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 as a prevailing concept in international fora in recent years. But does this "normative equivalency" between 'offline' and 'online' afford fully effective protection for the rights of online users? This is the question at the heart of this Article. We first review the development of human rights in cyberspace as conceptualized in international fora, and critically evaluate the normative equivalency paradigm adopted by international bodies for the application of human rights online. In the latter part of this Article, we attempt to describe the contours of a new *digital* human rights framework, which goes beyond the normative equivalency paradigm. We propose such a framework should be conceptualized as built upon existing human rights norms, but containing additional protections corresponding to unique features and challenges of actors and activity in cyberspace. After laying down the normative justifications, for recognizing new digital human rights, we offer a typology of three generations in the evolution of digital human rights.

I. INTRODUCTION

The Cambridge Analytica incident,[1] and other high profile incidents[2] involving harmful online practices, such as online hate speech,[3] propagation of 'fake news',[4] intrusive

[1]Rob Price, *The UK's privacy watchdog has fined Facebook £500,000 — the maximum amount — over Cambridge Analytica*, BUSINESS INSIDER (Jul. 11, 2018), https://www.businessinsider.com/uk-watchdog-ico-fines-facebook-500000-cambridge-analytica-2018-7

[2] Cassandra Cross, *Another Day Another Data Breach – What To Do When It Happens To You*, THE CONVERSATION (Jul. 4, 2018), https://theconversation.com/another-day-another-data-breach-what-to-do-when-it-happens-to-you-99150

[3] Press Release, Secretary General, *Hate Speech is Spreading like Wildfire on Social Media*, U.N. Press Release SG/SM/19578 (May 14, 2019). *See also* Charlie Warzel, *The New Zealand Massacre Was Made to Go Viral*, N.Y TIMES (Mar. 15, 2019), https://www.nytimes.com/2019/03/15/opinion/new-zealand-shooting.html

[4] European Commission for Democracy Through Law (Venice Commission), *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 (June 20, 2019), 7-11 and p.12 ¶46. *See also* Allcott, Hunt and Matthew Gentzkow, *Social Media and Fake News in the 2016 Election*, 31 JOURNAL OF ECONOMIC PERSPECTIVES, 211-236 (2017) (hereinafter: *Allcott*)

government surveillance programs[5] and revenge porn,[6] have led to increasing concerns about the safety of the digital environment and the limited protection it affords to basic human rights, such as privacy, personal security and participation on equal terms in political life. Such concerns have prompted, in turn, critical review of the adequacy of the existing international human rights framework for addressing the challenges of the digital age, and of the need for new human rights norms and implementation strategies, specifically designed for application to cyberspace.

Identifying the applicable legal framework governing cyberspace, and its relation with other national and international law norms, has become a particularly difficult challenge in the digital age. In the past, a prevalent notion among digital rights theorists and activists was that it should be regarded as a "civilization of the mind"[7] - a global social space operating through a 'social contract', which the individual users themselves implement.[8] According to this view, it should remain a space "free of intervention" from government power.[9] Over time, with the Internet becoming an essential, 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 it have become more and more untenable.

[5] Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Rep. *on Surveillance and Human Rights*, ¶2, U.N. Doc. A/HRC/41/35 (May 28, 2019) (hereinafter: *SR Expression, 2019*)

[6] Danielle Keats Citron; Mary Anne Franks, *Criminalizing Revenge Porn*, 49 WAKE FOREST L. REV. 345, 392 (2014). *See also* Owen Bowcott, *Revenge porn and 'cyber-flashing' laws go under review*, THE GUARDIAN (Jun. 26, 2019), https://www.theguardian.com/law/2019/jun/26/revenge-porn-and-cyber-flashing-laws-go-under-review

[7] John Perry Barlow, *Declaration of the Independence of Cyberspace*, (Feb. 8, 1996). https://www.eff.org/cyberspace-independence (hereinafter: *Barlow*) ("We will create a civilization of the Mind in Cyberspace. May it be more humane and fair than the world your governments have made before").

[8] David P. Fidler, *Cyberspace and Human Rights*. *In* RESEARCH HANDBOOK ON INTERNATIONAL LAW AND CYBERSPACE 96-97 (Nicholas Tsagourias ed., 2015). (Hereinafter: *Fidler*). For more initiatives see e.g: Dyson, Gilder, Keyworth and Toffler, *Cyberspace and the American Dream: A Magna Carta for the Knowledge Age* (initiative by the Progress & Freedom Foundation, 1994); Declaration of Internet Freedom, 2012.

[9] *Id*. *See also* Gill Lex, Redeker Dennis and Gasser Urs, *Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights* Berkman Klein Research Center, Publication No. 2015-15, p.18 (Nov. 9, 2015). (Hereinafter: *Gill, Redeker & Gasser*).

Furthermore, as the dependency on the Internet increases, the line between regulating 'online' and 'offline' lives becomes more and more blurred,[10] and it is no longer possible to describe the Internet as merely a "world of identities with no bodies".[11] The more cyberspace becomes a place where basic human rights might be enjoyed or infringed,[12] the greater is the expectation that local, regional and global governance bodies would take action to protect the rights of online users and prevent their abuse. Indeed, what methods and means can adequately ensure the protection and promotion of human rights online is an issue of growing concern for international and regional bodies, and public and private actors. In a series of resolutions issued in recent years, both the United Nations General Assembly (GA)[13] and the Human Rights Council (HRC)[14] have addressed this issue, departing from the position that the same human rights people have offline must be protected online as well. This position is referred to in this article as the 'normative equivalency' paradigm.

[10] Daniel Joyce, *Privacy in the digital era: human rights online?*, 16 MELB. J. INT. LAW. 270, 273 (2015). (Hereinafter: *Joyce*). *See also* Lorna McGregor, Daragh Murray and Vivian Ng, *Four ways your Google searches and Social Media Affect Your Opportunities in Life*, THE CONVERSATION (May 22 2018), https://theconversation.com/four-ways-your-google-searches-and-social-media-affect-your-opportunities-in-life-96809

[11] Barlow, *supra* note 7 ("A world that is both everywhere and nowhere, but it is not where bodies live").

[12] United Nations specialized agency for information and communication technologies - International Telecommunication Union (ITU), *The Quest For Cyber Peace*, at xi (foreword) (2011), https://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-PDF-E.pdf ("In the world of 2011, we enjoy the benefits of a boundless global information society, but with these benefits comes the threat of cyber attacks. They can arise anywhere, at anytime, and cause immense damage in the blink of an eye. This potential damage is increased exponentially by the linking of information and communication technologies (ICTs) with vital national infrastructures. We must act now to stem this growing threat").

See also United Nations High Commissioner for Human Rights (OHCHR), Rep. *The Right to Privacy In The Digital Age*, U.N. Doc. A/HRC/39/29, at ¶61(a) (3 Aug. 2018). (Hereinafter: *OHCHR Privacy Report 2018*). (The High Commissioner recommended states to "Recognize the full implications of new technologies, in particular data-driven technologies for the right to privacy, but also for all other human rights").

[13] G.A Res. 68/167 ¶3 (18 Dec. 2013) (hereinafter: *G.A Res 68/167*); G.A Res. 69/166 ¶3 (18 Dec. 2014); (hereinafter: *G.A Res 69/166*); G.A Res. 71/199 ¶3 (19 Dec. 2016); (hereinafter: *G.A Res 71/199*); G.A Res. 73/179 ¶3 (17 Dec. 2018) (hereinafter: *G.A Res 73/179*).

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

While some scholars claim that there is consensus around this position,[15] questions regarding necessary adjustments to human rights when interpreted and applied in cyberspace still remain.[16] Regarding the right to privacy, for example, the GA itself pointed to the "vast technological leaps"[17] that cast doubt on whether the existing human rights framework is sufficient to encompass the range of protections that individuals need when interacting online. Another example is the ongoing debate in international fora on whether Internet access should be merely understood as an essential condition for the fulfilment of freedom of expression and right of access to information, or also recognized as a new independent human right.[18]

But beyond the specific challenges associated with the recalibration of existing human rights to cyberspace, there lies a broader normative inquiry, that is, whether the basic 'normative equivalency' paradigm, embraced by the GA and HRC, is a fully satisfactory normative starting point, in light of the unique features of cyberspace. Arguably, cyberspace offers a fundamentally different environment for the enjoyment of human rights than the physical world. Unlike the physical space which States occupy, cyberspace is de-territorialized and de-centralized, and non-state actors play a dominant role in constructing it and operating therein.[19] In this digital environment, new needs and interests are constructed and the significance of pre-existing needs and interests may radically change. Such features render tenuous the 'fit' between territory-based and state-centered offline human rights and the individual and group protections necessary in cyberspace. It is not surprising that the 'normative equivalency' paradigm

[15] Rona, Gabor and Aarons, Lauren, State Responsibility to Respect, Protect and Fulfill Human Rights Obligations in Cyberspace. 8 J.NAT'L SECURITY L. & POL'Y (2016) (hereinafter: *Gabor*)

[16] Fidler, *supra* note 8 at 103.

[17] G.A Res. 69/166, *supra* note 13, at 2 ("Noting with appreciation general comment No. 16 of the Human Rights Committee on the right to respect of privacy, family, home and correspondence, and protection of honour and reputation, while also noting the vast technological leaps that have taken place since its adoption").

[18] S. Tully, *A Human Right to Access the Internet? Problems and Prospects*, 14(2) HRLRev. 175, 177-181 (2014) (hereinafter: *Tully*). See also *supra* note 89.

