is a global group of 26 governments, dedicated 'to advance internet freedom',[94] 12 of which are EU Member States.[95] The United States is also a founding member of the FOC.[96] The coalitions' participating states have dedicated themselves to share information amongst themselves on violations and other measures undermining freedom of expression and other human rights on the Internet.[97] For this purpose, they cooperate in international and regional organizations and with individual countries and engage with information and communication technology businesses from across the globe.[98] The most important pledge that the FOC's participating states made with regard to the support and protection for DDs, however, is to dedicate themselves to collaborate 'closely to support – both politically and through project aid – the ability of individuals, particularly those operating in repressive environments, to exercise their human rights through the internet and connection technologies'.[99] Since the coalition's establishment in December 2011[100] the participating states engaged in several activities in order to work towards those goals, such as gathering informally at thematically relevant conferences and intergovernmental meetings to share information and discuss strategies, issuing joint statements with regard to relevant developments and hosting the annual multi-stakeholder conferences, the Freedom Online Conferences.[101] EU Member States participating in the Freedom Online Coalition

[94] Freedom Online Coalition, 'The Freedom Online Coalition' <www.freedomonlinecoalition.com> accessed 16 May 2015.
[95] Freedom Online Coalition, 'Members' <www.freedomonlinecoalition.com/about/members> accessed 16 May 2015.
[96] Freedom Online Coalition, 'Freedom Online Coalition (FOC) Terms of Reference' 3 <www.freedomonlinecoalition.com/wp-content/uploads/2014/04/Nairobi-Terms-of-Reference.pdf> accessed 16 August 2015.
[97] Freedom Online Coalition, 'FOC Founding Declaration, Freedom Online: Joint Action for Free Expression on the Internet' 2, para. A <www.freedomonlinecoalition.com/wp-content/uploads/2014/04/1-The-Hague-FOC-Founding-Declaration-with-Signatories-as-of-2013.pdf> accessed 16 May 2015.
[98] Ibid para. D.
[99] Ibid para. B.
[100] Freedom Online Coalition, 'History' <www.freedomonlinecoalition.com/about/history> accessed 16 May 2015.
[101] Freedom Online Coalition, 'The Freedom Online Coalition – Fact Sheet' (last updated August 2014) <www.freedomonlinecoalition.com/wp-content/uploads/2014/08/Freedom-Online-Coalition-Basic-facts.pdf> accessed 16 May 2015.

therefore actively contribute to the goals to which the EU committed itself with regard to the protection of human rights online in general and the protection of DDs in particular.

When it comes to the support and protection of DDs, the most relevant concrete initiative, which has been launched by the FOC is the DDP, which will be discussed separately in the next section.

b) Digital Defenders Partnership

The DDP was founded in late 2012 and is an initiative aimed at 'keeping the internet open and free from emerging threats'.[102] It also strives to 'increase and better coordinate emergency support for the internet's critical users, such as bloggers, cyber activists, journalists and other online human rights defenders, whenever and wherever they are under threat'.[103] To that outcome, the DDP offers advice, tools and financial support. The DDP views itself mainly as a 'competitive grant making mechanism providing support to organisations and individuals working in the digital emergency field'[104].

Within the framework of the DDP grant system, three different types of grants are available:

i) Strategic partnership grants, which aim to improve capacity in the field of digital emergency response,

ii) direct support grants for organisations working on human rights, media or blogging which face a digital threat, such as a cyber-attack,

iii) small emergency grants, which should provide 'small and timely financial emergency assistance' for 'journalists, human rights defenders, NGOs, activists and bloggers' that are suffering from a cyber-attack.[105] Furthermore, the DDP provides DDs with a 'digital first aid kit', which 'offers a set of self-diagnostic tools for human rights defenders' and provides 'guidelines for digital first responders'.[106]

The DDP is managed by the international NGO Hivos, which is based in the Netherlands, and is funded by 6 EU Member States and the United States,[107] who together dedicated an initial € 2,5 million to the DDP.[108] Clearly, the DDP must be viewed as an initiative of EU Member States, which directly aims at the protection of DDs and therefore supports the realisation of the EU's policies towards DDs. Concrete examples of grants provided by the Digital Defenders Partnership are establishing 'safe internet access through VPNs', 'DDoS[109] mitigation for websites under attack', the setup of temporary digital security

[102] Digital Defenders Partnership, 'DDP' <https://digitaldefenders.org> accessed 16 May 2015.
[103] Ibid.
[104] Ibid.
[105] Digital Defenders Partnership, 'Grant Fact Sheet' <http://digitaldefenders.org/wordpress/wp-content/uploads/2014/04/Grant-fact-sheet-DDP-online.pdf> accessed 16 May 2015.
[106] Digital Defenders Partnership, 'The Digital First Aid Kit – Intro' <http://digitaldefenders.org/digitalfirstaid> accessed 17 May 2015.
[107] Freedom Online Coalition, 'The Freedom Online Coalition - Fact Sheet' (n 101).
[108] Hivos, 'Digital Defenders Partnership' <www.hivos.org/news/digital-defenders-partnership> accessed 16 May 2015.
[109] Distributed Denial of Service.

helpdesks and support for 'organizations that provide legal support to human rights defenders under threat'.[110]

The Netherlands provide resources of its Human Rights Fund (MRF) to support organisations, which support HRDs, including 'projects that help protect human rights defenders on the internet'.[111] This encompassed, *inter alia*, support to Frontline Defenders, which provides 'training and development of resource materials on security and protection, including digital security' for HRDs.[112] The Netherlands' actions in the protection and support for DDs can be seen as an example of good practice of EU Member States activities, which contribute to the goals set forth within the EU's policy framework.

4. Cooperation with Other International Organisations

The EU's cooperation with other international organisations with regard to support for DDs again is mainly based on cooperation with international organisations in the field of HRDs[113] on the one hand, and cooperation with international organisations in the field of freedom of expression on the other hand. The EU Human Rights Guidelines on Freedom of Expression Online and Offline contain a section devoted to 'public diplomacy in multilateral fora', in which the EU commits to encourage partner countries to support 'the mandate of the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression. The EU will also ensure close cooperation with the special rapporteurs with related mandates from the African Union (AU), Organisation of American States (OAS), OSCE and the Organisation of Islamic Cooperation (Council, 2014a, para. 52) and to 'step up its engagement with other international and regional organisations and mechanisms, including the UN (especially the Office of the United Nations High Commissioner for Human Rights (OHCHR) and UNESCO, OSCE, the CoE and other donors or entities supporting freedom of opinion and expression' (Ibid: para. 55).

In addition, the EU will 'promote Council of Europe's standards and OSCE commitments on freedom of opinion and expression [...] including by encouraging co-operation with the Steering Committee on Media and Information Society [...]' as well as to 'build synergies with the Commissioner for Human Rights of the Council of Europe regarding mutual activities to promote freedom of expression and enhance the safety of journalists' (Ibid: para. 61). Furthermore, the EU will explore 'ways to further strengthen the capabilities of and the cooperation with the Council of Europe and the OSCE representative on the Freedom of the Media' (Ibid: para. 62).

