Ceza Hukuku ve Kriminoloji Dergisi-Journal of Penal Law and Criminology 2022; 10(2): 281-305
ISSN: 2148-6646 / E-ISSN: 2602-3911

https://iupress.istanbul.edu.tr/en/journal/jplc/home

Research Article

DOI: 10.26650/JPLC2022-1213410

New Technologies through a Human Rights Lens: Reflecting on Personal Autonomy and Non-Discrimination

Yeni Teknolojilere İnsan Hakları Bakış Açısıyla Yaklaşmak: Kişisel Özerklik ve Ayrımcılık Yasağı

Saadet YÜKSEL[1]

[1]European Court of Human Rights, Strasbourg, France

ORCID: S.Y. 0000-0002-9454-4740

ABSTRACT

This article seeks to put new technologies, namely the internet and new forms of online communication, under a human rights lens, with a view to reflecting on the issues of personal autonomy and non-discrimination. In particular, the article utilises the perspective of the European Convention of Human Rights to examine firstly, the relationship between new technologies, freedom of expression, and online content moderation, and secondly, the challenges posed by the internet to the principle of non-discrimination. In reflecting upon new digital technologies and personal autonomy, the article firstly focuses on the balancing of personal autonomy and freedom of expression in online content moderation. It then explores the implications for personal autonomy of the collection of personal data and mass surveillance from a human rights perspective. Turning to the challenges posed by new technologies to the principle of non-discrimination, the article deals with the twin issues of addressing discriminatory behaviour online, and access to the internet and the digital divide.

Keywords: European Court of Human Rights, Personal autonomy, Non-discrimination, Digital technologies, Digital divide

ÖZ

Bu makale, kişisel özerklik ve ayrımcılık yapmama ilkeleri temelinde internet ve çevrimiçi iletişimin yeni biçimleri gibi günümüzün yeni teknolojilerini insan hakları hukuku merceğinden ele almaktadır. Bu çalışmada ilk olarak yeni teknolojiler, ifade özgürlüğü ve çevrimiçi içerik moderatörlüğü arasındaki ilişki; ikinci olarak da internetin ayrımcılık yapmama ilkesi bağlamında ortaya çıkardığı zorluklar Avrupa İnsan Hakları Sözleşmesi perspektifinden ele alınarak incelenmektedir. Bu çalışma yeni dijital teknolojiler ve kişisel özerklik kavramlarını ele alırken, ilk olarak çevrimiçi içerik denetiminde kişisel özerklik ve ifade özgürlüğü arasında kurulması gereken dengeye odaklanmaktadır. Daha sonra, kişisel verilerin toplanması ve kitlesel gözetlemenin kişisel özerklik üzerindeki etkileri insan hakları perspektifinden ele alınmaktadır. Son olarak yeni teknolojilerin ayrımcılık yapmama ilkesi bağlamında ortaya çıkardığı zorluklara dönen makale, çevrimiçi ortamda ayrımcı davranışları ele almanın doğurduğu benzer nitelikli sorunlar olan internete erişim ve dijital bölünme meselelerini incelemektedir.

Anahtar Kelimeler: Avrupa İnsan Hakları Mahkemesi, Kişisel özerklik, Ayrımcılık yasağı, Dijital teknolojiler, Dijital bölünme

Submitted: 02.12.2022 • **Accepted:** 26.12.2022 • **Published Online:** 06.01.2023

Corresponding author: Saadet Yüksel

Citation: Yüksel, S, 'New Technologies through a Human Rights Lens: Reflecting on Personal Autonomy and Non-Discrimination' (2022) 10(2) Ceza Hukuku ve Kriminoloji Dergisi-Journal of Penal Law and Criminology, 281. https://doi.org/10.26650/JPLC2022-1213410

I. Introduction

There can be little doubt that the internet and new forms of online communication present contemporary challenges for human rights law. Nowhere is this more apparent than in the current backlash – or 'techlash' as it has come to be termed – against internet intermediaries, such as Facebook, Twitter, and Google, for their decisions regarding the types of content which may or may not be shared, how personal data is accessed and stored, and how internet intermediaries determine the limits of free expression on their platforms.[1]

While there are many important human rights issues raised by new technologies, including freedom of expression, the right to private life, access to remedies, and the responsibility of states and non-state actors, this paper will focus on two key human rights considerations that arise in respect of new technologies. The first is the relationship between new technologies, freedom of expression, and online content moderation. The second concerns the challenges posed by the internet to the principle of non-discrimination.

II. New Digital Technologies and Personal Autonomy

This section will address two distinct issues pertaining to the relationship between the internet and personal autonomy: first, how human rights law balances the right to free expression with personal autonomy in the context of online content moderation; second, the pressing issue of the compatibility of mass surveillance and data collection with personal autonomy.

A. Balancing Personal Autonomy and Freedom of Expression in Online Content Moderation

Personal autonomy is at the heart of human rights law and has been recognised as an essential component of the right to respect for private life.[2] Although the task of appropriately balancing the right to freedom of expression with the right to respect

1 For usage of the term "techlash" in relation to falling "trust in the technology sector", see Darrell M West, 'Techlash Continues to Batter Technology Sector', *Brookings* (2 April 2021) https://www.brookings.edu/blog/techtank/2021/04/02/techlash-continues-to-batter-technology-sector/; see also, on the topic of backlash against internet intermediaries, Adam Satariano, 'Europe is Reigning in Big Tech Giants. But Some Say It's Going Too Far', *New York Times* (6 May 2019) https://www.nytimes.com/2019/05/06/technology/europe-tech-censorship.html.

2 See, generally, Jill Marshall, *Personal Freedom through Human Rights Law? Autonomy, Identity and Integrity under the European Convention on Human Rights* (Martinus Nijhoff, 2009) 56-57.

for private life is long-standing and has been the subject of academic attention,[3] the emergence of the internet has presented new challenges for protecting personal autonomy while simultaneously safeguarding free expression.

The first challenge is that the internet has expanded the reach of free expression. It has been observed that the internet "has been conceptualized as a forum for free expression with near limitless potential for individuals to express themselves and to access the expression of others".[4] Following this, the internet has been deemed a "central and indispensable means of exercising the right to freedom of expression",[5] insofar as it facilitates global interconnectedness and has lowered the costs of participating in public discussion.[6] Perhaps most significantly, the internet has been observed as transforming public discussion from a passive to active activity, in which users actively express their views rather than passively digesting information, as was often the case with traditional forms of print media.[7] While the internet's role in facilitating free expression may be a welcome development, one consequence that has been noted is the greater reach of online content as opposed to traditional printed content,[8] meaning that offensive, harmful, and defamatory comments made online are typically accessible to and seen by a large number of people. This has resulted in the significant challenge of moderating content online to ensure that free expression does not impinge too much on personal autonomy. For example, data has been noted as showing that in the last quarter of 2020 alone Facebook reviewed approximately 1.1 million posts or comments per day that had been reported by users to determine whether to remove the content.[9] Consequently, encroachments into personal autonomy may occur more easily and quickly online than they do in traditional forms of print media, raising important questions about how to strike the delicate balance between free expression and personal autonomy in the era of online communication.

3 See, for example, Eric Barendt, 'Balancing Freedom of Expression and Privacy: The Jurisprudence of the Strasbourg Court' (2009) 1 Journal of Media Law 49.

4 Dawn C. Nunziato, 'The Death of the Public Forum in Cyberspace' (2005) 20 Berkeley Technology Law Journal 1115, 1115.

5 Alan Sears, 'Protecting Freedom of Expression over the Internet: An International Approach' (2015) 5 Notre Dame Journal of International and Comparative Law 171, 172.

6 Ryan Shandler and Daphna Canetti, 'A Reality of Vulnerability and Dependence: Internet Access as a Human Right' (2019) 52 Israel Law Review 77, 79.

