



## UvA-DARE (Digital Academic Repository)

### Human Rights in Technology -- A Need for a New Norm

De Busser, E.

**Publication date**

2025

**Document Version**

Final published version

**Published in**

Case Western Reserve Journal of International Law

**License**

Unspecified

[Link to publication](#)

**Citation for published version (APA):**

De Busser, E. (2025). Human Rights in Technology -- A Need for a New Norm. *Case Western Reserve Journal of International Law*, 57(1), 109-138. Article 7.  
<https://scholarlycommons.law.case.edu/jil/vol57/iss1/7/>

**General rights**

It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

**Disclaimer/Complaints regulations**

If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: <https://uba.uva.nl/en/contact>, or a letter to: Library of the University of Amsterdam, Secretariat, P.O. Box 19185, 1000 GD Amsterdam, The Netherlands. You will be contacted as soon as possible.

# HUMAN RIGHTS IN TECHNOLOGY— A NEED FOR A NEW NORM

*Els De Busser\**

## ABSTRACT

The field of cyber security has relied on norms quite heavily to govern the behavior of states and non-state actors in cyberspace. However, existing norms do not offer guidance on integrating attention to human rights into the design and development of digital consumer products. This Paper introduces a way to foresee the human rights impact of new technology combined with a form of governance that regulates problems we do not know exist yet.

I.	INTRODUCTION .....	109
II.	RULES, NORMS, AND PRINCIPLES .....	113
	A. <i>Norms as an Instrument of International Cyber Security Governance</i> .....	118
	B. <i>International Law and Norms</i> .....	119
	C. <i>Existing Sets of Norms</i> .....	122
	D. <i>Human Rights in a Regulative Norm</i> .....	126
III.	PROPOSING A NORM ON HUMAN RIGHTS IN TECHNOLOGY .....	132
	A. <i>By-Design Thinking</i> .....	132
	B. <i>The Addressees of the Norm</i> .....	133
	C. <i>Who Is Protected by the Norm?</i> .....	135
IV.	CONCLUDING ON A NEW NORM .....	136

## I. INTRODUCTION

Cyberspace is governed by norms more than by conventions or laws.<sup>1</sup> There have already been a number of attempts to create cyber norms, with the most notable attempt being the norms

---

\* Associate Professor, Institute for Information Law, University of Amsterdam.

1. Martha Finnemore & Duncan B. Hollis, *Constructing Norms for Global Cybersecurity*, 110 AM. J. INT'L L. 425, 436 (2016).

drafted by the United Nations Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security (U.N. GGE).<sup>2</sup> Even if we can understand why norms seem to work better than multilateral legal instruments in the intricate area that is international cyber security, what is remarkable about the existing norms is their lukewarm attention to human rights.<sup>3</sup> Often the protection of human rights is restricted to a specific set of human rights, or human rights protection is only linked to cyber-attacks or the instability of cyberspace.<sup>4</sup> The noteworthy absence in the discussion of human rights in cyberspace is the attention for the “hidden” effects of digital technology on human rights. The hidden effects are those that are not immediately perceivable and are also not necessarily caused by an intent to harm. These hidden harms exist because the essential protective mechanisms to prevent harmful effects are not in place.<sup>5</sup> These harms occur in the context of digital products being used by consumers and by state actors, such as government services, often even being used in armed conflict.<sup>6</sup> This Paper will unpack why this is important and how a norm should be shaped around the use of digital technology in these contexts.

---

2. Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2014), transmitted by Letter dated 26 June 2015 from the Chair of the Group Established Pursuant to G.A. Resolution 68/243, ¶ 13, U.N. Doc. A/70/174 (July 22, 2015) [hereinafter Governmental Experts Report].
3. Martha Finnemore, *Cybersecurity and the Concept of Norms*, CARNEGIE ENDOWMENT FOR INT’L PEACE (Nov. 30, 2017) <https://carnegieendowment.org/research/2017/11/cybersecurity-and-the-concept-of-norms?lang=en> [perma.cc/74QH-RTQ4].
4. Glob. Comm’n on the Stability of Cyberspace, *Advancing Cyberstability*, at 19 (Nov. 2019); MICROSOFT, A DIGITAL GENEVA CONVENTION TO PROTECT CYBERSPACE (2017); U.N. OFF. FOR DISARMAMENT AFF.’S, VOLUNTARY, NON-BINDING NORMS FOR RESPONSIBLE STATE BEHAVIOUR IN THE USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGY: A COMMENTARY, at 95, 109–10, U.N. Sales No. E.18.IX.3 (2017).
5. See E. Tendayi Achiume, (Special Rapporteur on Contemporary Forms of Racism, Racial Discrimination, Xenophobia and Related Intolerance), *Racial and Xenophobic Discrimination and the Use of Digital Technologies in Border and Immigration Enforcement*, U.N. Doc. A/75/50289 (Nov. 10, 2020).
6. *Id.*

In the fast-evolving world of cyberspace, new software or hardware is produced at a rapid tempo, and their impact on individuals and society is not always clear until harm occurs.<sup>7</sup> The effects of digitalization are often hidden. In addition, new functionalities or uses of existing software or hardware can also significantly impact individuals and/or society. Knowing whether or not these novelties constitute appropriate or inappropriate behavior is a crucial yet often layered and complex question. The adverse effects of technology are frequently not perceivable until an individual, organization, or community puts the technology to use. At that point, harm may already have occurred. The damage can be financial but can constitute a human cost as well.<sup>8</sup> Examples of radicalization via YouTube,<sup>9</sup> or the significant problems with biometrics,<sup>10</sup> or the discriminating algorithms in the Netherlands<sup>11</sup> and in Jordan<sup>12</sup> show the complicated issue of governing technology in practice. Essentially, the difficulties with regulating technology is that its adverse effects are not always known at the moment rules are created. This is often referred to as the “pacing problem.”<sup>13</sup> It is mostly brought up in a legal

