# Online service providers as human rights arbiters

*Rikke Frank Jørgensen and Anja Møller Pedersen[[1]](#footnote-1)*

*Abstract*

Within the EU, governments increasingly encourage online service providers to engage in co- and self-regulatory measures to prevent harmful and illegal content in the online sphere. As part of this tendency, governments shape schemes of liability for third-party content around the online service providers (intermediaries), giving them strong incentives to block, filter or take down content upon notification or request by public authorities to avoid liability. Concern has been raised, that the intermediaries are being used to implement public policy with limited oversight and accountability with severe implications on human rights. Drawing on case-studies of three EU directives, including the E-commerce directive, the chapter illustrates how measures of blocking, filtering, and take down of content in co- and self-regulatory frameworks interfere with the human rights standards related to freedom of expression and information. It further discusses current approaches towards human rights responsibilities of private actors, with a particular focus on the UN Guiding Principles on Business and Human Rights. The chapter concludes that self-regulatory frameworks are insufficient to counter the human rights challenges related to intermediaries, which play a crucial role for online public participation.

Introduction

It is commonly argued that the internet has a profound value for freedom of opinion and expression, as it magnifies the voice and multiples the information within the reach of everyone who has access to it. As such it has become the central global public forum (Kaye, 2015). However, it is largely a commercial domain with infrastructure and services in the hands of private companies. To participate in public life online, individuals must engage with a variety of online service providers (intermediaries) such as access providers, search engines, social media platforms etc. and rely on them for exercising their fundamental rights, for example, freedom of expression and information. In this sense, online service providers set the limits and boundaries for public participation in the online domain.

Since the mid-nineties, EU regulators have enlisted these intermediaries in a variety of co- and self-regulatory schemes to disable or remove alleged illegal content on the internet. As part of this, the EU model of limited liability for third-party content has been developed, but also contested, not least because of its unclear legal provisions, which create incentives for the intermediaries to over-block in order to avoid liability.

Each time content is blocked, filtered or taken down by an intermediary, that action has an impact on both the freedom of expression of the speaker and the freedom information of the end-user that the information was intended to reach. Concern has been raised, that the intermediaries are being used to implement public policy with limited oversight and accountability with severe implications on human rights (Brown, 2010; Callahan, Gercke, de Marco, & Dries-Ziekenheiner, 2009; Douwe Korff for the Council of Europe, 2014; Kuczerawy, 2015; Tambini, Leonardi, & Marsden, 2008).

Drawing on examples from EU regulation; the directive on electronic commerce (the E-commerce directive), the directive on combating the sexual abuse and sexual exploitation of children and child pornography, and the directive on the enforcement of intellectual property rights (IPR), the chapter examines EU content-regulation from a freedom of expression and rule of law perspective. Any interference by the state with freedom of expression and information must comply with the rule of law and meet the strict criteria laid down in international human rights law; it must be prescribed by law, pursue a legitimate aim and be proportionate (Council of Europe, 2014, para. 47). However, as argued by the authors, the current regulatory schemes are insufficient to provide the standards and compliance mechanisms required to meet these standards. Moreover, as human rights bind only states, not private actors, by allowing or even encouraging private actors to interfere with online expressions and information (content), without the necessary safeguards, states de facto neglect their human rights obligations and escape the strict requirements, which would have been otherwise incumbent upon them if they had applied the restrictions themselves.

As an alternative (and widely promoted) approach, the authors discusses the UN Guiding Principles on Business and Human Rights that serve as the prevailing soft law standard for the human rights responsibility of private actors. In line with recent research on internet gatekeepers (Laidlaw, 2012)[[2]](#footnote-2) the chapter argues that self-regulatory approaches are insufficient to solve the above human rights challenges caused by intermediaries, not least when they have the capacity to impact democratic life in a way traditionally reserved for public institutions.

The remaining part of this chapter proceeds as follow. First, it introduces the challenges that online content regulation poses to the right to freedom of expression and information, focusing in particular on blocking, filtering and take-down of content. Next, these challenges are exemplified by EU-regulation related to co- and self-regulatory schemes of intermediary liability (the E-commerce directive) and the fight against alleged illegal content (child pornography and IPR infringements). Third, the UN Guiding Principles on Business and Human Rights are discussed, and finally, the authors provide specific conclusions on these challenges.

Online freedom of expression

The right to freedom of expression is codified in all major human rights treaties, at the international level, most notably in the Universal Declaration of Human Rights (1948) and the International Covenant on Civil and Political Rights (1966); and at the European level, in the European Convention on Human Rights and Fundamental Freedoms (ECHR) (1950) and the Charter of Fundamental Rights of the European Union (CFREU) (2000).

The ECHR defines a right to “to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers” under article 10(1), and the possible restrictions to that right in Article 10(2).[[3]](#footnote-3) These restrictions must be “prescribed by law”, follow a “legitimate aim” and be “necessary in a democratic society”, commonly referred to as the proportionality test (Council of Europe, 2014, para. 47). Freedom of expression includes all forms of expression, without any distinction to content and through any medium (Jacobs, 1961, 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). This is also confirmed in the first UN resolution on human rights on the internet from 2012 (United Nations Human Rights Council, July 5, 2012).

