Freedom of Expression in the Internet

Hertig Randall, Maya

How to cite

HERTIG RANDALL, Maya. Freedom of Expression in the Internet. In: Schweizerische Zeitschrift für internationales und europäisches Recht, 2016, vol. 26, n° 2, p. 235–253.

This publication URL: https://archive-ouverte.unige.ch/unige:87712

Freedom of Expression in the Internet

Maya Hertig Randall*

The internet offers vastly enhanced communicative opportunities. At the same time, its ability to amplify ideas and information in space and time also entails greater potential to cause harm than traditional means of communication. Against this background, the first part of this paper examines to what extent courts have extended traditional free speech principles to communication in the internet. In the light of the classic free speech framework, the second part analyses the specific challenges raised by internet-based communication, including, for instance, the lack of a clear, transparent regulatory framework, the risks of automated systems of speech control and collateral censorship, and the difficulties to reconcile the need to afford victims of hate speech and other crimes effective protection with the concern to prevent a chilling effect detrimental to the legitimate exercise of freedom of expression.

Table of Contents

I. Introduction

Technological advances and related concerns have been part of the history of communication and freedom of expression. The U.S. Supreme Court highlighted this in a case extending the constitutional free speech guarantee to videogames, holding that «[...] whatever the challenges of applying the Constitution to ever-advancing technology, ‹the basic principles of freedom of speech and the press, like the First Amendment's command, do not vary› when a new and different medium for communica-

* Professor of Constitutional Law at Geneva University, LL.M. (Cambridge). Without indication to the contrary, all websites mentioned were last accessed on 10 March 2016.

tion appears».[1] An analysis of freedom of expression in the internet needs to be grounded on the principles reflecting the main values and functions underlying free speech. The first part of this study will set out the freedom of expression framework. It will highlight the main free speech principles and show their relevance for internet-based communication.[2] Although the basic free speech principles «do not vary», the European Court of Human Rights (ECtHR) has rightly pointed out that technological advances, including the internet, raise new challenges and may require adjustments «according to the technology's specific features in order to secure the protection and promotion of the rights and freedoms concerned.»[3] The second part will outline the main challenges raised by the specific features of communication in the internet and show how they have been tackled in the case law. The focus of the paper will be on the case law of the ECtHR.[4] Decisions of other international tribunals (mainly the European Court of Justice [ECJ]) and of domestic courts will also be relied upon to show different solutions in a comparative perspective.

II. The Free Speech Framework

A. The Scope of Freedom of Expression

Effective communication is an interactive process, involving different actors with changing roles. When we communicate, we speak, write, listen, respond, seek, transmit and disseminate information and opinions. Not surprisingly, international human rights guarantees protect the free flow of communication in a comprehensive way, from the perspective of both the speaker and the recipient, and independently on the mode or form of communication.[5] Art. 19 ICCPR, for instance, enshrines the «freedom to seek, receive and impart information and ideas of all kinds [...] either orally, in writing or in print, in the form of art, or through any other media of his choice.»

1 U.S. Supreme Court, *Brown v. Entertainment Merchants Association*, 564 U.S. 08-1448 (2011), p. 2.

2 For a study examining to what extent old frames are adapted to the internet, see András Sajó & Clare Ryan, «Judicial Reasoning and New Technologies. Framing, Newness, Fundamental Rights and the Internet», in: O. Pollicino & G. Romeo (eds.), The Internet and Constitutional Law: The Protection of Fundamental Rights and Constitutional Adjudication in Europe, London/New York 2016, p. 3–25.

3 ECtHR, no. 33014/05, 5 May 2011, *Editorial Board of Pravoye Delo and Shtekel v. Ukraine,* § 63.

4 For studies on the ECtHR's case law on freedom of expression in the internet, see e.g. Jon Barata Mir & Marco Bassini, «Freedom of Expression in the Internet: Main Trends of Case Law of the European Court of Human Rights», in: O. Pollicino & G. Romeo supra note 2, p. 71–93; Nina Vajić & Voyatzis Panayotis, «The Internet and Freedom of Expression: A ‹Brave New World› and the ECtHR's Evolving Case-law, in: J. Casadevall *et al.* (eds.), Freedom of Expression: Essays in Honour of Nicolas Bratza, Oisterwijk 2012, p. 391–407.

5 See Human Rights Committee, *General Comment 34,* 12 September 2011, 1.CCPR/C/GC/34, § 12.

Importantly for the internet, this right is protected «regardless of frontiers»[6] and extends not only to speakers and recipients but also to intermediaries. Whilst intermediaries are important enablers of traditional communication, they are indispensable to internet-based speech. The transmission of online expression depends on a whole series of actors which participate in different ways in the dissemination of information and ideas. This complex chain involves,[7] for instance, internet service providers (ISPs), data processing and web hosting providers, search engines and social media platforms.[8] State measures targeting intermediaries are thus likely to have an impact on internet users, impairing their right to receive, impart and access information.

Several judgments of the ECtHR underscore this point. *Yildirim v. Turkey* concerned collateral internet blocking.[9] The applicant owned a Google-hosted website on which he published his academic work and opinions on various topics. As a result of a criminal court order to block access to all Google sites in Turkey, his website was shut down although it was unrelated to the criminal proceedings. The blocking order had been issued to prevent access to one particular Google-hosted website which included content deemed offensive to the memory of Atatürk.

The ECtHR first recalled its case law stressing the importance of the internet as a means of communication:

> In the light of its accessibility and its capacity to store and communicate vast amounts of information, the Internet plays an important role in enhancing the public's access to news and facilitating the dissemination of information in general. [10]

The Court then acknowledged the role of intermediaries as facilitators of internet-based communication: it found that Google sites was a «service designed to facilitate the creation and sharing of websites within a group and thus constitutes a means of exercising freedom of expression».[11] Noting that Art. 10 ECHR applied also to the means of dissemination and protected not only the right to impart information and ideas but also the right of the public to receive them,[12] the Court found that the collateral effect of the wholesale blocking order amounted to an unjustified interference with the applicant's right to freedom of expression. The blocking order was not based on a strict legal framework regulating the scope of a ban and providing for judicial

6 See also Art. 10 § 1 ECHR.

7 Bertil Cottier, «Le droit ‹suisse› du cyberspace ou le retour en force de l'insécurité juridique et de l'illégitimité», 134 ZSR (2015) II, p. 191–257, 209, mentioning the complexity of the dissemination chain as one caracteristic feature of communication in the internet.