- 
7. KAREN YEUNG, COUNCIL OF EUR., RESPONSIBILITY AND AI 68 (2019).
  8. Finnemore & Hollis, *supra* note 1, at 433.
  9. *E.g.*, Gonzalez v. Google LLC, 598 U.S. 617 (2023) (ISIS use of YouTube).
  10. William Crumpler, *How Accurate Are Facial Recognition Systems—and Why Does It Matter?*, CTR. FOR STRATEGIC & INT’L STUD. (Apr. 14, 2020), <https://www.csis.org/blogs/strategic-technologies-blog/how-accurate-are-facial-recognition-systems-and-why-does-it> [perma.cc/A2E7-RRGF] (highlighting the inaccuracies of facial recognition systems and their error rates overall).
  11. Amnesty Int’l, *Xenophobic Machines: Discrimination Through Unregulated Use of Algorithms in the Dutch Childcare Benefits Scandal*, AI Index EUR 35/4686/2021 (Oct. 25, 2021).
  12. Hum. Rts. Watch, *Automated Neglect— How the World Bank’s Push to Allocate Cash Assistance Using Algorithms Threatens Rights* (June 2023).
  13. Gary Marchant et al., *Governing Emerging Technologies Through Soft Law: Lessons for Artificial Intelligence*, 61 JURIMETRICS J. 1, 4 (2020) (citing Gary E. Marchant, *The Growing Gap Between Emerging Technologies and the Law*, in THE GROWING GAP BETWEEN EMERGING TECHNOLOGIES AND LEGAL-ETHICAL OVERSIGHT: THE PACING PROBLEM 19, 22–23 (Gary E. Marchant et al. eds., 2011)).

context, as the time-consuming process of creating new legal rules is infamous.<sup>14</sup>

The question of how the pacing problem could be solved or mitigated is a complicated one. Any attempt to solve or mitigate the pacing problem would have to combine a way to anticipate the impact of a new technology with a form of governance that regulates problems that we do not know exist yet. A way out of this conundrum could be to focus on principles or norms rather than legal rules. Principles and norms offer guidance on what is acceptable and what is not acceptable on a higher level of abstraction than the more detailed and specific legal rules.<sup>15</sup> It is not feasible to create a new law for every new type of technology. It is, however, feasible to have a set of more abstract principles or norms guiding the decision-making process on whether a new type of technology is desirable in line with ethics and human rights, among other priorities. The implementation of norms in the cyber security realm is a complex sum of institutions and mechanisms<sup>16</sup> that deserves its own research and falls beyond the scope of this Paper.

This Article turns to the concept of norms and principles also because the debate around embedding human rights into the design and development of technology is linked with international law in two ways. First, international law governs the behavior of States as the main actors in the global legal sphere.<sup>17</sup> Digital technology can hardly be tied to one particular State or territory, because its production is spread over different countries, its functioning reaches beyond state borders, or both.<sup>18</sup> To govern digital technology as part of cyberspace, a form of governance must equally reach beyond State borders as it governs the

---

14. See Jasmijn Boeken, *From Compliance to Security, Responsibility Beyond Law*, 52 COMPUT., L. & SEC. REV. no. 105926, 2024, at 1, 2.

15. Finnemore & Hollis, *supra* note 1, at 441.

16. Ian Johnstone, *Implementing Cybersecurity Norms: The Design of International Institutions*, in BUILDING AN INTERNATIONAL CYBERSECURITY REGIME 111, (Ian Johnstone et al. eds., 2023).

17. Duncan B. Hollis, *A Brief Primer on International Law and Cyberspace*, CARNEGIE ENDOWMENT FOR INT'L PEACE (June 14, 2021), <https://carnegieendowment.org/posts/2021/06/a-brief-primer-on-international-law-and-cyberspace?lang=en> [perma.cc/NF9Y-L55T].

18. Finnemore & Hollis, *supra* note 1, at 459.

behavior of states. Second, States may be the main actors in the global legal sphere and international cyber security, but they are not the only ones. Private companies own a large part of what we call cyberspace and its infrastructure. In addition, private companies produce many consumer products as well as products used by government entities that fall under the definition of digital technology and have a cross-border reach.<sup>19</sup>

It is equally noteworthy that the debate around embedding human rights into the design and development of digital technology is linked with international humanitarian law since the use of personal data – especially the use of biometric data – plays a significant role in the development of specific weapon systems and other equipment used in armed conflict.<sup>20</sup> In some cases, such technology is commercially developed. In other cases, government entities may design and develop their own technology.<sup>21</sup>

This Paper will explore the possibility of relying on principles or norms instead of legal rules to bring more respect for human rights into the development of digital technologies. Part II will examine the concepts of rules, norms, and principles, and will address the need for a norm on human rights in technology. Part III will propose a new norm for establishing legal rules related to the development of new digital technology. Lastly, Part IV will conclude by summarizing the proposal and by emphasizing the importance of this new proposal in the international community.

## II. RULES, NORMS, AND PRINCIPLES

Rules, norms, and principles are often interchangeably used and not necessarily appropriately. Even though opinions on their precise meaning may differ, this Section defines each term and attempts to shed some light on that discussion in view of the central question about whether a regulatory tool would bring more attention to human rights into the development process of technologies.

---

19. *Id.* at 460.

20. Marten Zwanenburg, *Know Thy Enemy: The Use of Biometrics in Military Operations and International Humanitarian Law*, 97 INT'L L. STUD. 1404, 1411 (2021).

21. Austin Wyatt, *Charting Great Power Progress Toward a Lethal Autonomous Weapon System Demonstration Point*, 20 DEF. STUD. 1, 12–13 (2020).

Of the three concepts, it is easiest to distinguish rules from norms and principles. In a positive law context, a rule implies a relatively high level of specificity in describing a behavior and entails consequences when the actual behavior does not align with the described behavior. Clear rules help achieve legal certainty so that natural and legal persons know how to conduct themselves and what the consequence could be when they cross the line that the rule has drawn for them.<sup>22</sup>

The meaning of principles and norms—and in particular the distinction between both—is slightly more complicated. The strong connection between the two concepts does not help. We see a good example of the tether between principles and norms in the well-known theory by Lawrence Lessig on the modalities of regulation.<sup>23</sup> Lessig recognized law, norms, architecture, and market mechanisms as the four modalities of regulation. Though he does not include principles as a form of constraint or regulation, he does refer to principles when offering examples of the architecture of technology and how it steers our behavior in a certain direction.<sup>24</sup> This could mean that principles are embedded in the four modalities and thus constitute a foundation that finds its implementation via one of the four modalities. For example, the legality principle means that the criminal law of a country should form the basis for a prosecution, and that no one should be prosecuted for behavior that is not proscribed by law.<sup>25</sup> The principle thus finds its implementation in the way that a national criminal code is created and updated when new types of unacceptable behavior emerge that cannot be prosecuted by existing law.<sup>26</sup> Principles are also embedded in the mechanisms of the market, such as the principle of supply and demand or the principle of scarcity that make us want to buy products when

---

22. Finnemore & Hollis, *supra* note 1, at 441.

23. Lawrence Lessig, *The New Chicago School*, 27 J. LEGAL STUD. 661, 662–63 (1998).

24. Lawrence Lessig, Keynote Address at the Internet Political Economy Forum Cambridge Review of International Affairs: Architecting for Control 9–12 (May 11, 2000).