[19] Yuval Shany, *Contribution to Open Consultation on UN GGE 2015 Norm Proposals*, THE FEDERMANN CYBER SECURITY RESEARCH CENTER (January 2018), https://csrcl.huji.ac.il/sites/default/files/csrcl/files/contribution_un_gge_norm_proposals-_dd.pdf (hereinafter: *Shany*).

was recently criticized by the UN Special Rapporteur on the Right to Privacy, who argued that it cannot provide adequate protection for the right to privacy.[20]

The present article challenges the over-reliance of human rights bodies on the 'normative equivalency' paradigm and suggests a typology for identifying three stages in the development of digital human rights norms that goes beyond the existing paradigm and facilitates the emergence of a new normative framework. Although the chronological and conceptual boundaries between the three stages are somewhat blurred, it is possible to identify within them 'ideal type' legal constructs that helps us to map the development of digital human rights in ways similar to the manner in which the language of human rights generations has helped us in the past to theorize the development of human rights in the physical world.[21]

According to the proposed typology one can identify three generations of digital human rights: **The first generation** involves processes of significant adjustment of offline human rights to the online world. **The second generation** features the emergence of new digital rights – that is, rights that protect online activities that do not have close parallels in the offline world. Although such second generation digital human rights may be traced back to existing offline human rights, the new progenies are not fully subsumed in the rights they originate from, and it would be hard to fully capture the interests and the human needs that they protect if they will not be recognized as stand-alone digital human rights. In other words, they go significantly beyond the 'normative equivalency' paradigm. **The third generation of online human rights** includes rights belonging to new *online personae*. An online persona is the digital representation of natural persons or legal entities, such as corporations, who can exist separately from the human beings that created them. For example, digital persons may outlive the physical persons who created them or have a separate identity. Arguably, the

[20] Special Rapporteur on the Right to Privacy, Rep., U.N Doc. A/HRC/37/62, p.26 ¶6 (Feb. 28, 2018). ("When 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") (hereinafter: *SR Privacy, 2018*).

[21] JOSEPH 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 (University Press of America, 1998). *See also* R.L Zohadi, *The Generations of Human Rights*, 1 INTLSTUD 95, 97-107 (2004).

independent set of legal interests held by digital personae justifies constituting them as independent holders of new sets of rights.

Ultimately, recognizing digital human rights designed to apply online requires us to consider the ethical foundations underlying human rights law, explore the outer limits of international human rights law, and examine the contemporary discourse on the intersection between human rights and digital space. The following parts discuss and critically evaluate the contemporary debate surrounding such issues in international law, as well as in international decision making and policy setting circles.

II. THE DEVELOPMENT OF DIGITAL HUMAN RIGHTS IN INTERNATIONAL FORA

General Assembly and Human Rights Council Resolutions on Digital Human Rights

The application and interpretation of human rights law in cyber-space has been the subject of multiple resolutions adopted by UN human rights bodies in recent years. In 2012, the Human Rights Council asserted that "the same rights people have offline must also be protected online".[22] In a series of resolutions adopted since then, both the Human Rights Council[23] and the General Assembly[24] have reiterated the notion that human rights apply in the digital 'online world' as they apply in the 'offline world', embracing thereby the 'normative equivalency' paradigm.

Over the years, General Assembly and Human Rights Council 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.[25] For example, whereas in 2013 the GA Resolution requested states to review their procedures,

[22] HRC 20/8, *supra* note 14, ¶1 at 2.

[23] *Supra* note 14.

[24] *Supra* note 13. *See also:* Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, *Rep.* ¶5, U.N. Doc. A/HRC/35/22 (Mar. 30, 2017) (hereinafter: *SR Expression, 2017*). *See also*: Gabor, *supra* note 15, at 503. Anja Mihr, *Good cyber governance: The human rights and multi-stakeholder approach*, GJIA 24, 28 (2014). (hereinafter: *Mihr*).

[25] Compare, for example, operative clause 4 and operative clause 5 in G.A Res. 69/166 and G.A Res. 71/199 respectively, *supra* note 13. *See also:* HRC 20/8 and HRC 32/13, *supra* note 14.

legislation and practices with regard to surveillance of communications,[26] 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.[27] A 2016 GA Resolution (Resolution 71/199), also mentioned the growing concern regarding the sale of personal data, and called on states to enhance protection against such practices and develop preventive measures and sanctions in addition to remedies to victims.[28]

Notably, the 2016 GA Resolution explicitly addressed the duties imposed on private technology companies.[29] Although the general expectation that private companies meet their obligations according to the UN Guiding Principles on Business and Human Rights was already mentioned in previous resolutions,[30] Resolution 71/199 includes such an expectation in an operative paragraph directed at companies (alongside operative paragraphs directed at states), and adds on a new requirement: to inform online users about the collection, sharing and retention of their data and to establish transparency policies.[31] The Resolution also encourages private companies to take steps in order to provide safe communication for users, including by introducing technical solutions.[32] Resolution 71/199 thus appears to mark a move away from the state-centric approach to human rights obligations taken in previous GA and HR Council resolutions, acknowledging the key role played by private actors in the protection and implementation of human rights online.[33]

Moreover, it appears that both the General Assembly and the Human Rights Council increasingly acknowledge the broad interplay between the right to privacy and other

[26] G.A Res. 68/167, *supra* note 13, at ¶4(c).

[27] G.A Res. 69/166, *supra* note 13, at ¶4(e).

[28] G.A Res. 71/199, *supra* note 13, at ¶5(f)-(g)

[29] *Id*, at ¶6.

[30] *See for e.g*: G.A Res. 69/166, *supra* note 13, at 3; Human Rights Council Res. 28/16, UN.Doc. A/HRC/28/16, p. 3 (March 26, 2015) (hereinafter: HRC 28/16)

[31] G.A Res. 71/199, *supra* note 13, at ¶6. *See also:* G.A Res 73/179, *supra* note 13, at ¶7.

[32] G.A Res. 71/199, *supra* note 13, at ¶7.

[33] Shany, *supra* note 19, at 4.

human rights, mainly the right to freedom of expression and the right to seek and receive information. 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.[34]

The normative assumptions underlying UN resolutions

A broader look the UN resolutions adopted in recent years under agenda items titled 'the right to privacy in the digital age' and 'the promotion, protection and enjoyment of human rights on the Internet', suggests that the relevant UN bodies are 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, they also enjoy online. Pursuant to this paradigm, the Internet is one medium among many 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 or discrimination, 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.[35]

The second proposition is that states should actively facilitate safe access for individuals to the Internet.[36] This proposition is based on the insight that cyberspace is becoming an increasingly important arena for enjoying human rights,[37] and that the digital divide and problem of digital illiteracy are leaving behind large numbers of individuals without having the ability to effectively exercise their human rights.[38] In the same vein, states should address online security concerns,[39] so as to ensure that the Internet is a safe and trustworthy environment, where individuals are able to freely

[34] G.A Res. 71/199, *supra* note 13, at 3.

[35] See e.g., HRC 26/13, *supra* note 14, at 1-2.

[36] See, e.g: HRC 20/8, *supra* note 14, ¶3 at 2; HRC 26/13, *supra* note 14, ¶3 at 2.

[37] See, e.g*:* HRC 26/13, *supra* note 14, at 1-2*;* G.A Res. 73/179, *supra* note 13, at 2-3.

[38] See, e.g: HRC 32/13, *supra* note 14, ¶4 at 3; G.A Res 73/179, *supra* note 13, at 3.

[39] See, e.g*:* HRC 26/13, *supra* note 14, ¶5 at 2.

operate, realize their capabilities and enjoy their rights.[40] To that effect, states are expected to curb abuses of the rights of users on the Internet, by way of imposing sanctions against violators,[41] providing remedies for victims[42] and taking necessary preventive measures.

Significantly, among the potential abuses that the resolutions mention, one finds intrusive online state surveillance activities[43] undertaken without effective oversight mechanisms,[44] entailing the collection and interception of data[45], aggregation of metadata and the sale of personal data.[46] Such practices would be regarded as abusive if they fail to comply with principles of necessity, proportionality, non-arbitrariness and lawfulness.[47] Other potential abuses noted in the resolutions are online incitement,[48]

[40] *Id*, ¶1 at 2 ("Noting also the importance of building confidence and trust in the Internet, not least with regard to freedom of expression, privacy and other human rights so that the potential of the Internet as, inter alia, an enabler for development and innovation can be realized").

[41] G.A Res 71/199, *supra* note 13, at ¶5(f).

[42] G.A Res 69/166, *supra* note 13, ¶4(e).

[43] Other international human rights bodies have grappled extensively with the problems of online surveillance, including the Human Rights Committee and the Special Rappaport for the Right to Privacy. See: Anja Seibert-Fohr, *Digital Surveillance, Meta Data and Foreign Intelligence Cooperation: Unpacking the International Right to Privacy*, available at: SSRN: https://ssrn.com/abstract=3168711 (April 25, 2018) (hereinafter: *Seibert-Fohr*) ; Yuval Shany, *On-Line Surveillance in the case-law of the UN Human Rights Committee* (July 2017) available at: https://csrcl.huji.ac.il/people/line-surveillance-case-law-un-human-rights-committee; Prof. Joseph A. Cannataci, United Nations Special Rapporteur on the Right to Privacy, *Draft Legal Instrument on Government Surveillance and Privacy* (January 10, 2018), available at: https://www.ohchr.org/Documents/Issues/Privacy/DraftLegalInstrumentGovernmentLed.pdf (hereinafter, *Draft Legal Instrument on Surveillance and Privacy*).

[44] G.A Res. 68/167; G.A Res. 69/166; G.A Res. 71/199, *supra* note 13. HRC 28/16, *supra* note 30; HRC 32/13, *supra* note 14. *See also* OHCHR Privacy Report 2018, *supra* note 12 at ¶33.

[45] G.A Res. 69/166, *supra* note 13, at 2.

[46] G.A Res. 71/199, *supra* note 13, at 3.

[47] G.A Res. 71/199, *supra* note 13, at 2; G.A Res 69/166, *supra* note 13, at 2. ; HRC 28/16, *supra* note 30, at 2. *See also*: Anne Cheung and Rolf H. Weber, *Internet Governance and the Responsibility of Internet Service Providers*, 26 Wis.Int'l L.J. 403 (2008) (hereinafter: *Cheung&Weber*); KITTICHAISAREE KRIANGSAK, PUBLIC INTERNATIONAL LAW OF CYBERSPACE 1-22 (Springer, 2017) (hereinafter: *Kittichaisaree*).

[48] HRC 26/13, *supra* note 14, ¶6 at 2.

online harassment of human rights defenders[49] and the purposeful disruption of access to information online.[50]

The third normative proposition is that protection of digital human rights 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 relevant stakeholders in order to promote and protect human rights online and address the challenges posed for human rights by new communication technology.[51] 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.[52] Still, the precise nature of this responsibility and the remedies it entails, remains unclear.[53] It may be noted in this regard that the Special Rapporteur on the Right to Freedom of Opinion and Expression has been focusing in recent years on the application of freedom of expression in the digital age, with a specific emphasis on the role of private actors in protecting freedom of opinion and expression. In a recent Report, he emphasized the need for "radical transparency and meaningful accountability", including public and ICT sector accountability mechanisms.[54]

Though neither the Assembly or the Council' resolutions are binding, they reflect growing awareness by global political elites of the importance of respecting international human rights in the digital sphere, and indicate some willingness by states to take steps to address the unique threats and challenges for human rights found in

[49] G.A Res. 71/199, *supra* note 13, at 4. *See also*: HRC 28/16, *supra* note 30.