8 On the impact of intermediaries on internet-based communication, see Rebecca Mc Kinnon *et al.*, Fostering Freedom Online: The Role of Internet Intermediaries, Paris 2014.

9 ECtHR, no. 3111/10, 18 December 2012, *Ahment Yildirim v. Turkey*.

10 *Yildirim,* supra note 9, § 48, quoting ECtHR, no. 3002/03 and 23676/03, 10 March 2009, *Times Newspapers Ltd v. the United Kingdom (nos. 1 and 2*), § 27.

11 *Ibid.,* § 49.

12 *Ibid.,* § 50.

protection to prevent possible abuses.[13] Moreover, the ECtHR underscored the extensive collateral damage of wholesale blocking. The respect for freedom of expression would have required the authorities to weigh the different interests at stake, taking into account the collateral effects of the blocking order and examining less far reaching measures, which they failed to do.[14] Although the Court's reasoning was related to the principle of legality, considering that the Turkish legislation did not satisfy the foreseeability requirement under the Convention,[15] it shows that wholesale blocking raises serious concerns in the light of the proportionality principle.[16]

In the *Yildirim* case, the Turkish government had not disputed that the applicant had standing to file an application related to the blocking order, as he was prevented to access his own website. By contrast, victim status was controversial in two applications filed by internet users who claimed that they were indirectly affected by injunctions blocking access to websites:[17] in *Akdeniz v. Turkey*,[18] the blocking measure targeted music websites on the grounds that they disseminated musical works in breach of copyright law. *Cengiz and Others v. Turkey*[19] concerned access to YouTube, blocked on the grounds that it contained videos deemed insulting to the memory of Atatürk. Interestingly, the ECtHR reached a different outcome in both cases: in *Akdeniz,* it denied the applicant victim status, arguing that he was, like other internet users, indirectly affected by the blocking order, which was not sufficient to be considered a victim in terms of Art. 34 ECHR.[20] As a user of the blocked websites, the applicant was only deprived of one means to listening to music among many others and could access a wide range of musical works by means entailing no breach of intellectual property rights.[21] Moreover, the applicant had not claimed that the websites in question disseminated information of specific interest to him or that he had been deprived of a major source of communication. The applicant's possibility to participate in debates on matters of general interest had therefore not been adversely affected.[22]

13 *Ibid.*, § 68.
14 *Ibid.*, § 66.
15 *Ibid.*, § 67. On the requirement that limitations of freedom of expression be based on law, see infra, section 1. C.
16 The importance of the proportionality principle, and the further criteria governing internet blocking orders are stressed in the concurring opinion of Judge Pinto De Albuquerque (with references to relevant soft-law instruments).
17 See Art. 34 ECHR: «The Court may receive applications from any person, nongovernmental organisation or group of individuals *claiming to be the victim* of a violation [...] of the rights set forth in the Convention [...]» (emphasis added).
18 ECtHR (dec.), no. 20877/10, 11 March 2014, *Akdeniz v. Turkey*.
19 ECtHR, no. 48226/10 and 14027/11, 1 December 2015, *Cengiz and Others v. Turkey*.
20 *Akdeniz*, supra note 18, § 24.
21 *Ibid.*, § 25.
22 *Ibid.*, § 26.

By contrast, the ECtHR declared the application admissible in *Cengiz,* holding that the victim status requirement had to be applied in a flexible manner.[23] The Court distinguished the *Cengiz* case from *Akdeniz* mainly on two grounds. Firstly, it held that the applicants, Turkish academics, were active users of YouTube, who accessed videos and uploaded material related to their academic work. Considering that the blocking order had prevented access to YouTube for a long period of time and negatively impacted the applicants' work, it amounted to an interference with their right to seek and impart information.[24] Secondly, the Court analysed the characteristics of the targeted website. It described YouTube as a platform which was not only disseminating musical and artistic work but was also a very popular forum for political debates and political and social activities.[25] YouTube offered an outlet for political information ignored by traditional media, enabling citizen journalism to emerge.[26] Due to these characteristics, its potential impact and its level of accessibility, YouTube was a unique website for which there was no equivalent alternative.[27]

The ECtHR's case law on internet blocking shows the Court's willingness to extend the scope of freedom of expression to internet users and its awareness of the importance of internet-based communication. At the same time, the ECtHR has been cautious not to open the floodgate to applications filed by internet users, assessing victim status on a case-by-case basis. As will be shown, the different outcomes reached in *Yildirim* and *Cengiz,* on the one hand, and *Akdeniz,* on the other hand, reflect the Court's understanding of the values underlying freedom of expression and the related functions of the free speech guarantee.

B. Free Speech Values and Functions

The ECtHR's free speech philosophy is expressed in the famous Handyside dictum:[28]

> 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. [...] it is applicable not only to «information» or «ideas» that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb the State or any sector of the population. Such are the demands of that pluralism, tolerance and broadmindedness without which there is no «democratic society».[29]

The Court's dictum highlights that freedom of expression is not only protected for the sake of the individual but also for the sake of the community as a whole. It is

23 *Cengiz*, supra note 19, § 55.
24 *Ibid.,* § 57.
25 *Ibid.,* § 51.
26 *Ibid.,* § 52.
27 *Ibid.,* § 53.
28 On Handyside expressing the Court's free speech philosophy, see ECtHR, no. 15948/03, 10 July 2008, *Soulas and others v. France*, § 34.
29 ECtHR, no. 5493/72, 7 December 1976, *Handyside v. the United Kingdom*, § 49.

vindicated both as an end and a means:[30] free speech is vindicated both for its intrinsic worth, derived from its function to protect individual autonomy and self-fulfilment, and for its instrumental value in advancing democracy and social progress.