25. Andrew Novak, *The Principle of Legality*, in THE UNIVERSAL DECLARATION OF HUMAN RIGHTS— A COMMENTARY 270, 271 (Humberto Cantú Rivera ed., 2023).

26. *Id.* at 272–73.

they are in short supply.<sup>27</sup> Finally, principles can also lie at the basis of norms.<sup>28</sup> The principle of access to justice can lead to the norm of creating more online options for citizens living in remote areas to participate in hearings without the physical and financial burden of traveling long distances, or can even lead to a legal obligation for courts to provide online hearings.<sup>29</sup>

Finnemore and Hollis go one step further and recognize principles as a type of norm.<sup>30</sup> More specifically, they see principles as a broad level of specificity of the behavioral aspect of norms, stating, “principles set forth broad considerations for evaluating future behavior without providing any particular norm for the behavior itself.”<sup>31</sup> This makes principles a type of norm that are not so much focused on the outcome as they are on the process.<sup>32</sup> The uncoupling from the outcome gives principles the flexibility that is often needed to see norms work in a wide variety of cultural, political, and technological contexts. Principles should be viewed as directions, guiding the course that behavior should take without defining an end goal. Such guardrails can function in similar ways, yet also exist in different contexts. For example, principles allow for a legislator to give more specific rules. They also allow corporations to make informed decisions on long-term strategies.<sup>33</sup> In a short-term context, principles can facilitate decision-making with regard to, for example, the research and development process of new technologies or the abandonment of a harmful algorithm, or one that causes financial, physical or psychological harm.<sup>34</sup> Principles could therefore offer an answer when brand-new technologies bring up brand-new questions on

- 
27. Lessig, *supra* note 23, at 662–63.
  28. Glob. Comm’n on the Stability of Cyberspace, *supra* note 4, at 20.
  29. See e.g., BAR COUNCIL OF ENG. & WALES, A LENS ON JUSTICE: THE MOVE TO REMOTE JUSTICE 2020–2024, at 60–61 (2024).
  30. Finnemore & Hollis, *supra* note 1, at 440–41.
  31. *Id.* at 441.
  32. *Id.* at 441, 444.
  33. See generally Lessig, *supra* note 23 (explaining how internet innovation followed changing principles).
  34. Nari Johnson et. al., *The Fall of an Algorithm: Characterizing the Dynamics Toward Abandonment*, 2024 ASS’N FOR COMPUTING MACH. CONFERENCE ON FAIRNESS, ACCOUNTABILITY, & TRANSPARENCY 337, 343 (2024).

ethical development, application, or on their impact on human rights.

Finnemore and Hollis' perspective on principles can work well to overcome the effects of the pacing problem. Viewing principles as a more general functioning form of norms can create a framework for regulating problems that we do not know exist yet. Principles are active on a higher level of abstraction<sup>35</sup> and thus can work in a range of geographical, chronological, cultural, and political circumstances. For example, offering citizens physical and/or online access to justice would be a specification of the principle of access to justice. The same can be said about giving citizens more specific rights, such as the right to a fair trial, the right to a translator, or the right to necessary [online] information, including applicable laws and jurisprudence. This does not mean that access to justice should look the same in every country in the world. It also does not mean that access to justice in 1830 should look the same as access to justice in 2025. It means that the principle can and should be interpreted considering the circumstances of the time and location.

Formulating principles for putting forward new types of acceptable behavior regarding technology could therefore address the concern that any attempt to solve or to mitigate the pacing problem would have to combine a way to anticipate the impact of a new technology with a form of governance that regulates problems we do not know exist yet. First, relying on principles rather than rules would effectively guide all involved in the development of new technology and could also, as such, offer guidance on how to assess the impact of any new technology. Second, principles as a type of norm are also forms of governance that regulate future problems.<sup>36</sup> By presenting larger themes on a sufficiently high level of abstraction instead of limiting guidelines and rules to only specific or known issues, principles can stand the test of time and even be relied on for guidance in dealing with issues we are unable to predict. The Global Commission on the Stability of Cyberspace (GCSC) understood this reasoning when it put forward four high-level principles guiding the decision-

---

35. Glob. Comm'n on the Stability of Cyberspace, *supra* note 4, at 20.

36. Finnemore & Hollis, *supra* note 1, at 441.

making of the actors involved and identifying the norms stemming from these four principles.<sup>37</sup>

As the pacing problem focuses on the governance of technology from a mostly legislative point of view, a question that is often overlooked is the role of organizations – corporate and public – in developing algorithms that turn out to be harmful.<sup>38</sup> Within organizations, regulatory mechanisms also exist to make decisions on governance, such as codes of conduct and internal regulations or rules.<sup>39</sup> These organizations can – and should – use such levels of governance to intervene in the development process of technology in case harm is caused or could be caused by the use of the technology.

A salient example thereof is the process of renouncing harmful algorithms.<sup>40</sup> This topic is still academically underdeveloped, but one group of researchers has recently succeeded in shedding some light on the matter.<sup>41</sup> Johnson et al. analyzed 40 cases of algorithm abandonment.<sup>42</sup> They identified the factors leading to the final decision to relinquish an algorithm.<sup>43</sup> The factors include the following: patterns that evolved around the awareness of the use of an algorithm by those who interacted with a technology; transparency around the values behind the algorithm and around the process of making decisions; dependency of the algorithm on other systems; access to the algorithm; and visibility of criticism and the effectiveness of oversight.<sup>44</sup> These findings could help formulate principles that could, in turn, help establish mechanisms that provide guidelines for creating algorithms that are not harmful. For example, transparency as a principle or as a rule is not new. In fact, the European Union’s AI Act contains several legal provisions based on transparency as a principle for

---

37. Glob. Comm’n on the Stability of Cyberspace, *supra* note 4, at 18–19.

38. Johnson et. al., *supra* note 34.

39. ORG. FOR ECON. COOP. & DEV. [OECD], THE GOVERNANCE OF REGULATORS: OECD BEST PRACTICE PRINCIPLES FOR REGULATORY POLICY 10 (2014).