[50] HRC 32/13, *supra* note 14, at 2.

[51] G.A Res. 71/199, *supra* note 13, at 2; G.A Res. 69/166, *supra* note 13, at 3; HRC 32/13, *supra* note 14, *at* 3; HRC 26/13, *supra* note 14, at 2; HRC 32/13, *supra* note 14, at 3.

[52] G.A Res. 69/166, *supra* note 13, at 3; G.A Res 71/199, *supra* note 13, ¶6.

[53] Yael Ronen, *Big Brother's Little Helpers: The Right to Privacy and the Responsibility of Internet Service Providers*, 31 UTRECHT J. INT'L & EUR. L., 72 (2015) (hereinafter: *Ronen*). *See also*: Emily C. 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 Pitt. J.TECH. L. & POL'Y, 69-70 (2011) (hereinafter: *Miletello*).

[54] Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, *Rep*. ¶64-72, U.N Doc. A/HRC/38/35 (April 6, 2018) (hereinafter: *SR Expression 2018*).

cyber-space. The resolutions also generate an expectation that human rights should guide Internet governance.

The Special Rapporteur on the Right to Privacy

Another indication of the growing attention paid by the UN to human rights in the digital age has been the appointment in 2015 by the Human Rights Council 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.[55] In a recent report, the Special Rapporteur reiterated the General Assembly's concern about the significant gap that exists between the existing legal framework for the protection on the right to privacy and contemporary challenges.[56] For example, the Special Rapporteur noted with concern that in the era of big data, information no longer needs to be 'personalized' in order to identify any specific individual,[57] and that new technologies can reveal highly personal private details.[58] It is precisely because of this significant gap between legal regulation and the power of technology that the Rapporteur has criticized over-reliance on the normative equivalency approach found in the UN Resolutions on digital human rights. According to the Special Rapporteur, the position according to which 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.[59] There is thus an urgent need, he maintained, to develop a comprehensive international legal framework that would provide the necessary normative guidelines for the protection of the right to privacy in the digital age.[60]

[55] HRC 28/16, *supra* note 30, at ¶4.

[56] SR Privacy 2018, *supra* note 20, at 26-28.

[57] *Id*. at ¶54.

[58] *Id*. ¶5 at 25.

[59] *Id*. ¶6 at 26 ("When 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"). *See also* ¶28 at 29: "…In order to resolve problems of jurisdiction in cyberspace, this can be only provided by detailed international law which does not yet exist in the surveillance sector, including in the European region".

[60] *Id*. at ¶29-31. ("In order to create such a clear and comprehensive legal framework it is essential that an international legal regime regulating issues of jurisdiction in cyberspace be properly developed, with a commonly agreed set of principles to establish what state behavior in cyberspace and that especially related to surveillance and cyber-espionage, is acceptable, why and when").

Digital human rights and private actors

The call to develop a new human rights framework for the digital 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 often find themselves being subject to competing pressures: Online users – their customers– demand effective protection of their basic rights (privacy, freedom of expression, etc.), whereas certain governments wish to utilize online platforms, search engines and the like to obtain information on individuals and groups, in order to control and suppress activities on cyberspace which they consider undesirable. As a result, technology companies face increasing governmental regulation, requiring them to remove offensive expressions.[61] In situations of this kind, technology companies must decide whether or not to adjust their usage policies to the applicable governmental regulation, bearing in mind the fact that government may try to exert control over the physical infrastructure that they use, or try to sanction them or curtail their activities if they fail to comply with domestic law and policy.[62] At the same time, since technology companies operate across multiple jurisdictions with widely divergent laws, it would be extremely difficult for them to adopt business standards and practices that are compatible with all relevant domestic laws.[63] This is especially the case when domestic laws conflict with the companies' internal policies and the ideological dispositions of their management and owners, or where acceding to the demands of local governments might adversely affect the public image of the relevant companies.

In light of the normative uncertainty and regulatory instability surrounding the application of digital human rights, some international initiatives for developing common online human rights policies have emerged from processes heavily involving private actors. Recent examples include the Toronto Declaration on Machine Learning Standards, calling on both governments and private companies to ensure that algorithms

[61] Miletello, *supra* note 53.

[62] SR Expression 2018, *supra* note 54, at 19.

[63]SR Expression 2018, *supra* note 52, at 4-6. See also: Kittichaisaree, *supra* note 47, at 49-50, 95-97; Andreas Zimmermann, *International Law and 'Cyber Space*' 3(1) ESIL, p.6. (2014) (hereinafter: *Zimmermann*).

respect basic principles of equality and non-discrimination;[64] a variety instruments created under the auspices of ICANN (the Internet Corporation for Assigned Names and Numbers), with a view to protecting human rights online (which includes reference to various human-rights principles and norms);[65] and other multi-stakeholder initiatives on international Internet governance alluding to human rights as core guiding principles.[66] These initiatives underscore the growing support among relevant stakeholders for the need to better define the digital human rights framework and to develop human-rights friendly policies that would be specifically suited for cyberspace.[67]

The upshot of this short survey of recent international standard-setting attempts is that there is broad consensus around the notion that international human rights provide a basic framework for protecting the rights of online users and that it should guide the future development of Internet governance.[68] There is also broad consensus that much work remains to be done in order to overcome the challenges of applying 'offline' human rights online. Two particularly difficult structural challenges that stand out in this regard are digital divides across and within countries[69] and lack of transparency in

[64] The Toronto Declaration: Protecting the right to equality and non-discrimination in machine learning systems, May 16, 2018 (initiated by *Accessnow* at RightsCon Toronto 2018) available at: https://www.accessnow.org/the-toronto-declaration-protecting-the-rights-to-equality-and-non-discrimination-in-machine-learning-systems/

[65] The Internet Corporation for Assigned Names and Numbers (ICANN), Human Rights Impact Assessment (May 25, 2019), *available at*: https://www.icann.org/en/system/files/files/summary-report-hria-15may19-en.pdf. See also: Fidler, *supra* note 8 at 116.

[66] See *supra* note 141. See also: The Christchurch Call to Eliminate Terrorist and Violent Extremist Content Online https://www.christchurchcall.com/index.html (hereinafter: *The Christchurch Call*)

[67] OHCHR Privacy Report 2018, *supra* note 12, at ¶48-49.

[68] Mihr, *supra* note 24, at 24-26. *See also*: SR Expression 2018, *supra* note 54, at ¶41,70.

[69] United Nations specialized agency for information and communication technologies - International Telecommunication Union (ITU), *Digital Inclusion for All*, (November 2019) *available at:* https://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. Many of the unconnected live in least developed countries, landlocked developing countries and small island developing states. Globally, over 1 billion new internet users have been added over the last 4 years, however substantial digital divides persist between more and less connected countries, communities, and people"). *See also*: ANDREW MURRAY AND MATHIAS KLANG, HUMAN RIGHTS IN THE DIGITAL AGE 5 (2004) (hereinafter: *Murry&Klang*).

corporate decision making and software design.[70] 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 to generate a more accurate picture on human rights violations and even to predict future violations.[71]

On the conceptual level, the adequacy of the normative equivalency paradigm to comprehensively capture all digital human rights can be questioned. It is doubtful whether this paradigm succeeds in effectively addressing the particular challenges of the current digital environment, which is deterritorialized, decentralized, and dominated by private actors and gives rise to new or different needs and interests. As a result, strictly adhering to the offline human rights framework may constitute a straightjacket, hindering the development of a more suitable set of legal protections. A new theory and typology of digital human rights law might therefore need to be developed. The next part of the article attempts to lay down some guiding principles, which may facilitate the identification and definition of digital human rights. It also suggests possible directions for future development that go beyond the normative equivalency paradigm.

III. DEVELOPING NEW DIGITAL RIGHTS FOR CYBER-SPACE

Critique of the normative equivalency paradigm

As the previous part shows, international human rights standards have been re-interpreted in recent years with a view to tackling the new challenges posed by the current digital age (with most attention being given to the right to privacy and freedom of expression).[72] Still, the full suitability of offline human rights to an online digital environment, which the normative equivalency paradigm assumes is open to challenge.

---

[70] SR Expression 2017 *supra* note 24, at ¶7 and ¶82. See also: Penney, Jonathon and McKune, Sarah and Gill, Lex and Deibert, Ronald J., *Advancing Human Rights-by-Design in the Dual-Use Technology Industry* JOURNAL OF INTERNATIONAL AFFAIRS, *71*(2), 103 (December 20, 2018).

[71] Charlotte Arnaud, *opportunities in the new digital age*, The UN Refugee Agency (UNHCR) Blog (October 26, 2017) https://www.unhcr.org/blogs/opportunities-in-the-new-digital-age/; Corinna Frey, Marian Gatzweiler, *How Tech can Bring Dignity to Refugees in Humanitarian Crises*, THE CONVERSATION (2 May, 2018) https://theconversation.com/how-tech-can-bring-dignity-to-refugees-in-humanitarian-crises-94213

[72] Land, Molly, *Toward an International Law of the Internet*, *HARV. INT'L LJ* 54, 393, 437-442 (2013) (hereinafter: *Land*)

Such a challenge is not directed against the propriety of extending of some offline human rights to cyberspace; rather, it questions the automatic and uncritical nature of the extension.

There is a vast literature on the unique attributes of cyberspace and the difficulties in applying national and international law to it.[73] Whereas national and international legal systems are built around the principle of territorial sovereignty, which delineates the regulatory powers of different states (subject to a number of extra-territorial exceptions), the deterritorialized nature of cyberspace and the global reach of online services, products and transactions, creates a haunting regulatory challenge.[74] Although international human rights law applies extra-territorially, such application is linked to notions of control or direct and reasonable foreseeable impact over the enjoyment of rights and does not result, as a rule, in imposing on states general obligations to protect individuals located in other countries.[75] 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 use. Under these circumstances, focusing exclusively on governments as the principal duty-bearers, as international human rights law normally does, might create a wide gap between the sweeping reach of the law and the reality in which states exercise power over individuals only in some distinct fields of online activity. Note that even as regulators of online activity, the role of states in practice is often marginal, as some Internet and social media companies are exceptionally powerful entities, much better situated to regulate online conduct than states.

