The European Journal of International Law Vol. 32 no. 4

It's the End of the (Offline) World as We Know It: From Human Rights to Digital Human Rights – A Proposed Typology

Dafna Dror-Shpoliansky[*] and Yuval Shany[**]

Abstract

'The same rights that people have offline must also be protected online' is used in recent years as a dominant concept in international discourse about human rights in cyberspace. But does this notion of 'normative equivalency' between the 'offline' and the 'online' afford effective protection for human rights in the digital age? This is the question at the heart of this article. We first review the development of human rights in cyberspace as they were conceptualized and articulated in international fora and critically evaluate the normative equivalency paradigm adopted by international bodies for the online application of human rights. We then attempt to describe the contours of a new digital human rights framework, which goes beyond the normative equivalency paradigm. We offer in this connection a typology of three 'generations' or modalities in the evolution of digital human rights – the radical reinterpretation of existing rights, the development of new rights and the introduction of new right and duty holders. In particular, we focus on the emergence of new digital human rights, present two prototype rights (the right to Internet access and the right not to be subject to automated decision) and discuss the normative justifications invoked for recognizing these new digital human rights. We propose that such a multilayered framework corresponds better than the normative equivalency paradigm to the unique features and challenges of upholding human rights in cyberspace.

> When we encounter something unprecedented, we automatically interpret it through the lenses of familiar categories, thereby rendering invisible precisely that which is unprecedented.
>
> – S. Zuboff, *The Age of Surveillance Capitalism*[1]

[*] PhD Candidate, Hebrew University, Jerusalem, Israel; Visiting PhD Student, University of Toronto Faculty of Law, Canada; Research Fellow, Cyber Law Program, Federmann Cyber Security Research Center, Jerusalem, Israel. Email: dafnadror@gmail.com.

[**] Hersch Lauterpacht Chair in Public International Law; Director of Cyber Law Program, Federmann Cyber Security Research Center, Hebrew University, Jerusalem; Vice-President for Research, Israel Democracy Institute, Jerusalem, Israel. Email: shany.yuval@gmail.com.

[1] S. Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (2019), at 12.

1 Introduction

The Cambridge Analytica scandal[2] and other high-profile incidents[3] involving harmful online practices, such as the dissemination of online hate speech[4] and disinformation (or 'fake news'),[5] intrusive government surveillance programmes[6] and revenge porn,[7] have led to increasing concerns about the safety of the digital environment and the limited protection it affords to basic human rights of online users, such as privacy, personal security and participation on equal terms in political life. Such concerns have prompted, in turn, a critical review of the adequacy of the existing international human rights framework for addressing the challenges of the online environment and of the need for new human rights norms and implementation strategies specifically designed for application in cyberspace.

Identifying the applicable human rights framework governing cyberspace and its relation to other national and international law norms has become a particularly difficult challenge in the digital age. In the early days of the Internet, a prevalent notion among digital rights theorists and activists was that it should be regarded as a 'civilization of the mind'[8] – a global social space operating through a 'social contract', which individual users themselves implement.[9] According to this view, the Internet should remain a space 'free of intervention' from government power.[10]

2 R. Price, 'The UK's Privacy Watchdog Has Fined Facebook £500,000 – the Maximum Amount – over Cambridge Analytica', *Business Insider*, July 2018, available at www.businessinsider.com/uk-watchdog-ico-fines-facebook-500000-cambridge-analytica-2018-7.

3 C. Cross, 'Another Day Another Data Breach – What to Do When It Happens to You', *The Conversation* (2018), available at https://theconversation.com/another-day-another-data-breach-what-to-do-when-it-happens-to-you-99150.

4 UN Secretary General, Hate Speech Is Spreading Like Wildfire on Social Media, UN Press Release SG/SM/19578, 14 May 2019; see also C. Warzel, 'The New Zealand Massacre Was Made to Go Viral', *New York Times*, 15 March 2019, available at https://www.nytimes.com/2019/03/15/opinion/new-zealand-shooting.html.

5 European Commission for Democracy through Law, Joint Report of the Venice Commission and of the Directorate of Information Society and Action Against Crime, Digital Technologies and Elections, Adopted by the Council of Democratic Elections at its 65th meeting, 20 June 2019, at 7–11, 12, para. para. 46; see also Allcott and Gentzkow, 'Social Media and Fake News in the 2016 Election', 31 *Journal of Economic Perspectives* (2017) 211.

6 Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Report on Surveillance and Human Rights (SR Expression 2019), UN Doc. A/HRC/41/35, 28 May 2019, para. at 3, para. 2.

7 Citron and Franks, 'Criminalizing Revenge Porn', 49 *Wake Forest Law Review* (2014) 345, at 392; see also O. Bowcott, 'Revenge Porn and "Cyber-flashing" Laws Go under Review', *The Guardian* (2019), available at www.theguardian.com/law/2019/jun/26/revenge-porn-and-cyber-flashing-laws-go-under-review.

8 J.P. Barlow, *Declaration of the Independence of Cyberspace* (1996), available at www.eff.org/cyberspace-independence.

9 Fidler, 'Cyberspace and Human Rights', in N. Tsagourias (ed.), *Research Handbook on International Law and Cyberspace* (2015), 94, at 96–97. For more initiatives, see, e.g., E. Dyson *et al.*, *Cyberspace and the American Dream: A Magna Carta for the Knowledge Age* (1994), available at www.pff.org/issues-pubs/futureinsights/fi1.2magnacarta.html; Declaration of Internet Freedom (2012), available at declarationofinternetfreedom.org/.

10 *Ibid.*; see also Gill, Redeker and Gasser, 'Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights', 15 *Berkman Klein Research Center* (2015) 1, at 18.

Over time, with the Internet and other means of communication over cyberspace becoming an essential and integral part of the contemporary lives of billions of people, affecting directly or indirectly almost every aspect of society and human welfare, expectations that governments and governmental regulation would stay clear of cyberspace have become more and more untenable. Furthermore, as the dependency on cyberspace has increased, the line between regulating 'online' and 'offline' lives has become more and more blurred,[11] and it is no longer possible to describe the Internet as merely a 'world of identities with no bodies'.[12] The more cyberspace becomes a site where basic human rights are enjoyed or infringed,[13] the greater is the expectation that public bodies charged with upholding human rights norms would take action to protect the rights of online users.

Indeed, the protection and promotion of human rights online is an issue of growing concern for international organizations operating in the field of human rights.[14] In a series of resolutions issued in recent years, both the United Nations General Assembly (GA)[15] and the Human Rights Council (HRC)[16] have addressed this topic, embracing the position that the same human rights that people have offline must be protected online as well. This position is referred to in this article as the 'normative equivalency' paradigm. While some scholars claim that there is consensus over the normative equivalency paradigm,[17] questions regarding necessary adjustments to human rights norms when interpreted and applied in cyberspace are increasingly raised.[18] Regarding the right to privacy, for example, the GA itself has pointed to 'vast technological leaps' that cast doubt on whether the existing human rights framework adequately encompasses the range of protections that individuals need when interacting online.[19] Another example, which will be discussed further in Section 4 of this article,

[11] Joyce, 'Privacy in the Digital Era: Human Rights Online?', 16 *Melbourne Journal of International Law* (2015) 270, at 273; see also McGregor, Murray and Ng, *Four Ways Your Google Searches and Social Media Affect Your Opportunities in Life* (2018), available at https://theconversation.com/four-ways-your-google-searches-and-social-media-affect-your-opportunities-in-life-96809.

[12] Barlow, *supra* note 8.

[13] International Telecommunication Union (ITU), *The Quest for Cyber Peace* (2011), at xi, available at www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-PDF-E.pdf; see also United Nations (UN) High Commissioner for Human Rights (OHCHR), Report on The Right to Privacy in the Digital Age (OHCHR Privacy Report 2018), UN Doc. A/HRC/39/29, 3 August 2018, at 15, para. 61(a).

[14] Land, 'Toward an International Law of the Internet', 54 *Harvard International Law Journal* (2013) 393, at 437–442.

[15] GA Res. 68/167, 18 December 2013, para. 3; GA Res 69/166, 18 December 2014, para. 3; GA Res. 71/199, 19 December 2016, para. 3; GA Res. 73/179, 17 December 2018, para. 3.

[16] Human Rights Council (HRC) Res. 20/8, UN Doc. A/HRC/RES/20/8, 5 July 2012, at 2, para. 1; HRC Res. 26/13, UN Doc. A/HRC/RES/26/13, 26 June 2014, at 2, para. 1; HRC Res. 32/13, UN Doc. A/HRC/RES/32/13, 1 July 2016, at 3, para. 1; HRC Res. 38/7, UN Doc/HRC/RES/38/7, 5 July 2018, at 3, para. 1.

[17] Rona and Aarons, 'State Responsibility to Respect, Protect and Fulfill Human Rights Obligations in Cyberspace', 8 *Journal of National Security Law and Policy* (2016) 503.

[18] Fidler, *supra* note 10, at 103.

[19] GA Res. 69/166, *supra* note 16, at 2.

is the ongoing debate in international fora on whether access to the Internet should be recognized as a new independent human right.[20]

But beyond the specific challenges associated with the recalibration of the existing human rights framework to cyberspace, there lies a broader normative inquiry – that is, whether, in light of the unique features of cyberspace, the normative equivalency paradigm, embraced by the GA and the HRC, is a suitable normative baseline. Unlike physical space occupied by states, cyberspace is de-territorialized and de-centralized, and non-state actors play a dominant role in constructing it and operating therein.[21] In this digital environment, new needs and interests present themselves, and pre-existing threats and challenges assume radically different implications. Such features render tenuous the 'fit' between offline human rights and the specific protections required in cyberspace. It is for this reason that the normative equivalency paradigm was sharply criticized by the United Nations (UN) special rapporteur on the right to privacy, who argued that it cannot afford adequate protection for the right to privacy in the digital age.[22]

This article discusses the reliance of international human rights bodies on the normative equivalency paradigm as well as attempts by norm makers and norm shapers to develop a new human rights framework for the digital age. It suggests, in this regard, a typology for identifying different stages in recent efforts to develop international digital human rights law in ways that go beyond the normative equivalency paradigm. According to the typology proposed, three 'generations' or modalities can be identified:

- The first generation involves far-reaching processes of adjustment of offline human rights to the online world.
- The second generation features the emergence of new digital human rights – that is, rights that protect online needs and interests that do not have close parallels in the offline world. Although second-generation rights may be genealogically traced back to existing offline human rights, the new progenies are not fully subsumed in the human rights from which they originate.
- The third generation comprises rights belonging to new online personae – that is, digital or virtual representations of natural persons or legal entities that exist and exercise rights separately from the human beings or legal entities that created them. This third generation of rights is also expected to focus more and more attention on the direct human rights obligations of technology companies exercising de facto governance power over the online user.

[20] Tully, 'A Human Right to Access the Internet? Problems and Prospects', 14 *Human Rights Law Review* (2014) 175, at 177–181.

[21] Y. Shany, *Contribution to Open Consultation on UN GGE 2015 Norm Proposals* (2018), available at https://csrcl.huji.ac.il/sites/default/files/csrcl/files/contribution_un_gge_norm_proposals-_dd.pdf.

[22] Special Rapporteur on the Right to Privacy, Report on Security and Surveillance (SR Privacy 2018), UN Doc. A/HRC/37/62, 28 February 2018, at 26, para. 6 ('[w]hen dealing with technologies such as the Internet it is simplistic and naïve to be content with a statement that "whatever is protected off-line is protected on-line". That is a hopelessly inadequate approach to the protection of privacy in 2018').

Section 2 discusses and critically evaluates contemporary international law debates and practices surrounding digital human rights and introduces the main criticisms directed against the normative equivalency paradigm. Section 3 then proposes a new three-generational typology for the evolution of digital human rights, including recognizing new digital human rights. This requires us, in turn, to consider some of the ethical foundations underlying the emergence of new human rights, explore the outer limits for the development of international human rights law and examine the intersection between human rights and cyberspace. Section 4 proceeds to focus on the specific normative justifications that have been made in support of recognizing new digital human rights, illustrating this through an examination of normative developments pertaining to the right of access to the Internet and the right not to be subject to algorithmic decisions. Section 5 concludes.

2 The Development of Human Rights in Cyberspace in International Fora

A *GA and HRC Resolutions on Digital Human Rights*

The application and interpretation of human rights law in cyberspace has been the subject of multiple resolutions adopted by UN human rights bodies in recent years. In 2012, the HRC asserted that 'the same rights people have offline must also be protected online'.[23] In a series of resolutions adopted since then, both the HRC[24] and the GA[25] have reiterated the notion that human rights apply in the digital 'online world' as they apply in the 'offline world', thereby embracing the normative equivalency paradigm. Over the years, GA and HRC resolutions on digital human rights have become more explicit, encompassing a wider range of issues, moving beyond privacy online to structural issues, such as the digital divide and online discrimination, and imposing on states more onerous obligations.[26] For example, whereas in 2013, the GA requested states to review their procedures, legislation and practices with regard to the surveillance of communications,[27] the 2014 GA resolution also called on states to provide individuals whose right to privacy has been violated by unlawful or arbitrary surveillance with access to an effective remedy.[28] A 2016 GA resolution also

[23] HRC 20/8, *supra* note 17, at 2, para. 1.