7 See, Anupam Chander, 'Googling Freedom' (2011) 99 California Law Review 1, 11-12; Shandler and Canetti (n 6) 79.

8 Shandler and Canetti (n 6) 79.

9 Evelyn Douek, 'Governing Online Speech' (2021) 121 Columbia Law Review 759, 791.

Second, this problem is further complicated by the fact that drawing the line between free expression and moderating harmful or offensive content out of respect for personal autonomy is left largely to self-regulation by internet intermediaries.[10] Such platforms may have considerable impact in determining who may speak and what they may say,[11] and make decisions about content moderation according to their internal guidelines.[12]

This self-regulation model has led states to adopt a variety of regulatory responses in an attempt to reign in the significant degree of power exercised by internet intermediaries when moderating content. In Germany, the 2018 German Network Enforcement Act permits internet users to report content that, in their view, is illegal under the Criminal Code and requires the internet intermediary to remove the content within 24 hours or face a fine of up to 50 million euros.[13] A similar law was adopted in France, which required internet intermediaries to remove "manifestly illicit" content within 24 hours. The French law, however, was ruled unconstitutional as it violated the right to freedom of expression under the French Constitution.[14] Approaches such as those found in the relevant law outlined above have been the subject of concern in respect of both academics and the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (UN Special Rapporteur), who posit that such approaches pose risks to freedom of expression[15] and sit at odds with the traditional approach of providing free expression with "breathing space", rather than adopting

10 See, generally, Agnès Callamard, 'The Human Rights Obligations of Non-State Actors' in Rikke Franke Jørgensen (ed), *Human Rights in the Age of Platforms* (MIT Press, 2019) 191-192; Rikke Frank Jørgensen, 'Human Rights and Private Actors in the Online Domain' in Molly K Land and Jay D Aronson (eds), *New Technologies for Human Rights Law and Practice* (Cambridge University Press, 2018) 243, 244-45.

11 See, generally, Jillian C York and Ethan Zuckerman, 'Moderating the Public Sphere' in Rikke Franke Jørgensen (ed), *Human Rights in the Age of Platforms* (MIT Press, 2019) 137; see also Susan Benesch, 'But Facebook's Not a Country: How to Interpret Human Rights Law for Social Media Companies' (2020-2021) 38 Yale Journal on Regulation Bulletin 86, 93.

12 See for example Facebook Community Standards, available at: https://transparency.fb.com/fr-fr/policies/community-standards/.

13 See discussion in 'Report of the Special Rapporteur on Freedom of Opinion and Expression: Disinformation and Freedom of Opinion and Expression', UN Doc A/HRC/47/25, 13 April 2021, para. 58.

14 See, for further discussion, 'French Law on Illegal Content Online Ruled Unconstitutional: Lessons for the EU to Learn', *Patrick Breyer* (19 November 2020) https://www.patrick-breyer.de/en/french-law-on-illegal-content-online-ruled-unconstitutional-lessons-for-the-eu-to-learn/?lang=en.

15 See 'Report of the Special Rapporteur on the Right to Freedom of Opinion and Expression: Report on Content Regulation', UN Doc A/HRC/38/35, 6 April 2018, paras. 16–17; Evelyn Douek, 'The Limits of International Law in Content Moderation' (2021) 6 UC Irvine Journal of International, Transnational, and Comparative Law 37, 70; see also Thiago Dias Oliva, 'Content Moderation Technologies: Applying Human Rights Standards to Protect Freedom of Expression' (2020) 20 Human Rights Law Review 607, 608-610.

an overcautious approach.[16] The Council of Europe Steering Committee for Media and Information Society (CDMSI) in its Guidance Note on Content Moderation also observes that overly stringent laws on content moderation encourage internet intermediaries to censor content that falls into the "grey zone" between illegal content and legal and harmless content.[17]

In light of these varying responses, how has the European Court of Human Rights approached the issue of balancing freedom of expression and personal autonomy in content moderation decisions made by internet intermediaries? A review of the Court's case law on the balancing of article 8 with article 10 reveals that although the Court has recognised that internet intermediaries may be held liable for content on their platforms in limited circumstances, the Court's approach may seem largely in line with that of the UN Special Rapporteur and the CDMSI. The Court has refrained from adopting an overzealous approach to online content moderation. In assessing whether the domestic authorities have appropriately balanced freedom of expression and personal autonomy, the Court's case law demonstrates that it will take into account the following factors: (1) first, the severity of the language, which must amount to more than merely offensive or vulgar speech; (2) second, the reach of the online content; and (3) third, whether the online forum is professionally run on a commercial basis and invites users to comment on content it publishes.

It is apt to commence discussion of this issue by reference to the well-known case of *Delfi AS v. Estonia* (no. 64569/09, 16 June 2015), in which the Grand Chamber ruled that Estonia did not violate article 10 when it imposed civil liability on an internet news site for defamatory comments left by its readers in a comments section of an article it had shared about a ferry company. The judgment is noteworthy for its finding that an internet intermediary can be held liable for harmful or defamatory comments left by third parties, in the same manner as a traditional print media publisher. The Grand Chamber emphasised that this ruling "relates to a large professionally managed Internet news portal run on a commercial basis which published news articles of its

16 See, for reference to this approach in *New York Times Co. v. Sullivan*, 376 U.S. 254 (1964), Douek (n 15) 70; see also, for the approach in *Cohen v. California*, 403 U.S. 15 (1971), Kyle Langvardt, 'Regulating Online Content Moderation' (2008) 26 Georgetown Law Journal 1353, 1361.

17 Council of Europe Steering Committee for Media and Information Society (CDMSI), 'Content Moderation: Best Practices Towards Effective Legal and Procedural Frameworks for Self-Regulatory and Co-Regulatory Mechanisms of Content Moderation', (Guidance Note, adopted 19-21 May 2021), 25, available at: https://rm.coe.int/content-moderation-en/1680a2cc18.

own and invited its readers to comment on them",[18] and expressly stated that the ruling does not extend to other types of internet sites, such as discussion forums where users express their views "without the discussion being channelled by any input from the forum's manager" or a social media site where the content is user-generated.[19] In addition, the Court took into account the extreme nature of the comments and the fact that they were posted on a professionally-managed news portal run on a commercial basis;[20] indeed, Delfi was one of the largest news portals in Estonia,[21] and the comments had referred to "lynching".[22] Accordingly, the Court's ruling does not extend the imposition of liability for user-generated comments to any internet site. Rather, it is limited to those where the internet intermediary is an active publisher with a large audience and where the comments attain a certain level of severity.

The severity of the speech as well as the reach of the online content were also determinative factors in *Egill Einarsson v. Iceland* (no. 24703/15, 7 November 2017). In this case, the Court found a violation of article 8 where a well-known Icelandic figure had been called a "rapist" in an anonymous person's Instagram post, which also featured a photo of the applicant. The applicant had brought defamation proceedings in the Icelandic courts against the anonymous Instagram user, in which he was unsuccessful because the domestic courts concluded that the anonymous user's comments were "more invective than a factual statement" and therefore within his right to freedom of expression.[23] In the Court's view, however, Article 8 entailed that persons do not have to tolerate being publicly accused of violent criminal acts where these statements are not supported by facts, and the comment had reached a level of seriousness capable of damaging the applicant's reputation and engaging his right to private life under Article 8.[24] As well as finding that the comment was of a serious nature, citing *Delfi v. Estonia* the Court reasoned that online communications present a higher risk of harm to the enjoyment of the right to private life than that posed by

18 *Delfi AS v. Estonia* (no. 64569/09, 16 June 2015), para. 115. See, for more information, Robert Spano, 'Intermediary Liability for Online User Comments under the European Convention on Human Rights' (2017) 17(4) Human Rights Law Review 665-679.