The insight that free speech is an essential condition of a «democratic society» and its «progress» is also reflected in the case law of other international human rights bodies and in the jurisprudence of many constitutional courts.[31] Accordingly, the free flow of information on political matters, broadly defined as matters of public concern,[32] lies at the heart of freedom of expression. The democracy enabling function of free speech calls for strong protection of the media and other institutions of civil society (such as associations and NGOs) which in their role of «public»[33] or «social watchdogs»[34] check and criticise those in power, inform the citizenry, and shape public opinion on matters relevant to collective decision-making.

Based on the insight that democracy is not untrammelled majority rule and requires pluralism, tolerance and broadmindedness, freedom of communication calls for vigorous protection of minority views.[35] Protecting non-conforming and dissenting opinions is also a prerequisite of enhancing knowledge and progress.[36] The «truth-seeking function»[37] of freedom of expression is particularly relevant for research and provides, together with the argument from democracy, an important justification of academic freedom.[38]

The instrumental rationales underlying the protection of freedom of expression, highlighting the values of democracy and truth, inform the Court's approach adopted in the above-mentioned cases on internet blocking. Both *Yildirim* and *Cengiz* concerned academics and their ability to make a contribution to progress through their

30 This expression is inspired by the concurring opinion of Justice Brandeis in *Whitney v. California*, 274 U.S. 357 (1927).
For academic studies on the rationales for protecting freedom of expression, see mainly Frederick Schauer, Free Speech: A Philosophical Inquiry, Cambridge 1982; Eric Barendt, Freedom of Speech, 2nd ed., Oxford 2005.

31 See Maya Hertig Randall, «Human Rights Within a Multilayered Constitution: The Example of Freedom of Expression and the WTO», 16 UNYB (2012), p. 184–280, 226 f.; 231 ff.

32 See Maya Hertig Randall, *Ad Art. 16*, in: B. Waldmann, E. M. Belser & A. Epiney (eds.), Bundesverfassung. Basler Kommentar, Basle 2015, no. 42.

33 On the press as a «public watchdog», see e.g. ECtHR, no. 17488/90, 27 March 1996, *Goodwin v. United Kingdom*, § 36.

34 For actors of civil society as «social watchdogs», see e.g. ECtHR, no. 39534/07, 28 November 2013, *Österreichische Vereinigung zur Erhaltung, Stärkung und Schaffung eines wirtschaftlich gesunden land- und forstwirtschaftlichen Grundbesitzes v. Austria*, § 34.

35 See e.g. ECtHR, no. 7601/76, 13 August 1981, *Young, James und Webster v. United Kingdom,* § 63.

36 See the classic defense of freedom of expression by John Stuart Mill, On Liberty, London 1859, Chapter 2: Of the liberty of thought and discussion.

37 United States Supreme Court, *Hustler Magazine v. Falwell,* 485 US 46 (1988), p. 52.

38 Whilst contemporary constitutions tend to protect academic freedom as a separate liberty, under the ECHR it is protected under the general free speech guarantee of Art. 10 (see e.g. ECtHR, nos. 346/04 and 39779/04, 27 May 2014, *Erdoğan v. Turkey*, § 40).

work and to participate in debates on matters on general concern. The latter case moreover involved an internet platform which has become an important forum for political expression. Both cases thus concerned communication which lies at the core of free speech. By contrast, neither democracy nor the quest for truth was at the heart of the *Akdeniz* case. Nor did this case entail the same risk of using internet blocking as a means of silencing dissent. Besides the question of standing, the extent to which communication is related to free speech values is also an important factor to determine the limits of freedom of expression, both in general and on the internet.

C. Limitations of Freedom of Expression

Like most fundamental rights, freedom of expression is not absolute. Its exercise can be limited for the sake of protecting conflicting public interests and the rights of others. Accordingly, human rights instruments provide that state measures abridging freedom of expression are justified if they are (1) prescribed by law, (2) pursue a legitimate aim, and (3) are «necessary in a democratic society»[39], i.e. comply with the principle of proportionality.[40] As the grounds for limitation are broad,[41] they do in practice not significantly limit the states' ability to adopt measures interfering with freedom of expression.

The first requirement, expressing the principle of legality, plays a considerable role in the context of new technologies, including the internet. As law tends to lag behind the fast changing technological and social conditions, it is not uncommon that measures limiting freedom of expression are based on a legislative framework which has not been tailored to the internet and does not offer the necessary level of foreseeability.[42]

Of even bigger practical relevance is the proportionality requirement, which turns out to be decisive in the majority of cases. When assessing whether an interference with freedom of expression is proportionate, human rights bodies and many constitutional courts tend to adopt a methodology which the Canadian Supreme Court termed aptly a «contextual approach».[43] It implies weighing and balancing the competing interests at stake with a view to determining whether a fair and just balance has been struck between the exercise of freedom of expression and the oppos-

39 See Art. 10 § 2 ECHR; see also Art. 19 § 3 ICCPR and Art. 52 § 1 Charter of Fundamental Rights of the European Union; compare with Art. 36 of the Swiss Federal Constitution of 1999.

40 On the proportionality principle under the ECHR, see mainly Sébastien Van Drooghenbroeck, La proportionnalité dans le droit de la Convention européenne des droits de l'Homme: Prendre l'idée simple au sérieux, Brussels 2001.

41 See the list of interests which can justify an interference with freedom of expression under Art. 10 § 2 ECHR and Art. 19 § 3 ICCPR.