For example, at the European Development Days 2015, the Commission also invited the UN Special Rapporteur on the Situation of Human Rights Defenders. According to the last resolution of the UN

[110] Digital Defenders Partnership, 'Grants, Grant Examples' <https://digitaldefenders.org> accessed 16 August 2015.

[111] Government of the Netherlands, 'Action Plan for Human Rights Defenders' (15 June 2012) 3 <http://www.government.nl/files/documents-and-publications/reports/2012/06/15/action-plan-for-human-rights-defenders/action-plan-for-human-rights-defenders.pdf> accessed 26 May 2015.

[112] Front Line Defenders, 'About Front Line Defenders' <www.frontlinedefenders.org/about-front-line> accessed 26 May 2015.

[113] For the EU's actions regarding the promotion of HRDs rights in bilateral and multilateral fora, as well as the EU's cooperation with selected IOs regarding HRDs, see: FRAME D7.2 2015 (n 48) chapter VI.

Human Rights Council (HRC) on 'Protecting Human Rights Defenders', access and use of information technologies, including the internet should be promoted at all levels as an integral part of the freedom of opinion and expression (Human Rights Council, 2013a). Furthermore, a resolution by the HRC on the promotion, protection and enjoyment of human rights on the Internet of 2014 '*calls upon* all states to promote and facilitate access to the Internet' and '*affirms* that the same rights people have offline must also be protected online, in particular freedom of expression' (Human Rights Council, 2014). In addition, the HRC resolution on the right to privacy in the digital age of 2015 appoints a special rapporteur on the right to privacy with the task to, *inter alia*, identify possible obstacles to the promotion and protection of the right to privacy and to submit proposals and recommendations to the HRC including on challenges arising in the digital age (Human Rights Council, 2015a; General Assembly, 2013).

Regular contacts take place between the EU and the Council of Europe and OSCE representatives. Ahead of a mission to Azerbaijan, the EU Special Representative on Human Rights would meet with the Council of Europe Commissioner on Human Rights or the OSCE Representative on the Freedom of the Media. Studies produced by those institutions also provide guidance for the EU policies on ICT and Human Rights.[114] The strength of the Council of Europe lies in its analytical and conceptual work as visible from numerous reports and standard-setting recommendations of its bodies often elaborated with the help of experts on digital rights and freedoms. In the context of assistance to Ukraine, it recently has developed a course on Human Rights and the Internet (Turk, Kulesza and Pazluk, 2015). However, the Council of Europe lacks the policy instruments to address repressive policies on DDs globally, and partly even in Europe. Here, the EU could fill this gap with the policy instruments at its disposal. Different from the EU the CoE has no mandate to denounce global violations and it also lacks the political tools, like human rights dialogues. Furthermore, it has very limited soft powers when compared to the EU as an economic organisation.

5. Role of the Private Sector with regard to the Protection of DDs

While some companies have committed themselves to work towards the protection of human rights online,[115] others contribute to their restriction. Some businesses support, either voluntarily or because they are pressured by a state, human rights violations online, for example by developing or providing the necessary hardware, software or services. This role of businesses has already been referred to as the `privatisation` of censorship.[116] The EU acknowledges the important role of ICT companies in its EU Human Rights Guidelines on Freedom of Expression Online and Offline, stating that they `play a key role in ensuring and enabling freedom of expression, access to information and privacy on the and through

[114] See Council of Europe Commissioner for Human Rights, 'The rule of law on the Internet and in the wider digital world' (Issue paper, December 2014) <https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=2734552&SecMode=1&DocId=2262340&Usage=2> accessed 14 October 2015; for the activities of the OSCE Representative on the Freedom of the Media see OSCE, OSCE Representative on Freedom of the Media <www.osce.org/fom> accessed 14 October 2015.

[115] For example: The Global Network Initiative (GNI) is an initiative to protect and advance freedom of expression and privacy in the ICT sector, which has members such as Facebook, Google and Microsoft, but also NGOs and academia.

[116] European Commission, 'Freedom of Expression, Media and Digital Communications – Key Issues' (December 2012) 23 <www.eidhr.eu/files/dmfile/Mediastudy-Keyissues.pdf> accessed 17 May 2015. See also Chapter II.

telecommunications` (Council, 2014a, para. 34) and that the EU will, *inter alia*, promote `best practices and respect for human rights with regard to the export of technologies that could be used for surveillance or censorship by authoritarian regimes` (Ibid: para. 34 a.). The ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights, provided by the EU Commission in 2013 contributes to sharpening the awareness of companies by highlighting devices that 'restrict access to "political" content or allow state surveillance that is not in line with international human rights'.[117]

The EP, in its Digital Freedom Strategy, already acknowledged the fact that 'business in some countries involves a growing technological component in terms of the blocking of content and the monitoring and identification of human rights defenders, journalists, activists and dissidents' (European Parliament, 2012c, para. 6). Furthermore it stressed that 'the recognition and implementation of the principles of Corporate Social Responsibility (CSR) by [businesses] is necessary to guarantee the freedom of action and safety of human rights defenders as well as freedom of expression' (European Parliament, 2012c, para. 7). However, voluntary instruments such as CSR will not be sufficient on their own in protecting DDs from the negative human rights impact that may result from the involvement of businesses in the repression of citizens online and other human rights violations in connection with ICT. Especially the work of DDs can be hindered and obstructed by repressive governments with technology and other support provided by businesses. Therefore the EU must make sure to take all necessary measures to restrict the export of hardware, software, expertise and services which can be used to, or are specifically designed to, restrict or obstruct the lawful use of ICT under the applicable regional and international human rights standards, so that DDs are not negatively impacted by business operations.[118] The AFET is concerned about the 'fact that some EU-based companies may provide technologies and services that can enable such human rights violations' (European Parliament, 2015c, para. 25), and suggests *inter alia* that the EU should 'develop smart and effective policies to regulate the export of dual-use technologies, addressing potentially harmful exports of ICT products and services, at international level and within multilateral export control regimes and other international bodies' (Ibid: para. 50), and that 'the export of highly sensitive goods must be checked before they leave the EU, and that penalties are necessary in the event of violations' (Ibid: para. 60).

A review of research conducted with regard to the use of Internet censorship and surveillance technology used in the Middle East and North Africa (MENA) region showed that the 'vast majority' of such technology 'stems from Europe and North America', while also the technology used for mobile telephone surveillance is 'typically' imported from the aforementioned two regions (Wagner, 2012a, p. 5). This once again underscores the importance of regulating the conduct of businesses when it comes to the export of potentially harmful technology.

[117] European Commission, 'ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights' (June 2013) <https://ec.europa.eu/anti-trafficking/sites/antitrafficking/files/information_and_communication_technology_0.pdf> accessed 14 October 2015.

[118] See on the issue of coherence also Chapter II.