Since international human rights law binds states, not private actors, only limitations to freedom of expression by public authorities constitutes ‘interference’ in a legal sense. Accordingly, while 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, the same obligations are not imposed on private actors. However, additionally to these *negative obligations*, the ECtHR has also developed a theorem on *positive obligation*s of Member States. The positive obligations concern a state’s obligation to ensure that individuals may enjoy freedom of expression, even in conflicts with other private parties. In consequence, the 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, 28 June 2001, para. 45). The ECtHR has recognised such positive obligations in relation to Article 10, for instance in cases where plurality of media was at stake (Demuth v. Switzerland, 5 February 2003).[[4]](#footnote-4)

The Court’s doctrine on positive obligations does, however, draw limits to what can be expected of states, especially when state action premised on positive obligations touches upon other rights, such as property rights (Sluijs, 2011, 20). A landmark case in this respect is *Appleby*, which concerned the alleged positive obligation of a State to protect protesters’ freedom of expression on private property - a shopping centre - from which they had been removed (Appleby and Others v. the United Kingdom, 6 May 2003). The Court found that in a private sphere, a state’s positive obligation only arises where the bar on access to the property effectively prevents effective exercise of the freedom, or if it destroys the essence of the right. Due to alternative ways for meaningful exercise of the right, the essence of the right was not destroyed in the present case, and the positive obligations were not triggered. In general, the Court has stressed, that the State must strike a fair balance between the concurring rights, and the burden on the state must not be disproportionate.[[5]](#footnote-5)

In the online domain, interference with freedom of expression can take various forms, from inadequate guarantees of the right to privacy and protection of personal data, which inhibits the dissemination of opinions and information, to measures that either remove the content (take-down), or disable end-users’ ability to access it (filtering and blocking) (Deibert, Palfrey, Rohozinski, Zittrain, & OpenNet, 2010; La Rue, 2011).[[6]](#footnote-6)

As the digital infrastructure and online services are largely controlled by private companies, measures to remove or disable access to content require either cooperation from these service providers or coercion exercised upon them through ‘new-school’ techniques´ (Balkin, 2014, p. 3). These techniques are characterised by three features (1) collateral censorship; the state regulates one party (the intermediary) in order to control another, the speaker, (2) public/private cooperation and co-optation, and (3) new forms of digital prior restraints (Balkin, 2014, p. 4).

Scholars have repeatedly warned against the many practical as well as principal problems related to current European practices of content regulation (Callahan et al., 2009; Kuczerawy, 2015; McIntyre, 2010; Tambini et al., 2008). As argued by Korff, measures such as filtering and blocking are inherently likely to produce false positives (blocking sites with no prohibited material) and false negatives (when sites with prohibited material slip through a filter). Moreover, the criteria for blocking specific websites, and the lists of blocked websites, are often secret and remedies little known or non-existent. As regards their effectiveness, most blocking is easy to bypass, even for not very technically skilled people (Douwe Korff for the Council of Europe, 2014, p. 13).

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 “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).

There is an essential distinction between mandatory measures, which are based on law,[[7]](#footnote-7) and voluntary measures (self-regulation). Law-based removal or disabling access to online content constitutes an interference with freedom of expression and information under Article 10 of the ECHR, and must adhere to the criteria laid down in Article 10(2). Arguably, it is legitimate to remove or block clearly identified illegal content, such as child pornography. However, the aim of the measure, and the means used to obtain it remain crucial to determining whether the measure is proportional and thereby lawful. In cases where the interference is law-based and/or clearly encouraged by the state (co-regulation), the potential violation of freedom of expression and information is attributable to the state, and the human rights conflict thus a vertical conflict between the state and the intermediary, the speaker or the end-users. At some point, however – in the zone between co- and self-regulation – potential human rights violations may only be attributed to the state, indirectly, through its positive obligation to protect against potential violations between private parties.

Voluntary measures of content regulation, in contrast, cause a horizontal conflict between the intermediary who imposes the measure and the speaker (who is being blocked) or the end-user (who is denied access). Horizontal conflicts must be resolved under the state’s positive human rights obligations. 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. These cases are not as clear-cut as the vertical ones.

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 interference by the intermediary is normally 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 when a strict positive obligation arises is 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 (J. v. Hoboken, 2012, p. 148f).

In the following, we will illustrate how EU policy dealing with illegal content encourages online service providers to apply measures that effectively interfere with freedom of expression and information, without the required human rights safeguards.

EU regulation in conflict with freedom of expression

“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, United Nations Educational, & Cultural, 2014, p. 56).

Through a case-study of three EU directives; Directive 2000/31/EC on electronic commerce (E-commerce directive), Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography (child pornography directive), and Directive 2004/48/EC on the enforcement of intellectual property rights (IPR enforcement directive), the authors explore the implications of EU content regulation on freedom of expression and information and the rule of law. While the E-commerce directive sets up the general limits for intermediary liability for user-generated content, irrespective of the nature of the liability (criminal or civil), the other directives deal with either criminal offences (directive 2011/93/EU) or civil liability (directive 2004/48/EC). All of them contain obligations to either disable access to or take down alleged illegal content, and all of them imply that intermediaries must play an active role. Yet, neither of them frame this as human rights issues.