[24] See note 17 above.

[25] See note 16 above; see also Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Report on the Role of Digital Access Providers (SR Expression 2017), UN Doc. A/HRC/35/22, 30 March 2017, at 4, para. 5; see also Rona & Aarons, *supra* note 18, at 503. Mihr, 'Good Cyber Governance: The Human Rights and Multi-Stakeholder Approach', *Georgetown Journal of International Affairs*: *International Engagement on Cyber IV* (2014) 24, at 28.

[26] Compare, for example, operative clause 4 and operative clause 5 in GA Res. 69/166 and GA Res. 71/199 respectively, *supra* note 16; see also HRC 20/8 and HRC 32/13, *supra* note 17.

[27] GA Res. 68/167, *supra* note 16, para. 4(c).

[28] GA Res. 69/166, *supra* note 16, para. 4(e).

mentioned the growing concern regarding the sale of personal data and called on states to enhance protection against such practices.[29] Moreover, both the GA and the HRC increasingly acknowledge the broad interplay between offline and online human rights. For example, GA Resolution 71/199 acknowledges that the right to privacy and digital technology is an important component in the ability to realize economic, social and cultural rights.[30]

Arguably, the HRC and the GA were guided by three normative propositions. First, the dominant approach found in the resolutions is one of normative equivalency – that is, that the same rights that people enjoy offline should also be enjoyed online. Under this paradigm, the Internet is one medium among several in which human rights can be exercised. In order to ensure that rights, such as freedom of expression and the right to take part in public life, can continue to be meaningfully exercised online without hindrance, the aforementioned resolutions underscore that the Internet is a common resource, which is global, open and interoperable, and that Internet governance should preserve such right-friendly features.[31]

The second proposition is that states should actively facilitate safe access for individuals to the Internet.[32] This proposition is based on the insight that cyberspace is becoming an increasingly important arena for enjoying human rights[33] and that the digital divide and problems of digital illiteracy are leaving behind large numbers of individuals.[34] In the same vein, states are expected to address online security concerns,[35] so as to ensure that the Internet is a safe and trustworthy environment, where individuals are able to freely operate and enjoy their rights.[36] To that effect, states need to curb abusive practices that infringe on the rights of Internet users.[37] Among the potential abuses that the resolutions mention, one finds intrusive online surveillance activities[38] undertaken by state agencies without effective oversight mechanisms,[39] entailing the

[29] GA Res. 71/199, *supra* note 16, para. 5(f)–(g), para. 6. Notably, this resolution explicitly addresses the duties imposed on private technology companies; see also GA Res. 69/166, *supra* note 16, at 3; HRC Res. 28/16, 26 March 2015, at 3.

[30] GA Res. 71/199, *supra* note 16, at 3.

[31] See, e.g., HRC 26/13, *supra* note 17, at 1–2.

[32] See, e.g., HRC 20/8, *supra* note 17, at 2, para. 3; HRC 26/13, *supra* note 17, at 2, para. 3.

[33] See, e.g., HRC 26/13, *supra* note 17, at 1–2; GA Res. 73/179, *supra* note 16, at 2–3.

[34] See, e.g., HRC 32/13, *supra* note 17, at 3, para. 4; GA Res 73/179, *supra* note 16, at 3.

[35] See, e.g., HRC 26/13, *supra* note 17, at 2, para. 5.

[36] *Ibid.*, at 2, para. 1.

[37] GA Res. 71/199, *supra* note 16, para. 5(f); GA Res. 69/166, *supra* note 16, para. 4(e).

[38] Other international human rights bodies have grappled extensively with the problems of online surveillance, including the Human Rights Committee and the special rapporteur for the right to privacy. See Seibert-Fohr, *Digital Surveillance, Meta Data and Foreign Intelligence Cooperation: Unpacking the International Right to Privacy* (2018), available at https://ssrn.com/abstract=3168711; Shany, *On-Line Surveillance in the Case-law of the UN Human Rights Committee* (2017), available at https://csrcl.huji.ac.il/people/line-surveillance-case-law-un-human-rights-committee; J.A. Cannataci, United Nations Special Rapporteur on the Right to Privacy, Draft Legal Instrument on Government Surveillance and Privacy, 10 January 2018, available at www.ohchr.org/Documents/Issues/Privacy/DraftLegalInstrumentGovernmentLed.pdf.

[39] GA Res. 68/167; GA Res. 69/166; GA Res. 71/199, *supra* note 16. HRC 28/16, *supra* note 30; HRC 32/13, *supra* note 17; see also OHCHR Privacy Report 2018, *supra* note 14, para. 33.

collection and interception of data,[40] the aggregation of metadata and the sale of personal data.[41] Such practices are abusive if they fail to comply with principles of necessity, proportionality, non-arbitrariness and lawfulness.[42] Other abuses noted in the resolutions are online incitement,[43] online harassment of human rights defenders[44] and the purposeful disruption of access to information online.[45]

The third normative proposition is that the protection of digital human rights and human rights-friendly Internet governance must involve states as well as other relevant stakeholders, mainly private corporations, civil society and academia. All resolutions encourage multi-stakeholder engagement to promote digital human rights and call on states to engage with the relevant stakeholders in order to protect human rights online and address the challenges posed for human rights by new communication technology.[46] They also refer to the concept of corporate responsibility and call on companies to meet their responsibilities under the Guiding Principles on Business and Human Rights.[47] Still, the precise nature of this responsibility, and the remedies it entails, remains vague.[48]

Though neither the GA nor HRC resolutions are binding, they reflect a growing awareness by global political and legal elites of the importance of respecting international human rights in an online environment and indicate some willingness by states to take steps to address the unique threats and challenges for human rights found in cyberspace. Another indication of the growing attention paid by the UN to human rights in cyberspace has been the appointment in 2015 by the HRC of the first ever special rapporteur on the right to privacy, whose work focuses on the interpretation and application of the right to privacy in the digital age.[49] The special rapporteur has reiterated the GA's concerns about the significant gap between the existing legal

[40] GA Res. 69/166, *supra* note 16, at 2.

[41] GA Res. 71/199, *supra* note 16, at 3.

[42] GA Res. 71/199, *supra* note 16, at 2; GA Res. 69/166, *supra* note 16, at 2; HRC 28/16, *supra* note 30, at 2; see also Cheung and Weber, 'Internet Governance and the Responsibility of Internet Service Providers', 26 *Wisconsin International Law Journal* (2008) 403; K. Kittichaisaree, *Public International Law of Cyberspace* (2017), at 1–22.

[43] HRC 26/13, *supra* note 17, at 2, para. 6.

[44] GA Res. 71/199, *supra* note 16, at 4; see also HRC 28/16, *supra* note 30.

[45] HRC 32/13, *supra* note 17, at 2.

[46] GA Res. 71/199, *supra* note 15, at 2; GA Res. 69/166, *supra* note 15, at 3; HRC 32/13, *supra* note 16, *at* 3; HRC 26/13, *supra* note 17, at 2; HRC 32/13, *supra* note 17, at 3.

[47] HRC, Guiding Principles on Business and Human Rights, UN Doc. A/HRC/17/31, 16 June 2011; see also GA Res. 69/166, *supra* note 16, at 3; GA Res 71/199, *supra* note 16, para. 6.

[48] Ronen, 'Big Brother's Little Helpers: The Right to Privacy and the Responsibility of Internet Service Providers', 31 *Utrecht Journal of International and European Law* (2015) 72; see also Miletello, 'Page You are Attempting to Access Has Been Blocked in Accordance with National Laws: Applying a Corporate Responsibility Framework to Human Rights Issues Facing Internet Companies', 11 *Pittsburgh Journal of Technology Law and Policy* (2011) 1, at 64–65; Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Report on Online Content Regulation (SR Expression 2018), UN Doc. A/HRC/38/35, 6 April 2018, at 19–20, paras. 64–72 (calling for 'radical transparency and meaningful accountability', including public and information and communications technology sector accountability mechanisms).

[49] HRC 28/16, *supra* note 30, para. 4.

framework for the protection of the right to privacy and contemporary challenges.[50] For example, he noted with concern that, in the era of big data, information no longer needs to be 'personalized' in order to identify specific individuals.[51]

It is precisely because of this significant gap between legal regulation and the power of technology that the special rapporteur has criticized the over-reliance on normative equivalency that is found in the UN resolutions on digital human rights. According to the special rapporteur, the notion that individuals have the same offline and online rights is not sufficiently developed and fails to provide practical answers to many contemporary challenges to online privacy.[52] There is thus an urgent need, he has maintained, for developing a comprehensive international legal framework that would provide suitable normative guidelines for the protection of the right to privacy in the digital age.[53]

B *The Challenge of Applying a Normative Equivalency Paradigm*

The normative equivalency paradigm, which is at the front and centre of the approach taken by the GA and the HRC *vis-à-vis* the protection of the rights of online users, is premised on the adaptability of human rights norms that have been developed in the offline world to an online environment. This approach has been increasingly challenged, however, by scholars and practitioners. The challenge is not directed against the propriety of any extension of offline human rights to cyberspace – there is clearly a justification for extending most offline rights to online users; rather, it is the automatic and uncritical nature of the extension that has been questioned.

There is a vast literature on the unique attributes of the online environment and the difficulties in applying national and international law to cyberspace.[54] This literature lays out, among other things, the unique needs and interests of online users and the new threats and challenges they confront as well as the radically different configuration of power and control in the digital ecosystem. Whereas national and international legal systems are built around the principle of territorial sovereignty, which delineates the regulatory powers of each state (subject to a number of extraterritorial exceptions), the de-territorialized nature of cyberspace and the global reach of online services, products and transactions creates a haunting regulatory challenge.[55] Although the obligations of states under international human rights law apply extraterritorially, such application is still largely linked to notions of effective control over

[50] SR Privacy 2018, *supra* note 23, at 26–28.

[51] *Ibid.*, at 12, para. 54; at 25, para. 5.

[52] *Ibid.*, at 26, para. 6; at 29, para. 28.

[53] *Ibid.*, at 8–9, paras. 29–31.

[54] See, e.g., Zimmermann, 'International Law and "Cyber Space"', 3(1) *ESIL Reflections* (2014) 1, at 6; see also Mačák, 'From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers', 30 *Leiden Journal of International Law* (2017) 877.

[55] Schmitt, 'Grey Zones in the International Law of Cyberspace', 42(2) *Yale Journal of International Law Online* (2017) 1; Kohl, 'Jurisdiction in Cyberspace', in N. Tsagourias and R. Buchan (eds), *Research Handbook on International Law and Cyberspace* (2015) 30; Heintschel von Heinegg, 'Territorial Sovereignty and Neutrality in Cyberspace', 89 *International Law Studies* (2013) 17.

territory or the direct and reasonably foreseeable impact over the enjoyment of personal rights, and it does not lead to the sweeping imposition on states of obligations to protect the rights of individuals located in other countries.[56]

Add to that the fact that cyberspace is a decentralized sphere of activity dominated by private actors, not governments, that provide services, interact with users and enforce terms of service. Under these circumstances, focusing on governments as the principal duty-bearers, as international human rights law normally does, creates a wide gap between the ambitious protective agenda underlying international human rights law and a reality in which states exercise direct power over individuals and technology companies only in some distinct fields of online activity. Note that, even as regulators of online activity, the role of states is often marginal in practice, as some technology companies are exceptionally powerful entities, much better situated than states to regulate online conduct. The actual configuration of power, control and authority in cyberspace, where technology companies sometimes serve as a buffer against governmental abuse of power,[57] should also arguably influence the way in which offline human rights are adjusted for application online.[58]

The upshot of these considerations is that a significant gap exists between the conditions in the offline and online environments and that such a gap may render the automatic and uncritical extension of rights from one environment to the other – that is, the normative equivalency paradigm – 'hopelessly inadequate'.[59] As we further claim below, this notion of inadequacy appears to support the development of new digital human rights, liberated from the shadow of offline human rights, since the latter are ill-equipped to afford effective protection of the full gamut of needs and interests of online users.