19 *Delfi AS v. Estonia* (no. 64569/09, 16 June 2015).

20 Ibid, para. 162.

21 Ibid, para. 129.

22 Ibid, para. 18.

23 *Egill Einarsson v. Iceland* (no. 24703/15, 7 November 2017), para. 13.

24 Ibid, para. 52.

traditional print media.[25] Accordingly, the Court found that the domestic courts had failed to strike a fair balance between the rights to private life and freedom of expression, resulting in a violation of article 8.[26]

While *Delfi v. Estonia* and *Egill v. Iceland* may demonstrate that the Court is willing to impose limits on freedom of expression online in certain circumstances, a series of other cases demonstrate the Court's reluctance to unduly restrict free expression where online comments are merely vulgar or offensive, are made on private social media pages or blogs, and have only a small audience. In *Tamiz v. United Kingdom* (no. 3877/14, 12 October 2017, Decision on Admissibility), the Court held that comments made about the applicant on a private blog did not attain a level of severity sufficient to enliven the protection of article 8. The Court was inclined to agree with the national courts that the comments largely amounted to no more than "vulgar abuse",[27] which is protected by article 10. The Court took the view that most readers of comments on a blog post would understand the comments to be conjecture which should not be taken seriously.[28] In line with the Court's observation in *Delfi v. Estonia* that intermediary liability does not generally attach to a blog run for private purposes, the Court in the present case reinforced the view that it would be inappropriate to impose liability on a private blog host without unduly restricting freedom of expression.

These considerations were also determinative in *Pihl v. Sweden* (no. 74742/14, 7 February 2017, Decision on Admissibility). In this case, a defamatory comment was published on the blog of a small non-profit association about the applicant. The Swedish courts rejected the applicant's claim that the non-profit association was liable for the comment made by a third party. The Court found the application inadmissible as manifestly ill-founded. In balancing the applicant's right to respect for his private life with the right to freedom of expression of the person(s) running the blog, the Court concluded that the Swedish courts had appropriately balanced these competing considerations.[29] The judgment indicates four key factors in its assessment: (1) first, while the comment on the blog was offensive, it did not amount to an incitement to violence or hate speech; (2) second, it had been posted on a small blog with a small

25 Ibid, para. 46.

26 Ibid, para. 53.

27 *Tamiz v. United Kingdom* (no. 3877/14, 12 October 2017) para. 81.

28 Ibid.

29 *Pihl v. Sweden* (no. 74742/14, 7 February 2017), paras. 37-38.

audience; (3) third, it was taken down after the applicant complained to the non-profit association; (4) fourth, it only appeared on the blog for approximately nine days.[30] Thus, again in *Pihl* it may be observed that the severity of the speech, the size of the audience of the speech, and the nature of the intermediary's platform were the key considerations that guided the Court's assessment.

The severity of the language used online was again determinative in *Savva Terentyev v. Russia* (no. 10692/09, 28 August 2018), where the Court found a violation of article 10 due to the fact that the applicant had been convicted by a domestic court of inciting hatred after leaving offensive comments about police officers in a comment on a blog post. The Court considered that the domestic courts failed to refer to any factors or context which could show that the applicant's comment could have actually encouraged violence and put the police officers at risk.[31] In light of noting that it is the interplay between various factors that remove a particular statement from the protection of Article 10, the Court stated that while offensive, the impugned statements could not be seen as an incitement to violence rather than an emotional reaction to what was perceived as abusive police conduct.[32] In contrast, the domestic courts had focused on the nature and wording of the statements, rather than analysing these in the context of the relevant discussion.[33]

The Court's reluctance to impose liability on internet intermediaries is also evident in *Høiness v. Norway* (no. 43624/14**,** 19 March 2019). In this case, a Norwegian newspaper had posted stories online about the applicant, who was a well-known lawyer and commentator in Norway. In a comment forum, many internet users posted vulgar and defamatory comments about the applicant, but the Norwegian courts refused to impose civil liability on the internet forum host. The Court held that there had been no violation of article 8 because the Norwegian courts had acted within their margin of appreciation when striking a balance between the applicant's right under article under 8 and the forum host's rights under article 10.[34] The reconcilability of this outcome with that in *Delfi v. Estonia* is not immediately clear, given that the Court had ruled that Estonia's imposition of liability on a commercial news publisher did not in fact violate Article

30 Ibid, para. 37.

31 *Savva Terentyev v. Russia* (no. 10692/09, 28 August 2018), para. 78.

32 Ibid, para. 84.

33 Ibid, para. 82.

34 *Høiness v. Norway* (no. 43624/14**,** 19 March 2019), para. 75.

10. There are two key points to note in this regard: first, in the present case, the Court took account of the fact that the newspaper was "a large, commercially run news portal".[35] However, the critical factor appeared to be that the debate forums were not "particularly integrated" with the news articles, and therefore could not "be taken to be a continuation of the editorial articles".[36] Second, unlike in *Delfi v. Estonia*, the Court noted that the users' comments did not amount to hate speech or an incitement to violence,[37] and were removed by the newspaper within 13 minutes of being notified of them by the applicant's lawyer.[38] Consequently, what emerges from this case is an emphasis by the Court on the severity of the language and the extent to which the user-generated comments are connected with the commercially-run news business.

The Court has also paid particular attention to the need to safeguard freedom of expression where the online comments concern political debate. In *Renaud v. France* (no. 13290/07, 25 February 2010), the applicant was convicted of defaming and publicly insulting a local mayor on an internet site of the association of which he was president and webmaster. The Court noted that the comments made on the internet site were based on "a general critique of municipal policy" on the part of the applicant's political association[39] and his conviction was therefore an infringement on his right to freedom of expression – a right which in the context of political debate lies at the heart of the concept of democratic society.[40]

While the Court's case law refrains from an overzealous approach to content moderation, the Court has nonetheless recognised that free expression may be limited in circumstances where the protection of vulnerable groups, such as minors, is concerned. For example, in *K.U. v. Finland* (no. 2872/02, 2 December 2008), the applicant was a 12 year old boy whose photo and personal information had been posted on an internet dating site by an unidentified person. The internet service provider refused to identify the person responsible and could not be compelled to do so by the police or the courts under law at the relevant time. The Court found that there had been a violation of article 8 because the Finnish law did not provide a framework that reconciled the various competing claims for protection in this context, namely freedom of expression online and the

35 Ibid, para. 71.
36 Ibid.
37 Ibid, para. 69.
38 Ibid, para. 73.
39 *Renaud v. France* (no. 13290/07, 25 February 2010), para. 38.
40 Ibid, para. 41.

protection of minors, as the overriding requirement of confidentiality of communications meant that an effective investigation could not be launched.[41] Displaying a similar concern towards vulnerable groups, the Chamber in *Sanchez v. France* (no. 45581/15, 2 September 2021) found that there had been no violation of a local councillor's right to freedom of expression under Article 10, in respect of his conviction for failing to promptly delete unlawful comments by others on the wall of his Facebook account, which was used during his election campaign.[42] It is important to note that the case is currently pending before the Grand Chamber. Therefore, it remains to be seen how exactly the Court will assess the issue of acceptable limits to freedom of expression under the Convention in the relevant context.

This line of cases attests to an acute consciousness of the Court about the challenges presented by the internet and online communications to the balancing of free expression and personal autonomy.

B. Personal Autonomy, the Collection of Personal Data and Mass Surveillance

The compatibility of mass surveillance and the collection of personal data with the rights to privacy and free expression have garnered considerable attention in recent years by academics, UN human rights mechanisms and the Council of Europe. While views in the scholarship diverge over whether mass surveillance via digital technologies can be compatible with the right to private life under human rights law,[43] the UN human rights mechanisms and Council of Europe bodies take the view that digital surveillance – including mass surveillance – is not in itself a violation of human rights, but nonetheless must be implemented in a manner that complies with the right to private life and the right to freedom of expression.