*Directive 2000/31/EC on E-commerce* sets up an Internal Market framework for electronic commerce (European Parliament and Council of the European Union, 2000). Pursuant to Article 2(a) and Recital 18, the directive is applicable to services provided by intermediaries, such as ISPs, search engines and social media platforms. Articles 12 – 14 set up ‘safe harbours’ under which an intermediary cannot be held liable for illegal content generated by its users and protect private actors acting as intermediaries for three types of activities: ‘mere conduit’, ‘caching’ and ‘hosting.[[8]](#footnote-8) Furthermore, Article 15 prevents Member States from imposing general monitoring obligations on the intermediaries. During the public consultation in 2010, it became apparent, that the directive gave rise to various challenges, such as legal fragmentation and lack of clarity with respect to the liability provisions and their scope of application (European Commission, 2010). The Commission has since launched several initiatives to improve the system, but without any result. The recent Digital Single Market Strategy promises an improvement of EU content regulation with due regard to its impact on freedom of expression and information (European Commission, 2015), yet the initiative is still at an early stage, and results remain to be seen.

Blocking of alleged child pornography has been high on the EU policy agenda since the mid-nineties (European Commission, 1996a, 1996b). While earlier approaches prevailed towards self-regulation, the preferred path is now co-regulation (McIntyre, 2010, p. 2010ff.). *Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography* establishes minimum rules concerning the definition of criminal offences and sanctions for sexual abuse and exploitation of children (The European Parliament and the Council of the European Union, 2011). Pursuant to Article 25 and Recital 47, Member States shall take all necessary measures to ensure the removal of, or disabling access to, websites containing or disseminating child pornography and the directive is without prejudice to voluntary action (self-regulation) taken by the industry in that regard. Recital 25 and 47 requires that account is taken to the rights of the end-users, and that the measures provide for adequate safeguards. However, the directive provides no guidance in the matter.

Turning to copyright, the music and film industries have - for more than a decade - searched for solutions to fight alleged infringements, for instance targeting file sharing in peer-to-peer networks. Earlier, lawsuits were the primary means, whereas regulation via intermediaries is now the preferred path (Brown, 2010, p. 3). To prevent IPR infringements across Member States, the EU has adopted *Directive 2004/48/EC on IPR enforcement* (European Parliament and Council of the European Union, 2004).[[9]](#footnote-9) Without prejudice to the E-commerce directive, it concerns the measures, remedies and sanctions necessary to ensure IPR enforcement (Articles 9 – 13 and 16). Pursuant to Article 17 and Recital 29, Member States shall encourage the industry to take an active part in the fight against piracy and counterfeiting, for instance by developing codes of conduct dealing with the matter, thus encouraging self-regulation. To the extent intermediaries use of blocking, filtering and takedowns, freedom of expression limitations are likely to occur. Recital 32 of the directive recognises the respect for fundamental rights, but mainly IPR protection, moreover the directive offers no guidance in the matter. Besides lack of compliance with the rule of law and Article 10(2) of the ECHR, this may lead to massive blocking of legitimate file exchanges as the intermediaries are not the best placed to assess whether a specific use of IPR protected work is legitimate.

*Vertical and horizontal human rights conflicts*

The three directives are examples of the current EU ‘co-regulatory’ approach towards content regulation (Frydman, Hennebel, & Lewkowicz, 2008, p. 5). ‘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 private and public players (Frydman et al., 2008, pa. 1).[[10]](#footnote-10) It may be restricted to cover regulation that contains a legally formalised role of public authorities (J. v. Hoboken, 2012, p. 140), or include state participation in a broader sense (MacKinnon et al., 2014, p. 56). It differs from a ‘command and control’ model in which drafting, implementation and enforcement is solely on the hands of public authorities, but also from ‘self-regulation’ where private actors make the rules and enforce them without any public intervention (Schulz & Held, 2001, p. A-2), such as the UK model for countering child pornography (Brown, 2010, p. 3).

Due to an increasing pressure on the intermediaries, the current co-regulatory practices may foster self-regulation, in particular as this is either presupposed (the E-commerce directive), accepted as a possible means (Article 25 and Recital 47 of the child pornography directive) or directly encouraged (Article 17 and Recital 29 of the IPR enforcement directive) by the three EU directives. Although self-regulation is praised as an effective tool to redress illegal or harmful speech (The United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression, & the African Commission on Human and Peoples’ Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information, June 1, 2011), it entails severe human rights and rule of law challenges (Douwe Korff for the Council of Europe, 2014; La Rue, 2011, para. 38ff.).

In the following, these challenges are discussed, drawing on the analysis of the EU directives.