The actual configuration of power, control and authority in cyberspace, where technology companies sometimes serve as buffer against governmental abuse of

[73]Zimmermann, *supra* note 63. *See also*: Kubo Mačák, *From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers*, 30 LEIDEN JOURNAL OF INTERNATIONAL LAW 877–899 (2017)

[74] Michael N. Schmitt, *Grey Zones in the International Law of Cyberspace*, 42:2 THE YALE JOURNAL OF INTERNATIONAL LAW (2017); Uta Kohl, *Jurisdiction in cyberspace*, RESEARCH HANDBOOK ON INTERNATIONAL LAW AND CYBERSPACE 30–54 (2015);Wolff Heintschel von Heinegg, *Territorial Sovereignty and Neutrality in Cyberspace*, 89 INTERNATIONAL LAW STUDIES 17 (2013).

[75] UN General Assembly, *International Covenant on Civil and Political Rights*, ¶2(1), Dec. 10, 1966, 999 U.N.T.C 171; MARKO MILANOVIC, *EXTRATERRITORIAL APPLICATION OF HUMAN RIGHTS TREATIES: LAW, PRINCIPLES, AND POLICY* (OXFORD UNIVERSITY PRESS, 2011).

rights,[76] and sometimes government serve as a check on the power exercised by technology companies should influence the way in which offline human rights are re-interpreted when exercised online.[77] As the Special Rapporteur Special Rapporteur on the Right to Privacy noted, a significant technological gap may render an automatic transfer of rights from the offline to online "hopelessly inadequate".[78]

The normative inquiry: Justifying the creation of new digital human rights

The doubts concerning the adequacy of the normative equivalency paradigm for protecting human rights online invite a normative inquiry: under what conditions should new digital human rights be developed for protecting basic individual rights in cyberspace in light of the new or different needs and interests of online users.[79] This question invites in turn a mapping exercise, identifying protection gaps in the existing legal framework, which is premised on the online application of offline human rights. Such gaps may be filled – where appropriate - by new digital human rights.[80] Another line of inquiry examines whether online human rights that have been recognized in international instruments or are being advocated by activists and experts in the field, can be captured by the normative equivalency paradigm. If not, they too might influence the development of a new digital human rights framework.

Acknowledging digital rights as new human rights requires addressing key issues relating to the theory of human rights. That is, what qualifies an interest or value to be worthy of protection as a 'human right',[81] and under what conditions do such

[76] SR Expression 2017, *supra* note 24, at ¶ 82; Ronen, *supra* note 53, at 72.

[77] *Cheung&Weber supra* note 47, at 408-412.

[78] See *supra* note 20.

[79] Joyce, *supra* note 10, at 273 *("*"A methodological weakness of the Resolution's approach is linked with its symbolic affirmation of the need to migrate the protections afforded 'offline', such as privacy, to the 'online' world"). *See also*: Shany, *supra* note 19.

[80] Kay Mathiesen, *Human Rights for the Digital Age*, 29 JOURNAL OF MASS MEDIA ETHICS 2–18 (2014) (hereinafter: *Mathiesen*); Ashley Deeks, *an International Legal Framework for Surveillance*, 55 VA. J. INT'L L 291, 295-298, 327-338 (2014) (hereinafter: *Deeks*). ; Bill Thompson, The digital age of rights, BBC News (May 26, 2009). available at: http://news.bbc.co.uk/2/hi/technology/8068463.stm

[81] RONALD DWORKIN, TAKING RIGHTS SERIOUSLY (Harvard University Press; Fifth Printing edition 1978) (hereinafter: *Dworkin*) ; JOHN RAWLS, A THEORY OF JUSTICE (Revised edition, Harvard University Press, 1999) (hereinafter: *Rawls*).

justifications lead to the adoption of internationally legally binding norms.[82] At another level, the debate of online human rights poses the question of the elasticity of human rights: Are they evolving norms that change over time in accordance with the developing needs of society, or do human rights norms have fixed contents inherent to the experience of being human, which transcends time, place or technology?[83]

Responding to such fundamental questions exceeds the scope of the present article. For our purposes, we will concentrate on the process of social recognition of new rights[84] – that is, on calls for positively acknowledging them in the form of an international legal instrument or through interpreting existing instruments. Such social recognition is inevitably tied to a moral claim about the justification for protecting the interests or values captured by the new right, the fear of abuse of power in the absence of a right, which is often based on historical experience of exploitation and injustice, and an assertion relating to the universality of the said moral claim and fear of abuse.[85] We first illustrate the relevance of this approach through examining calls for recognizing a new human right to Internet access, and then move on to offer a typology of calls relating to other online human rights.

The Right to Internet Access - A New Digital Human Right?

A paradigmatic example of a call for creating or recognizing a new digital human right can be found with relation to the so-called right to Internet access. Under the normative equivalency paradigm, new technologies, including the Internet, are simply new platforms or methods of communication for exercising existing human rights. As a

---

[82] Charles Beitz, *What Human Rights Mean*, 132 DAEDALUS 36–46 (2003). (hereinafter: *Beitz*); See also Andrew Moravcsik, *The Origins of Human Rights Regimes: Democratic Delegation in Postwar Europe*, 54 INTERNATIONAL ORGANIZATION 217–252 (2000); Louis Henkin, *International Human Rights as Rights*, 1 CARDOZO L. REV. 425 (1979).

[83] J. Raz, *Legal Rights*, 4 OXFORD JOURNAL OF LEGAL STUDIES 1–21 (1984) (hereinafter: *Raz, Legal Rights*); J. Roland Pennock, *Rights, Natural Rights, and Human Rights—a General View*, 23 NOMOS 1–28 (1981).

[84] See *supra* note 80. Also see: Jules L. Coleman, *Negative and Positive Positivism*, 11 J. LEGAL STUD. 139, 140, 150-151 (1982).

[85] Mary Glendon, *Knowing the Universal Declaration of Human Rights*, 73 NOTRE DAME LAW REVIEW 1153 (1998); See also ANTONIO CASSESE, REALIZING UTOPIA: THE FUTURE OF INTERNATIONAL LAW (2012) 136-137. Douglas Donoho, *Relativism Versus Universalism in Human Rights: The Search for Meaningful Standards*, 27 STANFORD JOURNAL OF INTERNATIONAL LAW 345, 357 (1991).

result, they should be regulated in a manner similar to the manner in which other media platforms or communication methods that individuals use for exercising their human rights are regulated. Put differently, the Internet facilitates the exercise of human rights, such as freedom of expression, and protection of access to the Internet may derive from the need to respect and ensure such other human rights. Still, such a right of access does not constitute a stand-alone human right recognized in detachments from other human rights it helps to realize. Yet, a closer look at the right to Internet access suggests that with time, such access has become much more than merely a means to realize other rights; it is emerging as a right in and of itself.

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.[86] While the report did not declare a "right to access", La Rue emphasized the "positive obligation of states to facilitate the right to freedom of expression via the Internet".[87] Subsequently, David Kaye, who replaced La Rue as Special Rapporteur for Freedom of Expression, focused his attention also on the duty of technology companies to promote digital expression and to resist restrictions on access to the Internet.[88]

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. The adverse implications of online content restrictions and interference with access, and state obligations in this regard were repeatedly underscored.[89]

[86]Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression *Rep.* U.N Doc. A/66/290 ¶ 80 (August 10, 2011) (hereinafter: *SR Expression 2011*).

[87]*Id*, at ¶61.

[88]SR Expression 2017, *supra* note 24, at ¶47-50.

[89] Joint Declaration by The United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information, *Challenges to Freedom of Expression in the Next Decade* (July 10, 2019).; *See also* Parliamentary Assembly of the Council of Europe (PACE), *The Right*

In parallel to these developments, a number of academics have 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 Internet access and its potential to address the geo-political digital divide.[90] Furthermore, some states started to incorporate the right to access into their national legislation.[91] The combined effect of the non-binding resolutions, declarations and reports on the need to ensure universal access to the Internet, the growing discourse about the need to develop such a right and emerging state practice, may suggest a movement towards recognizing access to the Internet as a new digital human right, although it has not obtain such a status under international law yet.[92]

As for the ingredients of the right, one may note that, in his initial Report, La Rue focused on two main aspects of access: access to an Internet connection and access to online content.[93] He emphasized the unique nature and potential of the Internet, not just as another media, but as a new platform, an arena that would impact people's lives in a variety of ways.[94] With regard to access to an Internet connection, the issue of digital divide and access to telecommunication still poses a serious concern,[95] but, in recent

to Internet Access, Resolution 1987 (April 9, 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 23, at¶76; Tim Sandle, *UN thinks internet access is a human right*, BUSINESS INSIDER, https://www.businessinsider.com/un-says-internet-access-is-a-human-right-2016-7; David Kravetz, *U.N. Report Declares Internet Access a Human Right, WIRED*, https://www.wired.com/2011/06/internet-a-human-right.

[90] Paul De-Hert & Dariusz Kloza, *Internet (access) as a new fundamental right. Inflating the current rights framework?*, 3 EUROPEAN JOURNAL OF LAW AND TECHNOLOGY (2012). (hereinafter: *De-Hert& Kloza***)**; *Tully*, *supra* note 17 at 177-181.

[91] Nicola Lucchi, *Internet Content Governance & Human Rights*, 16 VANDERBILT JOURNAL OF ENTERTAINMENT AND TECHNOLOGY LAW 809 (2014).

[92] TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS. (Michael N. Schmitt ed., 2017) 195, ¶22. ; SR Expression 2018, supra note 52 at ¶6 ("International and regional bodies have urged States to promote universal Internet access"). Shackelford, *Exploring the 'Shared Responsibility' of Cyber Peace: Should Cybersecurity be a Human Right?* KELLEY SCHOOL OF BUSINESS RESEARCH PAPER 13-15, 38 (2017) (hereinafter: *Shackelford*).

[93] SR Expression 2011, *supra* note 86, at ¶2.

[94] *Id*, at ¶10.