In 2019, the UN Special Rapporteur released a "Report on the Adverse Effect of the Surveillance Industry on Freedom of Expression" (Report).[44] The Report observes that "[p]rivacy and expression are intertwined in the digital age, with online privacy serving

41 *K.U. v. Finland* (No. 2872/02, 2 December 2008), paras. 40, 49-50.

42 *Sanchez v. France* (no. 45581/15, 2 September 2021), para. 104.

43 See, for example, Eliza Watt, 'The Right to Privacy and the Future of Mass Surveillance' (2017) 21 International Journal of Human Rights 773, 782-3; Kristian P Humble, 'International Law, Surveillance and the Protection of Privacy' (2021) 25 International Journal of Human Rights 1, 4; Lisl Brunner, 'Digital Communications and the Evolving Right to Privacy' in Molly K Land and Jay D Aronson (eds), *New Technologies for Human Rights Law and Practice* (Cambridge University Press, 2018) 217, 227-228.

44 UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Report on the Adverse Effect of the Surveillance Industry on Freedom of Expression, UN Doc A/HRC/41/35, 28 May 2019.

as a gateway to secure exercise of the freedom of opinion and expression".[45] Surveillance not only infringes the right to private life, but also leads to the repression of freedom of expression as it can be employed to "silence dissent, sanction criticism or punish independent reporting (and sources for that reporting)".[46] The Report sets out recommendations which require: (1) first, that surveillance laws are clearly drafted and are not vague or overly broad, as required by human rights standards of legality; (2) second, that surveillance programs are subject to oversight by an independent body; and (3) third, that any individual whose rights are infringed by surveillance has access to legal redress.[47] These requirements have been echoed by bodies within the Council of Europe. The Guidance Note on Content Moderation recognises that content moderation involves the processing of personal data, including not only names but also religious beliefs, political opinions and trade union membership.[48] It emphasises the importance of clearly drafted legislation and recommends that states ensure that there are adequate legal grounds provided for in national legislation for the processing of this data and that internet intermediaries ensure that content moderation processes do not lead to data protection breaches.[49]

The compatibility of surveillance and data collection with the right to private life has been the subject of a number of cases before the European Court of Human Rights. Indeed, even in its early case law on the interception of telephone communications (*Klass and Others v. Germany* (no. 5029/71, 6 September 1978); *Malone v. United Kingdom* (no. 8691/79, 2 August 1984); *Halford v. United Kingdom* (no. 20605/92, 25 June 1997), the Court found that the use of technology for surveillance purposes engages the notion of "private life" under article 8. In *Liberty and Others v. the United Kingdom* (no.58243/00, 1 July 2008), this was extended to email communications. While the Court's case law may have evolved considerably over time as new digital technologies and methods of communication have developed, the Court has engaged in a rigorous analysis under Article 8 of surveillance programs displaying an alleged absence of adequate national safeguards against potential abuses of the technology. This trend has continued in the Court's case law on mass surveillance online, and the

45 Ibid, para. 24.

46 Ibid, para. 21.

47 Ibid, para. 66.

48 CDMSI, 'Content Moderation: Best Practices Towards Effective Legal and Procedural Frameworks for Self-Regulatory and Co-Regulatory Mechanisms of Content Moderation' (n 17) 30.

49 Ibid, 49.

jurisprudence may be viewed as aligning with the requirements identified– namely, clarity of the law, independent oversight, and avenues for redress – are similarly required under article 8 of the Convention.

The judgments in *Roman Zakharov v. Russia* (no. 47143/06, 4 December 2015) and *Szabó and Vissy v. Hungary* (no. 37138/14, 12 January 2016) provide helpful illustrations of how these requirements have been examined by the Court. In *Roman Zakharov v. Russia*, the Grand Chamber emphasised that it is essential for states to adopt detailed rules that clearly delineate the powers of authorities to conduct surveillance, "especially as the technology available for use is continually becoming more sophisticated".[50] It noted that the relevant legislation lacked adequate safeguards as it did not provide any details of the circumstances in which a person may be tracked, did not include specific rules on discontinuation of surveillance, and did not clearly outline when personal data that is irrelevant will be destroyed. Similarly, the anti-terrorist legislation under scrutiny in *Szabó and Vissy v. Hungary* – which allowed authorities to undertake mass surveillance of online communication – was overly broad in the view of the Court as it allowed the government to monitor the online communications of virtually any person in Hungary.[51] Moreover, it was solely within the power of the executive to make decisions and orders under the legislation, thereby failing the requirement that there exist independent oversight of surveillance programs.[52] The requirement of independent oversight is a principal recommendation made by the UN human rights mechanisms, who have emphasised that the absence of independent oversight of governmental surveillance programs is incompatible with the right to private life as codified in the ICCPR.[53] What the Court's case law on this point emphasises is that while independent oversight is necessary, it is not sufficient in itself. Rather, it must be accompanied by adequately drafted legislation that clearly defines the parameters of the surveillance program.

The Court's jurisprudence has also placed significant weight on the transparency of the surveillance program – in particular, notification to the individual concerned that they have been under surveillance – as an integral way to ensure the individual has access to redress. In *Roman Zakharov v. Russia*, the Court observed that a shortcoming in the legislation was that it did not provide effective remedies given the absence of

50 *Roman Zakharov v Russia* (no. 47143/06, 4 December 2015), para. 229.

51 *Szabó and Vissy v Hungary* (no. 37138/14, 12 January 2016), paras. 66, 67.

52 Ibid, paras. 80–85.

53 See UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (n 44) para. 25.

notification at any point of interceptions, or adequate access to documents relating to interceptions.[54] A similar shortcoming was observed by the Grand Chamber in *Bărbulescu v. Romania* (no. 61496/08, 5 September 2017). In the present case, the applicant was dismissed after his employer had monitored the content of his electronic communications and, in so doing, found that the applicant had breached the company's privacy policy. The Court held that there had been a violation of article 8 because the authorities had failed to determine whether the applicant had received prior notice from his employer of the possibility that his communications might be monitored; nor had they had regard either for the fact that he had not been informed of the nature or the extent of the monitoring, or the degree of intrusion into his private life and correspondence.[55] As regards the Court's criticism of the national courts' failure to consider whether the applicant had been informed of the monitoring, the UN Special Rapporteur and Human Rights Committee mirror the view that *ex post facto* notification to the individual that they had been under surveillance is a desirable way to ensure the transparency of a surveillance program, and to ensure that the individual has access to redress.[56]

The Court has also confronted the increasing use of cyber-hacking as part of surveillance programs. In *Privacy International and Others v. United Kingdom* (no. 46259/16, 7 July 2020, Decision on Admissibility), the applicants alleged that their online communications had been subject to cyber-hacking by the UK Government's intelligence services. While the Court ultimately found the application inadmissible as the applicants had failed to exhaust domestic remedies, it did take note of the particularly intrusive nature of the surveillance program and recalled the importance of implementing safeguards where the powers vested in the State are obscure, creating a risk of arbitrariness especially where the technology available is continually becoming more sophisticated.[57] However, such importance is reinforced in the context of exhaustion of domestic remedies.[58] In other words, as intended by article 35 of the Convention, it is stated that domestic courts should be provided with the possibility to rule on a matter where they have the potential to do so, which is particularly important in the context of secret surveillance programs.

54 *Roman Zakharov v. Russia* (no. 47143/06, 4 December 2015), para. 302.

55 *Bărbulescu v. Romania* (no. 61496/08, 5 September 2017), para. 140-141.

56 UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (n 44) para. 25.

57 *Privacy International and Others v. United Kingdom* (no. 46259/16, 7 July 2020), para. 45.