First, with respect to the human rights implications of co-regulation compared to self-regulation, the distinction between mandatory and voluntary content regulation is important. Mandatory content regulation is introduced and/or applied directly by the state and constitutes a *vertical human rights conflict* between the state and the intermediary, speaker or end-users. As such, the potential violation of freedom of expression is ‘prescribed by law’ and clearly attributable to the state. In contrast, voluntary content regulation in a self-regulatory scheme remains a *horizontal conflict* between the intermediary who imposes restrictions and the speaker/end-user who is subject to it. In practice, however, the distinction contains several grey zones. For instance, does active coercion of intermediaries to ‘voluntarily’ filter or block content, in the absence of a legal duty to do so, constitute an ‘interference’ with freedom of expression, and is it ‘prescribed by law’ in accordance with Article 10(2) of the ECHR? Moreover, at what stage may freedom of expression limitations be attributed to the state, when caused by ‘voluntary’ measures taken by intermediaries following state encouragement to do so?

Generally, 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 constitute ‘interferences’ with the right. Likewise, it is also difficult to argue that they fall within the positive obligations of the state

The positive obligations of the state are activated only when individuals are prevented from effectively exercising their right to freedom of expression, or when pluralism of the information environment would be clearly at stake. States hold a wide margin of appreciation (J. v. Hoboken, 2012, p. 148f.). However, 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, and the states may become responsible for *not* placing such a system on a legislative basis (Douwe Korff for the Council of Europe, 2014, p. 73):

‘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’ (Douwe Korff for the Council of Europe, 2014, p. 72)

However, it is not – at least not on a general basis – that easy to establish, ‘when’ an individual is effectively prevented from exercising his/her freedom of expression and thus, when the positive human rights obligations are triggered. As such, the above statement appears quite optimistic.

Second, all of the above directives accept or encourage blocking and/or takedowns, and they all either accept or encourage these measures to be taken through self-regulation, yet none of them frames such measures as limitations of / interferences with freedom of expression or acknowledge the human rights implications of such obligations / proposals. 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 due to lack of legal basis.

Third, the directives do not provide for common EU procedures for dealing with alleged illegal content, but only set up limits and suggestions for possible national means. Articles 12 – 14 of the E-commerce directive, for instance, do not stipulate that all Member States must implement a common EU liability scheme, but provide only for ‘safe harbours’ in which the Member States cannot impose liability on the intermediaries. Consequently, the liability schemes vary across Member States, resulting in great legislative fragmentation. This also became apparent during the 2010 public consultation on the directive (European Commission, 2010) and has led to calls for further harmonisation (EDRI and others, 2015). For instance, with general reference to the human rights obligations in the ECHR and the CFREU, Article 25(2) and the Recital 47 of the child pornography directive requires that account is taken to the rights of the end-users, and that the measures provide for adequate safeguards. The directive, however, does not explain the potential human rights issues at stake and how to prevent human rights violations.

Fourth, the 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 instance, whether a specific use of an IPR protected work is illegal, or whether content related to child pornography is distasteful or illegal. They are therefore likely to rely on requests to block or take down content without challenge, in particular when facing liability for illegal third-party content. This might lead to ‘over-compliance’ resulting in blocking and takedowns of legal content, which thus no longer follow a legitimate aim, or meet the strict criteria of proportionality required by Article 10(2) of the ECHR.[[11]](#footnote-11)

As argued by Korff, measures with an impact on fundamental rights, specifically blocking and filtering of websites, cannot ever be said to be ‘necessary’ and ‘proportionate’ to a ‘legitimate aim’ in a ‘democratic society’ if they are unsuited to achieve that aim, excessive in their effect, and lack procedural safeguards. For instance, blocking of child pornography related content: (i) does not stop sexual abuse of children or the sharing of images of such abuse; (ii) does stop access by the large majority of the population to sites that are not illegal; (iii) is based on secret criteria or lists that clearly do not have the quality of a ‘law’ in the ECHR sense; and (iv) is not subject to adequate remedy. This harms freedom of expression for those whose sites are wrongly blocked and for those who are effectively missing out on relevant information (Douwe Korff for the Council of Europe, 2014, p. 74).

In sum, codification and encouragement of co- and self-regulation within the EU, focuses more on the (perceived) effectiveness that such schemes provide for in the fight against illegal content, than on the human rights conflicts and rule of law concerns raised by these practices.

*Intermediary liability*

Schemes of limited liability are one of the mechanism used to enlist intermediaries in online content regulation. The E-commerce directive codifies these expectations by stipulating the conditions under which intermediaries cannot be held liable for third party content. However, its lack of clarity put pressure on the intermediaries to act as ‘gatekeepers’ of the online sphere.

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. Regulation thus becomes ‘decentralised’ (Morgan & Yeung, 2007, p. 280). As gatekeepers usually do not benefit from the misconduct they facilitate, although being in a position to prevent it, it can prove more effective to shape a liability scheme around gatekeepers as opposed to those breaking the rules (Laidlaw, 2010, p. 264), which may also be referred to a ‘collateral censorship’[[12]](#footnote-12). Hence, gatekeeping theory has been used to describe the tort doctrine of vicarious liability, for instance, in relation to 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 pursue 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 take-down provisions of the E-commerce directive.