[95]See *supra* note 69. *See also*: Shakelford, *supra* note 90 at 13 ("More than half of humanity is offline, with penetration rates being particularly low in Africa (28.3%").

years, new obstacles have been erected.[96] Such obstacles include Internet shutdowns, in particular during political uprisings or elections.[97] Still, access to online content enjoys even a more precarious level of protection, given the ability to disguise restrictive measures under benign headings, such as content regulation,[98] and curbing disinformation, propaganda[99] and "Fake News".[100] The exploitation of digital platforms to promote illegal activity may also result in excessive reaction by governments and Internet companies, including contents "*over*-regulation" (e.g., by "filtering").[101] Such excessive measures represent yet another source of limitation of access to the Internet.

The growing dominance of the Internet in the lives of peoples and groups of people underscore the need to develop a new human rights discourse to capture moral claims about respecting and ensuring access to online contents and services, and to protect individuals from abusive practices by governments – at times, with the cooperation of technology companies – limiting their access to the Internet. The centrality of online expression, online information, online education and online consumption of culture could certainly justify extending to access to the Internet the protection afforded by the existing relevant human rights norms (e.g., freedom of expression, the freedom to

[96] SR Expression 2018, *supra* note 54, at ¶12-21. See also Tully, *supra* note 18.

[97] David Kaye, *UN expert urges Cameroon to restore internet services cut off in rights violation*, OHCHR, https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=21165&LangID=E; James Griffiths, *Myanmar shuts down internet in conflict areas as UN expert warns of potential abuses*, CNN, https://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 expressio*n, https://www.amnesty.org/en/latest/news/2019/04/benin-internet-shutdown-on-election-day-is-a-blunt-attack.

[98] SR Expression 2018, *supra* note 54, at 6-8.

[99] *Id* at ¶13, ¶31.

[100] Allcott, *supra* note ¶4 at 211-36. Lily Kuo, *Beijing's new weapon to muffle Hong Kong protests: fake news*, THE GUARDIAN, August 11, 2019, https://www.theguardian.com/world/2019/aug/11/hong-kong-china-unrest-beijing-media-response.

[101] SR Expression 2018, *supra* note 54, at ¶32. *See also*: Jakub Dalek, Lex Gill, Bill Marczak, Sarah McKune, Naser Noor, Joshua Oliver, Jon Penney, Adam Senft, and Ron Deibert, *Planet Netsweeper*, 7-9 Citizen Lab Research Report 108 (University of Toronto, April 2018). The Report investigated Internet filtering technologies in 30 countries and found, for example: *Blocking sites across a range of political content, including websites affiliated with local political groups, opposition groups critical of government, local and foreign news portals, and regional human rights issues; Blocking Google searches for keywords related to LGBTQ identities such as "gay" and "lesbian"; Blocking access to news reporting on the Rohingya refugee issue*, and more. The Report mentions that an estimated value of the web content filtering market at $3.8 billion USD by 2022.

receive and impart information, the right to education and the right to culture). Still, it can also be claimed that the significance of access to the Internet for individuals and for society cannot be fully represented through encompassing the interests and values it serves within existing human rights protections pursuant to the normative equivalency paradigm.

In order to capture the full importance of the Internet as a unique public realm,[102] which serves as a gateway to whole new ways of human interaction, almost inexhaustible sources of information, a huge variety of services and, increasingly, new channels of communication and political participation, one might have to reconceptualize access to the Internet as a new human right. In fact, given the growing role of the Internet as a virtual environment for exercising human rights, the right to access may develop to become the digital equivalent to the Arendtian 'right to have rights'.[103] The combination of a basic need, a moral claim, a power imbalance and a history of abuse and injustice, support, and in fact predict a political push to recognize a digital human right of access to the Internet.

The next section explores the methodology for recognition new online human rights, and the typology for identifying new digital human rights that are in process of being recognized: extending by interpretation existing rights, conceptually developing new rights and identifying new right holders.

Identifying New Rights

What then would make access to the Internet an independent human right, and not merely a condition for realizing other human rights? The question of what justifies the development of a new human right remains unresolved both in legal theory, as well as in actual state practice.[104] Such uncertainty appear to reflect the open-endedness of the

[102] Zizi Papacharissi, *The virtual sphere: The internet as a public sphere*, 4 NEW MEDIA & SOCIETY 9–27, 21-22 (2016). *See also* G.A Res 71/199, *supra note 13*, ¶6 at 3.

[103] HANNAH ARENDT, THE ORIGINS OF TOTALITARIANISM 268 (1968).

[104] Beitz, *supra* note 82, at 37.

term human rights itself.[105] Still, it is possible to identify in the literature on the theory of human rights two principal approaches - normative and sociological approaches – which may aid us in determining whether or not to recognize a new human rights.

The normative approach has its roots in Natural Rights theory[106] and in the Kantian notion of human dignity.[107] It has been linked more recently to the notion of human "capabilities".[108] The theories of rights which were developed under these philosophical schools tend to posit that certain claims or interests are inherent to the human person and/or the universal human experience, and that satisfaction of these claims or interests 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").[109] Legal standards that give expression to such moral principles derive their legitimacy primarily from their underlying moral justifications.[110]

A second approach to the theory of rights concentrates on sociological factors and conceives of human rights as "human needs that have received formal recognition as rights through the sources of international law".[111] Under this approach, moral convictions or intuitions, human experience and the political expediency in legitimizing

---

[105] JAMES GRIFFIN, ON HUMAN RIGHTS 15 (2008), (hereinafter: *Griffin*). *For example, James Griffin has argued that "the term 'human right' is nearly criterionless", and that it is a far less determinate concept than most common nouns. See also:* Alon Harel, *Theories of Rights*, in THE BLACKWELL GUIDE TO THE PHILOSOPHY OF LAW AND LEGAL THEORY 191 (Martin P. Golding and William A. Edmundson ed., 2005).

[106] *Id*, at 10-14; *See also:* John Locke, *Chapter II, Of the State of Nature, sec 6, in* TWO TREATIES OF GOVERNMENT (1963); JOHN FINNIS, NATURAL LAW AND NATURAL RIGHTS 210-221 (1980)

[107] Kant Immanuel, groundwork of the metaphysics of moral *IN* PAUL GUYER AND ALLEN WILLIAM WOOD (ED.) THE CAMBRIDGE EDITION OF THE WORKS OF IMMANUEL KANT: PRACTICAL PHILOSOPHY (Cambridge University Press, 1992).433-435; *See also* Fernando R. Tesón, *The Kantian Theory of International Law*, 92 COLUM. L. REV. 53–102 (1992).

[108] NUSSBAUM M.C. & SEN A., THE QUALITY OF LIFE. (Oxford Clarendon Press, 1993)

[109] Griffin, *supra* note 105, at 16 ("I have said that there is an Enlightenment notion of human rights, that it has an element of intension - namely, that a human right is a right that we have simply in virtue of being human—and an extension—roughly, the rights found in the United States Bill of Rights, in the French Declaration of the Rights of Man, and in certain key United Nations instruments*").*

[110] *Id*, at 11-13. *Also see* Guglielmo Verdirame, *Human Rights in Political and Legal Theory*, in ROUTLEDGE HANDBOOK OF INTERNATIONAL HUMAN RIGHTS LAW 25-35 (Scott Sheeran and Sir Nigel Rodley ed.,2014) (hereinafter: *Verdirame*).

[111] Stephen P. Marks, *Emerging Human Rights: A New Generation for the 1980s*, 33 Rutgers L. Rev. 435, 453 (1981) (hereinafter: *Marks*)

political power all serve as possible motivations for law makers to confer upon certain claims or interests the status of human rights. Ultimately, this positivist approach justifies the existence of rights on the basis of legal considerations – its adoption in legal instruments such as constitutions or international treaties.[112]

It appears as if normative approaches to human rights theory do not sit well with a new independent 'right to access the Internet'. Accessing the Internet seems to be peripheral to the core rights which derive intrinsically from human nature, human experience or human dignity. The ability to conceptualize such a claim or interest in obtaining access to the Internet as morally justified is further complicated by the digital divide between the 'haves' and the 'haves not', which establishes a relationship between needs, claims and human experiences, on the one hand, and a particular stage of technological advancement.[113] Such a relationship is not found in other human rights that capture needs, claims and experiences that allegedly transcend time, place and technology. Yet, the development of a discourse about the moral imperative for addressing structural causes for injustice and inequality and about 'capabilities' as a source for justifying human rights,[114] informs the debate over the status of all new digital human rights, including the right to access the Internet.

Furthermore, the 'capabilities' conception of human rights revolves around protecting personhood. Human rights are aimed at effectively protecting individual autonomy and choices, inter alia, by ensuring the availability of basic resources and access to information that renders liberty and choice-making meaningful.[115] As a result, broad accounts of human rights posit that human rights should reflect much more than

---

[112] JOSEPH RAZ, THE AUTHORITY OF LAW: ESSAYS ON LAW AND MORALITY (1979); *See also* MARTIN P. GOLDING & WILLIAM A. EDMUNDSON, THE BLACKWELL GUIDE TO THE PHILOSOPHY OF LAW AND LEGAL THEORY 29-45 (2004); Scott Sheeran, *The relationship of International Human Rights Law and General International Law: Hermeneutic constraint, or pushing the boundaries?* in ROUTLEDGE HANDBOOK OF INTERNATIONAL HUMAN RIGHTS LAW 100-101 (Scott Sheeran and Sir Nigel Rodley ed.,2014).

[113] See *supra* note 68.

[114] MICHAEL WALZER, THICK AND THIN: MORAL ARGUMENT AT HOME AND ABROAD (1994); *See also* Martha C Nussbaum, *Capabilities and Human Rights*, 66 FORDHAM LAW REVIEW 273 (1997); Morton Winston, *Human Rights as Moral Rebellion and Social Construction*, 6 JOURNAL OF HUMAN RIGHTS 279–305 (2007).

[115] Griffin, *supra* note 105, at 33-34.