42 See e.g. *Yildirim*, supra note 9.

43 See e.g. Supreme Court of Canada, *R. v. Keegstra*, [1990] 3 SCR 697, p. 737.

ing values. Two elements inform this analysis: firstly, the weighing and balancing process needs to be fact sensitive and take into account all the relevant circumstances of the particular case.[44] For instance, the potential of harm of expression does not only depend on the chosen wording, but also on the political and social context in which the statements are made.[45] Whilst the gravity of the harm weighs in favour of limiting freedom of expression, the severity of the interference is a countervailing factor. Considering the long legacy of pervasive censorship, prior restraint is subject to strict scrutiny.[46] The same holds true for drastic sanctions, such as criminal charges or high penalties.[47]

Secondly, the proportionality analysis must consider the values underlying freedom of expression and a «democratic society».[48] When weighing and balancing the various interests at stake, the values of democracy and truth underlying freedom of expression tilt the scales in favour of free speech. Accordingly, the ECtHR and other human rights bodies accord political speech, broadly defined, a high level of protection: restrictions targeting the media, NGOs, political parties and politicians are subject to strict scrutiny;[49] in the same vein, politicians' reputation and privacy is protected to a lesser degree than that that of private figures.[50] Conversely, when expression is at the periphery of free speech concerns, courts tend to adopt a deferential approach. In the above mentioned *Akdeniz* case, for instance, the ECtHR recalled its long standing case law on the principles governing the standard of review in free speech cases: whilst there is little scope under Art. 10 § 2 of the Convention for restrictions of political speech or debates on questions of public interest, States are afforded a wide margin of appreciation when purely commercial interests are at stake.[51] This is generally the case for commercial advertising or expression infringing intellectual property rights which pursues commercial aims and is not aimed at making a contribution to an ongoing debate of general interest, as was the case in *Akdeniz*.

Following the example of the U.S. Supreme Court, the ECtHR affords speech on matters of public interest some breathing space: as «erroneous statement is inevitable

44 *Ibid.,* p. 737.

45 See for instance the ECtHR's case law with respect to incitement to violence (see e.g. ECtHR, no. 18954/91, *Zana v. Turkey,* 25 November 2009, § 57 ff.) and to hate speech (see ECtHR (GC), no. 27510/08, 15 October 2015, *Perinçek v. Switzerland*, § 204 ff.; § 242 ff.).

46 See Jean-François Flauss, «The European Court of Human Rights and the Freedom of Expression», 84 Indiana L. J. (2009), p. 809–849, 821.

47 *Ibid.,* p. 822.

48 See *Keegstra,* supra note 43, p. 736 f.; 759 ff.

49 See Hertig Randall, supra note 31, p. 231 f.

50 *Ibid.*

51 *Akdeniz,* supra note 18, § 28. For other judgments concerning internet-based expression in which the Court afforded a wide margin of appreciation, see ECtHR (GC), no. 16354/06, 13 July 2012, *Mouvement raëlien suisse v. Switzerland,* § 61; no. 36769/08, 10 January 2013, *Ashby Donald and others v. France*, § 41 f.

in free debate»,[52] it may sometimes be necessary to protect false statements to prevent true statements from being chilled. The U.S. Supreme Court eloquently illustrated the so-called «chilling effect» in a case involving an ordinance that imposed criminal liability on booksellers for offering obscene writings for sale independently on the actual knowledge of the content of the material. Such a harsh rule would induce self-censorship, impeding «the distribution of all books, both obscene and not obscene [...]».[53] Similary, harsh sanctions have an effect beyond the particular case, as they deter people from exercising their right of freedom of expression. Due to the legal uncertainty and lack of foreseeability, vaguely formulated laws also have a dissuasive effect.

The principles outlined so far equally apply to freedom of expression on the internet.[54] When carrying out the proportionality analysis, courts are however faced with the difficulty that the special features of internet-based communication weigh on both sides of the scales in the balancing process. On the one hand, tribunals need to consider, that «[i]nternet has now become one of the principal means by which individuals exercise their right to freedom of expression and information [...].»[55] On the other hand, they cannot be oblivious to the fact that communication via the internet frequently entails a greater risk of harm than traditional means of communication,[56] as information can be disseminated at low cost to a large public and is difficult to remove, in line with the saying «the internet never forgets».[57]

III. Challenges raised by the Internet

A. Mass communication

Under the traditional free speech paradigm, outlined above, the compatibility of measures limiting freedom of expression with human rights norms is assessed on an individual basis, involving a context sensitive analysis and guarantees of judicial protection. This approach has become marginalised with respect to freedom of expression in the internet, as it is not well adapted to mass communication. Faced with the challenge to come to terms with mass communication, companies or states resort to automated methods, such as filtering, to regulate harmful expression. Automated

52 U.S. Supreme Court, *NAACP v. Button,* 371 U.S. 415 (1963), p. 433.

53 U.S. Supreme Court, *Smith v. Calinfornia,* 361 U.S. 147 (1959).

54 See Principle 1 of the Declaration on freedom of communication on the Internet adopted by the Committee of Ministers of the Council of Europe on 28 May 2003: «Member States should not subject content on the Internet to restrictions which go further than those applied to other means of content delivery».

55 See *Yildirim,* supra note 9, § 54.

56 See ECtHR, no. 33014/05, 5 May 2011, *Editorial Board Pravoye Delo and Shektel v. Ukraine*, § 63.

57 See Cottier, supra note 7, p. 208.

technologies raise the difficulty that they achieve either too much or too little. The inability to take all the circumstances of each case into account makes them prone to being either over- or underinclusive.[58] In the first instance, they turn out to be ineffective to weed out harmful expression, in the second case, they interfere with the legitimate exercise of freedom of expression. As filtering systems block speech automatically and often without procedural protection for the speaker or an individualized analysis of the speech at issue, they raise difficulties in the light of the free speech framework.

