German Law Journal (2023), **24**, pp. 461–472
doi:10.1017/glj.2023.35

CAMBRIDGE UNIVERSITY PRESS

ARTICLE

Special Issue: International Law and Digitalization

Digital Rights and the Outer Limits of International Human Rights Law

Yuval Shany

Hebrew University of Jerusalem, Jerusalem, Israel
Email: shany.yuval@gmail.com

(Received 12 April 2023; accepted 12 April 2023)

Abstract

This article explores the extent to which key normative and institutional responses to the challenges raised by the digital age are compatible with, or interact with, changes in key features of the existing international human rights law (IHRL) framework. Furthermore, the article claims that the IHRL framework is already changing, partly due to its interaction with digital human rights. This moving normative landscape creates new opportunities for promoting human rights in the digital age, but might also raise new concerns about the political acceptability of IHRL. Following an introduction, Section B of the article will describe the development of digital human rights, using a "three generations" typology. Section C will explain how new developments in the field of digital human rights coincide with broader developments in IHRL, including: the extra-territorial application of human rights, obligations on governments to actively regulate private businesses and the erosion of normative boundaries separating specific human rights treaties from other parts of IHRL and international law. These two segments are followed by concluding remarks.

Keywords: Digital human rights; extraterritoriality of human rights; positive obligations; systemic integration; business and human rights

A. Introduction

While human rights theory often presents human rights as pre-political, imbued with natural law features—including norms derived from natural rights philosophy, religious beliefs, pure reason, or putative human capabilities—which transcend time and place.[1] International human rights law (IHRL) has always involved more concrete and contingent dimensions, anchored in a specific time and place, and in a particular political, economic, technological and cultural context.[2] This is because the evolution of international law depends on distinct political "acts of recognition" carried out through the adoption of legal specific instruments and through actual state practice, and shaped, in turn, as much by practical considerations about the actual needs and expectations of political constituencies as by high theory about what the contents of human rights law should

[1]*See e.g.*, Edward Hall and Dimitrios Tsarapatsanis, *Human Rights, Legitimacy, Political Judgement*, 27 RES PUBLICA 171, 172 (2021); Peter Jones, *Which Rights?, in* HUMAN RIGHTS ROUTLEDGE ENCYCLOPEDIA OF PHILOSOPHY (2006), https://www.rep.routledge.com/articles/thematic/human-rights/v-1/sections/which-rights.

[2]*See e.g.*, International Covenant on Economic, Social and Cultural Rights arts. 8, 13, Dec. 16, 1966, 993 U.N.T.S. 3 (involving trade union rights and the right to primary, secondary and high education) [hereinafter ICESCR].

be. As a result, it is not surprising that Vasak was able to situate his "three generations of IHRL" typology in specific historical epochs,[3] corresponding to dramatic political, economic, technological and cultural developments: Revolutions against absolute monarchs or foreign kings informed by ideas of the age of enlightenment; the rise of the welfare state in the aftermath of the industrial revolution; and national emancipation in the age of decolonization influenced by ideas of international solidarity and national self-determination. In the same vein, the Universal Declaration of 1948, which largely serves as a normative road map for the international human rights movement, explicitly addressed some of the specific societal and technological challenges of the time, such as ensuring access to media across frontiers, protecting trade unions, and promoting technical education.[4] The same can be said for the 1966 Covenants, which addressed basic features of modern social-democratic states, including the need to establish a system for social insurance and to ensure fair and free periodic elections.[5]

In all cases involving the articulation and adoption of international declarations and treaties, a process of social recognition had occurred. In the course of those processes, human rights were transformed from abstract moral ideas or claims into a particular set of legal rights and obligations, or, in the case of soft law instruments, into concrete social expectations and policy recommendations. Such acts of transformation are often responsive to the changing needs and expectations of specific constituencies, to the new risks and challenges individuals and societies confront due to changing economic, technological, and cultural conditions. They are also responsive to actual historical experiences of abuse of power and injustice that support the introduction of new rights that are typically designed to empower individuals and groups of individuals at the expense of government institutions.

Arguably, the contemporary "digital revolution" and its related offshoots represent yet another technological development with major economic, political, and cultural ramifications.[6] Like others before it, this revolution also invites a process of normative transformation involving the translation of abstract ideas about "digital rights" or "principles for the digital age" into concrete legally-recognized human rights norms through a process of law-interpretation and law-making—i.e., through the articulation of new legally binding or soft law instruments. The UN Human Rights Council and General Assembly have approached the challenge of adapting IHRL to the digital age by adopting a slew of non-binding resolutions that advocate the extension of offline human rights to activities and interactions online.[7] The EU Commission has also issued a Declaration on Digital Rights and Principles for the Digital Age in which it took the necessary steps to ensure respect for the rights of individuals both offline and online.[8] This approach avoids

[3]Karel Vasak, *A 30-Year Struggle: The Sustained Efforts to Give Force of Law to the Universal Declaration of Human Rights*, 11 THE UNESCO COURIER 29 (1977).

[4]G.A. Res. 217 (III) A, Universal Declaration of Human Rights (Dec. 10, 1948), arts. 19, 23, 26 [hereinafter UDHR].

[5]ICESCR, *supra* note 2, at art. 9; International Covenant on Civil and Political Rights art. 25, Dec. 16, 1966, 999 U.N.T.S. 171.

[6]*See e.g.*, KLAUS SCHWAB, THE FOURTH INDUSTRIAL REVOLUTION 3 (2017). Among the offshots of the digital revolution one can mention the connectivity revolution, the AI revolution, the big data revolution, the cloud revolution and their fusion with other new technologies, such as blockchain, natural language processing, and biometrics.