3 Developing New Digital Rights for Cyberspace

A *The Desirability of Creating New Human Rights*

The doubts surrounding the adequacy of the normative equivalency paradigm for effectively protecting human rights online[60] and the related efforts to develop new digital human rights[61] invite a normative inquiry: under what conditions should new

[56] International Covenant on Civil and Political Rights (ICCPR) 1966, 999 UNTS 171, Art. 2(1); Human Rights Committee, General Comment no. 36 Article 6: Right to Life, UN Doc. CCPR/C/GC/36, 30 October 2018, at 63, para. 22. See generally M. Milanovic, *Extraterritorial Application of Human Rights Treaties: Law, Principles, and Policy* (2011).

[57] SR Expression 2017, *supra* note 26, para. 82; Ronen, *supra* note 49, at 72.

[58] Cheung & Weber, *supra* note 43, at 408–412.

[59] See note 23 above.

[60] Joyce, *supra* note 12, at 273; Shany, *supra* note 22.

[61] Mathiesen, 'Human Rights for the Digital Age', 29 *Journal of Mass Media Ethics* (2014) 2; Deeks, 'An International Legal Framework for Surveillance', 55 *Virginia Journal of International Law* (2014) 291, at 295–298, 327–338; Thompson, *The Digital Age of Rights*, 26 May 2009, available at http://news.bbc.co.uk/2/hi/technology/8068463.stm.

digital human rights be developed for protecting online users? This question, in turn, invites a mapping of protection gaps in the existing legal framework. Such gaps may be filled, where appropriate, by new digital human rights. A complementary line of inquiry examines whether new digital human rights advocated by activists and experts in the field in response to new needs and interests can be effectively captured by the normative equivalency paradigm. Recognizing digital rights as human rights requires, in turn, an engagement with key questions under the theory of human rights, including what generalizable claims or social practices qualify to be worthy of protection as 'human rights'[62] and under what conditions do justifications in support of recognizing new human rights lead to the adoption of binding norms under international law.[63] From another perspective, the debate over online human rights poses the question of the elasticity of human rights norms: to what extent are they evolving norms that can change over time, in accordance with the changing needs of society?[64]

Responding in full and in earnest to such fundamental normative questions exceeds the scope of this article. Rather, our goal is to describe and analyse some of the actual tensions holding between existing human rights norms and the new needs and interests of online users as well as offering a typology for actual processes of social recognition of new digital human rights[65] – that is, categorizing efforts made by state and non-state actors to positively acknowledge digital human rights by way of reinterpreting existing legal instruments or formulating new ones. Nevertheless, the sociological and normative dimensions of the debate over recognizing new digital human rights are not fully divorced from one another since the process of social recognition is inextricably tied to the acceptance by norm makers that there exists a moral justification for protecting new needs and interests as well as an awareness of the risk of an abuse of power in the absence of a recognized human right (a concern that is often based on historical experiences of exploitation and injustice).[66] Theories justifying the emergence of new human rights can therefore assist in understating the motivations of state and non-state actors for recognizing new digital human rights.

What would then motivate norm makers to support the recognition of new digital rights, such as the right of access to the Internet and a right not to be subject to an automated decision, as opposed to viewing them as mere conditions for realizing existing human rights? The question of what justifies the development of a new human

[62] R. Dworkin, *Taking Rights Seriously* (5th edn, 1978); J. Rawls, *A Theory of Justice* (rev. edn, 1999).

[63] Beitz, 'What Human Rights Mean', 132 *Daedalus* (2003) 36; see also Moravcsik, 'The Origins of Human Rights Regimes: Democratic Delegation in Postwar Europe', 54 *International Organization* (2000) 217; Henkin, 'International Human Rights as Rights', 1 *Cardozo Law Review* (1979) 425.

[64] Raz, 'Legal Rights', 4 *Oxford Journal of Legal Studies* (1984) 1; Pennock, 'Rights, Natural Rights, and Human Rights: A General View', 23 *Nomos* (1981) 1.

[65] Coleman, 'Negative and Positive Positivism', 11 *Journal of Legal Studies* (1982) 139, at 139–140, 150–151.

[66] Glendon, 'Knowing the Universal Declaration of Human Rights', 73 *Notre Dame Law Review* (1998) 1153; see also Cassese, 'A Plea for a Global Community Grounded in a Core of Human Rights', in A. Cassese (ed.), *Realizing Utopia: The Future of International Law* (2012) 136, at 136–137; Donoho, 'Relativism versus Universalism in Human Rights: The Search for Meaningful Standards', 27 *Stanford Journal of International Law* (1991) 345, at 357.

right remains unresolved both in legal theory as well as in actual state practice.[67] Such uncertainty appears to reflect the open-endedness of the term 'human rights' itself.[68] The literature on the theory of human rights offers two principal approaches – normative and sociological – to justifying or explaining the emergence of human rights. The normative approach has its roots in natural rights theory[69] and in the Kantian notion of human dignity.[70] It has been linked more recently to the notion of 'human capabilities'.[71] The theories of rights developed under these philosophical schools tend to associate certain needs or interests with an inherent human condition and a universal human experience. Satisfaction of basic human needs or interests or validation of practices protecting them can be justified on the basis of pre-political or extra-legal moral principles ('a right that we have simply in virtue of being human').[72] Legal standards that give expression to such principles derive their legitimacy primarily from their underlying moral justification.[73]

A second approach found in the theory of rights concentrates on sociological processes of recognition, which often entail legal validity. For example, international human rights law norms are understood as 'human needs that have received formal recognition as rights through the sources of international law'.[74] Under a sociological approach, moral convictions or intuitions, human experience, actual protection gaps and the political expediency in legitimizing political power through demonstrating commitment to human rights serve as possible motivations for norm makers to confer upon certain claims the status of human rights. Once recognized in law, human rights can be defended on the basis of a formal legal consideration – their validation under one of the methods by which law is created.[75]

Recognizing new human rights, however, meets two principled objections. First, the proliferation of human rights has been criticized for leading to the dilution of existing rights ('when everything is a human right nothing is').[76] Second, if, according

67 Beitz, *supra* note 64, at 37.

68 J. Griffin, *On Human Rights* (2008), at 15; see also Harel, 'Theories of Rights', in M.P. Golding and W.A. Edmundson (eds), *The Blackwell Guide to the Philosophy of Law and Legal Theory* (2005) 191.

69 J. Locke, 'Of the State of Nature', in *Two Treaties of Government* (1963); J. Finnis, *Natural Law and Natural Rights* (1980), at 210–221.

70 Kant, 'Groundwork of the Metaphysics of Moral', in P. Guyer and A.W Wood (eds), *The Cambridge Edition of the Works of Immanuel Kant: Practical Philosophy* (1992), at 433–435; see also Tesón, 'The Kantian Theory of International Law', 92 *Columbia Law Review* (1992) 53.

71 M.C. Nussbaum and A. Sen, *The Quality of Life* (1993).

72 Griffin, *supra* note 69, at 16.

73 *Ibid.*, at 11–13; see also Verdirame, 'Human Rights in Political and Legal Theory', in S. Sheeran and N. Rodley (eds), *Routledge Handbook of International Human Rights Law* (2014) 25, at 25–35.

74 Marks, 'Emerging Human Rights: A New Generation for the 1980s', 33 *Rutgers Law Review* (1981) 435, at 453.

75 J. Raz, *The Authority of Law: Essays on Law and Morality* (2nd edn, 1979); see also Bix, 'Legal Positivism' in M.P. Golding and W.A. Edmundson (eds), *The Blackwell Guide to the Philosophy of Law and Legal Theory* (2005) 29; Sheeran, 'The Relationship of International Human Rights Law and General International Law: Hermeneutic Constraint, or Pushing the Boundaries?', in Sheeran and Rodley, *supra* note 74, 79, at 100–101.

76 S. Kaplan, 'When Everything Is a Human Right, Nothing Is', *Foreign Policy* (2019), available at https://foreignpolicy.com/2019/09/06/when-everything-is-a-human-right-nothing-is; Cranston, 'Human Rights Real and Supposed', in M.E. Winston (ed.), *The Philosophy of Human Rights* (1989) 121, at 121–128.

to normative theories of rights, human rights have intrinsic moral value, which is pre-political, universal, timeless and derivative from basic aspects of the human condition or experience,[77] it is difficult to accept that new human rights can suddenly emerge in response to political or technological developments.[78] Still, practice shows that states and non-state actors have often supported the creation of new rights through allusion to the instrumental need for responding to change in order to ensure the continuing relevance of human rights norms and the effective protection of individuals against new threats to their basic needs and interests.[79] Like 'living instrument' interpretation doctrines, it has been asserted that human rights law has to evolve in order to correspond to changing societal conditions.[80]

Indeed, declining to recognize new human rights notwithstanding changes in society brought about by new technology might result in protection gaps, which could indirectly discourage certain activities for no particular good reason. For example, in the digital human rights context, failing to adjust political rights to conditions in cyberspace – including through the creation of new rights, if necessary – might result in privileging traditional offline political activism at the expense of new forms of online activism. Furthermore, it has been claimed that even the Universal Declaration of Human Rights itself has already included some elements responding to the particular contemporaneous needs of industrialized societies, such as technical education, trade unions or social security.[81] We can therefore posit that, whereas, on the moral plane, human rights might have certain immutable features, such as liberty or dignity, the decision to recognize human rights in any given political or legal context tends to be responsive to changing circumstances, to evolving societal conditions and to new technologies.

The position that human rights law should respond to new developments is further reinforced by the fact that international human rights instruments have been evolving continuously in the post-World War II era, becoming more and more specific in their legal provisions in response to new needs and interests and new forms of oppression and injustice.[82] In the same vein, the adoption of specific legal instruments using the language of rights to protect and promote online activity suggests that the process of developing new digital human rights has already begun. Some regional treaties, such as the Budapest Convention on Cybercrime,[83] the European Union (EU)

77 Griffin, *supra* note 69, at 10; Beitz, *supra* note 64, at 37–38; Wang, 'Time to Think About Human Right to the Internet Access: A Beitz's Approach', 6 *Journal of Politics and Law* (2013) 67.

78 Alston, 'Conjuring Up New Human Rights: A Proposal for Quality Control', 78 *American Journal of International Law* (*AJIL*) (1984) 607, at 607–609.

79 *Ibid.*

80 Beitz, *supra* note 64, at 38; see also Marks, *supra* note 78, at 440, 451–452.

81 Beitz, *supra* note 64, at 43; Universal Declaration of Human Rights, GA Res. 217A (III), 10 December 1948.

82 Sheeran and Rodley, 'The Broad Review of International Human Rights Law', in Sheeran and Rodley, *supra* note 74, 3.

83 Convention on Cyber Crime, 23 November 2001, 185 ETS (entered into force 1 July 2004); see also the older, but highly relevant, Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, 28 January 1981, 108 ETS (entered into force 1 October 1985).

General Data Protection Regulation (GDPR)[84] and the African Union Convention on Cyber Security and Personal Data Protection,[85] use the language of human rights in connection with the regulation of digital technology, as have the UN resolutions described in Section 2 of this article.[86] Scholars have also been calling for the elaboration of new international legal instruments on digital rights, which would include specific language on the application of traditional human rights in cyberspace.[87]

Such developments can be explained as reflecting growing acceptance by state and non-state actors of the moral significance of the needs and interests protected under digital human rights, the risk that those in power would unjustifiably deny or restrict the exercise of such rights and the practical utility of protecting them through a new legal instrument. Some of the relevant initiatives also appear to be informed by an interest in legitimizing Internet governance by presenting it as human rights friendly in nature.

The process of developing new digital human rights through international law is not free from other controversies as well.[88] One pragmatic concern is that developing new rights and departing from the normative equivalency paradigm might be regarded as throwing into question the application of existing international human rights law norms to online activity,[89] notwithstanding the interpretive efforts applied by international treaty monitoring and other international law-interpreting and law-applying bodies.[90] Another concern is that the project of creating new rights at the international level siphons away attention from the need to develop just and politically acceptable cyber-governance structures and to strengthen accountability mechanisms and institutions.[91] Still, as the following sections show, the wider the distance is between traditional human rights and the challenges of the digital space, the greater the pressure is on existing human rights norms and institutions to adapt in order to accommodate the needs and interests of online users. Without specific standard-setting efforts, which acknowledge the unique problems, opportunities and structures of power holding in cyberspace, traditional human rights law might bend through drastic reinterpretation beyond its breaking point and cease to serve as a widely accepted normative framework for the digital age.

B *International Initiatives for Enumerating Digital Human Rights*

The process of developing new digital human rights is not completely novel. In the last three decades, a variety of international and regional initiatives have sought to

[84] Council Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR), OJ 2016 L 119.

[85] African Union Convention on Cyber Security and Personal Data Protection, 27 June 2014, 23rd Session of the Assembly, Equatorial Guinea.

[86] See notes 16 and 17 above.

[87] See note 62 above; see also Draft Legal Instrument on Surveillance and Privacy, *supra* note 39.