However, the EU liability framework of the E-commerce directive entails several challenges, of which four will be pointed out below.

First, the liability distinctions of the directive remain rather unclear.[[13]](#footnote-13) To benefit from a safe harbour, intermediaries must 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). It remains unclear, however, what constitutes ‘actual knowledge’ or ‘awareness of facts or circumstances´ or what it takes to act ‘expeditiously’[[14]](#footnote-14) and thus what it takes to benefit from a safe harbour.[[15]](#footnote-15) The interpretation of the provisions thus differs across borders, leading to legal fragmentation (European Commission, 2012, p. 32ff.) and creating incentives for over-compliance.

Second, the directive regulates only exemptions from liability, but it does not protect the intermediaries from litigations aimed at injunctions, cf. Articles 12(3), 13(2) and 14(3). Consequently, Member States are not prevented from forcing the intermediaries to play an active role in law enforcement. Moreover, a court order to disconnect a user or block access to certain information is not necessarily accompanied by guidance to ensure compliance with the principle of proportionality in Article 10(2) of the ECHR and the risk of over-compliance is thus present.

Third, Articles 12–15 concern liability for illegal content, yet what counts as ‘illegal’ is determined by national law, and when assessed by an intermediary, who is not the best placed to do so, the risk of over-compliance is significant. Also, in contrast to the US approach, the directive does not distinguish between criminal and civil liability, but follows a horizontal approach defining one set of general rules applicable to any content; child pornography, IPR etc. (Frydman et al., 2008, p. 6). This may also lead to disproportionate handling of content (Kuczerawy, 2015, p. 52).

Fourth, in relation to caching, it is required that the intermediary does not ‘actively interfere’ with the transmission (Article 13). However, if an intermediary, due to government pressure, applies filters to disable access to child pornography according to Article 25 of the child pornography directive, it runs the risk of invoking liability, as it then actively interferes with the transmission.

This paradox does not seem to be envisaged by the directive, but it has become even more present with the recent Delfi judgment (Delfi AS v. Estonia, 16 June 2015). This is the first case, in which the ECtHR examined a complaint regarding liability for user-generated content. It illustrates important aspects of the limited liability scheme of the E-commerce directive, but also liability schemes framed around intermediaries more generally, and seems to increase the responsibilities of the intermediaries.

The case concerned whether Delfi, a large news portal, could be held liable for offensive comments (of which the majority constituted hate speech) posted on its website by anonymous third parties. Delfi took down the comments upon notification, six weeks after publication, yet defamation proceedings were still launched against it. Delfi claimed to be an intermediary falling under the safe harbours of the national transposition of the E-commerce directive. The ECtHR, however, found that Delfi acted – not as an intermediary – but as a media publisher (due to its degree of editorial control) and so it could not benefit from the safe harbours.[[16]](#footnote-16) Consequently, a key question became whether Delfi had been obliged to remove the comments before notification.

The Court considered, that Delfi exercised a substantial degree of control over the comments, beyond that of a purely *passive* service provider, thus falling outside the safe harbour of the directive. The majority of the authors were anonymous (why liability could not be placed elsewhere), and the proceedings did not have any severe consequences for Delfi (Ibid, paras. 144-151). The Court, furthermore, interpreted national legislation in 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. Given its substantial degree of control over the comments, the Court considered that such interference with Delfi’s freedom of expression was not disproportionate. Having regard to the ample possibilities for anyone to make his or her voice heard on the internet, the Court found that the obligation of a large news portal to take effective measures to limit the dissemination of hate speech and speech inciting violence could not be equated with private censorship. Particularly as the ability of a potential victim of hate speech to continuously monitor the internet is more limited than the ability of a large internet news portal to prevent or rapidly remove such comments (Ibid, paras. 157-158). With respect to clear hate speech and direct threats to the physical integrity of individuals, the rights and interests of others and of society as a whole, would thus entitle Member States to impose liability on news portals, failing to remove clearly unlawful comments without delay, even without notice from authorities or potential victims of the unlawful content, without contravening Article 10 of the ECHR (Ibid, paras. 159).

Several judges had dissenting opinions reflecting their concerns about the implications of the judgment. Some claimed, that it implied a requirement of constructive knowledge on *active intermediaries*,[[17]](#footnote-17) which would require, that all comments were monitored, and the fear of liability could lead to self-censorship (Delfi AS v. Estonia, 16 June 2015, Joint Dissenting Opinion of Judges Sajó and Tsotsoria, para. 1). Although not intending to censor expressions, by putting pressure and imposing liability on the intermediaries, governments are actually creating an environment of ‘collateral’ and private-party censorship (Balkin, 2014). When liable for user-generated content, an intermediary has strong incentives to self-censor, limit and deny users access to communicate via the platform in order to avoid liability and thereby impose prior restraints on its users’ expressions/information. Furthermore, the practices entail limited procedural safeguards, as action is taken not by a court, but private parties (Ibid, 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. Without actual knowledge of their existence, such duty in fact requires active intermediaries (news portals or blogs) to monitor all comments, similar to prior restraints (Ibid, paras. 34- 35) and prohibited by Article 15 of the E-commerce directive.[[18]](#footnote-18)