40. Johnson et al., *supra* note 34, at 338–39.

41. *Id.* at 340, 345.

42. *Id.* at 338.

43. *Id.* at 344–45.

44. *Id.*

algorithm developers and the organizations that use them.<sup>45</sup> The same can be said for oversight mechanisms and auditability.<sup>46</sup> This research on the abandonment of harmful algorithms shows how these existing principles have influenced the decisions on abandoning such algorithms and how long it took to reach that decision.<sup>47</sup>

Principles as a type of norm are not only used to address governments and tell them how they should behave when using technology. They can also be relied upon to address private organizations to design, develop and utilize technology in a more appropriate manner. Norms in general have been used in different configurations with the purpose of creating some certainty around acceptable behavior in cyberspace.<sup>48</sup>

A. *Norms as an Instrument of International Cyber Security Governance*

Discussions involving international cyber security cannot occur without touching upon the subject of norms, often referred to as “cyber norms,” or rules of acceptable behavior in cyberspace. The generally accepted definition of norms is standards “of proper behavior for actors with a given identity.”<sup>49</sup> What makes the path of norms such an inevitable path to take in cyber security governance, as opposed to other areas of interest such as aviation safety or healthcare? Certainly, the scale, the depth, and the speed with which harm can occur in all of these areas can be significant. However, in cyber security, the reliance on norms seems to be more top-of-mind than the reliance on international law because of the often-contested nature of international law,

---

45. Council Regulation 2024/1689, paras. 25, 60, 66, 67, 72, O.J. (L) 1.

46. *Id.* paras. 72, 73, 131.

47. *See generally* Johnson et al., *supra* note 34, at 351 (identifying socio-technical factors that differentiate algorithms that could be abandoned quickly).

48. *See, e.g.,* Liisi Adamson, *International Law and International Cyber Norms: A Continuum?*, in GOVERNING CYBERSPACE: BEHAVIOR, POWER, AND DIPLOMACY 19, 19–21 (Dennis Broeders & Bibi van den Berg eds., 2020).

49. Peter J. Katzenstein, *Introduction: Alternative Perspectives on National Security*, in THE CULTURE OF NATIONAL SECURITY: NORMS AND IDENTITY IN WORLD POLITICS 1, 5 (Peter J. Katzenstein ed., 1996).

the borderless nature of cyberspace, and the particular characteristic of norms being general in scope.

*B. International Law and Norms*

Binding international law is often considered to be a disputed form of governance in cybersecurity and finds itself therefore accompanied by a modality<sup>50</sup> of governance that is generally regarded as voluntary, not binding, and, for that reason, less demanding.<sup>51</sup>

Three characteristics of cyberspace contribute to the reasons why relying on the application of existing international law as a governance mechanism is not a given. First, the fact that we organized the world – through bloodshed as well as through peaceful transitions – in geographical territories that correspond to jurisdictions makes international law difficult to apply to cyberspace.<sup>52</sup> Within those jurisdictions, a ruler or government has the sovereign power to govern. That global organization does not work for a space that is by definition borderless. The border posts and lines we have firmly placed in the soil and painted on concrete cannot simply materialize in an intangible space. Knowing where the territory (and thus, the reign and responsibility) of one power ends and another begins would be impossible. Second, a large part of the technical layer of cyberspace is owned by private parties.<sup>53</sup> Servers, cables, routers, etc. are not necessarily the property of governments.<sup>54</sup> This particular situation creates a complex multistakeholder governance model that is known for difficult and delicate power dynamics.<sup>55</sup> Third, the existing body of international law does not

---

50. See generally Lawrence Lessig, *supra* note 23 (explaining how norms guide behavior rather than require it).

51. Adamson, *supra* note 48, at 19.

52. See Dennis Broeders & Bibi van den Berg, *Governing Cyberspace: Behavior, Power and Diplomacy*, in GOVERNING CYBERSPACE: BEHAVIOR, POWER, AND DIPLOMACY 1, 1–6 (Dennis Broeders & Bibi van den Berg eds., 2020).

53. *How Does Cyberspace Work?*, COUNCIL ON FOREIGN RELS.: CFR EDUC. (Jan. 31, 2023), <https://education.cfr.org/learn/reading/how-does-cyberspace-work> [<https://perma.cc/956R-ZZR9>].

54. See Rep. of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, ¶ 59, U.N. Doc. A/76/135 (July 14, 2021).

55. Broeders & van den Berg, *supra* note 52, at 2.

cover actions by intelligence agencies such as digital espionage, nor does it cover operations committed by those actors who are technically non-state actors but utilized by states as proxies to hide their involvement. The described actions are precisely the events that raise the biggest concern among states, yet international law is not the governance framework to rely on for regulating the behavior or holding someone accountable.<sup>56</sup>

The history of cyber norms originates from a fear expressed by the Russian Federation in 1998 that the latest information and communication technologies could form a new threat if used for purposes incompatible with international peace and security.<sup>57</sup> The concern that the unprecedented use of such technologies would violate international law was laid down in a sequence of U.N. G.A. resolutions to the U.N. Committee on Disarmament and Security, of which Resolution 53/70 was the first.<sup>58</sup> The reluctance from other states to regulate the use of information and communication technologies in a binding convention and the increase in cyber-attacks attributed to state actors eventually cleared the path for a different kind of governance.<sup>59</sup> With a focus on responsible state behavior in cyberspace, the mechanism of a U.N. GGE was introduced to discuss norms to govern the matter.<sup>60</sup> Five rounds of U.N. GGE discussions have resulted in a consensus that international law applies to cyberspace but failed to reach a consensus on how to apply international law provisions to this new domain.<sup>61</sup> The academic community has attempted to fill this gap by publishing commentaries<sup>62</sup> and manuals.<sup>63</sup>

---

56. Broeders & van den Berg, *supra* note 52, at 4 (citing Sergei Boeke & Dennis Broeders, *The Demilitarisation of Cyber Conflict*, 60 SURVIVAL 73, 79–85 (2018)); Tim Maurer, *A Dose of Realism: The Contestation and Politics of Cyber Norms*, 12 HAGUE J. ON RULE L. 283, 286–89 (2018).