58 Ibid.

Two recent judgments rendered by the Grand Chamber last year have continued to develop the Court's case law on mass surveillance: *Big Brother Watch and Others v. United Kingdom* (nos. 58170/13, 62322/14 and 24960/15, 25 May 2021) and *Centrum för Rättvisa v. Sweden* (no. 35252/08, 25 May 2021). In line with its existing case law, the Court acknowledged that bulk surveillance regimes do not *per se* violate article 8, but once again emphasised the importance of robust safeguards to protect against the risk of arbitrariness and abuse. In so doing, the Court reiterated that the requirements of clarity of the law, independent oversight, and avenues for redress are essential components of a lawful surveillance program.

In the well-known case of *Big Brother Watch and Others v. United Kingdom*, the Court heard complaints by journalists and human-rights organisations lodged after revelations by Edward Snowden about programs of surveillance and intelligence sharing between the USA and the UK. The two main issues put before the Grand Chamber were the following: (1) first, the bulk interception of communications; and (2) second, the receipt of intercept material from foreign governments and intelligence agencies. While the Court found violations of articles 8 and 10, it nonetheless recognised that mass surveillance is not inherently incompatible with the Convention, and that it is both "valuable" and of "vital importance" to national security.[59] However, that is not to say that the Court did so at the expense of privacy. On the contrary, the Court's judgment has been viewed as at least on its face emphasising a "privacy-protective" approach to mass surveillance.[60] Much like the UN human rights mechanisms have emphasised that it is the robustness of the domestic legal framework that determines the human rights compatibility of a mass surveillance program, the Court outlined eight considerations that it will take into account when conducting its "global assessment" of the surveillance program.[61]

59 *Big Brother Watch and Others v. United Kingdom* (nos. 58170/13, 62322/14 and 24960/15, 25 May 2021) paras. 323, 424.

60 See Marko Milanovic, 'The Grand Normalization of Mass Surveillance: ECtHR Grand Chamber Judgments in *Big Brother Watch* and *Centrum för Rättvisa*' *EJIL:Talk!* (26 May 2021), available at: https://www.ejiltalk.org/the-grand-normalization-of-mass-surveillance-ecthr-grand-chamber-judgments-in-big-brother-watch-and-centrum-for-rattvisa/.

61 (1) The ground on which bulk interception may be authorised; (2) the circumstances in which an individual's communications may be intercepted; (3) the procedure to be followed for granting authorisation; (4) the procedures to be followed for selecting, examining and using intercept material; (5) the precautions to be taken when communicating the material to other parties; (6) the limits on the duration of interception, the storage of intercept material and the circumstances in which such material must be erased and destroyed; (7) the procedures and modalities for supervision by an independent authority of compliance with the above safeguards and its powers to address non-compliance; and (8) the procedures for independent ex post facto review of such compliance and the powers vested in the competent body in addressing instances of non-compliance, *Big Brother Watch and Others v. United Kingdom* (nos. 58170/13, 62322/14 and 24960/15, 25 May 2021) para. 361.

Applying these principles to the surveillance regimes under examination, the Court, in respect of (1) the bulk interception of communications, held unanimously that there had been a violation of article 8. While the Court noted that a bulk interception regime did not in itself violate article 8, it had to be subject to "end-to-end safeguards".[62] The UK's regime was not subject to such safeguards because there were significant concerns about the quality of the law: the interceptions were not authorised by an independent body but by the Secretary of State; categories of search terms defining the kinds of communications that would become liable for examination had not been included in the application for a warrant; and search terms linked to an individual had not been subject to prior internal authorisation.[63] Moreover, while the regime was subject to independent oversight by the Interception of Communications Commissioner and the Investigatory Powers Tribunal, these oversight mechanisms did not offset the abovementioned shortcomings in the regime.[64] In light of this finding by the Court, it is clear that both the clarity of the law and the existence of independent oversight mechanisms are mutually reinforcing, and the existence of one cannot compensate for the absence of the other. The Court also found that the bulk interception regime had not contained sufficient protections for confidential journalistic material and therefore violated freedom of expression under article 10.[65]

However, in respect of (2) the intelligence sharing regime, the Court held that there had been no violation of articles 8 or 10. The Court concluded that relevant law had set out clear, detailed rules governing when intelligence services were authorised to request intercept material from foreign intelligence agencies and how, once received, the material requested should be examined, used, and stored.[66] It was also satisfied that the regime provided for independent oversight by the Interception of Communications Commissioner and an adequate *ex post facto* review by the Investigatory Powers Tribunal.[67] What becomes clear from the Court's thorough examination of the laws in this case is that the existence of independent oversight bodies is necessary for the compatibility of mass surveillance with article 8, but it is not sufficient in itself: the Court's "global assessment" of a surveillance program requires independent oversight

62 Ibid, paras. 350, 360.
63 Ibid, paras 368-427.
64 Ibid, para. 425.
65 Ibid, paras. 451-458.
66 Ibid, paras. 500-514.
67 Ibid.

to be accompanied by an adequately drafted domestic legal framework that contains sufficient guarantees against abuse.[68]

Similar considerations led the Court to find violations of the Convention by Sweden in *Centrum För Rättvisa v. Sweden*. In this case, a Swedish human rights organisation brought proceedings against Sweden for its bulk interception regime under the country's Signals Intelligence Act. The Grand Chamber ruled that the relevant regime violated article 8. In respect of the Swedish regime's bulk interception of communications, the Court found – contrary to the UK law where the authorisation of surveillance could be made by a member of the executive – that the Swedish law provided for authorisation to be made by an intelligence court, which was compliant with the Convention.[69] However, it was nonetheless found defective because it did not provide for the possibility of an effective *ex post facto* review, unlike the UK law.[70] In respect of intelligence sharing, the regime was found to be in violation of article 8 because it did not specify that Swedish intelligence agencies had to balance privacy interests when providing intercepted information to foreign entities.[71]

The Grand Chamber judgments in both *Centrum För Rättvisa v. Sweden* and *Big Brother and Others v. United Kingdom* align with the Court's reasoning in early cases such as *Klass and Others v. Germany* and *Liberty and Others v. the United Kingdom* on telecommunications and email interception. Yet, these recent decisions demonstrate how the Court, while remaining faithful to its earlier case law, is able to tailor its jurisprudence to new and increasingly sophisticated digital surveillance regimes.

What is evident from this survey of the Court's jurisprudence is that the Court adopts a stringent approach that requires end-to-end safeguards against any risk of abuse and requires adequately drafted legislation outlining the parameters of any mass surveillance program. Furthermore, the Court's assessment of the compatibility of mass surveillance programs with article 8 aligns with the observations made by UN and Council of Europe bodies regarding the increasing threats posed by mass surveillance to both the right to private life and the right to freedom of expression. The Court is therefore successfully taking on the challenging task of reconciling the genuine need to conduct surveillance for security purposes with the protection of fundamental rights. There is

68 Ibid, para. 360.

69 *Centrum För Rättvisa v. Sweden* (no. 35252/08, 25 May 2021), paras. 295–300.

70 Ibid, para. 369.

71 Ibid, paras. 327–330, 374.

no doubt that new means of surveillance will develop in the future and the Court may again be required develop its jurisprudence on online surveillance.

III. New Digital Technologies and Non-Discrimination

The internet poses several new challenges to the principle of non-discrimination under human rights law. This part will consider the scholarship and jurisprudence on two issues that human rights bodies and courts have previously considered or may need to grapple with in the near future: the first is the issue of regulating discriminatory behaviour online, and the second is the challenge posed by the "digital divide" and the growing calls for the recognition of a human right to internet access.