To sum up, legal uncertainty around the provisions of the E-commerce directive and its national transposition and the fear of liability for user-generated content may result in ‘over-compliance’ and thereby disproportionate limitations of freedom of expression and information. Moreover, it can lead to extra-legal pressure on intermediaries to self-regulate by blocking and filtering or not challenge requests to block or take down certain content. Also, as the victims often do not have the resources to challenge the measures, content may be blocked or removed without any – administrative or judicial – review. Such self-regulatory frameworks may not even provide for access to effective remedies, as required by Article 13 of the ECHR.

Without proper control or review mechanisms, nothing prevents human rights violations from occurring. Human rights obligations are briefly touched upon in the Preamble of the E-commerce directive,[[19]](#footnote-19) but it does not deal with the potential human rights conflicts, and is thus not sufficient to protect freedom of expression, particularly not as the directive has to be transposed to national law in 28 Member States.

An alternative approach – human rights responsibility of private actors

As illustrated, several challenges occur when law enforcement is delegated to intermediaries without sufficient rule of law safeguards. Moreover, and adding to the complexity, there is an increasing focus on the human rights responsibilities of internet companies, which put pressure on these private actors to both implement public policy (tackle illegal content) and respect human rights.

The key standard-setting document on the human rights responsibility of private actors is the United Nations ‘Guiding Principles on Business and Human Rights’(United Nations Human Rights Council, 2011) is 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 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 & Dhanarajan, 2015, p. 3).

The *first pillar* outlines 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, 2011, para. 1-10). 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, 2011, para. 11-24). Due diligence is envisaged to comprise four steps, taking the form of a continuous improvement cycle (United Nations Human Rights Council, 2011, para. 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. The *third pillar* 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, 2011, para. 25-31).

The Human Rights Council 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, 2011, 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).

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 access 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 it may also affect, directly or indirectly, billions of internet users.

Although online service providers have a responsibility to assess the human rights impact of their activities in order to minimise their negative impact, states are not thereby ‘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.

The UN Guiding Principles have been widely appraised for their role in raising human rights awareness among businesses, yet their effectiveness has also been questioned not least due to their voluntary and non-binding character (O'Brien & Dhanarajan, 2015, p. 3). Moreover, the UN Guiding Principles may move focus away 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 reality in EU Member States. As such, it is paramount, that states do not use or encourage self-regulation as a way to escape their own – hard law – human rights obligations, nor should they rely on the soft law responsibilities of businesses.

Laidlaw 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.) (Laidlaw, 2012, p. 11). Online gatekeepers that have the capacity to impact democratic life are expected to serve the public interest, however these companies 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 (Ibid, p. 46). To counter this challenge. It is suggested that the human rights obligations of these companies should increase according to the extent that their activities facilitate or impact democratic culture[[20]](#footnote-20) (Ibid, p. 241).

Within the UN system, attempts towards more legally binding human rights obligations for businesses have actually been taken. Although earlier attempts failed, the discussion on establishing such binding norms has continued among civil society and a group of states within the UN system (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 established an intergovernmental working group to elaborate on the instrument (United Nations Human Rights Council, 2014). 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).

The increasing focus on the human rights responsibilities of private actors adds to the complexity of the online service providers as discussed above. Aside from the state pressure to implement public policy with a view to counter illegal online content, 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. An online service provider 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 States as illustrated above, this may result in a severe negative impact on freedom of expression and information.

Hence, it might prove difficult for service providers to meet these contradictory expectations, in particular when the implementation of the said directives happens in co- or self-regulatory frameworks that offer limited guidance on how to obtain human rights compliance.

Conclusions

The authors have pointed to a number of human rights challenges that occur at the junction of the EU policies dealing with illegal content on the internet, with a particular focus on self-regulation and intermediary liability.

As illustrated, internet intermediaries are increasingly being enlisted to impose – in a mix of mandatory and voluntary schemes – restrictions on freedom of expression and information; without the safeguards that would apply to state interference in similar situations. 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, as soft law they do not solve the fundamental challenge raised in this chapter. Consequently, interference with EU citizens’ 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 internet-users’ ability to enjoy freedom of expression and information online. Yet, the intermediaries are subject to EU regulation, which does not maximise their adherence with international human rights standards, but creates ambiguity around liability for user-generated content and encourages self-regulation. Also and importantly, the measures deployed by the intermediaries do not comply with the rule of law test developed by the ECtHR in its case law on Article 10 of the ECHR.

The authors have highlighted how EU´s policy related to intermediary liability, IPR enforcement, and combating child pornography etc., may influence negatively on users’ freedom of expression and information online. As illustrated, the intermediaries operate 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) expectations of self-regulation (e.g. by blocking, filtering or take-down of content) as stipulated by the IPR enforcement directive and the child pornography directive; (2) liability schemes that expect them to expeditiously remove alleged illegal content in order to benefit from ‘safe harbours’ provisions; 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.