An efficient enforcement of such export restrictions is a necessary prerequisite to ensure the protection of DDs who work in a repressive environment.

F. Findings and Conclusions

The analysis of the EU policies on Digital Defenders, with a focus on freedom of expression, freedom of assembly, privacy and data protection leads to several conclusions, which can be grouped into coherence issues and questions on the effectiveness of EU action. In addition, proposals for strengthening EU actions towards DDs will be made.

1. Coherence Issues

Analysing the coherence of EU policy and actions towards DDs is not an easy task given the fact that there is neither a central document on the EU's policies towards Digital Human Rights Defenders, nor a unified instrument or mechanism for the implementation of such policies. Rather the EU's overall policy on DDs can be constructed from elements of several different thematic frameworks in the field of human rights within the various relevant thematic policy documents on Human Rights. The most important documents of reference in that regard are the EU Guidelines on Freedom of Expression Online and Offline and those on Human Rights Defenders, while other EU guidelines can also be relevant. Furthermore, the Digital Freedom Strategy as well as the No Disconnect Strategy are the main policies of thematic importance. Furthermore, the EU Strategic Framework on Human Rights and Democracy and the EU Action Plan on Human Rights and Democracy also encompass elements, which constitute a part of the EU's policy framework towards DDs.

With a view to concrete actions and implementation measures, the picture is similar. Several institutions and instruments play a role in the EU's endeavour to protect and support DDs. This includes the EIDHR, the EEAS or the EU Special Representative on Human Rights. The mere fact, however, that there is no single strategy of the EU to engage with HRDs and ICT neither at the policy level, nor at the implementation level, leads to the conclusion that the coherence of the EU's policies towards DDs should be strengthened, for example by making the involved actors and institutions aware of the fact that certain aspects of their work touch upon the thematic area of HRDs and ICT.

Problems relate to all types of coherence – horizontal coherence, i.e. between EU institutions as exemplified by the recommendations of the EP and the action of the Council in particular, vertical – between EU and the Member States, which are not always ready to translate the policies of the EU for the protection of DDs into their national policies, for example supporting freedom of expression on the Internet and between the external and internal dimensions of EU policies – for example when it comes to regulating EU companies on dual use goods.[119]

Feedback received from interviews suggests that in view of the increasingly limited space for the DDs, there is a need to step up action in line with the EU policies regarding the protection of DDs both at a

[119] See for the existing coherence issues also Tamara Lewis et al., 'Report on coherence of human rights policymaking in EU Institutions and other EU agencies and bodies' (FRAME Deliverable 8.1., 2014) and Tamara Lewis et al., EU and Member State competences in human rights (FRAME Deliverable 8.2., 2015) the latter providing several examples for coherence issues like in the field of data protection.

political and at a technical level as well as by increasing support for circumventing governmental restrictions through competent intermediaries. As ICT has become almost indispensable for processes strengthening democracy and human rights, Internet freedom and rights of Digital Defenders should be included in country strategies where appropriate and be given adequate attention by focal points. Member States missions should also be motivated to share the task, which often is too demanding to be undertaken by EU delegations alone. The annual strategy of the EIDHR and its programs could take the specific needs of DDs better into account.

Digital Defenders should be made aware of the opportunities available to them, which is not yet sufficiently done. More practical information could be disseminated on homepages of the Commission as well as through specialized NGOs. This could also be a major task for the Human Rights Defenders Mechanism, which should have a focus on digital defenders expressly for this reason. The availability of the relevant guidelines for all actors in the field should be improved. Based on feedback received, EU services should do their utmost to avoid bureaucratic approaches and take decisions preferably in close cooperation with digital defenders themselves.

The accessibility and capacity of EU focal points needs to be strengthened. The same is true for the competent services in Brussels. The focus on vulnerable groups as human rights defenders most in need is positive but has to be implemented more fully. For improved effectiveness it is also important to be as flexible as possible. For example, as threats against digital human rights defenders often include family members those deserve protection as well. Digital defenders should be given the opportunity to regularly meet physically in order to be able to exchange experiences and get updated on new opportunities without having to fear governmental repression. New legal regulations for bloggers should be reviewed on their conformity with international human rights and legal expertise provided to bloggers facing repression.

The EU should also engage with Internet companies to prevent the disclosure of the identity of or information on digital defenders to authoritarian governments and generally provide any information only on the basis of court orders. Justified efforts to step up cyber security must not be misused to restrict freedom of expression and information or other rights on the Internet. For any limitations the necessary criteria have to be met. There is a need for specific training of EU staff, both in Brussels as well as at the focal points, on the instruments and methodologies, which could benefit digital human rights defenders.

2. Effectiveness of EU Action

The effectiveness of the EU's action regarding the protection and support for DDs can be described as mixed. As could be established from interviews, some actions with the help of specialized NGOs are highly effective, as they enable DDs to get access to the full Internet or escape surveillance, while the general policies regarding freedom of expression are often not effective when it comes to keeping the Internet open for discourses on democracy and human rights as numerous new laws adopted in the last years in the global South, but also Eastern European countries restrict the access to or use of the Internet. The shrinking space of civil society to be observed in numerous countries is maybe best visible

in the fast increasing restrictions, censorship and surveillance measures related to the Internet (European Parliament, 2015c).

However, it should also be noted that supporting DDs may encounter specific difficulties as they are sometimes not clearly defined or working in a consistent way and because of the decentralized nature of the information society. DDs might find it difficult to use complicated technologies or encryption in a consistent way. Accordingly, the sustainability of support activities may become a problem.[120] Whether or not the EU actions for the protection and support of DDs could be more effective if there was a special EU policy document on DDs in place is hard to say. In any case, there is a need for a reinforced strategy to keep the Internet open by the EU and for its increased presence in the respective international forums and bodies. For example, in 2014 the UN Internet Governance Forum was held in Istanbul, which brought together about 1.500 participants, representing all stakeholders, i.e. civil society, governments, international organizations, business, technical community and academia in more than 100 panels and workshops. The EEAS was represented with one single person. Accordingly the voice of the EU in many relevant panels was absent. The same appears to be the case in other international conferences where freedom of expression and other human rights of DD are being discussed. The EU could also be more active in the Freedom Online Coalition as it shares similar objectives.

Finally, it should revise and update its Guidelines on Human Rights Defenders, which date from 2008 and hardly discuss support to DDs. They need to be brought at the level of and in conformity with recent guidelines like the one on freedom of expression online and offline and be made more inclusive by taking into account the experience with the work of the focal points and the new HRDM.