[7]See e.g., G.A. Res. 68/167, ¶ 3 (Dec. 18, 2013); G.A. Res. 69/166, ¶ 3 (Dec. 18, 2014); G.A. Res. 71/199, ¶ 3 (Dec. 19, 2016); G.A. Res. 73/179, ¶ 3 (Dec. 17, 2018); G.A. Res. 75/176, ¶ 3 (Dec. 16, 2020); Human Rights Council Res. 20/8, U.N. Doc. A/HRC/RES/20/8, at 2 ¶ 1 (July 5, 2012); Human Rights Council Res. 26/13, U.N. Doc. A/HRC/RES/26/13, at 2 ¶ 1 (June 26, 2014); Human Rights Council Res. 32/13, U.N. Doc. A/HRC/RES/32/13, at 3 ¶ 1 (July 1, 2016); Human Rights Council Res. 38/7, U.N. Doc/HRC/RES/38/7, at 3 ¶ 1 (July 5, 2018). For a discussion, see Dafna Dror-Shpoliansky & Yuval Shany, *It's the End of the (Offline) World as We Know It: From Human Rights to Digital Human Rights – A Proposed Typology*, 32 EJIL 1249 (2001).

[8]European Declaration on Digital Rights and Principles for the Digital Decade, Commission Decl. at Ch. 1, COM (2022) 28 final (Jan. 26, 2022).

https://doi.org/10.1017/glj.2023.35 Published online by Cambridge University Press

the perception of cyberspace as an IHRL-free "black hole," and continues a long-standing tradition of adjusting existing human rights to new and changing societal conditions.[9]

To be sure, the process of adaptation of old IHRL norms to new situations sometimes requires introducing significant changes in the scope and contents of pre-existing IHRL norms and in the manner of their application to previously unforeseen circumstances. For example, there is little doubt that the underlying rationales supporting freedom of expression apply both offline and online,[10] and that protection of the internationally recognized right to receive and impart information, "through any media," should cover the dissemination of contents on social media and other digital platforms.[11] Still, the different societal and technological contexts for the exercise of freedom of expression in a digital environment may invite a stronger regulatory response, especially with regard to offensive speech. That may be necessary due to the greater risks attendant to online hate speech (caused by differences in the speed, scope, and scale of dissemination of harmful online contents),[12] and the apparent "failure" of the online "marketplace of ideas" to effectively address the problem of disinformation (partly because of the distorting effects of algorithmic filter bubbles and echo-chambers that create incentives to disseminate controversial content).[13]

At times, the adaptation of the scope and content of offline rights to an online environment might require the development of new theoretical justifications for the right in question. For example, theories pertaining to the right to online privacy reveal a transition from protecting individuals against unjustified intrusion of their private and intimate spaces to protecting and managing personal information in both private and public settings.[14] Theories about privacy must increasingly consider how to shield individuals against undue manipulation of their wishes, thoughts, and opinions.[15]

Yet, in some cases, the normative gap between offline human rights and the needs and interests of online users reaches a troubling extent, suggesting that adaptation of an existing right is no longer feasible or would lead to "hopelessly inadequate" results.[16] In those circumstances, the development of new human rights—such as the right not to be subject to algorithmic decisions[17] or the right to be forgotten[18]—might be warranted.

Navigating between old and new norms involves difficult legal policy dilemmas. Creating new norms of IHRL does not necessarily require the introduction of a new IHRL framework, but it underscores the shortcomings of the existing framework. Yet, acknowledging the unsuitability of existing offline rights without there being a readily available new set of human rights to afford protection to online users creates the risk that individuals would be left neither here nor there—i.e., facing a protection gap. At the same time, sticking with the existing IHRL norms, even as they are increasingly viewed as inappropriate, also results in under-protection of online needs and interests. Worse still, it sends to states, technology companies, and other stakeholders a

[9]*See* Vasak, *supra* note 3; *see also* Samuel Moyn, The Last Utopia: Human Rights in History 225 (2010).

[10]*See e.g.*, David Kaye (Special Rapporteur on Freedom of Opinion and Expression), Rep., at 22 ¶ 57, U.N. Doc. A/74/486 (Oct. 9, 2019).

[11]UDHR, *supra* note 4, at art. 19.

[12]For a discussion, see Dror-Shpoliansky & Shany, *supra* note 7, at 1266–1267.

[13]*See* Dror-Shpoliansky & Shany, *supra* note 7, at 1266–267; *see also* Tomer Shadmy, *Content Traffic Regulation: A Democratic Framework to Address Misinformation*, 63 Jurimetrics 1 (2022).

[14]*See e.g.*, Helen Nissenbaum, Privacy in Context: Technology, Policy, and the Integrity of Social Life 231 (2009).

[15]*See e.g.*, Marcello Ienca & Roberto Andorno, *Towards New Human Rights in the Age of Neuroscience and Neurotechnology*, 13 Life Sci. Soc. Pol'y 1, 11–15 (2017).

[16]*See* Special Rapporteur on the Right to Privacy, Rep., at 26 ¶ 6, U.N. Doc. A/HRC/37/62 (Oct. 25, 2018).

[17]*See e.g.*, Regulation (EU) 2016/679 of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation), art. 21, OJ L 119/1 (2016) [hereinafter GDPR].

[18]*Id.* at art. 17.

https://doi.org/10.1017/glj.2023.35 Published online by Cambridge University Press

dangerously reassuring message that they may continue to proceed in a "business as usual" mode of operation.