"minimum conditions for any kind of life",[116] or necessary safeguards against extreme cases of abuse of governmental power.[117] Beitz, for example, claims that human rights aim to frame the "necessary conditions for political legitimacy or even social justice."[118] Human rights have, according to this approach, a key role to play in effecting and motivating political activity, standard setting, and enforcement.[119]

Against this background, it looks as if a moral case in favor of recognizing a right of access to the Internet as a human right can be made. As mentioned above, there is a wealth of information on the introduction of restrictions placed by governments on access to the Internet or to specific online contents, about the threat such practices pose to individual freedom and dignity,[120] and on its impact on society as a whole. Protecting access to the Internet as a human right would thus address what is increasingly a basic condition for meaningfully engaging in political life and pursuing social justice. Furthermore, as already noted, given the growing centrality of the online realm for communication, maintaining personal relations, consumption of information and participation in society, the economy and market of ideas, it already constitutes an important part of many people's personal and professional life, and their self-identity, without which their capabilities would remain unrealized. Protecting such basic needs from abuse of power could justify designating access to the Internet as an independent right, so as to effectively address the full gamut of individual needs and interests and to counter threats to them.[121]

For law-makers and activists, the main justification for identifying or recognizing a new right to Internet access may be, however, utilitarian: It is more effective to protect the

[116] Beitz, *supra* note 82, at 39.

[117] Wiktor Osiatynski, *The Historical Development of Human rights*, in ROUTLEDGE HANDBOOK OF INTERNATIONAL HUMAN RIGHTS LAW 9 (Scott Sheeran and Sir Nigel Rodley ed.,2014); Griffin, *supra* note 105, at 11. De-Hert& Kloza**,** *supra* note 88, at 3.

[118]Beitz, *supra* note 82, at 39

[119]*Id*, at 40. *See also* Verdirame, *supra* note 110, at 33-34.

[120] Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, *Rep*., ¶1-2 U.N Doc. A/71/373 (Sept. 6, 2016) (hereinafter: *SR Expression, 2016*).

[121] Michael L. Best, *Can the Internet be a Human Right?*, in HUMAN RIGHTS AND THE INTERNET 276-277 (Steven Hick, Edward F. Halpin, and Eric Hoskins ed., 2000) (hereinafter: *Best).*

underlying morally justified claims or interests through recognizing a new human right that would secure online connectivity and include guarantees for safe and meaningful online presence and use.[122] Such a new right of access would also support claims for effective protection of the entire online ecosystem in a manner would enhance the trust in the Internet platform as a whole, promoting thereby the realization of all offline and online human rights that depend on the integrity of the Internet. Finally, a new right may also address the particular challenge posed by the dominant role of private actors in Internet governance and the limited ability of offline remedies to address in real time the effects of harmful online activity. Arguably, it would be very difficult to demand that states effectively protect, promote, and facilitate[123] the multi-faceted needs and interests served by a right to Internet access, including by setting standards of conduct expected from Internet companies, through reliance on a 'second order' right to support the implementation of specific traditional human rights, such as freedom of expression or the right to education.[124]

The Desirability of Creating New Human Rights

Recognizing new human rights is now doubt an intricate process, which takes much time and effort. This process 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").[125] Second, if, according to traditional approaches to theories of rights, human rights have intrinsic moral value, which is pre-political, universal and related to basic aspects of human nature or experience,[126] it is

[122] JOHN STUART MILL, ON LIBERTY 14 (1859), (Batoche Books, Kitchener Ontario, 2001)

[123] *See e.g.*, Philip Alston, *Conjuring Up New Human Rights: A Proposal For Quality Control*, 78 AMERICAN JOURNAL OF INTERNATIONAL LAW 607–609 (1984).

[124] De-Hert and Kloza, *supra* note 88, at 10. *See also* Best, *supra* note 119.

[125] Seth Kaplan, *When Everything Is a Human Right, Nothing Is*, FOREIGN POLICY (6.9.2019), https://foreignpolicy.com/2019/09/06/when-everything-is-a-human-right-nothing-is; Morton E. Winston, *Human rights real and supposed*, *in* THE PHILOSOPHY OF HUMAN RIGHTS 121–128 (1989).

[126] Griffin, *supra* note 105, at 10; Beitz, *supra* note 82, at 37-38; Xiaowei Wang, *Time to Think about Human Right to the Internet Access: A Beitz's Approach*, 6 JOURNAL OF POLITICS AND LAW 67 (2013).

difficult to accept that new human rights can suddenly emerge in response to changing political or technological conditions.[127]

Still, practice shows that law makers and activists have often resorted to a different, more dynamic, approach to the development of new human rights, citing the instrumental need for responsiveness to change in order to ensure the ongoing relevancy of human rights law and the effective protection of individuals against new threats to their freedom, dignity and well-being.[128] Like with regard to claims in support of "living instrument" interpretation doctrines, this approach asserts that international human rights law has to be developed in order to correspond to the present needs of society.[129] In fact, it has been claimed that even the Universal Declaration of Human Rights itself "could not be said to be timeless" since it included some elements responding to the particular needs of industrialized societies, such as technical education, trade unions or social security.[130] We can therefore posit that whereas, on the moral plane, human rights have certain immutable features, the decision to claim or recognize human rights in a political or legal context, tends to be responsive to specific circumstances and to evolving human conditions and available technologies.

The position that human rights law should respond to new developments in technology is reinforced by the fact that human rights instruments have been evolving continuously, becoming more and more specific and addressing new social needs and new forms of oppression and injustice, as is evident from the proliferation of new human rights conventions and declarations.[131] Under such circumstances, declining to recognize new human rights in certain domains of human activity might result in a normative gap between protected and unprotected basic needs, which could indirectly discourage certain activities – for instance, by privileging offline activism by traditional political parties at the expense of new forms of online activism.

---

[127] Alston, *supra* note 121, at 607-609

[128] *Id.*

[129] Beitz, *supra* note 82, at 38. *Also see* Marks, *supra* note 109, at 440, 451-452.

[130] *Id*, at 43.

[131] Scott Sheeran and Sir Nigel Rodley, *The Broad Review of International Human Rights Law*, in ROUTLEDGE HANDBOOK OF INTERNATIONAL HUMAN RIGHTS LAW 3 (Scott Sheeran and Sir Nigel Rodley ed.,2014)

The conclusion 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 began. Already some regional treaties, such as the Budapest Convention on Cybercrime,[132], the EU General Data Protection Regulation (GDPR)[133] and the AU Convention on Cyber Security and Personal Data Protection,[134] use the language of human rights to regulate digital technology, as have the UN Resolutions described in Part One of this article.[135] Some scholars have also been advocating for the elaboration of an international treaty on digital rights, which would introduce specific language on the application of traditional human rights in a digital environment.[136] Such developments can be explained by the sociological approach to human rights as reflective of acceptance of the moral significance of digital rights (and the need to protect them through specifically tailored language of rights), the actual risk for denying or abusing them, and political need for legitimizing Internet governance.

Naturally, the project of developing new digital human rights is not free from controversy.[137] One concern is that developing new rights would be regarded as throwing into question the application of traditional human rights to online activity, notwithstanding the elasticity of their definitions,[138] and the interpretive efforts of treaty-monitoring bodies.[139] Another concern is that the project siphons away attention from the need to develop just and politically acceptable cyber-governance structures,

---

[132] Convention on Cyber Crime, *opened for signature* Nov. 23, 2001, 185 E.T.S. (entered into force July 1, 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 *Opened for signature* Jan. 28, 1981, 108 E.T.S (entered into force Oct. 1, 1985).

[133] Regulation (EU) 2016/679 of the European Parliament and of the Council of Europe on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, May 4, 2016, 95/46/EC (General Data Protection Regulation – GDPR). (hereinafter: *GDPR*).

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

[135] See *supra* note 13 and *supra* note 14.

[136] *See*, *supra* note 79. See also *Draft Legal Instrument on Surveillance and Privacy*, *supra* note 43.

[137] Tully, *supra* note 18, at 180-185.; Mathiesen, *supra* note 80, at 4-7; *Fidler supra* note 8, at 107.

[138] Land, *supra* note 72 at 400-410.

[139] Seibert-Fohr *supra* note 43, at 11.

and to strengthen accountability mechanisms and institutions.[140] Still, as the following part shows, the wider is the distance between traditional human rights and the challenges posed by activities in a digital environment, the greater is the pressure on existing human rights norms and institutions to accommodate the new needs, interests and expectations of online users. Arguably, without specific standard setting, which acknowledges the unique problems, opportunities and structures of power existing online, traditional human rights law might bend beyond its breaking point, and cease serving as a widely-acceptable framework for Internet governance.

International Initiatives for the Conceptualization of Digital Rights: Three Generations of Digital Human Rights

The process of developing new digital human rights is not new. In fact, in the last three decades, a variety of international and regional initiatives have sought to promote particular rights online, and to use them to influence online user conduct, Internet regulation, and the configuration of online environments and data protection.[141] The documents formulated pursuant to such initiatives were sometimes referred to as 'digital

[140] Mihr, *supra* note 24, at 25.

[141] Gill, Redeker & Gasser, *supra* note 9, at 5-10. In their Research they review a collection of thirty initiatives, for example:
NERmundial, Global Multistakeholder Meeting on the Future of Internet Governance (April 23-24, 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* (May 19, 2010) *available at:* https://www.eff.org/deeplinks/2010/05/bill-privacy-rights-social-network-users.
Association for Progressive Communications (APC), *Internet Rights Charter* (November, 2006) *available at:* https://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 (OAS), Organization for Security and Co-operation in Europe (OSCE), African Commission on Human and Peoples' Rights on Human and Peoples' Rights (ACHPR), *Joint Declaration on Freedom of Expression and the Internet - International Mechanisms for Promoting Freedom of Expression* (June 1, 2001) *available at:* https://www.oas.org/en/iachr/expression/showarticle.asp?artID=848&lID=1.
Organization for Economic Co-operation and Development (OECD), *Communiqué on Principles for Internet Policy-Making* (OECD High Level Meeting on the Internet Economy, June 2011), *available at:* https://www.oecd.org/internet/innovation/48289796.pdf

bill of rights'.[142] In addition, different studies were conducted in an attempt to provide a more specific awareness by online users of their digital rights.[143]

One of the most notable initiatives that have emerged in recent years is the WSIS "Declaration of Principles". This is a declaration of 67 principles,[144] which was developed through several international forums held under the auspice of the United Nations[145] between the years 2003-2005, in which 175 States participated.[146] The WSIS Declaration tried to offer a framework of "common vision of the information society", which reaffirms respect for human rights and fundamental freedoms, as well as their interdependence and mutually reinforcing nature.[147] Specifically, the WSIS Declaration reaffirms Article 19 of the ICCPR (the right to freedom of opinion and expression) and emphasizes that communication is a basic human need that is central to the "information society".[148] 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.[149]

Another notable initiative is the Charter of Human Rights and Principles for the Internet[150] - a collaboration initiative undertaken by two multi-stakeholder frameworks

[142] Todd Davies, *Digital rights and freedoms: A framework for surveying users and analyzing policies in* SOCIAL INFORMATICS: PROCEEDINGS OF THE 6TH INTERNATIONAL CONFERENCE *(SocInfo 2014)* LUCA MARIA AIELLO & DANIEL MCFARLAND (eds.), 1-2 (Springer, 2014).(hereinafter: *Davies*).