[88] Tully, *supra* note 21, at 180–185; Mathiesen, *supra* note 62, at 4–7; Fidler *supra* note 10, at 107.

[89] Land, *supra* note 15, at 400–410.

[90] Seibert-Fohr, *supra* note 39, at 11.

[91] Mihr, *supra* note 26, at 25.

promote the recognition of online rights, with a view to influencing Internet regulation, the configuration of the online ecosystem and data protection practices.[92] The documents formulated pursuant to such initiatives were sometimes referred to as a 'digital bill of rights'.[93] In addition, several studies were conducted in recent decades in an attempt to further advance the development of digital human rights on the international plane.[94]

One of the most notable initiatives that have emerged in recent years is the World Summit on the Information Society's (WSIS) 'Declaration of Principles'. This is a declaration of 67 principles,[95] developed under the auspice of the UN[96] between the years 2003 and 2005, through fora in which 175 states participated.[97] The WSIS Declaration tried to offer a framework for a 'common vision of the information society', which reaffirms respect for human rights, their interdependence and mutually reinforcing nature.[98] Specifically, the WSIS Declaration reaffirms Article 19 of the International Covenant on Civil and Political Rights (ICCPR) (right to freedom of opinion and expression) and emphasizes that communication is a basic human need that is central to the 'information society'.[99] According to the declaration, there is a need to enhance an institutional and legal environment that would facilitate the existence of a 'trust framework', network security, privacy protection and a framework for reducing digital divides.[100]

[92] Gill, Redeker and Gasser, *supra* note 10, at 5–10. In their research, they review a collection of 30 initiatives – for example, NETmundial, a global multi-stakeholder meeting on the future of Internet governance, 23–24 April 2014, available at http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf; Electronic Frontier Foundation, A Bill of Privacy Rights for Social Network Users, 19 May 2010, available at www.eff.org/deeplinks/2010/05/bill-privacy-rights-social-network-users; Association for Progressive Communications, Internet Rights Charter, November 2006, available at www.apc.org/sites/default/files/APC_charter_EN_0_1_2.pdf; United Nations Special Rapporteur on Freedom of Opinion and Expression, Organization of American States, Organization for Security and Co-operation in Europe, African Commission on Human and Peoples' Rights on Human and Peoples' Rights, Joint Declaration on Freedom of Expression and the Internet – International Mechanisms for Promoting Freedom of Expression, 1 June 2001, available at www.oas.org/en/iachr/expression/showarticle.asp?artID=848&lID=1; Organization for Economic Co-operation and Development, Communiqué on Principles for Internet Policy-Making, June 2011, available at www.oecd.org/internet/innovation/48289796.pdf.

[93] Davies, 'Digital Rights and Freedoms: A Framework for Surveying Users and Analyzing Policies', in M. Aiello and D. McFarland (eds), *Social Informatics: Proceedings of the 6th International Conference* (2014) 1, at 1–2.

[94] *Ibid.*, at 8–10.

[95] ITU, Declaration of Principles, Building the Information Society: A Global Challenge in the New Millennium (WSIS Declaration of Principles), 12 December 2003, available at www.itu.int/net/wsis/docs/geneva/official/dop.html.

[96] GA Res. 56/183, 31 January 2002.

[97] WSIS Declaration of Principles, *supra* note 96; the first phase of the summit summary, available at www.itu.int/net/wsis/geneva/index.html; see also A. Murray and M. Klang, *Human Rights in the Digital Age* (2004), at 5.

[98] WSIS Declaration of Principles, *supra* note 96, paras 1–3.

[99] *Ibid.*, para. 4. ICCPR, *supra* note 57.

[100] WSIS Declaration of Principles, *supra* note 96, paras 10, 35.

Another notable initiative is the Charter of Human Rights and Principles for the Internet.[101] This charter is a collaborative initiative undertaken by two multi-stakeholder frameworks – the Internet Rights and Principles Coalition and the Internet Governance Forum – which was established following the WSIS forum.[102] The Charter introduces a list of rights and principles, aiming to provide a framework for 'upholding and advancing human rights for the online environment'.[103] Interestingly, the initiative defines 'rights' as international human rights that have been translated to a normative vocabulary relevant for the Internet.[104] 'Principles' are defined as features of the system that are required to support the realization of human rights.[105] Several studies conducted in order to analyse international digital human rights initiatives have tried to identify several core rights (or principles) that are frequently included in them.[106] Among the rights identified, one can mention the following:

- online privacy and data protection (including encryption);[107]
- data portability;[108]
- right to be forgotten;[109]
- right to access the Internet;[110]
- right to free online expression (which includes protection from hate speech);[111]
- right to net neutrality;[112]
- right to network equality and non-discrimination; and[113]
- right to Internet security and cyber-security.[114]

[101] The Internet Rights and Principles Dynamic Coalition (IRPC) and the Internet Governance Forum (IGF), The Charter of Human Rights and Principles for the Internet (IRPC Charter) (2014), available at https://www.ohchr.org/Documents/Issues/Opinion/Communications/InternetPrinciplesAndRightsCoalition.pdf.

[102] ITU, The Tunis Agenda for the Information Society, UN Doc. WSIS-05/TUNIS/DOC/6(Rev.1)-E, 18 November 2005, at 18, para. 72 (the second phase of the WSIS took place in Tunis on 16–18 November 2005; The Tunis Agenda for the Information Society provides the mandate for the IGF; see also Internet Governance Forum (2006), available at www.intgovforum.org/multilingual/ (the IGF is a forum for multi-stakeholder dialogue on public policy issues related to key elements of Internet governance issues, such as the Internet's sustainability, robustness, security, stability and development. The UN Secretary-General formally announced the establishment of the IGF in July 2006, and the first meeting was convened in October/November 2006).

[103] IRPC Charter, *supra* note 102, at 2.

[104] *Ibid.* ('[h]uman rights are international human rights as defined by international law. We have translated these directly to the internet with provisions such as freedom from blocking and filtering').

[105] *Ibid.* ('[b]y "Principles" we are talking about those internet policy principles or implementation principles that describe features of the system which are required to support human rights, these can be identified by the use of language such as "shall" and "must"').

[106] Davies, *supra* note 94.

[107] *Ibid.*, at 3; see also IRPC Charter, *supra* note 102, at 7.

[108] Davies, *supra* note 94, at 4; see also GDPR, *supra* note 85, Art. 20.

[109] Davies, *supra* note 94, at 4.

[110] *Ibid.*, at 6; see also IRPC Charter, *supra* note 102, at 7; Davies, *supra* note 94, at 6.

[111] IRPC Charter, *supra* note 102, at 16.

[112] Davies, *supra* note 94, at 7.

[113] *Ibid.*

[114] *Ibid.*

An overview analysis of digital initiatives, conducted at Harvard University's Berkman Center, suggests that proposed digital human rights can be grouped into seven categories: (i) basic or fundamental rights and freedoms; (ii) general limits on state power; (iii) Internet governance and civic participation; (iv) privacy rights and surveillance; (v) access and education; (vi) openness and stability of networks; and (vii) economic rights and responsibilities.[115] The typology of 'generations' that we propose in Section 4, however, is different and builds on the genealogy of digital human rights and on their normative distance from traditional human rights.

C *Private Initiatives on Digital Human Rights*

The call to develop a new human rights framework for the online environment is also echoed, at least to some extent, by initiatives undertaken by certain private technology companies. Such companies manage and, at times, own the digital platforms on which human rights are exercised, and they often find themselves subject to competing pressures: online users – their customers – demand effective protection of their basic rights, whereas governments wish to utilize online platforms to obtain information on individuals and groups in order to control and suppress activities on cyberspace which they consider to be harmful or unlawful.[116] In situations of this kind, technology companies must decide whether and how to adjust their terms of service to applicable or prospective governmental regulation.[117] Since technology companies operate across multiple jurisdictions with widely divergent laws, it is difficult for them to adopt general business standards and practices that are compatible with all relevant domestic laws and regulations.[118]

In light of the normative uncertainty and regulatory instability surrounding the application of digital human rights, it is not surprising that some international initiatives for developing international standards have emerged from processes that heavily involve private actors. Recent examples include the Toronto Declaration on Machine Learning Standards, which calls on both governments and private companies to ensure that algorithms respect basic principles of equality and non-discrimination;[119] a variety of instruments created under the auspices of the Internet Corporation for Assigned Names and Numbers, which are directed at protecting human rights online;[120] and other multi-stakeholder initiatives on international Internet governance,

[115] Gill, Redeker and Gasser, *supra* note 10, at 6–10. Other initiatives suggest to add a group of principles that relates to software freedom – for example, the ability to modify a code in software platform or the possibility of participatory design. See Davies, *supra* note 94.

[116] Miletello, *supra* note 49.

[117] SR Expression 2018, *supra* note 49, at 19.

[118] *Ibid.*, at 4–6; see also Kittichaisaree, *supra* note 43, at 49–50, 95–97; Zimmermann, *supra* note 55, at 6.

[119] Access Now and Amnesty International, The Toronto Declaration: Protecting the Right to Equality and Non-Discrimination in Machine Learning Systems (2018), available at www.accessnow.org/the-toronto-declaration-protecting-the-rights-to-equality-and-non-discrimination-in-machine-learning-systems/.

[120] The Internet Corporation for Assigned Names and Numbers, Human Rights Impact Assessment (2019), available at www.icann.org/en/system/files/files/summary-report-hria-15may19-en.pdf; see also Fidler, *supra* note 10, at 116.

alluding to human rights as the core guiding principles.[121] These initiatives underscore the growing support among a multiplicity of stakeholders for the need to better define the digital human rights framework and to develop human rights-friendly policies that would be specifically adapted for cyberspace.[122]

The upshot of this short survey of recent standard-setting initiatives is that there is a broad consensus around the notion that international human rights law can provide a normative framework for protecting the needs and interests of online users.[123] There is also a broad consensus that much work remains to be done in order to overcome the challenges of transposing offline human rights to an online environment. Two particularly difficult structural challenges that stand out in this regard are digital divides across and within countries[124] and the lack of transparency in corporate decision-making and software design.[125] At the same time, there is also a strong sentiment that new technologies can assist in promoting respect for human rights – for example, by creating new spaces for personal and political expression and by harnessing big data and artificial intelligence (AI) to generate a more accurate picture of human rights violations and risks of violations.[126]

D *A Proposed Typology: Three 'Generations' of Digital Human Rights*

The efforts to extend offline human rights norms to activities in cyberspace on the basis of the normative equivalency paradigm have encountered difficulties due to the unique attributes of cyberspace, which affect the ways in which human rights are enjoyed or can be abused. At a deeper level, however, a major flaw of the normative equivalency paradigm appears to be its approach to digital technology as a new tool or arena for exercising offline rights or governmental powers, as opposed to a conceptualization of digital space as giving rise to a new human condition and governance domain.[127]

Pursuant to the normative equivalency paradigm, access to the Internet, for example, comes squarely under the protection of the right to freedom of expression (Article 19 of the ICCPR) because the Internet is a medium that facilitates seeking, receiving and imparting information and ideas. A freedom of expression framework captures, however, only a small fraction of the needs and interests of online users and

[121] See note 93 above; see also Christchurch Call to Eliminate Terrorist and Violent Extremist Content Online, available at www.christchurchcall.com/index.html.

[122] OHCHR Privacy Report 2018, *supra* note 13, paras 48–49.

[123] Mihr, *supra* note 26, at 24–26; see also SR Expression 2018, *supra* note 49, at 14, 20, paras 41, 70.

[124] ITU, Digital Inclusion for All, November 2019, available at www.itu.int/en/mediacentre/backgrounders/Pages/digital-inclusion-of-all.aspx ('about half the world's people access and use the Internet. The other half do not'); see also Murray & Klang, *supra* note 98, at 5.

[125] SR Expression 2017, *supra* note 26, paras 7, 82; see also Penney *et al.*, 'Advancing Human Rights-by-Design in the Dual-Use Technology Industry', 71 *Journal of International Affairs* (2018) 103.

[126] Arnaud, 'Opportunities in the New Digital Age', *UN Refugee Agency (UNHCR) Blog* (2017), available at www.unhcr.org/blogs/opportunities-in-the-new-digital-age/; Frey and Gatzweiler, *How Tech Can Bring Dignity to Refugees in Humanitarian Crises* (2018), available at https://theconversation.com/how-tech-can-bring-dignity-to-refugees-in-humanitarian-crises-94213.

[127] See, e.g., Thwaites, 'Technologizing the Human Condition: Hyperconnectivity and Control', 53(4) *Educational Philosophy and Theory* (2020) 1, at 8.

the threats posed to them by abusive exploitation of the Internet by malicious actors. Nor does it fully accommodate the unique ethical, legal and policy challenges that arise out of the new ubiquitous space of the Internet where completely new forms of social interactions and relationships of power occur[128] and for which new vocabularies of rights and new categories of right holders and duty holders need to be developed. The limited 'fit' between traditional human rights, and the reality of digital technology, underlies past and current attempts to develop new digital human rights.