Yet, there are certain aspects of digital human rights that invite a reconsideration of some key features of IHRL: The predominance of the territorial model for the application of human rights obligations; the focus on responsibility of governments for human rights violations, as opposed to transnational companies and other non-state actors; and the propensity of IHRL bodies to apply IHRL instruments in isolation from other legal instruments.[19] This article explores the extent to which key normative and institutional responses to the challenges raised by the digital age are compatible with, or interact with, changes in the said aforementioned key features of the existing IHRL framework. In fact, this article claims that the IHRL framework is already changing in this regard, partly due to its interaction with digital human rights. These already-unfolding changes may create new opportunities for promoting human rights in the digital age, and could render the policy choice between change and stability of -IHRL- irrelevant. At the same time, the moving normative landscape might raise new concerns about the political acceptability of -IHRL- to states.

Following this introduction, Section B will describe the development of digital human rights, using the "three generations" typology that I have developed elsewhere (together with Daphna Dror-Shpoliansky).[20] Section C will explain how new developments in the field of digital human rights coincide with broader developments in IHRL, including the extra-territorial application of human rights, obligations on governments to actively regulate private businesses, and the erosion of normative boundaries separating specific human rights treaties from other parts of IHRL and international law. These segments are followed by concluding remarks.

B. The Three Generations of Digital Human Rights

I have suggested elsewhere—in an article co-written with Dafna Dror Shpoliansky—that IHRL bodies and stakeholders tend to respond to the challenges to the rights and needs of online users brought about by new digital technology via three principal sets of responses, which can be described as representing three "generations" of digital human rights.[21] The first generation involves a radical reinterpretation of existing human rights in order to allow them to meet the new conditions of the digital age.[22] The second generation involves the development of new digital human rights, corresponding to the new needs and interests of online users.[23] These second generation rights have no close parallels in the offline world. The third generation involves the recognition of new rights-holders and new duty-holders.[24]

The first generation of digital rights involves a dynamic reinterpretation of some of the basic elements comprising the definition of relevant offline rights, a new approach towards their manner of application, and, at times, a new theory justifying the existence of the right in question. This latter extension implies that first generation rights may, in some respects, be the continuation in name only of the original offline right. Online freedom of expression, mentioned above, is one example of a first generation digital right. The scope of the right has been expanded by international bodies to cover online expression,[25] and it has been argued that this

[19]*See e.g.*, Banković v. Belgium, App. No. 52207/99, ¶¶ 67–71 (Dec. 12, 2001) https://hudoc.echr.coe.int/eng?i=001-22099; Julie Fraser, *Challenging State-Centricity and Legalism: Promoting the Role of Social Institutions in the Domestic Implementation of International Human Rights Law*, 23 INT'L J. OF HUM. RTS. 974 (2019); Bruno Simma & Dirk Pulkowski, *Of Planets and the Universe: Self-Contained Regimes in International Law*, 17 EJIL 483, 511 (2006).

[20]*See* Dror-Shpoliansky & Shany, *supra* note 7.

[21]*See id.*

[22]*See id.* at 1266–1267.

[23]*See id.* at 1268–1269.

[24]*See id.* at 1269–1270.

[25]*See e.g.*, Kaye, *supra* note 10, ¶ 57.

https://doi.org/10.1017/glj.2023.35 Published online by Cambridge University Press

digitally-reconfigured right to freedom of expression now encompasses a derivative right to access the Internet.[26] At the same time, the application of limitations to freedom of expression has been advocated by human rights office holders more forcefully than before, given the unique manner in which offensive content is disseminated online and the distorting impact on public discourse caused by online disinformation.[27] Due to the heightened risk associated with offensive online speech, digital platforms have been encouraged by states and international bodies to develop and enforce effective content moderation rules.[28] The shift from the traditional hands-off position of IHRL bodies, which were generally skeptical towards speech regulation by governments,[29] to a more pro-regulatory stance, also reflects a change in the theoretical assumptions underlying freedom of expression and a fundamental shift in social conditions. In the offline world, the dominant condition was that of information scarcity, which suggested a need to release more information into a more-or-less unstructured market of ideas and information. But in the online world the paradigm appears to involve an excess of information in which socially harmful content might crowd out socially useful information. The result of this has been a claim in favor of structuring proactively an effective market of ideas and information. This would involve regulation that ensures that information disseminated online will be conducive to a well-informed and civilized public discourse.[30]

Another example of a first-generation digital human right is the right to online privacy. Here, too, the content of the right has undergone many changes, as did its manner of application and underlying theory. For example, the center of gravity of legal practices aimed at upholding the right to privacy has shifted from protecting individuals against intrusions of their private intimate spaces to protection of their personal data.[31] Now, with the rise of big data, the focus has shifted even farther from protecting information qualified as "private" in nature towards protection of all identifiable information, including publicly available information, from which private information can be gleaned.[32] These developments in law-interpretation and law-application are supported, as already noted, by a change in the theory underpinning privacy. The theoretical shift involves a move away from a dominant conception of privacy as a right to be left alone,[33] to notions of privacy involving the right to exercise control over personal data and its derivative uses,[34] including controlling inter-personal information flows[35] and preventing attempts to manipulate individuals' thinking process.[36]

Like first generation rights, second generation rights can also be implemented within the existing IHRL framework. The difference between the two generations is that the former involves, at least nominally, the invocation of existing offline rights, whereas the latter entails the

[26]*See e.g.*, Kaye (Special Rapporteur on the Freedom of Opinion and Expression), *Rep*., at 20–21 ¶ 79, U.N. Doc. A/HRC/32/38 (May 11, 2016).