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, which is outside their direct sphere of control. Looking through the prism of the right to freedom of expression and information, 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 are 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 are transposed to national law in 28 Member States, leading to legal fragmentation. In consequence, the intermediaries are left with self-devised codes of conduct while carrying out practices that affect users’ fundamental rights.

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 traditional human rights perspective. Until recently, the underlying rationales for addressing human rights issues at the EU level have been economic in nature and human rights, which are by nature non-economic, have been addressed as auxiliaries to the establishment of an Internal Market. As a result, important policy concerns from the perspective of human rights end up being addressed indirectly or not addressed at all.[[21]](#footnote-21)

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, May 12, 2014, para. 7), this has yet not been implemented in secondary EU law (such as the three above mentioned directives). 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. Also, a number of UN reports and resolutions adopted on freedom of expression on the internet since 2011 set standards in this field.

With the adoption of the Lisbon Treaty, fundamental rights play a more important role than ever within EU-law. Yet, EU standards and guidance for the protection and promotion of freedom of expression in the online domain is still lacking, particularly as it relates to the EUs 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 on the strategy is a crucial opportunity to emphasise that fundamental rights are firmly situated as the baseline of the EU vision and practices in this field.

*Bibliography*

Akandji-Kombe, J. (2007) *Positive obligations under the European Convention on Human Rights* [online] Council of Europe Human Rights Handbook Series. Available at: [http://www.echr.coe.int/LibraryDocs/DG2/HRHAND/DG2-EN-HRHAND-07(2007).pdf](http://www.echr.coe.int/LibraryDocs/DG2/HRHAND/DG2-EN-HRHAND-07%282007%29.pdf).

Appleby and others v. the United Kingdom [6 May 2003] App. no. 44306/98 (European Court of Human Rights).

Balkin, J. M. (2014) ‘Old-School/New-School Speech Regulation’ *Harvard Law Review* 127(8), 2296-2342.

Bavière, J. (2012) Injunctions against online search engine service providers [online]. International Bar Association. Available at: http://www.ibanet.org/Article/Detail.aspx?ArticleUid=7D602A2A-12FF-4E07-B525-32BE2993BE25.

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

Callahan, C., Gercke, M., de Marco, E., & Dries-Ziekenheiner, H. (2009) *Internet blocking. Balancing cybercrime responses in democratic societies*.

Council of Europe. (2014). *Recommendation CM/Rec(2014)6 of the Committeee of Ministers to member States on a guide to human rights for Internet users - Explanatory Memorandum*. Strasbourg: Council of Europe.

Council of the European Union (2014) *EU Human Rights Guidelines on Freedom of Expression Online and Offline*. Brussels: Council of the European Union.

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.

Delfi v. Estonia [16 June 2015] App. No. 64569/09 (European Court of Human Rights).

Demuth v. Switzerland [5 February 2003] App. no. 38743/97 (European Court of Human Rights).

EDRI and others (2015) *Open letter on intermediary liability protections in the digital single market to Vice-President of the European Commission Andrus Ansip* [Online] Available at: <https://edri.org/open-letter-on-intermediary-liability-protections-in-the-digital-single-market/> [Accessed 22 May 2016].

European Commission (1996a) *Communication from the Commission on Illegal and Harmful Content on the Internet (COM(1996) 487 final)*. Brussels: European Commission.

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

European Commission (2010) *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)*. Brussels: European Commission.

European Commission (2012) *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 (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.* Brussels: European Commission.

European Parliament and the Council (2000) *Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)*. OJ L 178, 17.07.2000.

European Parliament and the Council (2001) *Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society*. OJ 167/10, 22.06.2001.

European Parliament and the Council (2004) *Directive 2004/48/EC on the enforcement of intellectual property rights*. OJ L 157, 02.06.2004.

European Parliament and the Council (2011). *Directive 2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography*. OJ L 127, 29.04.2014.

Frydman, B. (2004) Coregulation: a possible model for global governance: In B. de Schutter & J. Pas, Eds., *About globalization, view on the trajectory of mondialisation.* pp. 227-242. Brussels: Brussels University Press.

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

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

Hoboken, J. (2014) *The European Approach to Privacy* [online] In: TPRC 42: The 42nd Research Conference on Communication, Information and Internet Policy. SSRN. Available at: [http://papers.ssrn.com/sol3/papers.cfm?abstract\_id=2418636##](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2418636) [Accessed 22 May 2016]

Jacobs, J. (1961) *The death and life of great American cities*. New York: Random House.

Kaye, D. (2015) *Report of the Special rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye*. Geneva: United Nations.

Korff, D. for the Council of Europe (2014) *The rule of law on the Internet and in the wider digital world - Issue Paper*. Strasbourg: Council of Europe.

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(1), 46-56.

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*. Geneva: United Nations.

Lagoutte, S. (2014) ‘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’ *Matters of Concern - Human Rights' Research Papers Series,* 2014/1.

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

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

MacKinnon, R., UNESCO (2014) *Fostering freedom online the role of internet intermediaries*. Paris: UNESCO.