B. Mass Surveillance

The internet does not only enable mass communication but offers also fertile ground for mass surveillance. In the digital age, governments resort to schemes aimed at monitoring substantial parts of the population across national borders with a view to fighting terrorism or other forms of criminality. Like the closely connected issue of internet anonymity, mass surveillance is generally thought of as a privacy issue. It raises, however, also free speech concerns,[59] as recognised in the well-known case *Digital Rights Ireland*.[60] The ECJ considered that the controversial Data Retention Directive 2006/24 pursued a legitimate aim, but concluded that the retention of all traffic data concerning fixed and mobile telephone communication, as well as internet access, e-mail and internet telephony amounted to a disproportionate «interference with the fundamental rights of practically the entire European population».[61] Although the ECJ examined the Directive mainly in the light of privacy rights protected in Art. 7 and 8 of the EU-Charter of Fundamental Rights, it considered that «it [was] not inconceivable that the retention of the data in question might have an effect on the use, by subscribers or registered users, of the means of communication covered by that directive and, consequently, on their exercise of the freedom of expression guaranteed by Article 11 of the Charter.»[62] Indeed, mass surveillance schemes amount due to their chilling effect to an indirect interference with freedom of expression. They are likely to dissuade at least certain users from making full use of their right to freedom of expression.

58 See Quentin Van Enis, «Les mesures de filtrage et de blocage de contenus sur l'internet: un mal (vraiment) nécessaire dans une société démocratique? Quelques réflexions autour de la liberté d'expression», 24 RTDH (2013), p. 859–886, p. 862.

59 On anonymity, privacy and freedom of expression, see Toby Mendel *et al.*, Global Survey on Internet Privacy and Freedom of Expression, Paris 2012.

60 Cases C-293/12 and 594/12, *Digital Rights Ireland Ltd./Ireland*, [2014] ECR I-238 (EU:C:2014:238)

61 *Ibid.*, § 56.

62 *Ibid.*, § 28.

C. Public-private Cooperation and Cooptation

The example of the Data Retention Directive highlights another characteristic feature of free speech regulation on the internet: its reliance on public-private cooperation and co-optation. Under the Directive, states have to adopt legislation imposing on providers of publicly available electronic communication services or of public communication networks the duty to retain certain data to insure its availability for the purpose of criminal investigation. Data retention thus involves the cooperation between public authorities and corporate actors. Much speech regulation on the internet follows this pattern, the main reason being that the necessary infrastructure for internet communication is privately owned.[63] Moreover, governments are frequently unable to target users directly, as they may be anonymous, pseudonymous, or outside the state's jurisdiction.[64] For these reasons, they need to secure assistance from private actors for the purposes of surveillance and speech control. Public-private cooperation is often induced by a «carrot or stick approach»,[65] including, for instance rules on liability and immunity of intermediaries.[66] As will be shown below, this approach entails considerable risks for freedom of expression on the internet. Many forms of public-private cooperation are also problematic, as they generated restrictions of freedom of expression (such as voluntary blocking mechanisms) which are not based on a clear and foreseeable legal framework.

D. Low Visibility and Lack of Transparency

Public-private cooperation and co-optation exacerbate another feature of regulation of internet-based communication, its low visibility and lack of transparency. Under the classic free speech paradigm, measures limiting freedom of expression, including prior restraint, are generally dealt with on a case-by-case basis, within a due process framework. This involves judicial oversight, resulting in reasoned judgments open to public scrutiny. By contrast, automated control mechanisms like filtering are frequently based on unknown criteria and entail low visibility.[67] The lack of transparency is detrimental to both public awareness and public oversight. As Balkin argues, government and private actors may prefer speech regulation to remain largely invisible. Unlike under the traditional paradigm, they do not rely on deterrence. Instead of chilling speakers, «they may want most people just to chill out.»[68] The more perva-

63 Jack M. Balkin, «Old-School/New-School Speech Regulation», 127 Harvard L. R. (2014), p. 2296–2342, 2305.
64 *Ibid.,* p. 2308.
65 *Ibid.,* p. 2299.
66 See infra, section F.
67 See Balkin, supra note 63, p. 2341.
68 *Ibid*., p. 2342.

sive online surveillance, filtering and blocking become, the more likely they are to be perceived as «normal, unobtrusive and inoffensive.»[69]

Not all internet users have been willing to «chill out»: speech regulation on the internet has gone hand in hand with private initiatives[70] and with calls for more transparency directed both at governments and private actors.[71] In response to these demands, Google was the first company to start publishing bi-annual transparency reports in 2010. These include information on the number of government demands for content restriction and transmission of data.[72] Google was, however, confronted with new demands for transparency in the aftermath of the ECJ's well-known *Google Spain* judgment on the «right to be forgotten».[73] Once Google started handling requests for delisting, demands for information were voiced. A letter signed by eighty academics, for instance, stressed that the public had an eminent interest in receiving information about the numbers, the type of cases handled, the process and the criteria used to assess delisting claims.[74] Given the magnitude of delisting, which has concerned almost 400 000 requests for removal so far,[75] relevant information touches on a matter of public interest, enabling discussions on whether the right balance is struck between privacy and freedom of expression and, ultimately, on the advantages and drawbacks of «the right to be forgotten» itself. Without public information and scrutiny, Google has great leeway to shape these debates on a matter in which it has the role of «judge, jury and executioner».[76]

69 In this sense Balkin, supra note 63, p. 2342.

70 See for instance the Lumen project of the Berkman Center for Internet & Society aimed at collecting and analyzing requests to remove content from online (<https://lumendatabase.org/pages/about>).

71 For Soft law instruments, see e.g. Recommendation CM/Rec(2007)11 of the Committee of Ministers to member states on promoting freedom of expression and information in the new information and communications environment, 26 September 2007 (calling for transparency of filtering mechanisms (see point II.ii.); Recommendation CM/Rec(2012)3 of the Committee of Ministers to member States on the protection of human rights with regard to search engines, 4 April 2012, § 6 ff.

72 See MacKinnon, supra note 8, p. 123.

73 Case C-131/12, *Google SL and Google Inc./Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, [2014] ECR 317 (EU:C:2014:317).

74 See Jemima Kiss, «Google must be more open on ‹right to be forgotten›, academics warn in letter», The Guardian, 14 May 2015, available at <http://www.theguardian.com/technology/2015/may/14/google-right-to-be-forgotten-academics-letter>.