[27]*See e.g.*, Kay (Special Rapporteur on the Freedom of Opinion and Expression), *Rep*., at 17–18 ¶¶ 58–59, U.N. Doc. A/HRC/44/49 (Apr. 23, 2020).

[28]*See e.g.*, European Parliament Legislative Resolution of 5 July 2022 on the Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and Amending Directive 2000/31/EC, at ¶¶ 56–58, COM (2020) 0825 final (July 5, 2022).

[29]*See e.g.*, Human Rights Committee, *General Comment No. 34 - Article 19: Freedoms of Opinion and Expression*, ¶¶ 21–36, U.N. Doc. CCPR/C/GC/34 (2011).

[30]*Cf.* Saskatchewan (Human Rights Commission) v. Whatcott, [2013] 1 S.C.R. 467 (Can.), ¶ 114 ("hate speech can also distort or limit the robust and free exchange of ideas by its tendency to silence the voice of its target group").

[31]*See e.g.*, Orla Lynskey, The Foundations of EU Data Protection Law 101–02 (2015).

[32]*See e.g.*, Francesca Bosco et al., *Profiling Technologies and Fundamental Rights and Values: Regulatory Challenges and Perspectives from European Data Protection Authorities*, *in* Reforming European Data Protection Law 3, 16–19 (Serge Gutwirth, Ronold Leenes & Paul de Hert eds., 2015).

[33]*See* Samuel D. Warren II & Louis Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 205 (1890).

[34]*See e.g.*, Leonhard Menges, *A Defense of Privacy as Control*, 25 J. Ethics 385, 393 (2021).

[35]*See e.g.*, Nissenbaum, *supra* note 14, at 231.

[36]*See e.g.*, Robert H. Blank, Intervention in the Brain: Politics, Policy and Ethics 80 (2013).

https://doi.org/10.1017/glj.2023.35 Published online by Cambridge University Press

introduction of new digital rights. Among rights proposed or actually developed as part of this development, one may mention the following: An independent new right to access the Internet,[37] which stems from an understanding of access to the Internet as a prerequisite for the enjoyment of a broad range of digital rights and interests (far exceeding the traditional right to seek, receive and impart information); a new right to informational self-determination,[38] which acknowledges that the manner of representation of personal information online constitutes an extension of the human person and should be effectively controlled by the relevant data subject; and the new right not to be subject to automated decisions in important matters, which protects the right and interest of individuals to be free from arbitrary and non-accountable exercise of *de facto* power through algorithms and to exist in a non-*datafied* form.[39]

These first and second generation human rights do not require a formal change in the IHRL framework. Still, they stand in considerable tension with that framework. This is because the enjoyment of digital rights is heavily dependent on the conduct of private companies—especially Internet service providers and online Internet platforms.[40] The business model and technology these companies utilize might have a more significant impact on the ability to enjoy digital human rights than governmental regulation. The effects of this private conduct can extend to determining access to Internet sites; to the collection, retention, and retrieval of personal information; to targeting the dissemination of information to particular individuals; to the facilitation of data portability; and to decisions regarding content moderation policies, differential privacy, and algorithmic transparency. Yet, despite the new privatized reality governing the enjoyment of rights, IHRL bodies continue to focus on reviewing the legality of government conduct rather than on the business operations of private companies.[41] Furthermore, because technology companies tend to operate on a global level, using international supply-chains and infrastructure sites, their dependence on any particular host or home state might be minimal. Naturally, this limits states' ability to, and interest in, controlling these companies' activities. As a result, the model of indirect regulation of businesses in order to advance human rights concerns, a model that is built around addressing the regulatory and adjudicatory powers of the relevant states, has limited traction in the real world of digital technology.[42]

The third generation of digital rights involves, unlike the first and second generations, a move away from the traditional IHRL paradigm. It entails the recognition of digital rights held by online persons that are separate from the rights enjoyed by the physical persons that created them. Such a move in the direction of creating new legal personalities is supported by policy rationales comparable to those that led in private law to the granting of legal rights to corporations and other legal entities.[43] The third generation of rights also involves the direct imposition of obligations on Internet service providers, online platforms, and other technology companies.[44] Such new rights and obligations go beyond the traditional state-centric configuration of -IHRL- that revolves only around rights for natural persons and concomitant obligations for states. Furthermore, because

[37]*See e.g.*, Internet Governance Forum, The Charter of Human Rights and Principles for the Internet (2014), art. 1, https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/Communications/InternetPrinciplesAndRightsCoalition.pdf.

[38]*See e.g.*, Theo Hooghiemstra, *Informational Self-Determination, Digital Health and New Features of Data Protection*, 5 Eur. Data Prot. L. Rev. 160, 171–72 (2019).

[39]Alistair Markland, *Epistemic Transformation at the Margins: Resistance to Digitalisation and Datafication within Global Human Rights Advocacy*, 36 Glob. Soc'y 113, 114–16 (2022).

[40]*See e.g.*, Mariarosaria Taddeo & Luciano Floridi, *New Civic Responsibilities for Online Service Providers*, *in* The Responsibilities of Online Providers 1 (Mariarosaria Taddeo & Luciano Floridi eds., 2017).

[41]*See e.g.*, Rikke Frank Jørgensen, *Human Rights and Private Actors in the Online Domain*, *in* New Technologies for Human Rights Law and Practice 243, 253 (Molly K. Land ed., 2018).