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

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

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

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\*.*

Perrin v. the United Kingdom [18 October 2005] App. no. 5446/03 (European Court of Human Rights).

Ruggie, J. G. (2014) ‘A UN Business and Human Rights Treaty?’ *HARVARD Kennedy School*.

Schulz, W., & Held, T. (2001) *Regulated Self-Regulation as a form of modern Government*. Hamburg: Verlag Hans-Bredow-Institut

Sluijs, J. P. (2011) *From Competition to Freedom of Expression: Introducing Art. 10 ECHR in the European Network Neutrality Debate. TILEC Discussion Paper* 2011-040.

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

United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression, & the African Commission on Human and Peoples’ Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information. (June 1, 2011). *Joint Declaration on Freedom of Expression on the Internet* Retrieved from

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

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*. Geneva: United Nations.

United Nations Human Rights Council (2014) *Resolution 26/... 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*. Geneva: United Nations.

VGT Verein Gegen Tierfabriken v. Switzerland [28 June 2001] App. No. 24699/94 (European Court of Human Rights).

1. Rikke Frank Jørgensen is Senior Researcher at the Danish Institute for Human Right. Anja Møller Pedersen is PhD fellow at the Danish Institute for Human Rights and the University of Copenhagen. This chapter draws on the Case Study on ICT and Human Rights (Policies of EU), Work Package No. 2 – Deliverable No. 2.3, which was published in March 2016 as part of and funded by the EU FP7 FRAME project. [↑](#footnote-ref-1)
2. As of July 2015, Laidlaw’s PhD thesis has been published under the title *Regulating Speech in Cyberspace*, by Cambridge University Press. [↑](#footnote-ref-2)
3. See (Council of Europe, 1950) Available at: <http://www.echr.coe.int/Documents/Convention_ENG.pdf> [↑](#footnote-ref-3)
4. See, also, (Jean-François Akandji-Kombe, 2007) [↑](#footnote-ref-4)
5. “In determining whether or not a positive obligation exists, regard must be had to the fair balance that has to be struck between the general interest of the community and the interests of the individual, the search for which is inherent throughout the Convention. The scope of this obligation will inevitably vary, having regard to the diversity of situations obtaining in Contracting States and the choices, which must be made in terms of priorities and resources. Nor must such an obligation be interpreted in such a way as to impose an impossible or disproportionate burden on the authorities” (Appleby and others v. UK, 2003, para. 40) [↑](#footnote-ref-5)
6. ‘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 search for information (La Rue, 2011, para. 29). ‘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 (Delfi AS v. Estonia, 16 June 2015) para. 13. [↑](#footnote-ref-6)
7. Including both content regulation, which is implemented and enforced directly by states, and content regulation, which is based on law, but implemented and/or enforced by private companies (co-regulation). [↑](#footnote-ref-7)
8. Search engines are not formally covered by the E-commerce directive (Frydman, 2004) However, most Member States grant search engines an exemption from liability, either by analogy with caching or hosting, or as derived from general principles of tort law, (Javier Martínez Bavière) P. 241. [↑](#footnote-ref-8)
9. The EU has also adopted the copyright directive, (European Parliament and Council of the European Union, 2001) [↑](#footnote-ref-9)
10. Co-regulation may also be referred to as ‘privatised law enforcement’, (Douwe Korff for the Council of Europe, 2014) p. 85. [↑](#footnote-ref-10)
11. This presupposes, that such limitations happen within mandatory / co-regulatory frameworks in which the potential human rights violations derive from public authorities and constitute ‘interferences’. In voluntary / self-regulatory frameworks the question is whether such limitations fall under the state’s positive human rights obligations and thus, whether the state has ensured a proper balance between the rights of the individuals. [↑](#footnote-ref-11)
12. 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, 2014) [↑](#footnote-ref-12)
13. As discussed extensively by e.g. Hoboken, (J. v. Hoboken, 2012) [↑](#footnote-ref-13)
14. 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. [↑](#footnote-ref-14)
15. As stressed in the Digital Single Market Strategy (European Commission, 2015) Para. 3.3.2. [↑](#footnote-ref-15)
16. The ECtHR, however, stressed that the findings could not be transferred to discussion forums or social media platforms (Ibid, para. 116). [↑](#footnote-ref-16)
17. Hosts who provide their own content and open their intermediary services for third parties to comment on that content [↑](#footnote-ref-17)
18. It could be argued, that the strict liability resulted from the clear illegal nature of the comments, (Delfi AS v. Estonia, 16 June 2015, Concurring opinion of Dissenting Judges Raimondo, Karakas, De Gaetano and Kjølbro ) Concurring opinion by Dissenting Judges Raimondo, Karakas, De Gaetano and Kjølbro. [↑](#footnote-ref-18)
19. 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’. [↑](#footnote-ref-19)
20. 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. [↑](#footnote-ref-20)
21. This point has also been raised by Hoboken (2014) in relation to privacy and data protection. See (J. Hoboken, August 15, 2014) [↑](#footnote-ref-21)