3. Proposals for Strengthening EU Action

a. The EU should combine its different sources of information, coming from delegations, civil society organizations and other reports, to better identify the specific situation and needs as well as gaps in protection and support of DDs. For this purpose, past actions and projects should be evaluated with regard to shortcomings and examples of good practice.

b. The EU should step up action to counter negative trends and to improve the political and legal environment for DDs including their freedom of association online, thereby using the human rights tool box. This relates to the increasing restrictions by new legislations, for example registration duties for bloggers, prohibition of using tools of anonymization and restrictions of the privacy of online journalists and bloggers, as well as the increasing use of surveillance technologies. Digital whistle-blowers should be treated as human rights defenders. For this purpose the multilateral as well as the bilateral level should be used, in particular human rights dialogues.

c. Strict controls of the export of ICT goods and services that can be used for surveillance and other human rights violations is required. Cooperation with internet intermediaries should be sought to protect DDs against inquiries by repressive governments.

[120] Information based on interviews conducted by the author.

d. EU representatives should become more active in international fora discussing digital rights, like the Internet Governance Forum, and regional fora such as EuroDIG (European Dialogue on Internet Governance), and support an open Internet in general and DDs in particular.

e. Specific support needs to be provided for digital safety regarding awareness, encryption and circumvention tools, including mechanisms to avoid being tracked. For this purpose, DDs need assistance with managing digital security risks through training and mentoring. More generally, online journalists, DDs and pertinent civil society organizations need to be provided with training and technology to empower them against restrictions by authoritarian regimes.

f. It is suggested to bring existing contents and rules in Guidelines and other documents relevant to DDs together in a comprehensive way to make them more accessible and visible. The EU should provide information tools on existing support mechanisms with information on whom to address, on focal points and specialized NGOs. It could share manuals on implementation of Guidelines with the beneficiaries. In particular, information how the Human Rights Defenders Mechanism can serve DDs should be widely communicated.

g. There is a need to improve accessibility and capacity of EU focal points, but also central services in Brussels. In addition, it would be important to provide particular training for EU staff to better understand the needs of DDs and how to address them.

h. Finally, it is suggested to update and modernize the Guidelines on HRDs to include recent developments and the specific situation of DDs.

G. Bibliography

1. Legal and Policy Instruments

a) Council of Europe

Committee of Ministers, 'Recommendation of the Committee of Ministers to Member States on a Guide to Human Rights for Internet users' (16 April 2014) CM/Rec (2014) 6.

Parliamentary Assembly, 'Resolution on mass surveillance' (21 April 2015) 2045(2015).

b) European Union

(1) Legislation

Council Decision 2012/440/CFSP of 25 July 2012 appointing the European Union Special Representative for Human Rights [2012] OJ L 200/21.

Council Decision 2015/260/CFSP of 17 February 2015 extending the mandate of the European Union Special Representative for Human Rights [2015] OJ L 43/29.

European Parliament and Council Regulation (EU) 1889/2006 of 20 December 2006 on establishing a financing instrument for the promotion of democracy and human rights worldwide [2006] OJ L 386/1.

European Parliament and Council Regulation (EU) 235/2014 of 11 March 2014 establishing a financing instrument for democracy and human rights worldwide [2014] OJ L 77/85.

European Parliament Budget Adoption (EU, Euratom) 2014/65/EU of 19 February 2014, Definitive adoption of Amending budget No 8 of the European Union for the financial year 2013 [2014] OJ L 49/13.

(2) Other Documents

European Commission, 'Delivering on the Arab Spring – Highlights of the Semester July-December 2011' <www.enpi-info.eu/files/publications/Delivering%20on%20the%20Arab%20Spring.pdf> accessed 4 June 2015. [2011a]

——, 'A Partnership for Democracy and Shared Prosperity with the Southern Mediterranean' (Communication) COM (2011) 200 final. [2011b]

—— 'Internet Policy and Governance Europe's role in shaping the future of Internet Governance' (Communication) COM (2014) 72 final. [2014a]

—— 'Commission Implementing Decision on the adoption of a special measure for the financing of the Work Programme 2014 for the European Instrument for Democracy and Human Rights (EIDHR)' C(2014) 5142. [2014b]

—— 'Action Plan on Human Rights and Democracy (2015-2019) "Keeping human rights at the heart of the EU agenda"' (Communication) JOIN (2015) 16 final. [2015a]

—— 'Commission Implementing Decision of 1 April 2015 on the Annual Action Programme 2015 for the European Instrument for Democracy and Human Rights (EIDHR) to be financed from the general budget of the European Union' C(2015) 2025 final. [2015b]

—— 'Report on the Implementation of Regulation (EC) No. 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items' COM (2015) 331 final. [2015c]

—— 'Commission Staff Working Document on Implementing the UN Guiding Principles on Business and Human Rights - State of Play' SWD(2015) 144 final. [2015d]

Council, 'EU Guidelines on Human Rights Defenders' (8 December 2008).

—— 'EU Strategic Framework and Action Plan on Human Rights and Democracy' (25 June 2012).

—— 'EU Annual Report on Human Rights and Democracy in the World in 2012' (13 May 2013).

—— 'EU Human Rights Guidelines on Freedom of Expression Online and Offline' (12 May 2014). [2014a]

—— 'EU Annual Report on Human Rights and Democracy in the World in 2013' (23 June 2014). [2014b]

—— 'EU Annual Report on Human Rights and Democracy in the World in 2014' (22 June 2015). [2015a]

—— 'Council Conclusions on the Action Plan on Human Rights and Democracy 2015 - 2019' (20 July 2015). [2015b]

European Parliament, 'Report on a Digital Freedom Strategy in EU Foreign Policy', A7-0374/2012, 15 November 2012. [2012a]

—— 'Report on a Digital Freedom Strategy in EU Foreign Policy', Explanatory Statement, A7-0374/2012, 15 November 2012. [2012b]

—— 'Resolution of 11 December 2012 on a digital freedom strategy in EU foreign policy' 2012/2094(INI). [2012c]

—— 'Resolution of 2 March 2015 on the Annual Report on Human Rights and Democracy in the World 2013 and the European Union's policy on the matter' 2014/2216 (INI). [2015a]

—— 'Report on "Human rights and technology: the impact of intrusion and surveillance systems on human rights in third countries"', A8-0178/2015, 3 June 2015, Rapporteur: Marietje Schaake. [2015b]

—— 'Resolution of 8 September 2015 on "Human rights and technology: the impact of intrusion and surveillance systems on human rights in third countries"', 2014/2232 (INI). [2015c]

c) United Nations

General Assembly 'Resolution 68/167 on the right to privacy in the digital age' (18 December 2013) UN Doc. A/RES/68/167.

Human Rights Council, 'The promotion, protection and enjoyment of human rights on the Internet' (5 July 2012) UN Doc. A/HRC/20/8.

—— 'Resolution 22/6 on protecting human rights defenders' (12 April 2013) UN Doc. A/HRC/RES/22/6. [2013a]

—— 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue' (17 April 2013) UN Doc. A/HRC/23/40. [2013b]

—— 'Resolution 26/13 on the promotion, protection and enjoyment of human rights on the Internet' (14 July 2014) UN Doc. A/HRC/RES/26/13.