57. Adamson, *supra* note 48, at 20.

58. G.A. Res. 53/70, at 2 (Jan. 4, 1999).

59. Broeders & van den Berg, *supra* note 52, at 1, 3–4.

60. G.A. Res. 73/266, *Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, at 2–3 (Jan. 2, 2019). For a full overview, see Adamson, *supra* note 48, at 19, 21–25.

61. U.N. OFF. FOR DISARMAMENT AFF., *supra* note 4, at 95.

62. *Id.* at ix–x.

63. TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 83 (Michael N. Schmitt ed., 2013); TALLINN

At the same time, cyber norms have been notoriously hard to pin down.<sup>64</sup> This goes for defining, identifying, and enforcing them, especially in the area of cyber security governance. The confusion is fueled by the number of variables that are at play when it comes to [cyber] norms. Finnemore and Hollis rely on the traditional definition of a norm by Katzenstein<sup>65</sup> to distinguish the components of identity, behavior, propriety, and collective expectations.<sup>66</sup> The identity of the addressees of the norm is often assumed to be states, yet can also include groups of states, specific government actors, or corporations who own and govern part of the infrastructure that makes up part of what we call cyberspace.<sup>67</sup> A norm can address different types of behavior and aim to regulate it in a certain way, but it can also introduce new rights, roles, or organizations.<sup>68</sup> A third variable of the behavioral component is the specificity with which the acceptable or unacceptable behavior is described by the norm—norms can have a legal basis, yet can also rest on a cultural, professional standard or a political foundation.<sup>69</sup> Lastly, the acceptance of the norm by the members of a community gives it either a strong or weak platform from which to function. Cyber norms are thus not homogenous and should not be handled or studied that way.

Keeping the aforementioned definition of norms and the four norm components in mind, it is reasonable to state that cyber norms are a source of knowledge on what is and what is not allowed in cyberspace. However, that does not yet mean that they are clear-cut and complete rules dictating how a variety of state and non-state actors should behave. That also does not mean that cyber norms cover all appropriate and inappropriate behaviors in cyberspace. On the contrary, just like in the decision-making

---

MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 41 (Michael N. Schmitt & Liis Vihul eds., 2017).

64. Broeders & van den Berg, *supra* note 52, at 5.
65. Katzenstein, *supra* note 49, at 5.
66. Finnemore & Hollis, *supra* note 1, at 438–39.
67. Broeders & van den Berg, *supra* note 52, at 5; Finnemore & Hollis, *supra* note 1, at 439–40.
68. See Finnemore & Hollis, *supra* note 1, at 455 (explaining how norms can address various behaviors and create duties, rights, actors and frameworks in relation to human rights and security, referencing the history of landmine bans as an example).
69. *Id.* at 441.

process of legal rules, norms emergence<sup>70</sup> can take a considerable amount of time, which could lead to the emergence of types of behavior not covered by any existing norms or rules.<sup>71</sup> New types of behavior can for that reason remain ungoverned for unknown periods of time, causing uncertainty among relevant actors on where the limits of acceptable behaviors lie and what the threshold for a reaction is.<sup>72</sup> Stating that cyber norms would be a form of “fast governance” and a worthy alternative to [international] law would be giving them too much credit. In 1998, Finnemore and Sikkink predicted that the process of norm creation would accelerate due to the active role that international organizations such as the United Nations are playing in pushing for certain norms and the increased global communication leading to homogenization of norms.<sup>73</sup> Still, considering the stages of the lifecycle of a norm and the uncertainties surrounding them, it would be incorrect to see norms as an essentially faster version of laws. It is important to note that norms are not necessarily alternatives to laws. On the contrary, laws often result from norms, manifesting as “expressions of norms that the international community accepts.”<sup>74</sup> There is thus a stronger link between law and norms than is often presented.

### C. *Existing Sets of Norms*

If we look at norms as a source of knowledge on what is and what is not allowed in cyberspace, we still have some gaps in our understanding of acceptable behaviors. The norms agreed upon by states do not cover all the behaviors that may be harmful.<sup>75</sup> Moreover, non-state actors started a number of norm-creating initiatives, such as technology-developing companies and non-governmental organizations.<sup>76</sup> Eggenschwiler and Kulesza already

---

70. Martha Finnemore & Kathryn Sikkink, *International Norm Dynamics and Political Change*, 52 INT’L ORG. 887, 896–905 (1998).

71. *Id.* at 895–902.

72. *Id.* at 895–96 (explaining how long the norm “life cycle” can take to take effect).

73. *Id.* at 909.

74. Adamson, *supra* note 48, at 27.

75. *See, e.g.*, Asaf Lubin, *The Liberty to Spy*. 61 HARV. INT. L.J. 197, 185 (2020).

76. *See* Jacqueline Eggenschwiler & Joanna Kulesza, *Non-State Actors as Shapers of Customary Standards of Responsible Behavior in*

made a valuable overview of these initiatives,<sup>77</sup> so I will not repeat that here. However, in view of the core question of this Paper, I will concentrate on what the main norm-setting initiatives say—and more importantly, do not say—about the impact of technology on human rights.

Of the existing sets of norms, the U.N. GGE report of 2015 contains possibly the most straightforward reference to human rights in Recommendation 13(e) with its four resolutions of the Human Rights Council<sup>78</sup> and the General Assembly<sup>79</sup> that focus on specific rights such as freedom of expression, privacy, and freedom of association.<sup>80</sup> The norm is formulated in its typical general configuration addressing States to respect these resolutions in ensuring the secure use of Information and Communication Technology (ICT).<sup>81</sup> How precisely the States do that is where they have the space to maneuver and decide on the most effective and efficient framework.<sup>82</sup> The norm thus sets a goal that the State pursues through its choice of the most appropriate means.