A. Addressing Discriminatory Behaviour Online

The first issue that the internet poses to the principle of non-discrimination is its ability to amplify and exacerbate discriminatory behaviour. While discriminatory behaviour and expression – including the dissemination of racist, sexist, and xenophobic remarks and content – is not new, the internet has transformed the way in which this content is communicated to audiences. As mentioned earlier, the use of internet fora allows users to gain a much broader reach and larger audience for the dissemination of harmful or offensive online content. The UN High Commissioner for Human Rights has acknowledged that minorities are disproportionately affected by discriminatory behaviour on the internet and are more likely to be the victims of online incitement to discriminate and commit violence,[72] an observation that was echoed by the Council of Europe Committee of Ministers in Recommendation CM/Rec(2018)2, which noted also that online discrimination on the basis of gender, race, and religion in particular "remain underreported and are rarely remedied or prosecuted".[73]

While the prevalence of discriminatory content online is simple enough to identify, devising a human rights-based solution to the issue is not so easy. There is a fine line between tackling discriminatory speech online and stifling free expression. So much has been explicitly acknowledged by the UN High Commissioner for Human Rights, who has recognised that the curtailment and stifling of dissent and opposing views

72 UN High Commissioner for Human Rights, 'Statement by United Nations High Commissioner for Human Rights, Michelle Bachelet at the 13th Session of the Forum on Minority Issues: Hate Speech, Social Media and Minorities' (19 November 2020), available at: https://www.ohchr.org/en/statements/2020/11/statement-united-nations-high-commissioner-human-rights-michelle-bachelet-13th?LangID=E&NewsID=26519. .

73 Committee of Ministers, 'Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries', 7 March 2018, preamble para. 3.

may be an unintended consequence of dealing with hate speech.[74] It may also be important to recognise that while the internet may exacerbate the issue, it may not be the root cause of discriminatory behaviour.[75] Accordingly, tackling discriminatory behaviour on the internet is only one part of the solution to the broader issue of addressing discriminatory behaviour both online and offline.

This challenge is reflected in the jurisprudence of the Court, which has on numerous occasions been required to address the issue of discriminatory speech online and its compatibility with articles 8 and 14 of the Convention. One case involving discriminatory behaviour and the internet is *Willem v. France* (no. 10883/05, 16 July 2009). The Court found that there had been no violation of article 10 because the applicant's conviction and fine were justifiable by the courts,[76] who reasoned that the call for the boycott interfered with the normal exercise of a trader's business because of their belonging to a particular nation.[77] While the Court did not expressly address discrimination on the basis of nationality under article 14 of the Convention, the case nonetheless provides an insight into the Court's view that states may impose limits on an individual's freedom of expression where such expression is discriminatory.

A particularly pertinent issue concerning digital technologies and non-discrimination is the online dimension of violence against women. Whilst violence against women has been recognised as a human rights violation for some time, due to the existence of new technologies it has evolved from its traditional form into new forms such as cyberviolence. This issue has garnered the attention of the CEDAW Committee, which has recognised both that gender-based violence can occur online and in other digital environments, and that cyberbullying including revenge porn disproportionately impacts women and girls.[78] Much like the progress made by the CEDAW Committee with respect to online violence against women,[79] the Court's jurisprudence has similarly

74 UN High Commissioner for Human Rights (n 72).

75 See, for example, Talia Joundi, 'Freedom of Expression, Discrimination, and the Internet: Legislative Responses and Judicial Reactions' (2015) 13 Canadian Journal of Law and Technology 191, 201.

76 *Willem v. France* (no. 10883/05, 16 July 2009), paras. 38-40.

77 Ibid, para. 16.

78 See CEDAW Committee, General Recommendation No. 35 on Gender-Based Violence, updating General Recommendation No. 19, UN Doc CEDAW/C/GC/35, 26 July 2017, para. 20; CEDAW Committee, General Recommendation No. 36 on the Right of Girls and Women to Education, UN Doc CEDAW/C/GC/36, 16 November 2017, para. 70.

79 For an overview of CEDAW Committee's role in tackling violence against women, see Christine Chinkin and Keina Yoshida, 'CEDAW: Global leader in Tackling Violence against Women and Girls' (2020) 4 European Human Rights Law Review 347–358.

positioned the Court as a leader in addressing online violence against women. In the recent case of *Buturugă v. Romania* (no. 56867/15, 11 February 2020), the applicant criticised the domestic authorities' refusal to consider her complaint concerning her former husband's breach of the confidentiality of her electronic correspondence, which was closely linked to her complaint of domestic violence. The Court held that there had been a violation of article 3 and article 8, and in doing so importantly acknowledged cyberbullying as a recognised aspect of violence against women and girls.[80] Moreover, the Court acknowledged the variety of forms that cyberbullying could take, including: cyber breaches of privacy, intrusion into the victim's computer and the capture, and sharing and manipulation of data and images, including private data. [81]

The Court specifically addressed the issue of "revenge porn" in *Volodina v. Russia (No. 2)* (no. 40419/19, 14 September 2021) - that is, the non-consensual sharing of intimate images online. Comparably to the recognition by the Council of Europe's Group of Experts on Action against Violence against Women and Domestic Violence (GREVIO) that revenge porn falls within the meaning of "sexual harassment" within the Istanbul Convention, the Court acknowledged that states have positive obligations in relation to acts of cyberviolence including revenge porn under Article 8 of the Convention.[82] As in *Buturugă v. Romania,* the Court was tasked with considering whether the domestic authorities' failures to investigate and prosecute repeated acts of cyberviolence against a women by her former partner amounted to a violation of article 8. The Court reiterated that cyberviolence against women is integrally linked with physical violence against women and is yet "another facet of the complex phenomenon of domestic violence".[83] The judgment is noteworthy because it marks the first time that the Court has addressed the relatively new issue of "revenge porn" and demonstrates the Court's ability to recognize new forms of cyberviolence as acts of violence against women and violations of the Convention.

B. Access to the Internet and the Digital Divide

A second issue of non-discrimination that has arisen in recent years is the acknowledgment of the need to address the "digital divide" through the recognition of a human right to

80 *Buturugă v. Romania* (no. 56867/15, 11 February 2020), para. 74.

81 Ibid.

82 GREVIO, 'General Recommendation No. 1 on the Digital Dimension of Violence against Women', GREVIO(2021)20, adopted on 20 October 2021, para. 38, available at: https://rm.coe.int/grevio-rec-no-on-digital-violence-against-women/1680a49147; *Volodina v. Russia (No. 2)* (no. 40419/19, 14 September 2021), para. 68.

83 *Volodina v. Russia (no. 2)*, para. 49.

internet access.[84] It has been discussed that the growing digital divide poses significant challenges to the full realisation of the right to freedom of expression in a non-discriminatory manner.[85] The "digital divide" has been defined as referring to the gap between persons who can access and use the internet and those who cannot.[86] Additionally, it has been described as an "extremely complex and multi-faceted phenomenon" which involves a "complex inter-play of a wide range of social, economic, political, cultural and technological factors".[87] The digital divide poses significant challenges for non-discrimination because research demonstrates that the digital divide fractures along gendered, racial, and class divides, with women, ethnic and racial minorities, and the poor disproportionately lacking access to the internet.[88]

In recognition of the fact that the internet has become the primary means through which people receive and impart information and therefore exercise their right to freedom of expression, there is ongoing debate as to whether human rights law does or should provide for a right to internet access.[89] The crux of this argument is that the internet has become so significant for communication and expression that it should no longer be conceptualised solely as a vehicle through which to facilitate freedom of expression and other rights. Rather, a proposed "right to internet access" should be recognised, which would place positive obligations on states to facilitate access to and use of the internet.[90]

84 See, for example, UN, 'Don't Let the Digital Divide Become the New Face of Inequality: UN Deputy Chief', *UN News* (27 April 2021), available at: https://news.un.org/en/story/2021/04/1090712.

85 See, for example, Antonio Segura-Serrano, 'Internet Regulation and the Role of International Law' (2006) 20 Max Planck Yearbook of United Nations Law 192, 264-70.