75 See the data available in google's transparency report, <https://www.google.com/transparencyreport/removals/europeprivacy/?hl=en>.

76 See Julia Powles, «Google's data leak reveals flaws in making it judge and jury over our rights», The Guardian, 14 July 2015, available at <http://www.theguardian.com/technology/2015/jul/14/google-data-leak-right-to-be-forgotten>.

E. Anonymity

Being able to communicate without giving away one's identity has always been considered crucial in the light of free speech values and functions. The U.S. Supreme Court stressed the importance of anonymous expression in a judgment handed down in 1995, holding that «[u]nder our Constitution, anonymous pamphleteering is not a pernicious, fraudulent practice, but an honorable tradition of advocacy and of dissent. Anonymity is a shield from the tyranny of the majority.»[77]

The internet opens unprecedented possibilities to communicate anonymously or using pseudonyms, which makes internet-based communication particularly appealing. It thus comes as no surprise that international soft law instruments request States to respect the right to communicate anonymously and stress the link between anonymity and the protection against online surveillance.[78]

The right to communicate anonymously or pseudonymously is, however, a double edged sword.[79] Whilst it is an essential component of a democratic society, enabling vigorous expression of dissent and criticism, it can be used as a cover for criminal offenses, including, for instance, hate speech, threats, incitement to violence and child pornography. As anonymity provides for separation between a person's identity and his or her action, it reduces inhibition and is conducive to antisocial behaviour.[80] The «distancing that occurs on the Internet»[81] reinforces the risks entailed by anonymous speech. It favours dehumanization and «ultimately provides a faceless victim»,[82] resulting in a loss of empathy.[83] Moreover, it has been argued that «[o]ur emerging online media landscape has created a new public forum without the traditional social norms and self-regulation that typically govern our in-person exchanges».[84] Combating online abuse requires awareness raising, aimed at sensitising users to the fact that speech in cyberspace is no less likely to cause harm than face to face communication and needs to respect established social norms governing communication in the real world.[85] It also entails that the right to communicate anonymously

77 United States Supreme Court, *McIntyre v. Ohio Elections Commission*, 514 U.S. 334 (1995), p. 334–385.

78 See for instance Principle 7 of the Declaration on freedom of communication on the internet, supra note 54. For an analysis under Swiss law, see Rolf H. Weber & Urike I. Heinrich, «Existiert ein Recht auf Anonymität im Internet?», 132 ZSR (2013), I, p. 477–495.

79 See Rob Kling *et al.*, «Assessing Anonymous Communication on the Internet: Policy Deliberations», 15 The Information Society (1999), p. 79–90.

80 See Stacy M. Chaffin, «Comment. The New Playground Bullies of Cyberspace: Online Peer Sexual Harrassment», 51 Howard L. J. (2008), p. 773–818, 788 ff.

81 *Ibid.,* p. 793.

82 *Ibid.,* p. 793.

83 *Ibid.,* p. 793.

84 See Alastair Reid, «Why negative comments are like broken windows. A look at how and why the quality of content below the line can affect readers», 7 August 2013, available at <https://www.journalism.co.uk/news/managing-negative-abusive-comments-news/s2/a553747/>.

85 Reid, supra note 84.

or pseudonymously cannot be construed in absolute terms.[86] The ECtHR highlighted the limits of anonymous speech in *K.U. v. Finland,* holding that the right to communicate anonymously «cannot be absolute and must yield on occasion to other legitimate imperatives [...]».[87]

The European Convention does not only afford States leeway to limit freedom of expression with a view to protecting victims of online criminality but requires them to do so. Accordingly, the Court found that a legislative framework which did not provide for exceptions to confidentiality of telecommunications and precluded a service provider to divulge the identity of the IP address in the course of an investigation related to attempted sexual abuse of minors was not in line with the State's positive obligations under Art. 8 ECHR.[88]

F. Collateral Censorship and Liability of Intermediaries

Collateral censorship is another challenge linked to regulation of communication in the internet. It «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, as is the case of intermediaries with respect to end users.»[89] Collateral censorship creates strong chilling effects on the intermediaries. Faced with a risk of being held liable for B's speech, an intermediary A is likely to err on the side of safety and to censor content even if the conditions for limiting freedom of expression are not met.[90] This is all the more the case as A generally has no personal interest in the targeted expression, as he or she takes action against someone else's speech.

Considering the detrimental effect of collateral censorship on freedom of expression in the internet, soft and hard law instruments reflect the strong consensus that intermediaries should benefit from limited liability, which entails that they should not be required to systematically monitor the internet and be asked to remove content without having actual knowledge of its illegality.[91]

Both the ECJ and the ECtHR have handed down judgments offering interesting insights with respect to the duties and liability of intermediaries. In two judgments,

86 On the limits of anonymous communication, see for instance Principle 7 of the Declaration on freedom of communication on the Internet, supra, note 54.

87 ECtHR, no. 2872/02, 2 December 2008, *K.U. v. Finland,* § 49.

88 *K.U. v. Finland*, supra, note 87, § 48 ff.

89 See Balkin, supra, note 63, p. 2309.

90 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, 16 May 2011, A/HRC/17/27, § 42.

91 For an overview of the relevant European and international soft and hard law rules and principles on the liability of intermediaries, see ECtHR (GC), no. 64569/09, 16 June 2015, *Delfi AS v. Estonia*, § 44 ff.

Scarlet[92] and *Netlog*[93], the Luxemburg Court found that EU-law, including fundamental rights, precluded a national court from issuing an injunction against a hosting service provider, which required the installation of a filtering system to prevent copyright infringement. The Court reached this conclusion after considering the characteristics of the required technology: the latter applied indiscriminately to all end users for an unlimited period of time and, most importantly, would have required active monitoring of all data to prevent future infringement of intellectual property rights. The ECJ found that such a far-reaching obligation infringed the intermediaries' economic liberties. Moreover, it would potentially undermine freedom of information, as the system might not adequately distinguish between unlawful and lawful content. The filtering mechanism thus entailed the risk of blocking lawful communication.