—— 'Resolution 28/16 on the right to privacy in the digital age' (1 April 2015) UN Doc. A/HRC/RES/28/16. [2015a]

—— 'Report of the Special Rapporteur on extra judicial, summary and arbitrary executions, Christof Heyns, on the use of information and communication technologies to secure the right to life' (24 April 2015) UN Doc. A/HRC/29/37. [2015b]

d) National Legislation

Russian Federal Republic, Federal Law No. 97-03 (5 May 2014).

2. Literature

a) Books

Benedek W and Kettemann MC, *Freedom of Expression and the Internet* (Council of Europe Publishing 2013).

Frank Joergensen R, *Framing the Net: the Internet and Human Rights* (Edward Elgar Publishing 2013).

Horner L, Hawtin D and Puddephatt A, *Information and Communication Technologies and Human Rights* (European Union 2010).

Turk K, Kulesza J and Pazluk A, *Human Rights and the Internet* (Council of Europe Publishing 2015).

Wagner B, *After the Arab Spring: New Paths for Human Rights and the Internet in European Foreign Policy* (European Union 2012). [2012a]

——, *Exporting Censorship and Surveillance Technology* (Hivos 2012). [2012b]

b) Book Chapters

Benedek W, 'EU Human and Fundamental Rights Action in 2014' in Benedek W, Benoit-Rohmer F, Kettemann MC, Kneihs B, Nowak M (eds), *European Yearbook on Human Rights 2015* (NWV/Intersentia 2015), 79-103.

Dankwa A and Pahnecke O, 'Digital Human Rights Defence: The Challenges and Opportunities of using Social Media for Human Rights Documentation and Monitoring' in Benedek W, Benoit-Rohmer F, Karl W, Kettemann MC, Nowak M (eds), *European Yearbook on Human Rights 2014* (NWV/Intersentia 2014), 39-62.

Pearson G, 'Assessment of the Implementation of the EU Human Rights Strategy and Action Plan as Regard Business and Human Rights' in Benedek W, Benoit-Rohmer F, Kettemann MC, Kneihs B, Nowak M (eds), *European Yearbook on Human Rights 2015* (NWV/Intersentia 2015), 135-142.

c) Journal Articles

Allagui I and Kuebler J, 'The Arab Spring and the Role of ICTs - Editorial Introduction' (2011) 5 International Journal of Communication 1435.

Axford B, 'Talk About a Revolution: Social Media and the MENA Uprisings' (2011) 8 Globalizations 681.

Bennet K, 'European Union Guidelines on Human Rights Defenders: a review of policy and practice towards effective implementation' (2015) 19 The International Journal of Human Rights 908.

Dutt M and Rasul N, 'Raising Digital Consciousness: An Analysis of the Opportunities and Risks Facing Human Rights Activists in a Digital Age' (2014) 11 (20) SUR – International Journal on Human Rights 426.

Hofheinz A, 'The Internet in the Arab World: Playground for Political Liberalization' [2005] (3) International Politics and Society 78.

Leichtfried J, 'How the European Parliament Safeguards Human Rights on the Internet' (2012) 9 (1) Human Security Perspectives 15 <www.hs-perspectives.etc-graz.at/typo3/fileadmin/user_upload/ETC-Hauptseite/human_security/hs-perspectives/pdffiles/issue1_2012/5-HSP12_Leichtfried__FINAL_.pdf> accessed 1 October 2015.

Osman A and Samei M A, 'The Media and the Making of the 2011 Egyptian Revolution' (2012) 2 (1) Global Media Journal.

3. Reports

Jansen F, 'From digital threat to digital emergency' in Global Information Society Watch 2014, *Communications surveillance in the digital age* (Association for Progressive Communications (APC) and Humanist Institute for Cooperation with Developing Countries (HIVOS 2014).

Salem F and Mourtada R, 'Civil Movements: The Impact of Facebook and Twitter' (2011) 1 (2) Arab Social Media Report.

4. Electronic Sources

Al Jazeera, 'Timeline: Tunisia's uprising' (23 January 2011) <www.aljazeera.com/indepth/spotlight/tunisia/2011/01/201114142223827361.html> accessed 17 August 2015.

Article 19, 'The Right to Blog' (Policy Brief, 2013) <www.article19.org/data/files/medialibrary/3733/Right-to-Blog-EN-WEB.pdf> accessed 14 October 2014.

Chané AL, Hachez N, Lein B, Podstawa K and Wouters J, 'The Post-2014 EU Action Plan on Human Rights and Democracy. A Policy Brief' (FRAME) 3 <http://www.fp7-frame.eu//wp-content/materiale/policy_brief/02-FRAME%20Policy%20Brief%20No%202%20--Post%202014%20SFAP%20Policy%20Brief.pdf> accessed 17 November 2015.

Council of Europe Commissioner for Human Rights, 'The rule of law on the Internet and in the wider digital world' (Issue paper, December 2014) <https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=2734552&SecMode=1&DocId=2262340&Usage=2> accessed 14 October 2015.

Council of the European Union, 'The Council adopts the Guidelines on Freedom of Expression online-offline' (12 May 2014) <http://eeas.europa.eu/delegations/documents/the_council_adopts_the_guidelines_on_freedom_of_expression_online-offline_12_may_2014_en.pdf> accessed 17 May 2015.

Delegation of the European Union to Turkey, 'European Union Local Strategy to Support and Defend Human Rights Defenders in Turkey' <http://avrupa.info.tr/fileadmin/Content/Files/File/EIDHR/EU_local_strategy_on_HRD_draft_07012011_L-EN.pdf> accessed 12 November 2015.

Digital Defenders Partnership, 'DDP' <https://digitaldefenders.org/> accessed 16 May 2015.

—— 'Grants, Grant Examples' <https://digitaldefenders.org> accessed 16 August 2015.

—— 'Grant Fact Sheet' <http://digitaldefenders.org/wordpress/wp-content/uploads/2014/04/Grant-fact-sheet-DDP-online.pdf> accessed 16 May 2015.

—— 'The Digital First Aid Kit – Intro' <http://digitaldefenders.org/digitalfirstaid/> accessed 17 May 2015.

European Commission, 'Democracy and Human Rights, Small Grants' <www.eidhr.eu/side-panels/human-rights-defenders/small-grants> accessed 3 June 2015.

—— 'Digital Agenda: Karl-Theodor zu Guttenberg invited by Kroes to promote Internet freedom globally' (12 December 2011) <http://europa.eu/rapid/press-release_IP-11-1525_en.htm> accessed 17 May 2015.

—— 'Delivering on Human Rights Defenders' (Highlights of the Semester January-June 2012) 10 <www.eidhr.eu/files/dmfile/EIDHR_DeliveringonHumanRightsDefenders_Report.pdf> accessed 14 October 2015.

—— 'Freedom of Expression, Media and Digital Communications – Key Issues' (December 2012) <www.eidhr.eu/files/dmfile/Mediastudy-Keyissues.pdf> accessed 17 May 2015.

—— 'Commission plans guide through global Internet policy labyrinth' (13 May 2013) <http://ec.europa.eu/digital-agenda/en/news/commission-plans-guide-through-global-internet-policy-labyrinth> accessed 17 May 2015.