[42]*See e.g.*, David Bilchitz, *A Chasm between 'Is' and 'Ought'?: A Critique of the Normative Foundations of the SRSG's Framework and the Guiding Principles*, *in* Human Rights Obligations of Business: Beyond the Corporate Responsibility to Respect? 107, 136–37 (Surya Deva & David Bilchitz eds., 2013).

[43]*See* Dror-Shpoliansky & Shany, *supra* note 7, at 1269.

[44]*See id.* at 1269–1270.

https://doi.org/10.1017/glj.2023.35 Published online by Cambridge University Press

they are not necessarily linked to the state, the contents of third generation rights can focus on issues that uniquely appertain to relations between online users—digital persons—and online platforms or service providers, such as digital identity or legacy,[45] and net neutrality.[46]

The upshot is that the development of digital IHRL marks a significant shift from traditional IHRL, both in terms of introducing new human rights and in challenging fundamental features of the current system of IHRL protections. The success or failure of these paradigmatic changes is tied up with other, broader, changes to IHRL, some of which have influenced and been influenced by the emergence of digital human rights. These broad changes and their implications for the development of digital human rights are discussed in Section C below.

C. Digital Rights and Changes in IHRL

The body of IHRL norms which developed out of the 1948 Universal Declaration of Human Rights has traditionally concentrated on the interplay between governments and the individuals and groups subject to their authority, aiming to curb abuse of power by the former in ways that interfere with the enjoyment of basic rights by the latter. Because states and their governments are largely creatures defined by territorial sovereignty and territorial jurisdiction, the traditional approach to IHRL also had a strong territorial focus. The interplay between a government and the governed typically occured inside the relevant state's borders. The traditional approach to IHRL also had a strong focus on regulating governmental conduct—implicitly, and at times, explicitly, considering governments as a potential source of threat to human rights.[47] Given its narrow geographical and substantive focus, it is not surprising that human rights law has tended to take a backseat when confronted with other, more specific bodies of international law, such as international humanitarian law (IHL), which are not limited in the same geographical and substantive way. That allows them, for example, to address the extra-territorial activity of non-state actors.[48] Still, as shown below, most of these traditional features of IHRL are currently in the process of becoming eroded or transformed. Such developments facilitate the development of digital human rights and are, at the same time, facilitated by them, at least to some extent.

I. Digital Human Rights and Extraterritoriality

The territorial focus of IHRL is eroding. The European Court of Human Rights (ECtHR), together with the European Commission of Human Rights, have taken the lead in developing the notion of extra-territorial jurisdiction in certain cases involving effective control over areas—such as in cases involving belligerent occupation[49]— and the exercise of state agent authority over individuals—such as in the cases of foreign detention facilities or provision of consular services.[50] Still, the Court has maintained the position that extra-territorial application of the European Convention on Human Rights (-ECHR-) remains exceptional in nature.[51] Furthermore, it has rejected the proposition that the mere capacity to interfere with the enjoyment of a right entails jurisdiction over the right holder.[52]

[45]*See e.g.*, European Declaration on Digital Rights and Principles, *supra* note 8, at Ch. 5.

[46]*See* European Declaration on Digital Rights and Principles, *supra* note 8, at pmbl. recital 2.

[47]*See e.g.*, Benjamin Gregg, The Human Rights State: Justice Within and Beyond Sovereign Nations 174 (2016).

[48]*See e.g.*, Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), June 8, 1977, 1125 U.N.T.S. 609.

[49]*See e.g.*, Loizidou v. Turkey, App. No. 15318/89, ¶ 62 (Mar. 23, 1995), https://hudoc.echr.coe.int/fre?i=001-57920.

[50]*See e.g.*, Al-Skeini v. UK, App. No. 55721/07, ¶¶ 133–37 (July 7, 2011), https://hudoc.echr.coe.int/fre?i=001-105606.

[51]*See e.g.*, *Banković*, App. No. 52207/99; Georgia v. Russia (II), App. No. 38263/08, ¶ 114 (Jan. 21, 2021), https://hudoc.echr.coe.int/fre?i=002-13102.

[52]*See Banković,* App. No. 52207/99 ¶ 75.

https://doi.org/10.1017/glj.2023.35 Published online by Cambridge University Press

Other human rights bodies have embraced a more functional approach towards the extra-territorial application of -IHRL-. These include the Inter-American Court of Human Rights (I/A -CHR-), which in its 2017 Advisory Opinion on Human Rights and the Environment focused on the degree of control exercised by states over activities taking place inside their territories but which nonetheless cause trans-boundary environmental harm.[53] Similarly, the Human Rights Committee (H.R.C.), in its General Comment 36 of 2018, developed a jurisdictional standard covering conduct with extraterritorial effects that has "direct and reasonably foreseeable impact" on the enjoyment of the right to life.[54] Finally, in 2021, the Committee on the Rights of the Child embraced "reasonable foreseeability" of impact as the test for exercising extra-territorial jurisdiction in a climate change case.[55]