It is important to state that the U.N. GGE mandate restricts the content of their reports to “existing and potential threats in the sphere of information security and possible cooperative measures to address them.”<sup>83</sup> Considering this backdrop of international peace, stability, and security means that from the outset, any norm-setting on U.N. GGE level is by definition addressing states in the first place. In addition, the agreed-upon norms are inspired by those ICT related threats that can affect international peace, stability, and security, such as cross-border

---

*Cyberspace*, in GOVERNING CYBERSPACE: BEHAVIOR, POWER, AND DIPLOMACY 245–55 (Dennis Broeders & Bibi van den Berg eds., 2020).

77. *Id.*

78. Governmental Experts Report, *supra* note 2, ¶ 13(e); Human Rights Council Res. U.N. Doc. A/20/8 (July 16, 2012); Human Rights Council Res. U.N. Doc. A/26/13 (July 14, 2014).

79. G.A. Res. 68/167 (Jan. 21, 2014); G.A. Res. 69/166 (Feb. 10, 2015).

80. H.R.C. Res. 20/8, *supra* note 78; H.R.C. Res. 26/13, *supra* note 78; G.A. Res. 68/167, *supra* note 79; G.A. Res. 69/166, *supra* note 79.

81. Governmental Experts Report, *supra* note 2, ¶¶ 24, 25.

82. U.N. OFF. FOR DISARMAMENT AFF., *supra* note 4, at 111.

83. G.A. Res. A/RES/56/19, ¶ 4 (Jan. 7, 2002).

cyber-attacks that target critical infrastructure.<sup>84</sup> The same goes for the parallel track of the Open-Ended Working Group.<sup>85</sup> A harmful algorithm in a tax calculation app used by citizens of one particular country will therefore not immediately fall within the scope of human rights protection on the U.N. level or in international law in general.

Via the aforementioned resolutions, norm 13(e) refers to human rights in general. The norm includes the important phrase that the same rights that people have offline must also be protected online and thus, it sets the tone for a wide approach.<sup>86</sup> It also highlights particular rights, including the rights to freedom of expression, privacy, freedom of association and – with a link to the digital divide<sup>87</sup> – the right to education.<sup>88</sup> By maintaining the focus on a particular set of human rights, the impression prevails that only these specific human rights can be negatively affected by the use of ICTs and that is not the case. On the contrary, the right to equality and non-discrimination or fair trial rights in civil and criminal proceedings are examples of human rights that can be significantly impacted by technology.<sup>89</sup> I will come back to this in Section (d) of this Article.

Both the Paris Call for Trust and the Siemens Charter of Trust barely mention human rights protection.<sup>90</sup> While the Paris Call includes as its first principle the protection of individuals and infrastructure, its description leans heavily towards the prevention of and recovery from harm caused by malicious online

---

84. H.R.C. Res. 70/174, *supra* note 2.

85. Rep. of the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, at 2–3, U.N. Doc. A/AC.290/2021/CRP.2 (Mar. 10, 2021).

86. Barrie Sander, *Recommendation 13(e)*, in U.N. OFF. FOR DISARMAMENT AFF., *supra* note 4, at 95, 109–10 (highlighting the common language in H.R.C. Res. 20/8, H.R.C. Res. 26/13, G.A. Res. 68/167, and G.A. Res. 69/166).

87. *Id.* ¶¶ 58–59.

88. H.R.C. Res. 26/13, *supra* note 78, ¶ 4.

89. *See* Achiume, *supra* note 5.

90. PARIS CALL WORKING GROUP #4, ADVANCING INTERNATIONAL CYBER NORMS: MULTISTAKEHOLDER RECOMMENDATIONS (2021); *Uniting Global Leaders for a Secure Digital Future*, CHARTER OF TRUST [hereinafter *Charter of Trust Principles*], <https://www.charteroftrust.com/about> [<https://perma.cc/8J2Z-KE6F>].

activities.<sup>91</sup> The call does not elaborate further on the harm and does not mention specific human rights.<sup>92</sup> The ten principles of the Siemens Charter of Trust do not have human rights protection via international law in their scope; rather, the norms focus on commercial development of technology.<sup>93</sup> Attention for responsibility throughout the digital supply chain is the only principle that comes close to an indirect link with human rights.<sup>94</sup>

The set of norms created by the Global Commission on the Stability of Cyberspace (GCSC), also known as the Singapore Norms Package, consists of six norms that intend to complement and strengthen the existing U.N. GGE norms.<sup>95</sup> The first proposed norm is the most relevant for this short overview of attention for human rights in cyber security. The first norm, which is a norm to avoid tampering, stipulates that “State and non-state actors should not tamper with products and services in development and production, nor allow them to be tampered with, if doing so may substantially impair the stability of cyberspace.”<sup>96</sup> The GCSC further specifies that intentionally inserting vulnerabilities in software and/or hardware can have severe effects on the safe and secure use of the Internet and decrease trust in technology.<sup>97</sup> Such reasoning fits the regard for human rights in the development of technology; however the language that the GCSC uses is still limited to attacks and to situations involving intentional interference with a product before it is updated or put on the market.

This leads to one crucial caveat: the GCSC makes it clear in its explanation of the norm to avoid tampering that the norm must only target States’ interference with technology that affects the global stability of cyberspace.<sup>98</sup> Consequently, States can tamper with software or hardware in its development and

---

91. PARIS CALL WORKING GROUP #4, *supra* note 90, at 4.

92. *Id.*

93. *See* CHARTER OF TRUST, CYBERSECURITY POLICY MANIFESTO (2024).

94. *Id.*

95. Glob. Comm. on the Stability of Cyberspace, *Norm Package Singapore* (2018).

96. *Id.* at 9.

97. *Id.*

98. *Id.*

production stages or allow this to happen, when it does not negatively influence overall trust in cyberspace. Even though the document specifies that when a non-state actor performs such actions, domestic, civil, or criminal laws may describe such behavior as unacceptable, one can conclude that within its territorial borders a State could legally insert vulnerabilities or influence the design or development of a technology with [possibly] harmful effects for citizens.<sup>99</sup> The latter is a significant concern considering the examples of harmful algorithms that have come to the surface in recent years and clearly have wide ranging effects across borders. Section (d) of this Article will elaborate on these.