86 Cynthia K Sanders and Edward Scanlon, 'The Digital Divide is a Human Rights Issue: Advancing Social Inclusion through Social Work Advocacy' (2021) 6 Journal of Human Rights and Social Work 130, 131.

87 Daniel Paré, 'The Digital Divide: Why the 'The' is Misleading' in Matthias Klang and Andrew Murray (eds), Human Rights in the Digital Age (Routledge-Cavendish, 2004) 85-97, 97.

88 See, for example, OECD, 'Bridging the Digital Gender Divide' (Report, 2018) 24-25 https://www.oecd.org/digital/bridging-the-digital-gender-divide.pdf; see, also, Sylvia E Korupp and Marc Szydlik, 'Causes and Trends of the Digital Divide' (2005) 21 European Sociological Review 409.

89 See, for example, Segura-Serrano (n 85) 270; see, also, Oreste Pollicino, 'The Right to Internet Access: Quid Iuris?' in Andreas von Arnauld, Kerstin von der Decken and Mart Susi (eds), *The Right to Internet Access* (Cambridge University Press, 2020) 263, 264-68.

90 See, for example, Daniel Joyce, 'Internet Freedom and Human Rights' (2015) 26 European Journal of International Law 493; see, also, Shandler and Canetti (n 6) 78; Molly Land, 'Toward an International Law of the Internet' (2013) 54 Harvard International Law Journal 393, 422-23.

The Court's case law on this issue may be seen as mirroring the approach of the UN human rights mechanisms.[91] To date, the Court has not been tasked with examining whether inequality of access to the internet and the digital divide that disproportionately impacts minorities and other marginalised groups violates the Convention. However, that does not mean that the Court has turned a blind eye to internet access as a human right and the integral role it plays in the realisation of an individual's right to freedom of expression. Indeed, the Court has recognised the centrality of the internet to the enjoyment of the right to freedom of expression. For example, in *Cengiz and Others v. Turkey* (nos. 48226/10 and 14027/11, 1 December 2015), the Court expressed the view that the internet is "one of the principal means by which individuals exercise the right to freedom to receive and impact information and ideas".[92] The Court has also not shied away from finding a violation of article 10 where individuals' access to the internet has been unduly restricted by a state. In *Ahmet Yildirim v. Turkey* (no. 3111/10, 18 December 2012), the Court found a violation of article 10 where the applicant's access to Google Sites was blocked by the state. A similar outcome was reached in *Cengiz and Others v. Turkey* where a wholesale block on certain academics' access to YouTube was found to violate article 10.

In recent years, the Court's case law exhibits a growing recognition of the incompatibility of the digital divide with the rights guaranteed under the Convention. In both *Kalda v. Estonia* (no. 17429/10, 19 January 2016) and *Jankovskis v. Lithuania* (no. 21575/08, 17 January 2017), the Court expressly recognised that '"Internet access has increasingly been understood as a right, and calls have been made to develop effective policies to achieve universal access to the Internet and to overcome the "digital divide"'.[93] The Court considered in both cases that these developments reflect the important role the Internet plays in people's everyday lives, in particular since certain information is

91 The recognition of a so-called "right to internet access" is gaining traction within the UN human rights system but, to date, has not been recognised as a right. For example, the Human Rights Committee in its "General Recommendation 34 on Article 19: Freedoms of Opinion and Expression "recommended that State Parties to the ICCPR take all necessary steps to foster access to new media, including the internet, but nonetheless stopped short of recognising a right to internet access. A similar approach has been taken by the UN Special Rapporteur, who has conceded that "access to the Internet is not yet a human right" recognised under international law. See UNGA, 'Promotion and Protection of the Right to Freedom of opinion and Expression: Report of the Special Rapporteur on the Right to Freedom of Opinion and Expression', A/66/290, 10 August 2011, para. 61.

92 *Cengiz and Others v. Turkey* (nos. 48226/10 and 14027/11, 1 December 2015), para. 49.

93 *Kalda v. Estonia* (no. 17429/10, 19 January 2016) para. 52; *Jankovskis v. Lithuania* (no. 21575/08, 17 January 2017) para. 62.

exclusively available on Internet.[94] To be clear, the facts of these cases involved authorities' decisions to restrict prisoners' access to the internet and therefore involved an interference by authorities with the applicants' rights under article 10, resulting in a violation. Conversely, the proposed "right to internet access" that is gaining traction among scholars and UN human rights mechanisms is more concerned with authorities' failure to facilitate access to the internet, rather than their obligation not to interfere with the exercise of freedom of expression. While this precise issue has not arisen thus far in the Court's jurisprudence, *Kalda v. Estonia* and *Jankovskis v. Lithuania* nonetheless demonstrate that the Court is aware of the challenges posed by the digital divide and that it is poised to tackle this emerging and important issue.

IV. Conclusion

In sum, the internet and online communication pose acute challenges for the protection of personal autonomy and non-discrimination under human rights law. However, this survey of the Court's jurisprudence demonstrates that the Court is keenly aware of both the advantages and the complications that emerging technologies present for human rights. Furthermore, the Court is already in the process of developing a substantial body of case law that seeks to harness the benefits that new technologies bring while at all times ensuring that they do not compromise the enjoyment of the rights guaranteed by the Convention.

Peer-review: Externally peer-reviewed.
Conflict of Interest: The author has no conflict of interest to declare.
Grant Support: The author declared that this study has received no financial support.

Hakem Değerlendirmesi: Dış bağımsız.
Çıkar Çatışması: Yazar çıkar çatışması bildirmemiştir.
Finansal Destek: Yazar bu çalışma için finansal destek almadığını beyan etmiştir.

Kaynakça/References

A. Table of Cases

Ahmet Yildirim v. Turkey (no. 3111/10, 18 December 2012)
Bărbulescu v. Romania (no. 61496/08, 5 September 2017)
Big Brother Watch and Others v. United Kingdom (nos. 58170/13, 62322/14 and 24960/15, 25 May 2021)
Buturugă v. Romania (no. 56867/15, 11 February 2020)

94 Ibid.

Cengiz and Others v. Turkey (nos. 48226/10 and 14027/11, 1 December 2015)

Centrum För Rättvisa v. Sweden (no. 35252/08, 25 May 2021)

Delfi AS v. Estonia (no. 64569/09, 16 June 2015)

Egill Einarsson v. Iceland (no. 24703/15, 7 November 2017)

Høiness v. Norway (no. 43624/14**,** 19 March 2019)

Jankovskis v. Lithuania (no. 21575/08, 17 January 2017)

Kalda v. Estonia (no. 17429/10, 19 January 2016)

Klass and Others v. Germany (no. 5029/71, 6 September 1978)

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

Liberty and Others v. the United Kingdom (no. 58243/00, 1 July 2008)

Pihl v. Sweden (no. 74742/14, 7 February 2017)

Privacy International and Others v. the United Kingdom (no. 46259/16, 7 July 2020)

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

Sanchez v. France (no. 45581/15, 2 September 2021)

Savva Terentyev v. Russia (no. 10692/09, 28 August 2018)

Szabó and Vissy v. Hungary (no. 37138/14, 12 January 2016)

Tamiz v. the United Kingdom (no. 3877/14, 12 October 2017)

Volodina v. Russia (No. 2) (no. 40419/19, 14 September 2021)

Willem v. France (no. 10883/05, 16 July 2009)

Roman Zakharov v. Russia (no. 47143/06, 4 December 2015)

B. Table of International Materials

CEDAW Committee, General Recommendation No. 35 on Gender-Based Violence, updating General Recommendation No. 19, UN Doc CEDAW/C/GC/35, 26 July 2017.

CEDAW Committee, General Recommendation No. 36 on the Right of Girls and Women to Education, UN Doc CEDAW/C/GC/36, 16 November 2017.