We propose a framework based on three sets of actual responses to the unique challenges to existing international human rights law posed by digital technology: the radical reinterpretation of existing rights; the development of new digital rights; and the recognition of new right holders and duty holders. We maintain that these sets of responses tend to develop consecutively and that they represent a process of incremental divergence from traditional international human rights law; they are also embraced at varying degrees of acceptance by major state and non-state actors. The gradual movement from the traditional human rights framework to an increasingly novel digital human rights framework permits us to refer to these three modalities as different 'generations' of digital human rights law in ways that somewhat mirror Karel Vašák's famous conceptualization of the genealogy of international human rights law.[129]

The first generation of digital human rights is still premised on the normative equivalency paradigm. It comprises far-reaching interpretations of existing human rights law, which show awareness for the need for a significant recalibration of existing human rights norms with a view to rendering them suitable to protect new needs and interests in an online environment. Online content moderation and online privacy serve as prominent examples for such efforts for recalibration. The ability to disseminate hate speech online at a speed, scope, scale and ease not matched in the offline world, where traditional media outlets typically exercise editorial controls over mass circulation contents, has created a heightened risk of violence, social antagonism and discrimination.[130] In the same vein, the deliberate online dissemination of disinformation ('fake news') arguably contributes through algorithmic 'filter bubbles' to the emergence of distorted worldviews, seriously disrupting the 'market of ideas' on which democratic deliberation and public discourse are built.[131]

[128] See, e.g., Kerr and Barrigar, 'Privacy, Identity and Anonymity', in K. Ball, K. Haggerty and D. Lyon (eds), *Routledge Handbook of Surveillance Studies* (2012) 386, at 387.

[129] See Vašák, 'Human Rights: A Thirty-Year Struggle: The Sustained Efforts to Give Force of Law to the Universal Declaration of Human Right', 11 *UNESCO Courier* (1977) 29. For a discussion, see, e.g., Domaradzki, Khvostova and Pupovac, 'Karel Vasak's "Generations of Rights and the Contemporary Human Rights Discourse"', 20 *Human Rights Review* (2019) 423, at 424.

[130] See, e.g., HRC, Report of the Detailed Findings of the Independent International Fact-Finding Mission on Myanmar, UN Doc. A/HRC/39/CRP.2, 17 September 2018, at 339–342; Emma Irving, 'The Role of Social Media Is Significant: Facebook and the Fact Finding Mission on Myanmar', *Opinion Juris*, 7 September 2018, available at http://opiniojuris.org/2018/09/07/the-role-of-social-media-is-significant-facebook-and-the-fact-finding-mission-on-myanmar/; see also Christchurch Call, supra note 122.

[131] T. Nguyen, *Echo Chambers and Epistemic Bubbles* (2018), available at www.cambridge.org/core/journals/episteme/article/echo-chambers-and-epistemic-bubbles/5D4AC3A808C538E17C50A7C09EC706F0; see also note 6 above. But see Dubois and Blank, 'The Echo Chamber Is Overstated: The Moderating Effect of Political Interest and Diverse Media', 21 *Information, Communication and Society* (2018) 729.

Few, if any, equivalent phenomena can be found in the offline world. Applying traditional notions of freedom of expression with their narrow limitation provisions and associated high threshold for government interference to online speech is increasingly deemed inadequate to meet the grave risks posed by harmful online contents. Hence, human rights bodies find themselves in the unusual position of calling on governments and technology companies to engage in a form of censorship, through moderating or removing harmful online content and introducing new filtering mechanisms.[132] In this regard, the special rapporteurs for freedom of expression have explicitly called for applying Article 20 of the ICCPR, which requires the outlawing of certain forms of hate speech, and encouraged online platforms to develop practical and nuanced policies for countering online hate speech, incitement to violence and fake news.[133]

Online privacy concerns raise another set of technology-driven challenges, requiring a fundamental reassessment of existing legal doctrines, such as those distinguishing between data and metadata,[134] privacy safeguards in the private and public sphere (a question presented, for instance, by the use in public spaces of facial-recognition technology)[135] and anonymized and de-anonymized information[136] as well as doctrines regulating the encryption and decryption of data.[137] Arguably, effective protection of online privacy necessitates a radical departure from existing privacy laws.[138] Similar challenges, inviting the radical reinterpretation of existing international human rights law norms when applied online, can be found with respect to other human rights as well, including the right to take part in public affairs (for example, with respect to 'following' public officials' social media accounts)[139] and the right to security of person (for example, with respect to cyberbullying).[140]

[132] Council of Europe, Committee of Ministers, Recommendation to Member States on Measures to Promote the Respect for Freedom of Expression and Information with Regard to Internet Filters, Doc. CM/Rec (2008)6, para. I(xi); Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Report on the Right to Freedom of Opinion and Expression Exercised through the Internet (SR Expression 2011), UN Doc. A/66/290, 10 August 2011, at 22, para. 82; SR Expression 2019, *supra* note 7, paras 29–33; see also HRC, Report of the Special Rapporteur on the Sale of Children, Child Prostitution and Child Pornography: Mission to Kyrgyzstan, UN Doc. A/HRC/25/48/Add.1, 26 April 2013; Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Report on the Regulation of Online 'Hate Speech'(SR Expression 2019 (Regulation of Online 'Hate Speech'), UN Doc. A/74/486, 9 October 2019, at 14–15, paras 35–38.

[133] *Ibid.*, at 23, para. 58(b); see also SR Expression 2017, *supra* note 26, para. 77.

[134] OHCHR, The Right to Privacy in The Digital Age (OHCHR Privacy Report 2014), UN Doc. A/HRC/27/37, 30 June 2014, at 6–7, paras 18–20; see also Seibert-Fohr, *supra* note 39, at 12–13.

[135] OHCHR Privacy Report 2018, *supra* note 14, at 3–5, paras 6–7, 14.

[136] Report of the Special Rapporteur on the Right to Privacy (SR Privacy 2017), UN Doc. A/72/43103, 19 October 2017, at 20, para. 103.

[137] See, e.g., Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Follow-up Report on Encryption and Anonymity, UN Doc. A/HRC/38/35/Add.5, 13 July 2018, at 12, paras 29–31; see also OHCHR Privacy Report 2018, *supra* note 14, at 6, para. 20.

[138] SR Privacy 2017, *supra* note 137, at 26, para. 131(j); see also SR Privacy 2018, *supra* note 23, at 3–4, paras 2–7.

[139] *Knight First Amendment Institute at Columbia University v. Trump*, 18-1691 US 1 (2nd Cir., 2019).

[140] See, e.g., Parliamentary Assembly of the Council of Europe (PACE), Committee on Culture, Science, Education and Media, Internet Governance and Human Rights Report, 4 January 2019, at 15.

The second generation of digital rights represents a conscious attempt to steer norm makers away from the normative equivalency paradigm towards developing new international human rights law norms that have no close parallels in the offline world. Although these new digital human rights typically have one or more 'parent' offline rights, they protect unique needs and interests that are not fully and adequately covered by the parent right. Most of these rights are still in the development stage and have gained limited recognition as *lex lata* in international human rights law. Still, several of these digital rights have already found expression in specific international regimes, such as EU law, or in the domestic law of certain states. Other second-generation rights have been advocated in the academic literature and in documents laying down elements of *lex ferenda*. Indeed, many of the rights found in the digital rights initiatives surveyed above belong to this category of rights.

The development of second-generation rights is typically supported on the basis of one of two justifications or both of them: (i) the failure of existing human rights to effectively protect the needs and interests of online users, whose significance in the online world far exceeds their significance in the offline world and (ii) the emergence of new needs and interests that have no parallels in the offline world. The right to access the Internet, which is further discussed below, is a paradigmatic second-generation digital human right because the importance of access to the Internet for many online users in the digital age far exceeds the importance of access to traditional media for individuals in the offline world. Another example, also discussed below, is the emerging right not to be subject to automated decision-making (which has been embraced, to some extent, in the GDPR).[141] It is difficult to find a similar concern in the offline world; at most, one can draw some weak analogies to debates about a right to a jury of one's peers or the practice of deploying 'faceless judges'.[142]

Other potential rights that may be emerging as second-generation digital human rights include the right to data portability,[143] informational self-determination (that is, the ability to control one's online profile and personal data, including the right to be forgotten),[144] encryption[145] and cyber-security.[146] The importance of such rights in

[141] GDPR, *supra* note 85, Art. 22

[142] LaRue, 'A Jury of One's Peers', 33 *Washington and Lee Law Review* (1976) 841; Stockwell, 'A Jury of One's (Technically Competent) Peers?', 21 *Whittier Law Review* (2000) 645. On 'faceless judges', see Human Rights Committee, General Comment no. 32 on Article 14: Right to Equality before Courts and Tribunals and to a Fair Trial, UN Doc. CCPR/C/GC/32, 23 August 2007, para. 23; Human Rights Committee, *Becerra Barney v. Colombia*, UN Doc. CCPR/C/87/D/1298/2004, 11 July 2006, para. 7.2.

[143] GDPR, *supra* note 85, Art. 20; see also Swire and Lagos, 'Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique', 72 *Maryland Law Review* (2013) 335 (note that the writers refer to the right to data portability, which was included under Article 18 in the Draft General Data Protection Regulation from 2013).

[144] GDPR, *supra* note 85, Art. 17; see also Gill, Redeker and Gasser, *supra* note 11, at 8.

[145] W. Schulz and J. Hoboken, *Human Rights and Encryption* (2016), at 38.

[146] J. Kulesza and R. Balleste (eds), *Cybersecurity and Human Rights in the Age of Cyberveillance* (2016), at 1–17; see also Shackelford, 'Exploring the "Shared Responsibility" of Cyber Peace: Should Cybersecurity Be a Human Right?', Kelley School of Business Research Paper (2017), at 13–15, 38; IRPC Charter, *supra* note 102, at 15.

the online world may be roughly equated to the importance in the offline world of fundamental human rights, such as freedom of movement, the right to protect honour and reputation, the right to privacy and the right to security of person. Recognizing such rights as digital human rights can be justified on the basis of their fundamental importance for online users, the impossibility of effectively protecting them through traditional offline rights because of the lack of sufficiently close analogies in the offline world and the real risk posed to them by actual or potential abusive practices by state and non-state actors, including technology companies.

There are some indications that a third generation of digital human rights would also be emerging in the future. This third generation has limited support in existing law – whether at the national, regional or international level – but it builds on a discourse undertaken by human rights practitioners and scholars around the need for revising the traditional configuration of right holders and duty-bearers under international human rights law. Such a revision may be required in order to adequately capture new power configurations and social interactions in cyberspace, so as to effectively address new risks to the basic online needs and interests of individuals and groups of individuals.[147]

One particularly thought-provoking aspect of the discourse on new right holders and duty-bearers involves considering online persons as independent holders of digital rights[148] – that is, recognizing their 'digital' or 'virtual personality'.[149] Recognizing online profiles as digital or virtual persons with a right to engage in online activity that is distinct from the rights of the physical persons or legal entities that created them may provide such digital or virtual persons with more effective legal protection to facilitate their online activities in ways that are analogous to the protections afforded to the economic operations of corporations through the conferral on them of a legal personality. For example, digital or virtual persons may exercise their rights after the death of the persons that created them[150] and might have the ability to protect their reputation and intellectual property interests independently of their human ancestors. They may also claim an independent entitlement not to be discriminated against when compared to other digital or virtual persons.

Another part of the discourse about recognizing new legal subjects involves extending human rights obligations to technology companies.[151] To be sure, the discourse over the interplay between business and human rights is well developed in

147 IRPC Charter, *supra* note 102, at 18.

148 P.E. Agre and M. Rotenberg (eds), *Technology and Privacy: The New Landscape* (3rd edn, 2001), at 7–10; Clarke, 'The Digital Persona and Its Application to Data Surveillance', 10(2) *The Information Society* (1994) 77, at 77–92; Bert-Jaap, Hildebrandt and Jaquet-Chiffelle, 'Bridging the Accountability Gap: Rights for New Entities in the Information Society', 11 *Minnesota Journal of Law Science and Technology* (2010) 497, at 517–526, 559–561.

149 See, e.g., IRPC Charter, *supra* note 102, Art. 8(d). The Internet Rights and Principles Dynamic Coalition included a right to a 'virtual personality'.

150 Kutler, 'Protecting Your Online You: A New Approach to Handling Your Online Persona after Death', 26 *Berkeley Technology Law Journal* (2011) 1641, at 1645–1646.