What the GCSC norm to avoid tampering cleverly introduces in the realm of international cyber security is the so-called by-design thinking, a method for generating solutions known from other disciplines that are also applicable to the wicked problem of cyber security.<sup>100</sup> Embracing the approach of by-design-thinking is a practical way of anticipating the harmful impacts of technology by considering them in the earliest stages of development and making them impossible, or at least mitigating the harm as much as possible. This implies having access to the design and development stage of technology, which in practice means obtaining full cooperation from the private sector.<sup>101</sup>

#### *D. Human Rights in a Regulative Norm*

The preceding overview of existing norms underscores the low level of attention to the human rights field and the harms that result therefrom. It revealed that the damage stems from the lack of necessary protective safeguards, not from the intent to harm human rights. Additionally, in accordance with the traditional scope of international law and international cyber security, the language used by the existing sets of norms includes only cyber-attacks or threats to peace or the international stability of

---

99. *See id.* at 15.

100. Richard Buchanan, *Wicked Problems in Design Thinking*, DESIGN ISSUES, Spring 1992, at 5, 6; Horst W. J. Rittel & Melvin M. Webber, *Dilemmas in a General Theory of Planning*, 4 POL'Y SCI. 155, 159 (1973).

101. *See* Glob. Comm'n on the Stability of Cyberspace, *supra* note 4, at 35; CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY ET AL., SHIFTING THE BALANCE OF CYBERSECURITY RISK: PRINCIPLES AND APPROACHES FOR SECURE BY DESIGN SOFTWARE 8 (2023).

cyberspace.<sup>102</sup> That means that what is excluded is the day-to-day use of consumer products or digital technologies used for government services that fall outside of the scope of critical infrastructures. Yet, several examples have shown in recent years that vulnerabilities or bad design of consumer products – whether intentional or not – can cause harm to citizens and to society. In this Section, I will highlight some of these examples as well as the need for more attention to human rights beyond the right to privacy, data protection and free speech in the design and development process of routinely used software and hardware.

One of the most tragic examples originates from the Netherlands. The so-called Dutch childcare benefits scandal reached the international press in 2020,<sup>103</sup> triggered questions in the national parliament, and eventually led the Dutch government to resign in 2021.<sup>104</sup> At the basis of the scandal was an attempt by the Dutch tax authorities to fight organized tax fraud with childcare benefits by finding a way to predict who would be more likely to commit this type of fraud.<sup>105</sup> Using a data-driven approach, developing the right technology can help one to predict the future by using the past. Relying on historical data of known cases of fraud with benefits, the tax authorities introduced a self-learning algorithmic decision-making tool in 2013.<sup>106</sup> The risk classification system that was at the basis of this tool included Dutch citizenship as a label.<sup>107</sup> When signals registered that an individual with a particular nationality could be committing fraud, authorities requested more detailed information on all individuals with that nationality.<sup>108</sup> The Dutch

---

102. Governmental Experts Report, *supra* note 2, ¶ 13(a).

103. Thomas Erdbrink, *Government in Netherlands Resigns After Benefit Scandal*, N.Y. TIMES, <https://www.nytimes.com/2021/01/15/world/europe/dutch-government-resignation-rutte-netherlands.html> (Sept. 30, 2021); Silvia Amaro, *Dutch Government Resigns After Childcare Benefits Scandal*, CNBC (Jan. 15, 2021, 10:15 AM), <https://www.cnbc.com/2021/01/15/dutch-government-resigns-after-childcare-benefits-scandal-.html> [<https://perma.cc/4FPJ-PH3K>].

104. Erdbrink, *supra* note 103.

105. Amnesty Int'l, *supra* note 11, at 11.

106. *Id.*

107. *Id.* at 6.

108. AUTORITEIT PERSOONSGEGEVENS, BELASTINGDIENST/TOESLAGEN: DE VERWERKING VAN DE NATIONALITEIT VAN AANVRAGERS VAN

data protection authority concluded that this practice, in combination with manual selection by civil servants,<sup>109</sup> resulted in a discriminatory targeting of individuals with double nationality or individuals with a non-Dutch nationality.<sup>110</sup> The government investigated an estimated fifty thousand people as potential criminals with significant consequences for their personal lives.<sup>111</sup> Besides the financial cost – up to an estimated fourteen billion euros<sup>112</sup> – the use of the harmful algorithm in combination with other practices by the tax authorities resulted in a considerable human cost such as mental health issues, forced evictions, divorces, etc.<sup>113</sup>

In 2023, a similar example came to the surface in Jordan. The World Bank has taken a data-driven approach in setting up programs that deliver cash to citizens of participating countries based on an estimate of their income and welfare.<sup>114</sup> It is the way that this estimate is conducted that has led to the use of harmful algorithms. A report by Human Rights Watch describes Takaful, a cash transfer program to fight poverty in Jordan that was financed by the World Bank.<sup>115</sup> The report reveals how the algorithm used to assess eligibility for cash transfers was missing context-related indications, as it was based on fifty-seven socioeconomic indicators.<sup>116</sup> For example, ownership of a car

---

KINDEROPVANGTOESLAG [TAX AUTHORITIES/BENEFITS: THE PROCESSING OF THE NATIONALITY OF APPLICANTS OF CHILDCARE ALLOWANCE] 26–29 (2020) [hereinafter DUTCH DATA PROTECTION AUTHORITY REPORT].

109. Amnesty Int'l, *supra* note 11, at 17.

110. DUTCH DATA PROTECTION AUTHORITY REPORT, *supra* note 108, at 49–50.

111. Amnesty Int'l, *supra* note 11, at 13.

112. Marleen de Rooy & Jorn Jonker, *Herstel toeslagenaffaire dreigt ongekende strop te worden: nog 5 miljard extra* [Benefits Scandal Recovery Threatens to Become an Unprecedented Noose: An Additional 5 Billion], NOS (May 13, 2024, 6:00 PM), <https://nos.nl/artikel/2520340-herstel-toeslagenaffaire-dreigt-ongekende-strop-te-worden-nog-5-miljard-extra> [https://perma.cc/G8YG-RLYD].

113. Amnesty Int'l, *supra* note 11, at 13.

114. Hum. Rts. Watch, *supra* note 12, at 1–3.

115. *Id.* § II.