The ECtHR has also had the opportunity to deal with the liability of an intermediary for copyright infringement. In a decision handed down in 2013, it upheld the criminal conviction of the largest file sharing services on the Internet, The Pirate Bay, for assisting copyright infringement.[94] The Swedish authorities had argued that the website made available well-developed search functions and offered simple uploading and storing possibilities, which facilitated infringement of intellectual property rights. The Court framed the issue as involving two conflicting fundamental rights – the right to freedom of expression and the right to property. In line with its case law adopting a deferential approach in cases concerning commercial expression as opposed to speech on matters of public concern,[95] the ECtHR afforded the domestic authorities a wide margin of appreciation and found no violation of Art. 10 ECHR.

The ECtHR squarely confronted the question of intermediary liability in its Grand Chamber judgment *Delfi v. Estonia*.[96] The case arose from the following facts: Delfi, Estonia's biggest online news portal, published an article on ice-roads which generated many user comments, some of which contained gross insults, hateful statements and threats against a ferry owner. The domestic courts had held Delfi liable for the user generated comments, despite the fact that the company had removed them once it had been informed about their hateful content. The ECtHR largely endorsed the Estonian court's reasoning, finding against Delfi for several reasons. Firstly, the Grand Chamber accepted that Delfi was an active intermediary, which had some

92 Case C-70/10, *Scarlet Extended SA/Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, [2011] ECR I-11959 (EU:C:2011:771).

93 Case C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM)/ Netlog NV*, [2012], EU:C:2012:85.

94 ECtHR, no. 40397/12, 19 February 2013, *Fredrik Neij and Peter Sunde Kolmisoppi v. Sweden*. For a comment including a comparison to the ECJ's case law, see Alain Strowel, «Pondération entre liberté d'expression et droit d'auteur sur internet: de la reserve des juges de Strasbourg à une concordance pratique par les juges de Luxembourg», 25 RTDH (2014), p. 889–911.

95 See supra, II.C.

96 *Delfi*, supra note 91.

control over the user generated comments, and not only a passive, purely technical service provider. Its active role justified the conclusion that it could not rely on limited liability afforded to internet service providers under the E-Commerce Directive (Directive 2000/31/EC). Instead, Delfi was treated similar to traditional media, who do not benefit from immunity if they publish letters written by readers. Secondly, considering that internet-based expression entailed a greater risk of harm than statements published in the press, the Court underlined the extreme nature of the comments. Although the ECtHR acknowledged that the applicant company had taken certain measures for the prevention and removal of illegal comments, it considered it important that the automatic word-based filter used by Delfi failed to catch the impugned statements despite their blatant wording.[97] As a consequence, the comments stayed online for six weeks. Although a notice and take-down system, as employed by Delfi, was in many instances an adequate mechanism against offensive comments, the Court considered it compatible with freedom of expression to hold Internet news portals liable if they fail to react without delay, even without notice from the victims, by removing user comments which take the form of hate speech and direct threats to physical integrity. In support of this conclusion, the Court also noted that the ability of a large commercially run Internet news portal to continuously monitor the Internet exceeded that of potential victims of hate speech.[98] Thirdly, in weighing and balancing the rights at stake, the Court took into account that the damages awarded (EUR 320), were modest for a company like Delfi.[99]

The Delfi ruling entails that a legal framework which requires active intermediaries to continuously monitor the internet to escape civil liability is not incompatible with freedom of expression.[100] The Grand Chamber was however careful to limit the scope of its judgment in two ways: firstly, it made it clear that the judgment concerned one category of illegal statements, i.e. hate speech and direct threats to physical integrity.[101] Secondly, the Court emphasised that «[t]he present case relates to a large professionally managed Internet news portal run on a commercial basis which published news articles of its own and invited its readers to comment on them.»[102] It thus did «not concern other fora on the Internet where third-party comments can be disseminated, for example an Internet discussion forum or a bulletin board where users can freely set out their ideas on any topics without the discussion being channelled by any input from the forum's manager; or a social media platform where the platform pro-

97 *Ibid.,* § 156.
98 *Ibid.,* § 158.
99 *Ibid.,* § 160.
100 For a critical appraisal, see the Joint Dissenting Opinion of Judges Sajó and Tsotsoria in *Delfi,* supra note 96.
101 For the specificities of Hate speech online, see Iglinio Gagliardone *et al.*, Countering Online Hate Speech, Paris 2015, p. 13 ff.
102 *Delfi,* supra note 91, § 116.

vider does not offer any content and where the content provider may be a private person running the website or a blog as a hobby.»[103]

The underlying question in Delfi, whether an internet news portal run on a commercial basis was to benefit from limited liability, like passive intermediaries, or was rather to be treated like traditional media, shows that it is not always easy to apply the existing regulatory framework to the great variety of internet-based activities.

G. Fragmentation

As a global communications medium, the internet transcends national borders and creates online communities irrespective of geographic boundaries. However, internet communication does not escape domestic rules and jurisdiction, which coexist with self-regulatory schemes and private regulation. The coexistence of these regulatory schemes form a puzzle the pieces of which do not fit together neatly.[104] Regulatory fragmentation is a cause for concern both for free speech defenders and national regulators. For the latter, the global reach of the internet and the territorial limits of domestic legal orders is viewed as an obstacle to come to terms with pressing issues such as child pornography, defamation, extremist speech, intellectual copyright infringement and hate speech. In these areas, the legal framework varies considerably from one jurisdiction to the other.[105]

The lack of a unified conception of freedom of expression is a contributing factor to fragmentation. A paradigmatic example is the different approach to free speech adopted for instance in Europe and Canada, on the one hand, and in the United States, on the other hand. Whilst there is substantial overlap with respect to free speech values and functions, important differences exist regarding the level of protection afforded to freedom of expression and the method of adjudication.[106] European and Canadian Courts generally adopt a flexible, contextual balancing approach, whilst the U.S. Supreme Court favours a rules-oriented approach based on distinctions between various categories of speech and the purpose of the governmental

103 *Ibid.*, § 116.