Committee of Experts on Freedom of Expression and Digital Technologies (MSI-DIG), 'Content Moderation: Best Practices Towards Effective Legal and Procedural Frameworks for Self-Regulatory and Co-Regulatory Mechanisms of Content Moderation' (Guidance Note, 21 May 2021) 25 https://rm.coe.int/content-moderation-en/1680a2cc18.

Committee of Ministers, 'Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries', 7 March 2018.

Council of Europe Steering Committee for Media and Information Society (CDMSI) 'Content Moderation: Best Practices Towards Effective Legal and Procedural Frameworks for Self-Regulatory and Co-Regulatory Mechanisms of Content Moderation' (Guidance Note, adopted 19-21 May 2021), available at: https://rm.coe.int/content-moderation-en/1680a2cc18.

GREVIO, 'General Recommendation No. 1 on the Digital Dimension of Violence against Women' GREVIO(2021)20, adopted on 20 October 2021, available at: https://rm.coe.int/grevio-rec-no-on-digital-violence-against-women/1680a49147.

Human Rights Committee, 'General Comment No. 34 on Article 19: Freedoms of Opinion and Expression', CPR/C/GC/34, 29 July 2011.

OECD, 'Bridging the Digital Gender Divide' (Report, 2018) 24-25 https://www.oecd.org/digital/bridging-the-digital-gender-divide.pdf.

UN High Commissioner for Human Rights, 'Statement by United Nations High Commissioner for Human Rights, Michelle Bachelet at the 13th Session of the Forum on Minority Issues: Hate Speech, Social Media and Minorities' (19 November 2020), available at: https://www.ohchr.org/en/statements/2020/11/statement-united-nations-high-commissioner-human-rights-michelle-bachelet-13th?LangID=E&NewsID=26519.

UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, 'Report on the Adverse Effect of the Surveillance Industry on Freedom of Expression', UN Doc A/HRC/41/35, 28 May 2019.

UNGA Human Rights Council, 'Disinformation and Freedom of Opinion and Expression: Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression', UN Doc A/HRC/47/25, 13 April 2021.

UNGA Human Rights Council, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression: Note by the Secretariat', UN Doc A/HRC/38/35, 6 April 2018.

UNGA, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression', A/66/290, 10 August 2011.

C. List of References

Barendt E., 'Balancing Freedom of Expression and Privacy: The Jurisprudence of the Strasbourg Court' (2009) 1 Journal of Media Law 49.

Benesch S., 'But Facebook's Not a Country: How to Interpret Human Rights Law for Social Media Companies' (2020-2021) 38 Yale Journal on Regulation Bulletin 86.

Breyer P., 'French Law on Illegal Content Online Ruled Unconstitutional: Lessons for the EU to Learn', *Patrick Breyer* (19 November 2020), available at https://www.patrick-breyer.de/en/french-law-on-illegal-content-online-ruled-unconstitutional-lessons-for-the-eu-to-learn/?lang=en.

Brunner L., 'Digital Communications and the Evolving Right to Privacy' in Molly K Land and Jay D Aronson (eds), *New Technologies for Human Rights Law and Practice* (Cambridge University Press, 2018) 217-42.

Callamard A., 'The Human Rights Obligations of Non-State Actors' in Rikke Franke Jørgensen (ed), *Human Rights in the Age of Platforms* (MIT Press, 2019) 191.

Chander A., 'Googling Freedom' (2011) 99 California Law Review.

Chinkin C. and Yoshida K., 'CEDAW: Global leader in Tackling Violence against Women and Girls' (2020) 4 European Human Rights Law Review 347–358.

Douek E., 'Governing Online Speech' (2021) 121 *Columbia Law Review* 759.

Douek E., 'The Limits of International Law in Content Moderation' (2021) 6 UC Irvine Journal of International, Transnational, and Comparative Law 37.

Facebook Community Standards, available at: https://transparency.fb.com/fr-fr/policies/community-standards/.

Humble K.P., 'International Law, Surveillance and the Protection of Privacy' (2021) 25 International Journal of Human Rights.

Jørgensen R.F., 'Human Rights and Private Actors in the Online Domain' in Molly K Land and Jay D Aronson (eds), *New Technologies for Human Rights Law and Practice* (Cambridge University Press, 2018) 243.

Joundi T., 'Freedom of Expression, Discrimination, and the Internet: Legislative Responses and Judicial Reactions' (2015) 13 Canadian Journal of Law and Technology 191.

Joyce D., 'Internet Freedom and Human Rights' (2015) 26 European Journal of International Law 493.

Korupp S.E. and Szydlik M., 'Causes and Trends of the Digital Divide' (2005) 21 European Sociological Review 409.

Land M., 'Toward an International Law of the Internet' (2013) 54 Harvard International Law Journal 393.

Langvardt K., 'Regulating Online Content Moderation' (2008) 26 Georgetown Law Journal 1353.

Marshall J., *Personal Freedom through Human Rights Law? Autonomy, Identity and Integrity under the European Convention on Human Rights* (Martinus Nijhoff, 2009).

Milanovic M., 'The Grand Normalization of Mass Surveillance: ECtHR Grand Chamber Judgments in *Big Brother Watch* and *Centrum för Rättvisa*' *EJIL:Talk!* (26 May 2021) https://www.ejiltalk.org/the-grand-normalization-of-mass-surveillance-ecthr-grand-chamber-judgments-in-big-brother-watch-and-centrum-for-rattvisa/.

Nunziato D.C., 'The Death of the Public Forum in Cyberspace' (2005) 20 Berkeley Technology Law Journal 1115.

Oliva T.D., 'Content Moderation Technologies: Applying Human Rights Standards to Protect Freedom of Expression' (2020) 20 Human Rights Law Review 607.

Paré D., 'The Digital Divide: Why the 'The' is Misleading' in Matthias Klang and Andrew Murray (eds), *Human Rights in the Digital Age* (Routledge-Cavendish, 2004) 85-97.

Pollicino O., 'The Right to Internet Access: Quid Iuris?' in Andreas von Arnauld, Kerstin von der Decken and Mart Susi (eds), *The Right to Internet Access* (Cambridge University Press, 2020).

Sanders C.K. and Scanlon E., 'The Digital Divide is a Human Rights Issue: Advancing Social Inclusion through Social Work Advocacy' (2021) 6 Journal of Human Rights and Social Work 130.

Satariano A., 'Europe is Reigning in Big Tech Giants. But Some Say It's Going Too Far', *New York Times* (6 May 2019) https://www.nytimes.com/2019/05/06/technology/europe-tech-censorship.html.

Sears A., 'Protecting Freedom of Expression over the Internet: An International Approach' (2015) 5 Notre Dame Journal of International and Comparative Law 171.

Segura-Serrano A., 'Internet Regulation and the Role of International Law' (2006) 20 Max Planck Yearbook of United Nations Law 192.

Shandler R. and Canetti D., 'A Reality of Vulnerability and Dependence: Internet Access as a Human Right' (2019) 52 Israel law Review 77.

Spano R., 'Intermediary Liability for Online User Comments under the European Convention on Human Rights' (2017) 17(4) Human Rights Law Review 665-679.

UN, 'Don't Let the Digital Divide Become the New Face of Inequality: UN Deputy Chief', *UN News* (27 April 2021) https://news.un.org/en/story/2021/04/1090712.

Watt E., 'The Right to Privacy and the Future of Mass Surveillance' (2017) 21 International Journal of Human Rights 773.

West D.M., 'Techlash Continues to Batter Technology Sector', *Brookings* (2 April 2021) https://www.brookings.edu/blog/techtank/2021/04/02/techlash-continues-to-batter-technology-sector.

York J.C. and Zuckerman E., 'Moderating the Public Sphere' in Rikke Franke Jørgensen (ed), *Human Rights in the Age of Platforms* (MIT Press, 2019) 137.