—— 'ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights' (June 2013) <https://ec.europa.eu/anti-trafficking/sites/antitrafficking/files/information_and_communication_technology_0.pdf> accessed 14 October 2015.

—— 'Establishing a European Union Human Rights Defenders Mechanism, Open Call for Proposals 2014, Guidelines for grant applicants' (DG DEVCO, 3 December 2014) <https://webgate.ec.europa.eu/europeaid/online-services/index.cfm?ADSSChck=1425290260269&do=publi.getDoc&documentId=145307&pubID=136316> accessed 27 June 2015.

—— 'The Global Internet Policy Observatory (GIPO)' (last updated on 22 April 2015) <https://ec.europa.eu/digital-agenda/en/global-internet-policy-observatory-gipo> accessed 17 May 2015.

—— 'EU proposes new Joint Action Plan on Human Rights and Democracy' (29 April 2015) <http://europa.eu/rapid/press-release_IP-15-4893_en.htm> accessed 22 May 2015.

FIDH, 'Surveillance technologies "Made in Europe": Regulation needed to prevent human rights abuses' (Position Paper, 1 December 2014) <www.fidh.org/IMG/pdf/surveillance_technologies_made_in_europe.pdf> accessed 9 October 2015.

Freedom House, 'Freedom on the Net 2014' <https://freedomhouse.org/report/freedom-net/freedom-net-2014#.Vh5HWk0gmUk> accessed 14 October 2015.

Freedom Online Coalition, 'FOC Founding Declaration, Freedom Online: Joint Action for Free Expression on the Internet' <www.freedomonlinecoalition.com/wp-content/uploads/2014/04/1-The-Hague-FOC-Founding-Declaration-with-Signatories-as-of-2013.pdf> accessed 16 May 2015.

—— 'Freedom Online Coalition (FOC) Terms of Reference', <www.freedomonlinecoalition.com/wp-content/uploads/2014/04/Nairobi-Terms-of-Reference.pdf> accessed 16 August 2015.

—— 'History' <www.freedomonlinecoalition.com/about/history/> accessed 16 May 2015.

—— 'Members' <www.freedomonlinecoalition.com/about/members/> accessed 16 May 2015.

—— 'Statement on the Use and Export of Surveillance Technology' <www.freedomonlinecoalition.com/wp-content/uploads/2014/10/2-FOC-Joint-Statement-on-the-USe-and-Export-of-Surveillance-Technology-October-2014.pdf> accessed 9 October 2015.

—— 'The Freedom Online Coalition' <www.freedomonlinecoalition.com/> accessed 16 May 2015.

—— 'The Freedom Online Coalition – Fact Sheet' (last updated August 2014) <www.freedomonlinecoalition.com/wp-content/uploads/2014/08/Freedom-Online-Coalition-Basic-facts.pdf> accessed 16 May 2015.

Front Line Defenders, 'About Front Line Defenders' <www.frontlinedefenders.org/about-front-line> accessed 26 May 2015.

—— 'Human Rights Defenders Mechanism' <www.frontlinedefenders.org/EUHRD Mechanism> accessed 14 October 2015.

GHK Consulting Ltd/HTSPE, 'Mapping of temporary shelter initiatives for Human Rights Defenders in danger in and outside the EU, Final Report' (February 2012) <www.europarl.europa.eu/meetdocs/2009_2014/documents/droi/dv/504_mapping_/504_mapping_en.pdf> accessed 27 June 2015.

Government of the Netherlands, 'Action Plan for Human Rights Defenders' (15 June 2012) <www.government.nl/files/documents-and-publications/reports/2012/06/15/action-plan-for-human-rights-defenders/action-plan-for-human-rights-defenders.pdf> accessed 26 May 2015.

Hivos, 'Digital Defenders Partnership' <www.hivos.org/news/digital-defenders-partnership> accessed 16 May 2015.

Index on Censorship, 'Index policy paper: Is the EU heading in the right direction on digital freedom?' (20 June 2013) <www.indexoncensorship.org/2013/06/is-the-eu-heading-in-the-right-direction-on-digital-freedom/> accessed 17 May 2015.

Internet Rights and Principles Coalition, 'The Charter of human rights and principles for the Internet' (UN Internet Governance Forum 2014) <http://internetrightsandprinciples.org/site/wp-content/uploads/2014/06/IRPC_booklet_3rded_English.pdf> accessed 14 October 2015.

Khazan O, 'These Charts show how crucial Twitter is for Turkish protesters' (The Atlantic, 12 June 2013) <www.theatlantic.com/international/archive/2013/06/these-charts-show-how-crucial-twitter-is-for-the-turkey-protesters/276798/> accessed 14 October 2015.

marietjeschaake.eu, 'European Parliament endorses first ever Digital Freedom Strategy' (10 December 2012) <www.marietjeschaake.eu/2012/12/european-parliament-endorses-first-ever-digital-freedom-strategy/> accessed 16 August 2015.

Maurer T, Omanovic E, Wagner B, 'Uncontrolled Global Surveillance. Updating Export Controls to the Digital Age' (March 2014) <https://digitalegesellschaft.de/wp-content/uploads/2014/03/Uncontrolled-Surveillance_March-2014_final.pdf> accessed 9 October 2015.

Meijueiro L, 'Technical Development of the Online Platform for the Global Internet Policy Observatory – SMART 2014/0026' (April 2015) <www.giponet.org/sites/default/files/3.%20GIPO%20Technical%20Platform%20proposal.pdf> accessed 7 August 2015.

Monti C and Tomaszewski M, 'Building GIPO the Global Internet Policy Observatory', European Commission, <www.giponet.org/sites/default/files/1.%20Building%20GIPO%20-%20the%20Global%20Internet%20Policy%20Observatory.pdf> accessed 7 August 2015.

OpenNet Initiative, 'ONI Access: Denied Controlled Contested' <http://access.opennet.net/> accessed 14 October 2015.

OSCE, OSCE Representative on Freedom of the Media <www.osce.org/fom> accessed 14 October 2015.

Reporters without Borders, 'Enemies of the Internet. 2013 Report – Special Edition: Surveillance' (12 March 2013) <http://surveillance.rsf.org/en/wp-content/uploads/sites/2/2013/03/enemies-of-the-internet_2013.pdf> accessed 9 October 2015.

IV. Common Conclusions and Recommendations

The intimate relationship between human rights and Internet-related practices has received considerable attention amongst policy makers in the past years, including within the EU. In relation to the EU´s external policies, this has resulted in a number of promising actions such as the EU Human Rights Guidelines on freedom of expression online and offline that stipulate this fundamental right as the baseline for any EU human rights intervention in third countries. Other promising policies include the Digital Freedom Strategy by the European Parliament and the No Disconnect Strategy by the European Commission or the newly created Human Rights Defenders Mechanism and its potential relevance for the implementation of the EU Guidelines on Freedom of Expression Online and Offline.