At least in the case of the H.R.C., the development of a functional jurisdictional standard appears related to the emergence of digital human rights, and stemmed from engagement by the Committee with the right to privacy in connection with the extra-territorial application of online surveillance practices. In its 2014 review of the fourth periodic report of the United States, the Committee raised concerns about media reports describing surveillance activities undertaken by -US- security agencies both inside and outside U.S. territory. These episodes included the collection of bulk data and metadata, and the alleged wiretapping of European leaders.[56] The Committee recommended that the U.S. take the necessary measures to ensure that "any interference with the right to privacy complies with the principles of legality, proportionality, and necessity, regardless of the nationality or *location* of the individual whose communications are under *direct* surveillance."[57] It appears that the functional orientation of the recommendation reflected an awareness on the part of the Committee of the need to expand the scope of protection afforded by the ICCPR so that it would remain relevant as a meaningful constraint on state power in an age in which such power has been increasingly applied globally through new technology such as online surveillance technology or unmanned drones—the extra-territorial use of drones was another topic discussed in the same US periodic review session.[58]

II. Digital Human Rights and Positive Obligations

The traditional distinction between civil and political rights, on the one hand, and economic, social, and cultural rights, on the other hand, was manifested in a reading of the ICCPR that focused on negative obligations and a reading of the Internation Covenant on Economic, Social and Cultural Rights (ICESCR) that focused on positive rights.[59] That paradigm also has been significantly eroded in recent decades. In particular, the ECtHR and the H.R.C. have developed an extensive caselaw—for the Committee this includes its Concluding Observations and General Comments—that require governments to take active steps to protect individuals from measures undertaken by private actors that prevent them from enjoying their rights. These include crime prevention steps,[60] environmental regulation,[61] and welfare

[53]Advisory Opinion on the Environment and Human Rights of November 15, 2017 (I/A CHR), ¶ 102.

[54]Human Rights Committee, *General Comment No. 36: The Right to Life*, ¶¶ 22, 63 U.N. Doc. CCPR/C/GC/36 (2018).

[55]*Sacchi v. Argentina*, Views of the C.R.C. of Sept. 22, 2021, ¶ 10.7, U.N. Doc. CRC/C/88/D/104/2019 (2021).

[56]*See* Human Rights Committee, List of Issues in Relation to the Fourth Periodic Report of the United States of America (CCPR/C/USA/4 and Corr. 1), ¶ 22, U.N. Doc. CCPR/C/USA/Q/4 (2013); Human Rights Committee, Summary Record of the 3045th and 3046th Meetings (13-14 March 2014), U.N. Docs. CCPR/C/SR.3045 and CCPR/C/SR.3046 (2014).

[57]Human Rights Committee, Concluding Observations in the Fourth Periodic Report of the U.S.A., ¶ 22, U.N. Doc, CCPR/C/USA/CO/4 (2014)(emphasis added).

[58]*Id.* ¶¶ 9–10.

[59]*See e.g.*, Michael J. Dennis & David P. Stewart, *Justiciability of Economic, Social and Cultural Rights: Should There be an International Complaints Mechanism to Adjudicate the Rights to Food, Water, Housing and Health?*, 98 AJIL 462, 477 (2004).

[60]*See e.g.*, Osman v. UK, App. No. 23452/94, ¶ 115 (Oct. 28, 1998) https://hudoc.echr.coe.int/fre?i=002-6781; H.R.C., General Comment 36, *supra* note 54, ¶¶ 20–23.

[61]*See e.g.*, López Ostra v. Spain, App. No. 16798/90, ¶¶ 51–58 (Dec. 9, 1994), https://hudoc.echr.coe.int/fre?i=002-10606; H.R.C., General Comment 36, *supra* note 54, ¶¶ 26, 62.

https://doi.org/10.1017/glj.2023.35 Published online by Cambridge University Press

interventions.[62] Given the significant role played by technology companies in facilitating the enjoyment of digital human rights, including online free speech, online privacy and the right to be forgotten, it is hardly surprising that human rights officials, such as the UN Special Rapporteurs for Freedom of Expression and Privacy, have turned their attention increasingly towards the regulatory role of governments vis-à-vis technology companies.[63]

The move in the direction of imposing positive obligations on states in relation to putative violations mediated through private actors has two components of particular relevance to the realm of digital human rights. The first involves efforts to strengthen corporate responsibility through the Business and Human Rights platform. The second involves the extraterritorial reach of the human rights obligations of technology exporting countries.

Following the publication of the Ruggie Principles,[64] and the UN Guiding Principles on Business and Human Rights,[65] negotiations have been taking place under the auspices of the UN towards the conclusion of an international legally binding instrument on business and human rights.[66] The current draft instrument concentrates on the duty of states to regulate businesses, requiring them to exercise "human rights due diligence," to impose legal liability for human rights abuses, to see to it that remedies are provided to victims, and to engage in international cooperation in the implementation of the instrument.[67] No doubt, such a framework would also apply to technology companies whose activities affect the enjoyment of digital human rights, and, in particular, to those operating online platforms, providing Internet services and developing AI products.[68]

Another development relates to efforts to indirectly regulate private business enterprises by imposing positive duties to do so on their home states. It revolves around the expectation that states in which multi-national corporations (MNCs) are incorporated or headquartered should protect foreign victims harmed by MNC conduct by regulating their extra-territorial activities, including through the imposition of export controls. As already indicated, the 2017 Inter-American Court advisory opinion confirmed the existence of state obligations to ensure that activities originating from within their territory and having trans-boundary environmental impact would not infringe the human rights of individuals located elsewhere.[69] The Committee on the Rights of the Child has taken a similar approach with respect to the alleged failure of states to take adequate preventive and precautionary measures to address climate change.[70] These decisions seem to mirror parallel developments in domestic jurisprudence relating to the regulation of extra-territorial impacts caused by the activities of locally-based private businesses.[71]

[62]*See e.g.*, Z v. UK, App. No. 21830/93, para. 70 (May 10, 2001), https://hudoc.echr.coe.int/fre?i=001-58032; H.R.C., General Comment 36, *supra* note 54, ¶ 26.