151 See note 30 above; Ronen, *supra* note 49; SR Expression 2018, *supra* note 49.

international law and has already resulted in the conclusion of important international instruments, such as the UN Guiding Principles on Business and Human Rights,[152] and efforts are currently undergoing to formulate a new treaty in the field.[153] Still, whereas in traditional spheres of activity the turn to corporate responsibility is largely driven by concerns that businesses, especially transnational corporations, are not effectively subject to governmental regulation, in cyberspace, technology companies are the de facto and, at times, de jure regulators. Thus, they represent for online users a form of regulatory power, stronger in many ways and more direct than national governments. Under those circumstances, it may be justified to subject Internet companies directly to human rights obligations, especially those correlating to digital human rights,[154] and to reconceptualize in human rights terms important Internet governance policies such as net neutrality or net interoperability.[155]

Although the chronological and conceptual boundaries between the three 'generations' described here are somewhat blurred, it is still possible to identify in them 'ideal type' legal constructs that helps us to map the trajectory of the development of digital human rights in ways that are similar to the manner in which the language of human rights generations has helped to conceptualize stages in the development of human rights in the offline world.[156] Furthermore, the proposed genealogy of digital human rights tends to reflect distinct stages of departure from the traditional human rights paradigm: while the first generation of rights builds upon traditional human rights, the second generation departs from existing rights, creating new 'progeny rights'. The third generation goes further by creating a whole new structure comprising new rights, right holders and duty-bearers (a move resembling the move from individual rights to solidarity rights in Vašák's original three generations scheme).[157]

As the generations of digital human rights progress along this typology – new interpretations, new rights and new right structures – they are less and less grounded in *lex*

[152] Guiding Principles, *supra* note 48.

[153] Open-Ended Intergovernmental Working Group on Transnational Corporations and Other Business Enterprises with Respect to Human Rights, *Legally Binding Instrument to Regulate, in International Human Rights Law, the Activities of Transnational Corporations and Other Business Enterprises*, 16 July 2019, available at www.ohchr.org/Documents/HRBodies/HRCouncil/WGTransCorp/OEIGWG_RevisedDraft_LBI.pdf; OHCHR, Report on the Fifth Session of the Open-Ended Intergovernmental Working Group on Transnational Corporations and Other Business Enterprises with Respect to Human Rights, UN Doc. A/HRC/43/55, 9 January 2020.

[154] SR Expression 2017, *supra* note 26, at 21, paras 82–83; OHCHR Privacy Report 2018, *supra* note 13, at 12–13, paras 43–49.

[155] Union des consommateurs, A Charter of Rights for Internet Users: For a Canadian Perspective (2019), at 25, available at https://uniondesconsommateurs.ca/wp-content/uploads/2020/01/811429-rapport_Charte-droits-internautes_final-Eng.pdf; Reventlow, *The Digital Rights Future We Want: Imagining a Universal Declaration of Digital Rights* (2018), available at: https://digitalfreedomfund.org/the-digital-rights-future-we-want-imagining-a-universal-declaration-of-digital-rights/.

[156] J. Wronka, *Human Rights and Social Policy in the 21st Century: A History of the Idea of Human Rights and Comparison of the United Nations Universal Declaration of Human Rights with United States Federal and State Constitutions* (rev. edn, 1998); see also Zohadi, 'The Generations of Human Rights', 1 *International Studies Journal* (2004) 95, at 97–107.

[157] Alston, 'A Third Generation of Solidarity Rights: Progressive Development or Obfuscation of International Human Rights Law?', 29 *Netherlands International Law Review* (1982) 307.

lata and more and more in *lex ferenda*. The centrality of the role played by technology companies in ensuring the enjoyment of digital human rights also increases along the same trajectory: while the first generation of digital human rights retains considerable focus on state power (for example, in the field of regulating online surveillance), the focus of second generation rights is on the policies of technology companies (for example, erasing data covered by a right to be forgotten or allowing data portability). Third-generation digital rights almost exclusively involve technology companies, which control the very existence of online persons or data subjects.

4 Prototypes of New Digital Human Rights

A *The Right to Access the Internet*

A paradigmatic illustration of the trend of gradually moving away from the normative equivalency paradigm by creating or recognizing new (second-generation) digital human rights can be found with relation to claims for an independent right to access the Internet. As explained above, under the normative equivalency paradigm, new technologies, including the Internet, are viewed as simply offering new tools or methods for exercising offline human rights. Accordingly, access to the Internet is to be regulated in a manner similar to which access to other media platforms or communication methods that individuals use for exercising their offline human rights is regulated. Specifically, it has been claimed that the Internet facilitates the exercise of human rights, such as freedom of expression and the right to participate in the conduct of public affairs, and that protection of access to the Internet may consequently derive from the need to respect and ensure these human rights. Pursuant to this line of reasoning, there is no need to recognize a right of access to the Internet as a separate stand-alone human right. Yet a closer look at normative developments relating to access to the Internet suggests that, with time, such access is increasingly being regarded as much more than merely a means to realize other rights; rather, it is emerging as a right in and of itself. This is because of the extraordinary social impact of the Internet on the human condition – which is unmatched by any post-1945 development in media technology[158] – and the conceptualization of the online ecosystem as a new realm of human interaction rather than as just a new type of media. As a result, interfering with access to the Internet constitutes a new type of violation for which offline rights do not provide a suitable vocabulary.[159]

[158] Bryson, 'The Artificial Intelligence of the Ethics of Artificial Intelligence: An Introductory Overview for Law and Regulation', in D. Dubber, F. Frank and S. Das (eds), *The Oxford Handbook of Ethics of AI* (2020) 1, at 3 ('everything humans deliberately do has been altered by the digital revolution, as well as much of what we do unthinkingly').

[159] Çali, 'The Case for the Right to Meaningful Access to the Internet as a Human Right in International Law', in A. von Arnauld, K. von der Decken and M. Susi (eds), *The Cambridge Handbook of New Human Rights: Recognition, Novelty, Rhetoric* (2020) 276, at 280.

In 2011, Frank La Rue, the special rapporteur on the promotion and protection of the right to freedom of opinion and expression, issued a report focusing on the right to seek, receive and impart information through the Internet.[160] While the report did not declare a 'right to access the Internet', La Rue emphasized the 'positive obligation of states to facilitate the right to freedom of expression via the Internet'.[161] Subsequently, David Kaye, who replaced La Rue as special rapporteur, focused his attention on the duty of technology companies to resist restrictions on access to the Internet.[162] Other global and regional bodies have reiterated the importance of ensuring access to the Internet as an indispensable component for realizing freedom of expression and the freedom to seek, receive and impart information as well as other rights, such as the right to education. They repeatedly have underscored the adverse implications of online content restrictions and interference with access as well as state obligations in this regard.[163]

In parallel to these developments, a number of academics have explicitly called for the establishment of access to the Internet as a new human right, employing the language of rights to underscore the intrinsic value of access to the Internet and its potential to address the geopolitical digital divide.[164] Furthermore, some states have started to incorporate the right to access the Internet into their national legislation.[165] The combined effect of non-binding resolutions, declarations and reports on the need to ensure universal access to the Internet, the growing academic discourse about the need to develop a new right to that effect and emerging state practice suggests a movement towards recognizing access to the Internet as a new digital human right, although it has not yet obtained binding status under international law.[166]

[160] *SR Expression 2011*, *supra* note 133, at 22, para. 80.

[161] *Ibid.*, para. 61.

[162] SR Expression 2017, *supra* note 26, at 14–15, paras 47–50.

[163] Joint Declaration by the United Nations Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe Representative on Freedom of the Media, the Organization of American States Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights Special Rapporteur on Freedom of Expression and Access to Information, Challenges to Freedom of Expression in the Next Decade (2019), available at www.osce.org/files/f/documents/9/c/425282.pdf; see also PACE, Res. 1987, The Right to Internet Access, 9 April 2014; Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, Standards for a Free, Open and Inclusive Internet (2016), para. 35; SR Expression 2017, *supra* note 26, para. 76; T. Sandle, 'UN Thinks Internet Access Is a Human Right', *Business Insider*, 22 July 2016, available at www.businessinsider.com/un-says-internet-access-is-a-human-right-2016–7; D. Kravetz, 'U.N. Report Declares Internet Access a Human Right', *Wired* (2011), available at www.wired.com/2011/06/internet-a-human-right.

[164] De-Hert and Kloza, 'Internet (Access) as a New Fundamental Right. Inflating the Current Rights Framework?', 3 *European Journal of Law and Technology* (2012) 3; Tully, *supra* note 21, at 177–181.

[165] Lucchi, 'Internet Content Governance and Human Rights', 16 *Vanderbilt Journal of Entertainment and Technology Law* (2014) 809; Pollicino, 'The Right to Internet Access', in A. von Arnauld, K. von der Decken and M Susi (eds), *The Cambridge Handbook of New Human Rights: Recognition, Novelty, Rhetoric* (2020) 263.

[166] M.N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2017), at 195, para. 22; see also SR Expression 2018, *supra* note 49, at 4, para. 6; Shackelford, *supra* note 147.

As for the components of the new digital right, one may note that La Rue focused in his initial report on two main aspects of access: access to an Internet connection and access to online content.[167] With regard to access to an Internet connection, the digital divide, involving limited access to telecommunication in many parts of the world, still poses a serious concern.[168] Furthermore, in recent years, new obstacles have been erected[169] – in particular, Internet shutdowns during political upheavals or election periods.[170] Access to online content enjoys an even more precarious level of protection in practice, given the ability of governments to disguise restrictive measures under benign headings, such as harmful content regulation[171] and curbing disinformation, propaganda[172] or 'fake news'.[173] The real problem of exploitation of digital platforms to promote illegal activity sometimes results in excessive reaction by governments and Internet companies, including the over-regulation of contents (for example, by *ex ante* content filtering).[174]

Ultimately, the process of social recognition of the right to access the Internet is informed by normative considerations internalized by relevant norm makers. The growing dominance of the Internet in society underscores the need to develop a new human rights discourse in order to capture moral claims about respecting and ensuring access to online contents and services and protecting individuals from abusive practices by governments – at times, with the cooperation of technology companies – resulting in limiting their access to Internet services. The centrality of online expression, online information, online education and online consumption of culture could certainly justify extending to the right to access the Internet the protections afforded by the relevant offline human rights norms (for example, freedom of expression, the freedom to receive and impart information, the right to education and the right to take part in cultural life). Still, it can also be claimed that the significance of access to the Internet for individuals and for society as a whole cannot be fully represented through shoehorning it into human rights norms that protect only some of the needs and interests of online users in obtaining access.

[167] SR Expression 2011, *supra* note 133, para. 2.

[168] See note 125 above; see also Shackelford, *supra* note 147, at 13.

[169] SR Expression 2018, *supra* note 49, at 6–8, paras 12–21; see also Tully, *supra* note 21.

[170] OHCHR, UN Expert Urges Cameroon to Restore Internet Services Cut Off in Rights Violation (2017), available at www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=21165&LangID=E; see also J. Griffiths, 'Myanmar Shuts Down Internet In Conflict Areas As UN Expert Warns of Potential Abuses', *CNN*, 25 June 2019, available at www.cnn.com/2019/06/25/asia/myanmar-internet-shutdown-intl-hnk/index.html; Amnesty International, 'Benin: Internet Shutdown on Election Day Is a Blunt Attack on Freedom of Expression', *Amnesty*, April 2019, available at www.amnesty.org/en/latest/news/2019/04/benin-internet-shutdown-on-election-day-is-a-blunt-attack.

[171] SR Expression 2018, *supra* note 49, at 12, paras 6–8.

[172] *Ibid.*, at 31, at para. 13.

[173] Allcott, *supra* note 6, at 211–36. L. Kuo, 'Beijing's New Weapon To Muffle Hong Kong Protests: Fake News', *The Guardian*, 11 August 2019, available at www.theguardian.com/world/2019/aug/11/hong-kong-china-unrest-beijing-media-response.

[174] SR Expression 2018, *supra* note 49, at 12, para. 32; see also Citizen Lab, Planet Netsweeper, April 2018, at 7–9, available at https://citizenlab.ca/2018/04/planet-netsweeper/.

Arguably, in order to fully capture the significance of the Internet as a unique public sphere,[175] which serves as a gateway to a whole new space for human interaction, almost inexhaustible stores of information, a huge variety of services and, increasingly, new channels of communication and political and economic participation, one ought to reconceptualize access to the Internet as a new and independent human right. In fact, given the growing role of the Internet as a virtual environment for exercising digital human rights, the right to access the Internet may grow to become the digital equivalent to the Arendtian 'right to have rights'.[176] The combination of basic needs and interests, a moral consequentialist claim, a power imbalance between states, technology companies and online users and a history (albeit relatively short) of the denial and abuse of users' online needs and interests seems to support, and, in fact, predict, a political push to recognize a digital human right of access to the Internet.