However, as identified in the study on DDs, several challenges persist in relation to the actual support from the EU and its Member States towards human rights defenders in third countries. These challenges relate to the shrinking space for their activities as a result of censorship and surveillance practices by an increasing number of states and their efforts to limit human rights like freedom of expression, information and association, but also privacy and data protection in their online dimension.

In relation to the EU's internal policies, the study on Self-Regulation and Freedom of Expression and Information iterated that while the EU is formally committed to human rights and fundamental freedoms, its internal policies does not sufficiently address the human rights challenges caused by its policies dealing with illegal content. The study highlighted a number of issues related to a lack of legal safeguards (ensuring compliance with Article 10(2) of the ECHR), uncertainty about key notions in the directives, limited means of transparency and accountability, different and often conflicting expectations towards intermediaries, a lack of guidance to Member States, etc. These issues have been raised on several occasions, such as during the evaluation of the E-commerce directive and the consultations on the notion-and-action procedures, but a solution has yet to be found. While the Digital Single Market Strategy recognises the fundamental right to freedom of expression, it does not in substantiate the protection of this right vis-à-vis current EU policies on content regulation. As the strategy intends to analyse the need for new measures to tackle illegal content on the Internet, it provides an ideal opportunity to strengthen safeguards and guidance to ensure that any measure of content regulation is compliant with human rights standards.

In this final part, the authors will not repeat the conclusions made by the study on internal and external policies, respectively, but point to a selection of cross-cutting observations and recommendations.

- **Observation 1:** Human rights seem to be framed and addressed primarily in relation to the EU's external policy, while they appear less visible and elaborated in relation to the EU's internal policies related to technological factors. As stressed by the recent report on Human Rights and

Technology by the European Parliament,[121] digital freedom and free trade must be promoted and protected simultaneously.

- **Recommendation 1:** The EU must ensure that the relevant human rights standards are integrated as the baseline and benchmark for any EU ICT policy – internal and external – with an impact on fundamental rights.

- **Observation 2:** Whereas privacy, data protection, and cyber security have received considerable attention over the past years, similar attention has not been accorded to freedom of expression, despite its status as an EU fundamental right. The EU lacks a coherent and solid policy framework for online freedom of expression/information, in particular related to its internal policies. Given the increasing amount of policy issues related to online freedom of expression, both internally and externally, the EU would benefit from a strengthened effort in this area. An overall framework might contribute to greater compliance with fundamental rights in specific areas of policy development, such as the area of ´notion-and action´ procedures, and/or in a future revision of the E-commerce directive, the IPR enforcement directive, and the child pornography. Although important, the EU Human Rights Guidelines on freedom of expression online and offline are not sufficient, as they focus primarily on the EU´s external policies, and do not acknowledge the human rights issues discussed in the above study on Self-regulation and Freedom of Expression.

  The current lack of coherence between the internal and external policy on freedom of expression appears contradictory and may be countered through a human rights-based re-orientation of efforts targeting online illegal content, placing these initiatives firmly within a freedom of expression/information and rule of law framework.

- **Recommendation 2:** The EU should commence analysis and consultations with a view to drafting a comprehensive EU policy on online freedom of expression – in particular as it relates to self-regulation and the tackling of illegal content - and take into account both the internal and external dimension of EU policy in this regard. The ongoing work in relation to the Digital Single Market Strategy is a natural point of departure for greater coherence between the internal dimension and the external dimension of online freedom of expression/information.

- **Observation 3:** In the digital domain, private actors play an increasingly significant role in all spheres of social activities, yet sufficient safeguards are not in place to ensure that their practices respect human rights standards. The EU, through the EU ICT Sector Guide, has played an active role in translating the UN Guiding Principles on Business and Human Rights to the ICT sector. Yet, there is limited analysis and guidance on the positive state obligation vis-à-vis these

[121] COUNCIL OF THE EUROPEAN UNION. 2015. Report on 'Human rights and technology: the impact of intrusion and surveillance systems on human rights in third countries'. A8-0178/2015. 3 June 2015. Rapporteur: Marietje Schaake.

private actors, despite their crucial role and impact on individuals' ability to enjoy freedom of expression and the right to privacy in the online domain.

- **Recommendation 3:** The EU should develop guidance on the positive state obligations in relation to Article 8 and 10 of the ECHR and likewise Article 7, 8 and 11 of the CFREU.

- **Observation 4:** In its report and resolution on human rights and technology, the European Parliament highlights the impact of intrusion and surveillance systems on third countries, and notes the responsibility of Member States and companies with respect to the export of surveillance technology. The EU ICT Sector Guide could be updated and made more responsive to these concerns. This would encourage Member States to do the same with their national legislations in this domain and improve the conditions under which DDs have to work and support freedom of expression/information online and the openness of the Internet.

- **Recommendation 4:** The EU should strengthen its efforts to make export controls on intrusion and surveillance technology more effective. For this purpose, EU as well as Member States legislation and policies should be reviewed and the implementation more closely monitored.

- **Observation 5:** The EU develops a wide range of policies – both internally and externally – that have an impact on the way individuals may enjoy their fundamental rights and freedoms. Despite a formal commitment to carry out human rights impact assessment (HRIA) on all legislative proposals, it remains unclear to which extent such assessments have systematically been conducted.[122]

- **Recommendation 5:** In line with the recent agenda for Better Regulation,[123] the EU should ensure that a human rights rights impact assessment is carried out and documented on all new (or revised) EU policies that have an impact on fundamental rights, with particular attention to freedom of expression/information and privacy/data protection in the online domain.

- **Observation 6:** The main standard-setting in the field of human rights and technology continues to occur within the Council of Europe, yet often without proper recognition at EU Member State level. The size, strength and political importance of the EU should be combined with the human rights expertise of the Council of Europe in order to ensure a stronger uptake of human rights compliant standards when EU Member States devise policies and regulation for the online domain.

[122] See Better Regulation and the new guidelines for EU Impact Assessment – What's in it for human rights and development?, (2015). Available from: <www.fp7-frame.eu/better-regulation-and-the-new-guidelines-for-eu-impact-assessments-whats-in-it-for-human-rights-and-development/> accessed 19 November 2015.
[123] See European Commission – Press Release. Better Regulation Agenda: Enhancing transparency and scrutiny for better EU law-making, (2015). Available from <http://europa.eu/rapid/press-release_IP-15-4988_en.htm> accessed 19 November 2015.

- **Recommendation 6:** The EU should work towards a closer partnership with the Council of Europe in the field of standard setting on technology and human rights.

- **Observation 7:** The Council of Europe has taken a lead in conceptualizing the protection of human rights online, but – with the exception of the European Court of Human Rights – lacks strong instruments of implementation and enforcement, in particular when it comes to DDs. Meanwhile, the Council of Europe is already implementing important projects for the European Union in the field of freedom of expression and with regard to other human rights. Here, the EU policies on human rights online can make a difference. However, closer cooperation with relevant organisations would strengthen EU action.