[143] *Id*, at 8-10. In his research, Davies presents a survey conducted in 2014 among Internet users, which shows the relative importance that users attach to different digital rights and freedoms. According to the survey, the most important primary principle was 'privacy control'. Next highest were –'data portability' and 'creative control'.

[144] United Nations, International Telecommunication Union (ITU*), Declaration of Principles, Building the Information Society: a global challenge in the new Millennium*, World Summit on the Information Society (WSIS), Geneva (Dec. 12, 2003). Available at: https://www.itu.int/net/wsis/docs/geneva/official/dop.html (hereinafter: *WSIS Declaration of Principles*).

[145] General Assembly Res. 56/183, U.N Doc. A/RES/56/183 (Jan. 31, 2002).

[146] WSIS first phase summit summary, available at: https://www.itu.int/net/wsis/geneva/index.html. *See also*, Murry&Klang, *supra* note 69.

[147] *WSIS Declaration of Principles*, *supra* note 144, at ¶1-3.

[148] *Id* at ¶4.

[149] *Id* at ¶ 10 and 35

[150]The Internet Rights & Principles Dynamic Coalition (IRPC), and the Internet Governance Forum (IGF), *The Charter of Human Rights and Principles for the Internet* (August, 2014). *Available at:*

- the Internet Rights & Principles Coalition and the Internet Governance Forum (IGF), which was established following the WSIS forum.[151] The Charter introduces a list of rights and principles, aiming to provide a framework for "upholding and advancing human rights for the online environment".[152] Interestingly, the initiative defines 'rights' as international human rights which were translated to a normative vocabulary relevant for the Internet.[153] 'Principles' are defined as features of the system which are required to support the realization of human rights.[154]

Furthermore, several studies conducted in order to analyze different digital rights initiatives, have tried to identify several core rights (or principles) that are frequently included in the documents produced by such initiatives.[155] Among the rights identified in the literature, one can mention the following:

- Online privacy and data protection (including encryption and anonymity);[156]
- Data portability;[157]

https://www.ohchr.org/Documents/Issues/Opinion/Communications/InternetPrinciplesAndRightsCoalition.pdf (hereinafter: *IRPC Charter*)

[151]*The Tunis Agenda for the Information Society ¶72*, U.N Doc WSIS-05/TUNIS/DOC/6(Rev.1)-E, 18, November 2005. (The second phase of WSIS took place in Tunis from 16 -18 November 2005; *The Tunis Agenda for the Information Society* provides the Mandate for the Internet Governance Forum (IGF). See also: Internet Governance Forum, available at: https://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 United Nations Secretary-General formally announced the establishment of the IGF in July 2006 and the first meeting was convened in October/November 2006). https://www.intgovforum.org/multilingual/

[152] IRPC Charter, *supra* note 150, at 2.

[153]*Id* ("Human 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").

[154]*Id* ("By "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"").

[155] Davies, *supra* note 142.

[156] Davies, *supra* note 142, at 3 (The right to privacy according to Davis is detailed to sub-principles such as: originator-discretionary data control, data use transparency; usable privacy which requires that *privacy settings should be as clear and easy to use as possible*, and that data should not be retained without the consent if the user). Also see IRPC Charter, *supra* note 150, at 7.

[157] Davies, *supra* note 142, at 4. *See also*: GDPR, *supra* note 133, *Art.* 20

- Right To Be Forgotten;[158]
- Right to Internet access (including right to access Internet contents);[159]
- Right to freedom of online expression (which includes freedom from censorship and from hate speech).[160]
- Right to net neutrality; [161]
- Right to network equality and non-discrimination;[162]
- Right to Internet security and cyber security; [163]

An overview analysis of digital initiatives, conducted at Harvard University's Berkman Center, further suggests that digital rights can be grouped into seven categories: (A) basic or fundamental rights and freedoms, (B) general limits on state power, (C) Internet governance and civic participation, (D) privacy rights and surveillance, (E) access and education, (F) openness and stability of networks, and (G) economic rights and responsibilities.[164]

The typology we propose is somewhat different. It builds on the genealogy of digital rights, and on the difference in their approach to standard setting in the field and to the normative equivalency paradigm. Such typology helps us understand the policy choices

[158] Davies, *supra* note 142, at 4.

[159] *Id* at 6. Also see: IRPC Charter, *supra* note 150, at 7 ("Accessibility: Everyone has an equal right to access and use a secure and open Internet"); Davies, *supra* note 141, at 6. According to Davis this entails (a) the right to privacy, which includes the principle according to which public interceptions cannot be intercepted; (b) the right to anonymous speech; (c) freedom from censorship (d) Open access to all publicly funded data (e) democratically controlled security – government security policies must be transparent as possible to allow them to be publicly debated.

[160] IRPC Charter, *supra* note 150, at 16.

[161] Davies, *supra* note 142, at 7.

[162] *Id*

[163] *Id.*

[164]Gill, Redeker & Gasser *supra* note 9, at 6-10. Other initiatives suggest to add a group of principles which relates to software freedom, for example the ability to modify a code in software platform or the possibility of participatory design, see Davis, *supra* note 142.

underlying different initiatives for elaborating digital rights, as well as the outer limits of legal interpretation of the existing international human rights law platform for protecting and promoting claims, needs and interests of online users.

The proposed typology

Efforts to apply existing human rights norms to online activity on the basis of the normative equivalency paradigm which underscores the application of 'offline human rights' also online, reveal significant difficulties in the adaptation of these norms to the unique attributes of the cyber realm. Such unique attributes include dramatically different speed and scale of communication, harnessing of big data and artificial intelligence tools to process personal information, decentralized network and data management, prominent role for private entities in Internet governance, and the limited relevance of national borders for online activity (deterritorialization). Our proposed typology looks at three responses to these unique challenges: radical reinterpretation of existing rights, development of new rights and the recognition of new right-holders and duty-holders.

The **first generation** of digital rights is premised on the normative equivalency paradigm. Yet, it comprises of attempts to recalibrate existing human rights norms by reinterpreting them so that they would govern online activity. Content moderation and online privacy constitutes prominent examples for such recalibration efforts. The ability to disseminate hate speech online at a speed, scale and ease not matched in the offline world, where traditional media outlets have traditionally exercised editorial controls over contents in mass circulation, has created a heightened risk of violence, social antagonism and discrimination.[165] In the same vein, the deliberate online dissemination of disinformation ("fake news") creates through algorithm-based "echo chambers"

[165]See, e.g: Human Rights Council, *Report of the detailed findings of the Independent International Fact-Finding Mission on Myanmar*, U.N Doc.A/HRC/39/CRP.2, 339-342 (Sept. 17, 2018); Emma Irving, *The Role of Social Media is Significant: Facebook and the Fact Finding Mission on Myanmar*, OPINIO JURIS, (Sept. 7, 2018) at: http://opiniojuris.org/2018/09/07/the-role-of-social-media-is-significant-facebook-and-the-fact-finding-mission-on-myanmar/; *See also:* The Christchurch Call, *supra* note 66.

distorted world views, which seriously disrupt the "market of ideas' on which democratic deliberation and public discourse are built.[166]

Applying traditional notions of freedom of speech, press freedom and the right to seek, receive and impart information, with their narrow limitation provisions and the associated high bar for government interference, to such situations might be deemed inadequate. Hence, human rights bodies might find themselves in the unusual position of calling on governments and technology companies to moderate or remove online contents and to introduce filtering mechanisms.[167] Indeed, the Special Rapporteurs for Freedom of Expression have called for applying the legal framework found in articles 19 and 20 of the ICCPR by way of deriving from them specific online norms that would be enforceable by both governments and private actors, and which would provide transparent, practical and nuanced guidance for countering online hate speech, incitement to violence and fake news.[168]

Online privacy raises another set of technology-driven challenges, requiring a radically new interpretation of existing legal doctrines, such as those distinguishing between data and metadata,[169] privacy in the private and public sphere (a question posed inter alia by the prevalence of facial-recognition technology),[170] anonymized and deanonymized

[166] C. Thi Nguyen, *Echo Chambers and Epistemic Bubbles*, EPISTEME 1–21 (2018) *available at:* https://www.cambridge.org/core/journals/episteme/article/echo-chambers-and-epistemic-bubbles/5D4AC3A808C538E17C50A7C09EC706F0. *See also supra* note 4.

[167] Council of Europe, Committee of Ministers, CM/Rec (2008)6 ¶I(xi) *Recommendation to member states on measures to promote the respect for freedom of expression and information with regard to Internet filters*, (Adopted March 26, 2008) ; SR Expression 2011, supra note 84, at ¶82; SR expression 2019, supra note 5, at ¶*29-33*. *See also*: Report of the Special Rapporteur on the sale of Children, Child prostitution and Child pornography, Najat Maalla M'jid, Mission to Kyrgyzstan (26 April 2013); Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Rep. *on the regulation of online "hate speech"*, ¶35-38, U.N. Doc. A/74/486 (October 9, 2019). (hereinafter: SR expression 2019 (regulation of online "hate speech")).

[168] SR expression 2017, *supra* note 24, at ¶77; SR expression 2019 (regulation of online "hate speech") *supra* note 167, at ¶58(b).

[169] United Nations High Commissioner for Human Rights (OHCHR), Rep. *The Right to Privacy In The Digital Age*, U.N. Doc. A/HRC/27/37, at ¶18-20 (30 June 2014) (hereinafter: OHCHR Privacy Report 2014). See also Seibert-Fohr, *supra note* 43, at 12-13.