Recognizing a new right to access would also facilitate the development of a regulatory framework setting out the outer boundaries of the right. As with any other human right, the right of access to the Internet should be relative in nature and subject to necessary and proportionate limitations provided by law. Therefore, governments can, and should, at times, impose limitations on this new right.[177] In fact, it is precisely the fundamental nature of the needs and interests protected by the right to access that invites a regulatory framework governing decisions to block or de-platform users. The dramatic events that transpired in Washington, DC, on 6 January 2021, leading to the de-platforming of President Donald Trump by some of the largest technology companies, underscore the legal anomaly of leaving decisions affecting the enjoyment of basic digital rights exclusively in the hands of private actors.[178]

B *The Right Not to Be Subject to an Automated Decision*

Another cluster of second-generation rights comprises rights that have no equivalent 'parent right' within the traditional corpus of offline human rights. While the protected values at the core of these new claimed rights are drawn from the same depository of values from which many human rights derive – dignity, liberty, equality and self-realization – they respond to wholly new threats or challenges that did not really exist before the digital age. Using the normative equivalency paradigm to address these new concerns would almost inevitably be inappropriate and ineffective. The emerging right not to be subject to an automated decision well illustrates this sub-category of digital human rights.

In the digital age, significant decisions relating to various aspects of people's lives are increasingly transferred from the hands of human beings to algorithmic

[175] Papacharissi, 'The Virtual Sphere: The Internet as a Public Sphere', 4 *New Media and Society* (2016) 9, at 21–22; see also GA Res. 71/199, *supra* note 16, at 3, para. 6.

[176] H. Arendt, *The Origins of Totalitarianism* (1968), at 268.

[177] See generally Donnelly, 'The Relative Universality of Human Rights', 29(2) *Human Rights Quarterly* (2007) 281, at 293–295.

[178] Y. Shany, *From Rule of Law to Rule of Community Standards?* (2021), available at https://csrcl.huji.ac.il/blog/rule-law-rule-community-standards-yuval-shany.

machines. Algorithms are described as 'a list of instructions to be followed, like a recipe',[179] and algorithmic decision-making involves decisions based on data gathering, processing and analysis, which often predict human behaviour on the basis of scientific classifications and predictive formulas.[180] An automated decision-making system 'is a system that uses automated reasoning to aid or replace a decision-making process that would otherwise be performed by humans'.[181] Such decision-making systems have been introduced in a manner affecting the enjoyment of human rights in a variety of private and public contexts, including the approval of loans,[182] the allocation of housing,[183] the counting of votes,[184] immigration decisions[185] and sentencing recommendations.[186]

Much attention has been given in recent years to the use of algorithmic decision-making in US courts to assess the risk of recidivism in connection with judicial sentencing and bail decisions.[187] AI-based 'digital courts' have been deployed in China for the online resolution of certain civil cases,[188] and AI judges are being developed for small claims courts in Estonia.[189] Note that the use of algorithm-based technology almost inevitably depends in practice on the online communication of data

[179] D. Markus, F. Pasquale and S. Das, *The Oxford Handbook of Ethics of AI* (2020), at 6.

[180] Diakopoulos, 'Accountability in Algorithmic Decision Making', 59(2) *Communications of the ACM* (2016) 56, at 56–57; Huq, 'A Right to a Human Decision', 106 *Virginia Law Review* (2020) 611, at 614, 634; AI Now Institute, *Algorithmic Accountability Policy Toolkit* (2018), at 1–2, available at https://ainowinstitute.org/aap-toolkit.pdf; Law Commission of Ontario, *The Rise and Fall of AI and Algorithms in American Criminal Justice* (2020), at 8, available at www.lco-cdo.org/wp-content/uploads/2020/10/Criminal-AI-Paper-Final-Oct-28–2020.pdf; Lum and Chowdhury, 'What Is an "Algorithm"? It Depends Whom You Ask', *MIT Technology Review*, 28 February 2021, available at www.technologyreview.com/2021/02/26/1020007/what-is-an-algorithm.

[181] AI Now Institute, *supra* note 181, at 2; Algorithmic Accountability Act, H.R. 2231, 116th Cong. (2019).

[182] Binns *et al.*, 'It's Reducing a Human Being to a Percentage, Perceptions of Justice in Algorithmic Decisions', CHI Conference on Human Factors in Computing Systems, 2018, at 1.

[183] AI Now Institute, *supra* note 181, at 5.

[184] S. Vijayakumar, *Algorithmic Decision-Making* (2017), available at http://harvardpolitics.companylogo-generator.com/covers/algorithmic-decision-making-to-what-extent-should-computers-make-decisions-for-society/.

[185] International Human Rights Program and the Citizen Lab, *Bots at the Gate: A Human Rights Analysis of Automated Decision-Making in Canada's Immigration and Refugee System* (2018), available at https://citizenlab.ca/2018/09/bots-at-the-gate-human-rights-analysis-automated-decision-making-in-canadas-immigration-refugee-system/.

[186] *State v. Loomis*, No. 2015AP157-CR (Wis. Ct. App. 13 July 2016), available at www.wicourts.gov/sc/opinion/DisplayDocument.pdf?content=pdf&seqNo=171690.

[187] Berkman Klein Center for Internet and Society, Harvard Law School, *Algorithms in the Criminal Justice System: Assessing the Use of Risk Assessments in Sentencing. Responsive Communities Initiative* (2017), at 9–11, available at http://nrs.harvard.edu/urn-3:HUL.InstRepos:33746041; Vijayakumar, *supra* note 185.

[188] T. Vasdani, *Robot Justice: China's Use of Internet Courts* (2019), available at www.lexisnexis.ca/en-ca/ihc/2020-02/robot-justice-chinas-use-of-internet-courts.page; see also N. Connor, 'Legal Robots Deployed in China to Help Decide Thousands of Cases', *The Telegraph*, 4 August 2017, available at www.telegraph.co.uk/news/2017/08/04/legal-robots-deployed-china-help-decide-thousands-cases/.

[189] E. Niiler, 'Can AI Be a Fair Judge in Court? Estonia Thinks So', *Wired* (2019), available at https://www.wired.com/story/can-ai-be-fair-judge-court-estonia-thinks-so/.

or is integrated in online interactive systems. The shift from human to algorithmic decision-making is justified primarily on grounds of efficiency. Machines are cheaper, faster, more precise and have a greater capacity for processing large quantities of data than humans. Algorithms also hold the promise of removing biases and misconceptions that afflict human decisions through deliberate debiasing and following evidence-based decision-making.[190] Still, reliance on algorithmic decision-making, especially in the exercise of public authority relating to important personal and social interests, including in the exercise of judicial power, raises serious legal and ethical concerns, which, in turn, invite the attention of international human rights law bodies.

The normative debate on algorithmic decision-making mainly revolves around four main issues: lack of transparency, fairness and systematic bias, accountability and the ethical implications of delegating public authority to technology companies. The proprietary nature of the algorithm, and the difficulty in understanding the technical aspect of its operation, including the data set on which it relies,[191] how data is processed and the effects of machine learning, make algorithmic decision-making opaque for most persons affected by algorithmic decisions as well as for most human decision-makers who are assisted by it. This is the infamous algorithmic 'black box'.[192] Accordingly, algorithm-based decision-making stands at odds with the expectation that public authorities would operate in a transparent manner.[193] The need for transparency, which includes a need for motivated decisions, is particularly compelling for judicial decisions.[194] Another key judicial safeguard found in international human rights law is the right of litigants to know the identity of their judges.[195] The use of algorithmic machines to assist or substitute human judicial decision-making raises concerns about litigants' ability to access the reasons for the decision and to know who their judges are.

As for systematic bias, studies show that algorithmic decision-making technologies may perpetuate racial and gender prejudices.[196] Furthermore, difficult questions

[190] See Vijayakumar, *supra* note 185.

[191] Liu, Lin and Chen, 'Beyond State v Loomis: Artificial Intelligence, Government Algorithmization and Accountability', 27(2) *International Journal of Law and Information Technology* (2019) 122, at 133.

[192] Simmons, 'Big Data and Procedural Justice: Legitimizing Algorithms in the Criminal Justice System', 15 *Ohio State Journal of Criminal Law* (2018) 573; see also Abu-Elyounes, 'Contextual Fairness: Legal and Policy Analysis of Algorithmic Fairness', 1 *University of Illinois Journal of Law* (2020) 1, at 2–3.

[193] Sourdin, 'Judge v. Robot: Artificial Intelligence and Judicial Decision-Making', 41 *University of New South Wales Law Journal* (2018) 1114.

[194] ICCPR, *supra* note 57, Art. 14; Human Rights Committee, General Comment no. 32 Article 14: Right to Equality before Courts and Tribunals and to Fair Trial, para. 28–29 (GC no. 32), UN Doc. CCPR/C/GC/32, 23 August 2007; Human Rights Committee, *Timmers v. The Netherlands*, Communication no. 2097/2011, 2 February 2011, para. 7.2.

[195] GC no. 32, *supra* note 195, para. 23; see also Human Rights Committee, *Becerra v. Colombia*, Communication no. 1298/2004, 11 July 2006, para. 7.2 (relating to the use of 'faceless judges').

[196] Land and Aronson, 'Human Rights and Technology: New Challenges for Justice and Accountability', 16 *Annual Review of Law and Social Science* (2020) 223, at 225; see also AI Now Institute, *Litigating Algorithms: Challenging Government Use of Algorithmic Decision Systems* (2018), at 13–14, available at https://ainowinstitute.org/litigatingalgorithms.pdf; Angwin, Larson, Mattu and Kirchner, *Machine Bias* (2016), available at www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing; Kugler, *AI Judges and Juries* (2018), available at https://cacm.acm.org/magazines/2018/12/232890-ai-judges-and-juries/fulltext.

arise pertaining to the definition of 'algorithmic fairness'[197] and about the normative implications of new distinctions between individuals created by algorithmic decision-making that feeds on big data, potentially resulting in new forms of discrimination, unknown to existing human rights law.[198] These substantive problems of fairness and equality are further compounded by questions of accountability linked to the challenges of detecting biases in algorithmic systems given their non-transparent nature, the 'veneer of mathematical "neutrality"'[199] and the problem of placing responsibility for unfair or unjust outcomes on different links in the algorithmic machine's development and supply chain.[200]

The transition from human to algorithmic decision-making also marks a shift from the exercise of public authority by public bodies to private entities. Over and beyond the well-known concerns about the privatization of public functions and the delegation of public authority to private entities,[201] the opaque and multidimensional nature of algorithmic decision-making blurs the borderlines of responsibility and the division of authority between government and technology companies.[202] Moreover, the transfer of public decision-making authority from humans to machines entails substantially different moral consequences, as it involves a certain dehumanization of public authority. This is because algorithms capture human beings in their decision-making processes as data sets, subject to group categorization, the generalization of attributes and the prediction of conduct.[203] By contrast, decisions undertaken by human beings endowed with moral intuitions and moral agency often involve inter-personal interactions where each other's humanity is mutually recognized and where empathy and solidarity can be extended.[204]

[197] See Binns *et al.*, *supra* note 183, at 3; Abu-Elyounes, *supra* note 193, at 4–9; Land and Aronson, *supra* note 197, at 3.

[198] Mittelstadt *et al.*, 'The Ethics of Algorithms: Mapping the Debate', 3(2) *Big Data and Society* (2016) 1, at 12; see also Anya and Schwarcz, 'Proxy Discrimination in the Age of Artificial Intelligence and Big Data', 105 *Iowa Law Review* (2020) 1257; Chander, 'The Racist Algorithm', 115 *Michigan Law Review* (2016) 1023.

[199] Citizen Lab, To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada (2020), at 177, available at https://citizenlab.ca/2020/09/to-surveil-and-predict-a-human-rights-analysis-of-algorithmic-policing-in-canada/.

[200] Council of Europe, Expert Committee on Human Rights Dimensions of Automated Data Processing and Different Forms of Artificial Intelligence, A Study of the Implications of Advanced Digital Technologies (including AI Systems) for the Concept of Responsibility within a Human Rights Framework, Doc. DGI(2019)05 (2019), at 55.

[201] See, e.g., S. Joseph and M. Castan, *The International Covenant on Civil and Political Rights: Cases, Materials, and Commentary* (2013), at 753–754; see also High Court of Justice (Israel) 2605/05, *Academic Center of Law and Business v. Minister of Finance* (19 November 2009), at 63–66.

[202] Liu, Lin and Chen, *supra* note 192, at 137; Land and Aronson, *supra* note 197, at 4; Aust, 'Undermining Human Agency and Democratic Infrastructures? The Algorithmic Challenge to the Universal Declaration of Human Rights', 112 *AJIL Unbound* (2018) 334.