- **Recommendation 7:** The EU should cooperate more closely with other organisations pursuing similar objectives, especially regarding DDs. This includes organisations such as OSCE (Representative of Freedom of the Media), the European Commissioner for Human Rights, UNESCO and other relevant United Nations bodies and mechanisms.

- **Observation 8:** The EU is not sufficiently represented in international fora dealing with ICT and human rights, such as the Internet Governance Forum (IGF) and regional IGFs. In particular, the EEAS misses opportunities of international forums, which are preparing international policies on ICT and human rights. Relevant parts of the Commission in charge of the EIDHR are also absent as participation is often limited to DG Connect which mainly pursues economic and technological priorities.

- **Recommendation 8:** EU policies on ICT and human rights need to be promoted more strongly and become more visible in international forums, dealing with ICT and human rights, in particular in times when an open Internet is under threat.

- **Observation 9:** EU internal and external policies and instruments are not sufficiently visible and made available to the public at large and DDs in particular. There is no booklet or leaflet on EU human rights guidelines, easy to read versions, commentaries or video tools. This also relates to the internal dimension of freedom of expression and other human rights online. There is a lack of material offering examples of good practice, problems and success stories. In short, EU policies and instruments are badly promoted. The same is true for the instruments and opportunities to support DDs, the promotion of which is largely left to specific intermediary NGOs. As a result, there is a significant lack of awareness in parts of the DDs community and a need for a stronger visibility of EU action in this field.

- **Recommendation 9**: The EU needs to devote more personal and financial resources to create better awareness of its policies and instruments in support of human rights online as well as DDs, both in its external and internal dimensions. It needs to improve the visibility of its activities also as a matter of transparency and accountability. One way of improvement could go via the HRDM, in particular if it would have a specific focus on the needs of DDs.

- **Observation 10:** The EU Guidelines on Human Rights Defenders date back to 2008 and are not sufficiently comprehensive to fit present-day needs. In particular in comparison to the new EU Guidelines on Freedom of Expression Online and Offline, the need for an update becomes apparent, notably given the lack of an online dimension. The tools available for Human Rights Defenders have improved as shown, in particular, by the establishment of the EU human rights focal points, human rights country strategies and the creation of the new Human Rights Defenders Mechanism. However, Human Rights Defenders should be made better aware of the opportunities. In times of a shrinking space for Human Rights Defenders such action could be an important signal.

- **Recommendation 10:** The EU should update its Guidelines on Human Rights Defenders to include recent developments, make them more comprehensive and add an online dimension.

Common Bibliography

This section contains selected bibliographies for each part of the report. For full bibliographies, please refer to the table below:

1. Self-Regulation and Freedom of Expression and Information – Case study on potential human rights implications of the EU's internal policies

Council of Europe (2014c), 'Recommendation CM/Rec(2014)6 of the Committeee of Ministers to member States on a guide to human rights for Internet users'.

La Rue, Frank (2011), 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, A/HRC/17/27', (United Nations General Assembly, Human Rights Council).

Balkin, J. M., 'Old-School/New-School Speech Regulation' (2014) Harvard Law Review, 127 (8), 2296, 342.

Deibert, R., et al., *Access controlled : the shaping of power, rights, and rule in cyberspace* (Cambridge, Mass.: MIT Press 2010).

EDRI, 'Human Rights and privatised law enforcement' (EDRI, Brussels, 2013) Available from https://edri.org/wp-content/uploads/2014/02/EDRi_HumanRights_and_PrivLaw_web.pdf accessed 10 November 2015.

Frydman, B., Hennebel, L., and Lewkowicz, G., 'Public Stategies for Internet Co-Regulation in the United States, Europe and China' (2008) Working Papers du Centre Perelman de philosophie de droit, No 2007/6.

Korff, D., 'The rule of law on the Internet and in the wider digital world - Issue Paper' (2014).

Kuczerawy, A., 'Intermediary liability & freedom of expression: Recent developments in the EU notice & action initiative' (2015), Computer Law & Security Review: The International Journal of Technology, 31 (1), 46, 56.

Laidlaw, E. B., *Internet Gatekeepers, Human Rights, and Corporate Social Responsibility*, (London School of Economics and Political Science 2012).

MacKinnon, R. et al., United Nations Educational, Scientific, and Cultural, Organization, 'Fostering Freedom Online: The Role of Internet Intermediaries', (Paris: UNESCO 2014), Available from http://unesdoc.unesco.org/images/0023/002311/231162e.pdf.> accessed 10 November 2015.

Tambini, D., Leonardi, D., and Marsden, C. T., *Codifying cyberspace: communications self-regulation in the age of Internet convergence* (London; New York: Routledge 2008).

2. Review on EU Policies on Digital Defenders with a focus on Freedom of Expression – Case study on potential human rights implications of the EU's external policies

Council of the European Union, 'Council Conclusions on the Action Plan on Human Rights and Democracy 2015 - 2019' (20 July 2015). [2015b]

European Commission**,** A Partnership for Democracy and Shared Prosperity with the Southern Mediterranean' (Communication) COM (2011) 200 final.

European Commission, Commission Implementing Decision of 1 April 2015 on the Annual Action Programme 2015 for the European Instrument for Democracy and Human Rights (EIDHR) to be financed from the general budget of the European Union' C(2015) 2025 final.

European Parliament, 'Report on a Digital Freedom Strategy in EU Foreign Policy', A7-0374/2012, 15 November 2012.

'Resolution of 8 September 2015 on "Human rights and technology: the impact of intrusion and surveillance systems on human rights in third countries"', 2014/2232 (INI).

Benedek, W. and Kettemann, M. C., *Freedom of Expression and the Internet* (Council of Europe Publishing 2013).

Dankwa, A. and Pahnecke, O., 'Digital Human Rights Defence: The Challenges and Opportunities of using Social Media for Human Rights Documentation and Monitoring' in Benedek, W., Benoit-Rohmer, F., Karl, W., Kettemann, M. C., Nowak, M. (eds), *European Yearbook on Human Rights 2014* (NWV/Intersentia 2014), 39-62.

Digital Defenders Partnership, 'DDP' <https://digitaldefenders.org/> accessed 16 May 2015.

Frank Joergensen, R., *Framing the Net: the Internet and Human Rights* (Edward Elgar Publishing 2013).

Frontline Defenders, 'Human Rights Defenders Mechanism' <www.frontlinedefenders.org/EUHRD Mechanism> accessed 14 October 2015.

Horner, L., Hawtin, D. and Puddephatt, A., *Information and Communication Technologies and Human Rights* (European Union 2010).

Jansen, F, 'From digital threat to digital emergency' in Global Information Society Watch 2014, *Communications surveillance in the digital age* (Association for Progressive Communications (APC) and Humanist Institute for Cooperation with Developing Countries (HIVOS 2014).

Wagner, B., *After the Arab Spring: New Paths for Human Rights and the Internet in European Foreign Policy* (European Union 2012).