[170] OHCHR Privacy Report 2018, *supra* note 12, at ¶6-7, ¶14.

information, [171] and capacity to encrypt and decrypt data.[172] The right to online privacy thus requires, as suggested by the Special Rapporteur on Privacy, a radical departure from existing privacy laws.[173] Similar challenges requiring an innovative reinterpretation of existing human rights norms can be found with respect to other human rights, such as the right to take part in public affairs, the right to education, the right to culture and the right to security of person.

The second generation of digital rights represents a conscious move away from the normative equivalency paradigm aimed at developing new human rights that have no close or suitable parallels in the offline world. Many of the rights found in the digital rights initiative belong to this category of rights. Although these new digital human rights typically have one or more 'parent' offline rights, they protect unique needs that are not fully and effectively covered by the latter rights. The right to Internet access is a paradigmatic second generation digital human rights, mainly because traditional human rights fail to capture centrality of access to the Internet for the enjoyment of all digital rights (the digital equivalent of the right to have rights). Recognizing the right to access to the Internet as a new human right can therefore be justified on considerations of effective protection of the underlying basic needs, and as a reaction to practices of governmental restrictions on access to the Internet or specific contents therein.

Other potential rights which emerge as second generation digital rights can also be justified by reasons of the fundamental importance of the needs and interests they protect for online users, the impossibility of effectively protecting them through traditional offline rights and the prevalence of abusive practices by governments and technology companies. These include the putative rights to data portability,[174]

---

[171] Special Rapporteur on the Right to Privacy, *Rep.*¶103, U.N. Doc. A/72/43103 (October 19, 2017) (hereinafter: *SR Privacy 2017*).

[172] *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*, ¶29-31, U.N. Doc. A/HRC/38/35/Add.5 (July 13, 2018). *See also:* OHCHR Privacy Report 2018, *supra* note 12 at ¶20.

[173] SR Privacy 2017, *supra* note 171, at p.26, ¶131(j). *See also*: SR Privacy 2018, *supra* note 20, at ¶2-7.

[174]GDPR, *supra* note 133, *at Art.* 20. *See also*: Peter Swire & Yianni Lagos, *Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique*, 72 MD. L. REV 335–349

informational self-determination (i.e., ability to control one's online profile and personal data, including the right to be forgotten)[175] and cyber security.[176] The importance of such rights in the online world may be roughly equated to the importance in the offline world of the following fundamental rights, respectively: freedom of movement, right to protect honor and reputation and right to security of person.

Second generation rights may also emerge in response to concerns that have no clear parallel in the offline world. The emerging right not be subject to automated decision making (which is already reflected to some extent in the 2016 GDPR)[177] reflects a concern about delegation of governmental, and over time, judicial decision making, to AI-driven computers. It is difficult to find a similar concern in the offline world; at most, one can draw some analogies to debates about faceless judges or jury of one's peers[178], whose impact on international human rights law remains limited.

The third generation of digital human rights we anticipate revolves around an emerging discourse on the need to revise the traditional configuration of right-holders and duty-holders developed in international human rights law, so as to adjust it to interactions on digital space, with the risks to the basic needs and interests of individuals and groups of individuals they entail.[179] One part of this discourse proposes recognizing

(2013). (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).

[175] GDPR, *supra* note 133, *Art*. 17. *See also* Gill, Redeker & Gasser, *supra* note 9, at 8.

[176] CYBERSECURITY AND HUMAN RIGHTS IN THE AGE OF CYBERVEILLANCE (Joanna Kulesza and Roy Balleste ed., 2016), P. 1-17.; Shackelford, *supra* note 90; IRPC Charter, *supra* note 150, at 15. ("Right to Security of the Internet: Everyone has the right to enjoy secure connections to and on the Internet. This includes protection from services and protocols that threaten the technical functioning of the Internet, such as viruses, malware and phishing").

[177] GDPR, *supra* note 133, *at Art*. 22.

[178] Lewis LaRue, *A Jury Of One'S Peers*, 33 WASH. & LEE L. REV. 841 (1976); Davin M. Stockwell, *A Jury of One's (Technically Competent) Peers?*, 21 WHITTIER L. REV. 645 (2000). On *Faceless Judges* see: Human Rights Committee, *General Comment No. 32 Article 14: Right to equality before courts and tribunals and to a fair trial* ¶*23* U.N. Doc. CCPR/C/GC/32 (Aug. 23, 2007); *Becerra Barney v. Colombia* ¶.7.2. U.N. Doc. CCPR/C/87/D/1298/2004 (July 11, 2006).

[179] IRPC Charter, *supra* note 150, at 18. The Right to Privacy as it is defined in the "Charter on Human Rights and Principles for the Internet", includes the right to "Protection of virtual personality"*: Protection of the virtual personality: Everyone has a right to a virtual personality: The virtual personality of the human person, [i.e. the personal identification in information systems] is inviolable. Digital signatures, user names, passwords, PIN and TAN codes must not be used or changed by others without the consent of the owner. The virtual personality of human persons must be respected. However, the right to a virtual personality must not be misused to the detriment of others*

online personae as holders of digital rights.[180] Recognizing online profiles as digital or virtual persons with an interest to protect their online activity and features that is independent of the physical persons or entities that created them, may provide such digital or virtual persons with more effective legal protection to facilitate their online operations in the same way in which corporations obtained legal personality in order to facilitate their economic operations. For example, digital or virtual persons may exercise their rights after the death of the person that created them,[181] have the ability to protect their reputation and intellectual property independently of their creators and may claim an 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 Internet companies.[182] To be sure, the discourse over business and human rights is already well-developed, and has already resulted in the conclusion of important international instruments, such as the UN Guiding Principles on Business and Human Rights,[183] and there are attempts to formulate a binding treaty in the field.[184] Still, whereas in traditional spheres of activity, the turn to corporate responsibility is driven by the concern that businesses, especially transnational corporations, are not effectively subject to governmental regulation, in cyberspace,

[180] AGRE, PHILIP E., AND MARC ROTENBERG, eds. TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 7-10 (Mit Press, third printing 2001). Clarke, R., *The digital persona and its application to data surveillance*. 77-92 THE INFORMATION SOCIETY, 10(2); Koops Bert-Jaap, Mireille Hildebrandt, and David-Olivier Jaquet-Chiffelle, *Bridging the accountability gap: Rights for new entities in the information society* 497-503 MINN. JL SCI. & TECH.11 (2010).

[181] Noam Kutler, *Protecting Your Online You: A New Approach to Handling Your Online Persona After Death,* 26 BERKELEY TECH. L.J. (2011).

[182] See *supra* note 53.

[183] UN Human Rights Council, *Guiding Principles on Business and Human Rights*, UN Doc. A/HRC/17/31 (June 16, 2011).

[184] Open-ended intergovernmental working group on transnational corporations and other business enterprises with respect to human rights (OEIGWG), *Legally binding instrument to regulate, in international human rights law, the activities of transnational corporations and other business enterprises* (Draft, 16.7.2019) https://www.ohchr.org/Documents/HRBodies/HRCouncil/WGTransCorp/OEIGWG_RevisedDraft_LBI.pdf; Office of the High Commissioner for Human rights, *Report on the fifth session of the open-ended intergovernmental working group on transnational corporations and other business enterprises with respect to human rights*, U.N Doc A/HRC/43/55 (9 January 2020).

technology companies are the *de facto* and at times, *de jure* regulators. Thus, they represent for users a form of regulatory power, much stronger and more direct and prominent than traditional governments. Hence, there is a special impetus to subject Internet companies directly to human rights obligations vis-à-vis natural and legal persons who enjoy digital human rights.[185]

Thus, the third generation of digital rights, demands a possible modification regarding the mere subject of the rights. An independent online legal subject, might contribute to strengthen the protection of human rights online and would be a step toward a more holistic response to the variety of harmful practices occurring online to our own natural identity in the framework of its digital capacity.

IV. CONCLUSION

While the application of human rights and fundamental freedoms in cyberspace is becoming a well-accepted premise, the applicable legal framework governing cyberspace still remains an unresolved issue. International bodies, mainly the UN General Assembly and the Human Rights Council have adhered to a 'normative equivalency' approach. According to this approach, the *same* human rights individuals enjoy offline must be protected online as well.

In this Article we argue that the unique features of cyberspace put in question the desirability and feasibility of an automatic and exclusive application of this paradigm. Cyberspace is a substantially different set, far from the context in which human rights treaties and standards were developed. Unlike the offline arena which is state-centric, delimited, and dominated by governments, cyberspace is a de-territorialized and de-centralized virtual environment, one that is dominated by powerful private companies. In addition, the speed and scale of human interactions via the Internet differ from familiar offline structures (such as the written press). Therefore some well-established legal norms are not suited without adjustment to 'online conditions'. These gaps highlight the shortcomings of some existing legal concepts and structures developed in the offline world when applied to the online environment.

[185] SR Expression 2017, *supra* note 24, at ¶82-83; *OHCHR Privacy Report 2018*, *supra* note 12, at ¶43-49.

Accordingly, we contend that effective protection of human rights in the digital realm cannot be achieved by using traditional human rights alone; particular rights that are adapted, designed, and in part specifically tailored to apply in cyber-space are needed 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, recognizing a new, digital right is based on three main justifications: moral, sociological, and utilitarian.

We therefore propose a normative framework that goes, in some regards, beyond the normative equivalency paradigm. We attempt to provide a holistic response to the unique features of cyber-space by proposing a typology which identifies three stages in the development of digital human rights, and we expect human rights to continue developing along these trajectories.

As a first stage, we identify a process of radical reinterpretation of existing human rights, so that these would adapt to the needs, speed and conditions of the digital environment. This is the 'first generation' of digital rights. The 'second generation' of digital rights entails the development of new human rights, aimed to protect unique needs of the digital realm that are not fully covered by traditional human rights. And the 'third generation' of digital rights attempts to identify new right-holders and duty holders. It develops, inter alia, the concept of "virtual personality", a concept that possibly evolves to be an independent online legal subject, in a way that will strengthen the protection of online human rights, and pushes for the imposition of appropriate legal norms and accountability mechanisms for private Internet companies. Ultimately, the need for expansion of existing human rights, developing new human rights and incorporating of new right carriers and duty holders, possibly reflects upon the necessity for developing a new human rights paradigm for effectively protecting individual needs and interests in a digital environment.[186]

[186] KUHN THOMAS S., THE STRUCTURE OF SCIENTIFIC REVOLUTIONS (2d ed., 1970).