[203] Citizen Lab, supra note 200, at 171.

[204] Leubsdorf, 'Theories of Judging and Judge Disqualification', 62 *New York University Law Review* (1987) 237; Kuipers, 'Perspectives on Ethics of AI', in M.D. Dubber, F. Frank and S. Das (eds), *The Oxford Handbook of Ethics of AI* (2020), at 421.

It is against these unique features and challenges that calls have been made to develop a specific new human right that would preserve some aspects of human control over, or intervention in, automated decision-making.[205] Such a new human right would serve as the rough digital equivalent of the Anglo-American right to be tried by one's peers – a right that goes back in time to the Magna Carta of 1215.[206] Arguably, a new right not to be subject to an automated decision could supplement the shortcomings of offline international human rights law, which provides only a partial response, in non-specific terms, to the concerns associated with the growing use of algorithmic decision-making.[207]

In domestic law, a key legal holding accepting the logic of a right not to be subject to an automated decision in judicial matters can be found in the 2016 decision of the Wisconsin Supreme Court in *State v. Loomis*. The Court held there that judges may consult an algorithmic recidivism assessment programme but that the programme outcome can only be one factor in the final decision. The algorithmic assessment must not replace the judge's discretion, and the court is expected to explain the factors that were taken under consideration in addition to the algorithmic risk assessment, which is merely aimed at providing the court with more complete and accurate information.[208]

An even more notable development in the direction of establishing a right not to be subject to an automated decision-maker can be found in Article 22 of the GDPR, adopted by the EU in 2016. Article 22 provides data subjects with the right not to be subject to a decision based solely on automated processing, whenever such a decision 'produces legal effects concerning him or her or similarly significantly affects him or her'.[209] Although the GDPR is intended to regulate and protect EU data processors, controllers or subjects, it does cover certain extraterritorial processing activities involving or affecting EU data processors, controllers or subjects.[210] Some academics have already identified a process by which the GDPR is becoming the 'gold standard'

[205] Huq, *supra* note 181, at 614.

[206] W.S. Holdsworth, *A History of English Law* (1956), at 59, para. 39; see also Colin and Edwards, 'A Jury of Peers: A Comparative Analysis', *Journal of Criminal Law* (2004) 68, at 149–150. Since, under the US Constitution Sixth Amendment, the right to a jury trial also provides for a right to preclude the substitution of a jury with a judge, one can argue that in the same manner an individual should be allowed to preclude resort to a 'machine-judge'. See Huq, *supra* note 181.

[207] McGregor, Murray and Ng, 'International Human Rights Law as a Framework for Algorithmic Accountability', 68 *International and Comparative Law Quarterly* (2019) 309, at 342; Citizen Lab, *supra* note 200, at 34; see also Patgiri and Ahmed, 'Big Data: The V's of the Game Changer Paradigm', 18th IEEE International Conference on High Performance Computing and Communications, 12–14 December 2016, Sydney, Australia, at 17.

[208] *State v. Loomis*, *supra* note 187, paras 71–74.

[209] GDPR, *supra* note 85, Art. 22; see also Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, 21 April 2021, COM/2021/206 final, at para. 38; Goodman, Bryce and Flaxman, 'European Union Regulations on Algorithmic Decision-Making and a "Right to Explanation"', 38(3) *AI Magazine* (2017) 50, at 56.

[210] GDPR, *supra* note 85, Art. 3(2); see also Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, 18 May 2018, ETS 223, Art. 9(1)(a).

of regulation in the field.[211] If correct, this may support the emergence over time of a generally applicable new international digital human right not to be subject to an automated decision in decisions significantly affecting important areas of life.

C *The Normative Inquiry Revisited: Justifying the Creation of New Digital Human Rights*

When the general considerations derived from the theories of rights surveyed in Section 2 are applied to the process of recognizing new digital human rights, it appears as if some normative approaches to human rights theory do not sit particularly well with developing new digital rights, such as the right to access the Internet or the right not to be subject to an automated decision. Although such new rights reflect core human rights values, such as liberty and dignity, their specific contours depend on an external variable – a specific form of technology currently in use – and do not derive intrinsically from the human condition or universal experience. The ability to conceptualize a claim for obtaining access to the Internet or curtailing resort to algorithmic machines as morally justified is further complicated by the digital divide between the 'haves' and the 'haves not', which establishes a relationship between human needs and interests and a particular stage of technological advancement.[212] Such a relationship is not found in respect to many human rights that capture needs and interests that potentially transcend time, place and technology.

Yet engagement in a discourse about the moral imperative for addressing structural causes for injustice and inequality, with a view to advancing 'human capabilities',[213] can lend support to recognizing new digital human rights, including the right to access the Internet and the right not to be subject to an automated decision. Specifically, the human capabilities conception of human rights revolves around realizing human potential. Human rights are aimed, according to this approach, at effectively protecting individual autonomy and choices, *inter alia*, by ensuring the availability of resources and access to information that renders liberty and choice making a meaningful exercise.[214] As a result, human rights should reflect much more than the 'minimum conditions for any kind of life'[215] or the necessary safeguards against extreme cases of abuse of governmental power.[216] Charles Beitz, for example, claims that human rights should frame the 'necessary conditions for political legitimacy or even social justice'.[217]

[211] Lubin, 'The Rights to Privacy and Data Protection under International Humanitarian Law and Human Rights Law', in R. Kolb, G. Gaggioli and P. Kilibarda (eds), *Research Handbook on Human Rights and Humanitarian Law: Further Reflections and Perspectives* (forthcoming).

[212] See note 125 above.

[213] M. Walzer, *Thick and Thin: Moral Argument at Home and Abroad* (1994); see also Nussbaum, 'Capabilities and Human Rights', 66 *Fordham Law Review* (1997) 273; Winston, 'Human Rights as Moral Rebellion and Social Construction', 6 *Journal of Human Rights* (2007) 279.

[214] Griffin, *supra* note 69, at 33–34.

[215] Beitz, *supra* note 64, at 39.

[216] Osiatynski, 'The Historical Development of Human Rights', in Sheeran and Rodley, *supra* note 74, 9; Griffin, *supra* note 69, at 11; De-Hert and Kloza, *supra* note 165, at 3.

[217] Beitz, *supra* note 64, at 39–40.

Against this theoretical background, it looks as if a moral case in favour of recognizing new digital rights can be made. As mentioned above, there is a wealth of information on restrictions placed by governments on access to the Internet or to specific online contents, the threat such practices pose to individual freedom and dignity[218] and their negative impact on society as a whole. Without access to digital space and basic safeguards against the abuse of power, the capabilities of many individuals might be severely curtailed. In the same vein, the move from human to algorithmic decision-making brings with it, as indicated above, serious problems of transparency, fairness, accountability and inter-personal solidarity in connection with the exercise of public authority in important areas of life. Boxing in individuals into algorithmic categories entails a degree of dehumanization, limits their life possibilities and prevents individuals from making a conscious choice to 'unbelong' to any specific social group.[219] The combination of basic needs and risk of abuse could justify designating the two claimed rights as independent human rights, so as to effectively protect the full gamut of needs and interests of online users.[220]

For norm makers, the main justification for recognizing a new right to access the Internet and right not to be subject to an automated decision may be a utilitarian one: it is more effective to protect the morally justified claims underlying access to the Internet through recognizing a new human right that would secure online connectivity and include guarantees for safe and meaningful online presence and use than by way of extending existing rights that cover only some elements of online access. A thick right of access, containing elements of safe, open and free access on equal terms, could also support claims for effective protection of the entire digital ecosystem in a manner that would enhance the trust in Internet platforms as a whole, thereby promoting the realization of other offline and online human rights that depend on platform integrity. In the same vein, it is more effective to recognize a new human right not to be subject to an automated decision than to extend to cyberspace the existing right to due process, which does not specifically regulate algorithmic decision-making and is irrelevant for most non-judicial public decisions. Regulating through human rights norms the division of labour between human and algorithmic decision-makers would also make an important contribution to the human right-friendly development of AI, big data and other digital technologies applied in cyberspace.

Finally, new digital human rights may also be perceived as necessary to address the particular challenge posed by the dominant role of private actors in Internet and data governance and the limited ability of offline remedies to address in real time the

[218] Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Report on Contemporary Challenges to Freedom of Expression (SR Expression 2016), UN Doc. A/71/373, 6 September 2016, at 3, paras 1–2.

[219] Hebrew University of Jerusalem Federmann Cyber Security Research Centre and Essex University Human Rights Center, Expert Workshop on Human Rights and Algorithms in Decision-Making, May 2019, London, available at https://csrcl.huji.ac.il/sites/default/files/csrcl/files/human_rights_and_algorithms_in_decision-making_summary.pdf (comment by Alon Harel).

[220] Best, 'Can the Internet be a Human Right?', 4 *Human Rights and Human Welfare* (2004) 23; Çali, *supra* note 160.

effects of harmful activity in the digital space. Arguably, it would be very difficult for states to effectively protect, promote and facilitate the multifaceted needs and interests served by digital rights,[221] such as the rights to Internet access and not to be subject to an automated decision. More closely tailored digital human rights could convey more clearly to technology companies the standards of conduct that they are expected to follow than would general standards derived from traditional human rights, such as freedom of expression and the right to a fair trial.[222] Clear, precise and fit-for-purpose normative guidance would increase the legitimacy of making specific demands for implementation of digital human rights by state and non-state actors and is likely to improve compliance with international human rights law norms.[223] The emergence of a new vocabulary of digital human rights norms could also encourage online users to develop a sense of entitlement for enjoying online rights and facilitate over time the creation of suitable and effective remedies for violations that have occurred.[224] What is more, even if specific attempts to create new digital human rights would stop short of graduating into binding norms of international law, the mere conceptualization of specific claims as digital human rights has an added value in and of itself, as it can contribute to promoting legal interpretations and policies that embrace the values captured by the proposed new rights.[225]

5 Conclusion

While the application of human rights and fundamental freedoms in cyberspace is becoming a generally accepted premise, the applicable legal framework governing cyberspace still remains contested. International bodies, including mainly the GA and the HRC, have adhered to a normative equivalency paradigm, according to which the same human rights that individuals enjoy offline must be protected online as well. However, we have demonstrated in this article that the unique features of cyberspace put in question the desirability and feasibility of an automatic extension of offline human rights to cyberspace. This is because cyberspace represents a substantially different interactive environment, dissimilar to the context against which traditional human rights treaties and standards were developed.

Recent developments in the field of international standard setting and in the academic literature described in this article support the proposition that the effective

[221] See, e.g., Alston, *supra* note 79, at 607–609.

[222] De-Hert and Kloza, *supra* note 165, at 10; see also Best, *supra* note 221; Neumayer, 'Do International Human Rights Treaties Improve Respect for Human Rights?', 49 *Journal of Conflict Resolution* (2005) 925, at 951 (discussing the 'indirect effects of human right system').

[223] T.M. Franck, *The Power of Legitimacy among Nations* (1990); see also Finnemore and Sikkink, 'International Norm Dynamics and Political Change', 52 *International Organization* (1998) 887, at 906–907.

[224] Felstiner, Abel and Sarat, 'The Emergence and Transformation of Disputes: Naming, Blaming, Claiming', 15 *Law and Society Review* (1980) 631; Stevens, 'A Cyberwar of Ideas? Deterrence and Norms in Cyberspace', 33 *Contemporary Security Policy* (2012) 148, at 150.

[225] Cassel, 'Does International Human Rights Law Make a Difference', 2 *Chicago Journal of International Law* (2001) 121, at 123–124.

protection of human rights in cyberspace cannot be achieved by relying solely on existing international human rights law and that existing rights need to be adapted and complemented by new digital human rights in order to maintain effective protection of individual needs and interests in the digital age. As we have demonstrated with the right to Internet access and the right not to be subject to automated decisions, attempts to recognize new digital human rights and to support such rights by reference to moral considerations are already underway.

We have proposed in this article a typology of three stages in the development of international digital human rights law, which goes beyond the normative equivalency paradigm. The first generation of digital human rights comprises efforts to offer radical reinterpretations of existing human rights, which would adapt them to conditions in the digital age. The second generation entails the development of new digital rights, aimed at protecting unique online needs and interests that are not fully or effectively covered by the application of traditional human rights to cyberspace. A third generation might involve attempts to designate new right holders and duty holders. It could develop, *inter alia*, the concept of digital personality and directly impose appropriate legal obligations on private technology companies. The combined effect of these three generations might be the emergence of a new, comprehensive and fit-for-purpose human rights framework for the effective protection of individual needs and interests online.[226]

[226] But compare T.S. Kuhn, *The Structure of Scientific Revolutions* (4th edn, 2012), at 152 ('[p]robably the single most prevalent claim advanced by the proponents of a new paradigm is that they can solve the problems that have led the old one to a crisis').