[63]*See e.g.*, Irene Khan (Special Rapporteur on the Freedom of Opinion and Expression), *Rep.*, at 18 ¶¶ 90–91, U.N. Doc. A/HRC/47/25 (Apr. 13, 2021); David Kaye (Special Rapporteur on the Freedom of Opinion and Expression), *Rep.*, at 22 ¶ 57, U.N. Doc. A/74/486 (Oct. 9, 2019).

[64]*See* John Ruggie (Special Representative on Human Rights and Transnational Corporations and Other Business Enterprises), *Rep.*, U.N. Doc. A/HRC/8/5 (Apr. 7, 2008).

[65]*See* Office of the High Commissioner of the Human Rights Committee, *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework* (2011), https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf.

[66]*See Binding Treaty*, Business & Human Rights Resource Centre (2022), https://www.business-humanrights.org/en/big-issues/binding-treaty/.

[67]*See* Legally Binding Instrument to Regulate, in International Human Rights Law, the Activities of Transnational Corporations and Other Business Enterprises (third revised draft, Aug. 17, 2021), https://www.ohchr.org/sites/default/files/Documents/HRBodies/HRCouncil/WGTransCorp/Session6/LBI3rdDRAFT.pdf.

[68]*See e.g.*, The B-Tech Project, U.N. Human Rights Commission (last accessed Feb. 6, 2023), https://www.ohchr.org/en/business-and-human-rights/b-tech-project.

[69]*See* I/A HRC Advisory Opinion (2017), *supra* note 53.

[70]Sacchi, *supra* note 55.

[71]*See e.g.*, State of the Netherlands v. Urgenda Foundation, ECLI:NL:HR:2019:2007, Judgment (Sup. Ct. Neth. Dec. 20, 2019); Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court], Case No. BvR 2656/18/1, BvR 78/20/1, BvR 96/20/1, BvR 288/20, (Mar. 24, 2021), http://www.bverfg.de/e/rs20210324_1bvr265618en.html.

https://doi.org/10.1017/glj.2023.35 Published online by Cambridge University Press

The H.R.C. has had the opportunity to review the matter of export of digital products manufactured by private companies in its review of Italy in 2017. The Committee expressed concern about "allegations that companies based in the State party have been providing online surveillance equipment to Governments with a record of serious human rights violations and about the absence of legal safeguards or oversight mechanisms regarding the export of such equipment."[72] It therefore recommended that "measures are taken to ensure that all corporations under its jurisdiction, in particular technology corporations, respect human rights standards when engaging in operations abroad."[73] The matter of export controls relating to surveillance technology has also been taken up by the UN Special Rapporteur on Freedom of Expression, who has reported on the harmful effects on political expression of resort by governments to spyware programs, and called for a moratorium on the export of such technology.[74]

III. Digital Human Rights and Systemic Integration

The boundaries between IHRL and other branches of international law are also disappearing. In the past, IHRL treaty-monitoring bodies have tended to concentrate on interpreting and applying only the specific instrument with which they were entrusted. They seldom referred to other IHRL treaties or to state obligations arising out of other branches of international law, such as international humanitarian law (IHL), international refugee law, or international environmental law.[75] This "tunnel vision" approach has changed, and in recent decades there has been increased interest—in IHLR scholarship and practice—in the application of the principle of systemic integration (article 31(3)(c) of the Vienna Convention on the Law of Treaties)[76] and in giving effect to the 1993 Vienna Declaration formula concerning the indivisibility, interdependence, and interrelatedness of all human rights.[77] Consequently, IHRL treaty monitoring bodies now refer more frequently in their work to state obligations emanating from other international instruments. As a result of this development, the reach of their decisions and their potential normative influence has been extended.[78]

A similar phenomenon can be identified in connection to the application of digital rights. The prevalence of abusive online conduct, including criminal cyber-attacks, cyber-terrorism, and military cyber-attacks, has resulted in declarations about digital human rights mentioning concerns such as cyber security and to the need for a safe online environment.[79] This suggests an increased possibility for establishing links between IHRL and other legal instruments relating to cyberspace,

[72]Human Rights Committee, Concluding Observations on the Sixth Periodic Report of Italy, ¶ 36, U.N. Doc. CCPR/C/ITA/CO/6 (2017).

[73]*Id.* at ¶ 37. One source of standards governing the export of digital products can be found in best practices developed under the auspices of the Wassenaar Arrangement on Export Controls for Convention Arms and Dual-Use Goods and Technologies. *Best Practices and Guidelines*, The Wassenaar Arrangement (Dec. 1, 2022), https://www.wassenaar.org/best-practices/.

[74]*See e.g.*, Special Rapporteur on the Freedom of Opinion and Expression, *Rep.*, at 14–15, ¶¶ 48–49, U.N. Doc. A/HRC/41/35 (May 28, 2019).

[75]*See e.g.*, Simma & Pulkowski, *supra* note 19, at 511.

[76]Vienna Convention on the Law of Treaties art. 32, May 22, 1969, 1155 U.N.T.S. 331.

[77]Vienna Declaration and Programme of Action, U.N. Doc. A/CONF.157/23 (June 25, 1993).