104 The image of a puzzle is borrowed from Jonah Force Hill, Internet Fragmentation Highlighting the Major Technical, Governance and Diplomatic Challenges for U.S. Policy Makers, Cambridge Mass. 2012, available at <http://belfercenter.ksg.harvard.edu/files/internet_fragmentation_jonah_hill.pdf>.

105 Yaman Akdeniz, Freedom of Expression on the Internet. A study of legal provisions and practices related to freedom of expression, the free flow of information and media pluralism on the Internet in OSCE participating States, Report Commissioned by Office of the OSCE Representative on Freedom of the Media, 15 December 2011, p. 51 ff., available on <http://www.osce.org/fom/80723>.

106 For a study on the United States Supreme Court's free speech methodology from a European perspective, see Ivan Hare, «Method and Objectivity in Free Speech Adjudication: Lessons from America», 54 ICLQ (2005), 49–87. For comparative study of freedom of speech, Ronald J. Krotoszynski, The First Amendment in Cross-cultural Perspective: A Comparative Legal Analysis of Freedom of Speech, New York 2006.

measure. When the speech at issue is not considered as «low value» speech and enjoys full constitutional protection, there is virtually no room for restriction based on the content of the expression.[107] Hate speech regulation, and laws criminalizing genocide and/or Holocaust denial, for instance, which are widespread in Europe, are thus constitutionally proscribed in the United States.[108]

Hate speech and Holocaust denial are prominent examples to illustrate how different conceptions of freedom of expression affect the regulatory framework of internet-based communication, making it difficult to establish a coherent regulatory framework, either through treaty law or through convergence of domestic regulation.[109] On the international level, American free speech exceptionalism has left an imprint on the Cybercrime Convention.[110] To secure American ratification of the Convention, hate speech could not be tackled in the main agreement and had to be addressed separately in an additional protocol[111], which the U.S. did not sign.[112]

A relatively recent example showing the difficulties entailed by fragmentation of hate speech regulation is the *Sheppard and Whittle* case[113]: it concerned two United Kingdom citizens who owned and operated a white supremacist, neo-Nazi website called heretical.com hosted in California but accessible from the UK. Sheppard and Whittle used their website to upload racist and revisionist material, such as a pamphlet named «Tales of a Holohoax» describing the Holocaust as a Jewish invention. Printed versions of this pamphlet, which were disseminated in the United Kingdom, enabled the UK authorities to trace Sheppard and Whittle and to prosecute them for publishing racially inflammatory material. During the criminal proceedings, the accused argued unsuccessfully that the British court lacked jurisdiction, as the material had been published in the United States. Considering that the case at hand had substantial links to the United Kingdom, the court affirmed jurisdiction and convicted Sheppard and Whittle under the UK Public Order Act in 2009. However, the judg-

107 See Hare, supra note 106.

108 For a comparative study of hate speech and other forms of controversial speech, see the contributions in I. Hare & J. Weinstein (eds.), Extreme Speech and Democracy, Oxford/New York 2009; Michel Rosenfeld, «Hate Speech in Constitutional Jurisprudence: A Comparative Analysis», 24 Cardozo L. R. (2003), p. 1523–1567.

109 For a critical appraisal of the international legal framework, see Cottier, supra, note 7, p. 233 ff.

110 Convention on Cybercrime of 23 November 2001, CETS no. 185.

111 Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems of 28 November 2003, CETS no. 189. The Protocol covers racist and xenophobic material, defined as «any written material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors.» (Art. 2 § 1).

112 See Andrew Murray, Information Technology Law: The Law and Society, 2nd ed., Oxford 2013, p. 117 ff.

113 Murray, supra note 112, p. 129 ff. For an older well-known example, see the so-called *Licra v. Yahoo litigation* (for a summary, see Murray, supra note 112, p. 117 ff.).

ment, confirmed on appeal in 2010,[114] did not have any immediate impact on the website, as it was outside the United Kingdom's jurisdiction and protected by the First Amendment of the U.S. Constitution. The offending content remained online until Sheppard agreed to remove it in 2011 as a condition to obtain release on parole.[115] As Murray puts it, the UK courts «had successfully prosecuted the perpetrators of the crime, but the crime continued to be perpetrated.»[116]

More recent debates involving Twitter show that regulatory fragmentation is not an insurmountable obstacle to deal with hate speech. As a US based company, Twitter initially refused the hand over data to French prosecutors helping them to identify users sending hate tweets on First Amendment grounds but later changed course.[117]

IV. Conclusion

Ever-advancing technology has been a common thread of the history of communication. Accustomed to grappling with technological change, courts have quite naturally extended and applied the traditional free speech framework to online communication whilst acknowledging that the specific features of the new technology may require adjustments. One characteristic of the internet is that it offers greatly enhanced communicative opportunities whilst magnifying the potential for harm. The burgeoning case law of the ECtHR shows that it is not easy to draw the line between justified and unjustified restrictions of the right to communicate online. Further challenges arise from the fact that much free speech regulation on the internet occurs outside the classic free speech framework: automated methods of speech control, a regulatory framework marked by public-private cooperation, fragmentation and low transparency, for instance, need to be addressed if the internet is to remain an unprecedented facilitator of free speech in the future.

114 *R v. Sheppard & Whittle* [2010] EWCA Crim 65. Court Court of Appeal (Criminal Division).

115 Murray, supra note 112, p. 130.

116 Murray, supra note 112, p. 130.

117 See Somini Sengupta, «Twitter Yields to Pressure in hate Case in France», New York Times, 12 July 2013, available at <http://www.nytimes.com/2013/07/13/technology/twitter-yields-to-pressure-in-hate-case-in-france.html?_r=0>.