[78]*See e.g.*, I/A Advisory Opinion, *supra* note 53, at ¶ 44; H.R.C., General Comment 36, *supra* note 54, at ¶¶ 26, 31, 62, 64–66, 70; Hassan v. UK, App. No. 29750/09, para. 102 (Sept. 16, 2014), https://hudoc.echr.coe.int/fre?i=001-146501. Note that the reference to other bodies of law has not been free from controversy and concerns have been raised concerning the expertise of members in IHRL bodies in non-IHRL issues, and about the increased potential for inconsistent decisions across different international bodies. *See e.g.*, Shana Tabak, *Ambivalent Enforcement: International Humanitarian Law at Human Rights Tribunals*, 37 Mich. J. Int'l L. 661, 707–12 (2016).

[79]*See e.g.*, European Declaration of Digital Rights and Principles, *supra* note 8, at Ch. 5.

https://doi.org/10.1017/glj.2023.35 Published online by Cambridge University Press

such as the Budapest Convention on Cybercrime[80] and the EU General Data Protection Regulation (GDPR),[81] and between IHRL and international regulatory processes concerned with cyber security, such as the Wassenaar process for regulating dual use exports of technology.[82]

In the same vein, experts bodies and civil society groups dealing with the effects of the use of AI on IHRL have been paying close attention to the process taking place under the auspices of the Conference for Disarmament with respect to autonomous weapon systems,[83] as well as to broader regulatory developments in the field of AI, such as the Draft EU AI Regulations[84] and the White House's blueprint for an AI Bill of Rights.[85] In other words, as in other fields of IHRL, the more digital technology becomes embedded in a variety of legal, political, and economic contexts, the less feasible it would be to regulate its human rights implications in isolation from other bodies of domestic, regional, and international law as well as bodies of self-regulation and co-regulation.

D. Concluding Remarks

The rise of digital human rights law—in response to the fast changes relating to the introduction of and adaptation to new technology—is changing the nature of IHRL. The consequences of this have been the radical reinterpretation of existing human rights norms, the emergence of new digital human rights, and the extension of human rights law to new right-holders and duty-holders. Furthermore, developments relating to digital human rights are also contributing to, and are influenced by, broader changes in -IHRL-. This includes a functional approach to the extra-territorial application of -IHRL-, the expansion of positive obligations relating to the conduct of private companies, and the growing inclination to construe -IHRL- instruments and promote -IHRL- norms in light of other -IHRL- instruments and other international law norms.

One question that remains to be answered, and which exceeds the scope of the present article, is whether the development of digital human rights and the associated changes in the IHRL framework are sufficient to relieve the growing pressure on the enjoyment of human rights posed by new technologies and the structures of power and control that have accompanied their emergence and widespread adoption. The future trajectory of IHRL in the digital age depends to a large extent on the answer to this question. Furthermore, the backlash by certain states against structural changes in IHRL—manifesting themselves, for example, in the new UK Bill of Rights that is

[80]Convention on Cybercrime, July 1, 2004, E.T.S. 185.

[81]GDPR, *supra* note 17.

[82]*See* The Wassenaar Arrangment: On Export Controls for Conventional Arms and Dual-Use Goods and Technologies (adopted July 11–12, 1996), https://www.wassenaar.org/. *See also NGOs Call on the 41 Wassenaar Arrangement Govts. to Take Action Against Abuse of Surveillance Rechnologies*, Business & Human Rights Resource Centre (Dec. 5, 2014), https://www.business-humanrights.org/en/latest-news/ngos-call-on-the-41-wassenaar-arrangement-govts-to-take-action-against-abuse-of-surveillance-technologies/?companies=4457572.

[83]*See* H.R.C., General Comment 36, *supra* note 54, at ¶ 65; Alasdair Sandford & Josephine Joly, *'A Threat to Humanity', NGOs and Activists Call for a Ban on the Use of 'Killer Robots'*, Euronews (Dec. 15, 2021), https://www.euronews.com/2021/12/13/a-threat-to-humanity-ngos-and-activists-call-for-a-ban-on-the-use-of-killer-robots.

[84]*Commission 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*, COM (2021) 206 final (Apr. 21, 2021). *See also How the EU's Flawed Artificial Intelligence Regulation Endangers the Social Safety Net: Questions and Answers*, Human Rights Watch (Nov. 10, 2021, 10:06 AM), https://www.hrw.org/news/2021/11/10/how-eus-flawed-artificial-intelligence-regulation-endangers-social-safety-net.

[85]*Blueprint for an AI Bill of Rights*, The White House (Oct. 2022), https://www.whitehouse.gov/ostp/ai-bill-of-rights/. *See also ACLU Comment on the Release of Whitehouse Blueprint for an Artificial Intelligence Bill of Rights*, ACLU (Oct. 4, 2022), https://www.aclu.org/press-releases/aclu-comment-release-white-house-blueprint-artificial-intelligence-bill-rights#:~:text=We%20commend%20the%20Biden%20administration,color%20and%20people%20with%20disabilities.

https://doi.org/10.1017/glj.2023.35 Published online by Cambridge University Press

supposed to reduce the impact of ECtHR judgments relating to overseas military operations and to positive state obligations[86]—puts in question the political sustainability of the very developments on which the further evolution of digital human rights hinge.

Competing Interests. The author declares none.

Funding Statement. The research was conducted with the support of ERC Grant No. 101054745: the Three Generations of Digital Human Rights (DigitalHRGeneration3), https://3gdr.huji.ac.il/.

[86]*See* Bill of Rights Bill 2022–3, HC Bill [117] (U.K.).

Cite this article: Shany Y (2023). Digital Rights and the Outer Limits of International Human Rights Law. *German Law Journal* **24**, 461–472. https://doi.org/10.1017/glj.2023.35