116. *Id.* at 39.

makes a family less eligible for cash transfers, although the head of the family needs the car to drive to work and secure an income.<sup>117</sup> Similarly, higher utility bills would make a family ineligible regardless of whether they are living in uninsulated homes or are unable to afford new low energy-consuming appliances.<sup>118</sup> Like the Dutch example, the Takaful algorithm used a nationality indicator, ultimately excluding any family members with a non-Jordanian nationality.<sup>119</sup> Moreover, the Takaful mechanism requires an online registration without providing a non-digital alternative, ultimately excluding those citizens who cannot afford or are unable to operate a smartphone or computer.<sup>120</sup>

In a report from 2021, the then U.N. Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia, and related intolerance, E. Tendayi Achiume, wrote a comprehensive perspective on racial and xenophobic discrimination and the use of digital technologies in border and immigration enforcement.<sup>121</sup> Based on reports from countries and civil society, the report contains many accounts of how authorities use data and technology in the asylum procedure.<sup>122</sup> The practices described range from confiscating all data carriers verifying the identification of the refugee applicant, to creating risk profiles and combining data from databases set up for a different purpose.<sup>123</sup> Effectively, the use of technology amounts to the introduction of a digital type of border.<sup>124</sup>

Facial recognition technology and other forms of technology that aim to identify an individual based on biometric data are often used for intelligence related to criminal and military goals.<sup>125</sup>

---

117. *Id.* at 44.

118. *Id.*

119. *Id.* at 45.

120. *Id.* at 60–61.

121. Achiume, *supra* note 5.

122. *Id.* ¶ 2.

123. *Id.* § II.

124. Dennis Broeders, *The New Digital Borders of Europe: EU Databases and the Surveillance of Irregular Migrants*, 22 INT'L SOCIO. 71, 73 (2007).

125. Marten Zwanenburg, *Biometrics on the Battlefield*, LIEBER INST. W. POINT: ARTS. OF WAR (Oct. 21, 2020), <https://lieber.org>.

The biometric data that can identify an individual is far wider reaching than simply analyzing facial features.<sup>126</sup> Gait analysis<sup>127</sup> or human ear recognition<sup>128</sup> are among the recently developed methods facilitating individual identification. Especially in combination with other sets of data, such methods can have varying levels of success in correctly matching a person with a dataset.<sup>129</sup> This is precisely the issue: the margin of error of facial recognition and other biometrics-enabled identification methods is not conclusive. Where gait analysis is reported as having an eighty-eight percent accuracy rate<sup>130</sup> and ear recognition as having a ninety-eight percent accuracy rate,<sup>131</sup> research on facial recognition varies due to the margin of error being highly context-dependent and algorithm-dependent.<sup>132</sup> The most recent National Institute of Standards and Technology facial recognition vendor test resulted in a 99.97 percent accuracy rate for the best scoring algorithm<sup>133</sup> with the added disclaimer that perfect conditions are necessary for such a low margin of error. And perfect conditions

---

[westpoint.edu/biometrics-on-the-battlefield/](https://westpoint.edu/biometrics-on-the-battlefield/)  
[<https://perma.cc/WX8X-KH9U>].

126. Achiume, *supra* note 5, ¶ 11.
127. Claudia Álvarez-Aparicio et al., *Biometric Recognition Through Gait Analysis*, 12 SCI. REP., no. 14530, 2022, at 1, 1–2 (2022).
128. Asmaa Sabet Anwar et al., *Human Ear Recognition Using Geometrical Features Extraction*, 65 PROCEEDIA COMPUT. SCI. 529, 530 (2015).
129. Yunhong Wang et. al., *Combining Face and Iris Biometrics for Identity Verification*, in AUDIO- AND VIDEO-BASED BIOMETRIC PERSON AUTHENTICATION 805, 812 (Jozef Kittler & Mark S. Nixon, eds., 2003).
130. Álvarez-Aparicio et al., *supra* note 127, at 1.
131. Anwar et al., *supra* note 128, at 537.
132. See, e.g., Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 PROC. MACH. LEARNING RSCH. 1, 12 (2018); PETE FUSSEY & DARAGH MURRAY, THE HUM. RTS. BIG DATA & TECH. PROJECT, INDEPENDENT REPORT ON THE LONDON METROPOLITAN POLICE SERVICE'S TRIAL OF LIVE FACIAL RECOGNITION TECHNOLOGY 21 (2019).
133. Crumpler, *supra* note 10. For the full results of the NIST facial recognition vendor test, see PATRICK GROTHOR ET AL., NAT'L INST. OF STANDARDS & TECH., ONGOING FACE RECOGNITION VENDOR TEST (FRVT) PART 2: IDENTIFICATION (2018).

are hardly typical, especially in the context of intelligence, criminal, and military investigations and operations, such as the use of autonomous weapon systems.<sup>134</sup> In addition, it is these branches of law that are the most intrusive into individuals' private lives and can have the most severe consequences for those individuals and for society.<sup>135</sup> Not only can a false identification lead to the arrest of innocent people and infringe the presumption of innocence and fair trial rights, but in the worst-case scenarios, an overreliance on these technologies combined with autonomous weapons can lead to severe bodily injury or death.<sup>136</sup> For these reasons, it is crucial to not only invest in scientific research that sheds more light on the margin of error of these technologies, but also to decide what margin of error we find acceptable in which context.

The examples above show how too much focus on data and algorithmic decision-making and an insufficient view of the context and the people behind the data can result in undesirable consequences. The existing norms mentioned above either include human rights in their entirety but lack specificity, or include only those human rights that have the strongest relation to the use of the internet (such as privacy, freedom of speech, and freedom of association). The existing norms do not address certain human rights, including the right to equality and non-discrimination, the right to seek asylum, and the right to a fair trial.

Introducing a regulative norm—as opposed to a generative or constitutive norm—to push for consideration of more human rights would work here. As defined by Finnemore and Hollis, a regulative norm “creates duties or obligations that prescribe, prohibit or permit some activity (or inactivity).”<sup>137</sup> Applied to the current topic, that would mean that state and non-state actors ought to proactively consider human rights in the design and

---

134. Crumpler, *supra* note 10.

135. ICRC, *Artificial Intelligence and Machine Learning in Armed Conflict: A Human-Centred Approach*, 102 INT'L REV. RED CROSS 463, 474–75 (2021).

136. Submission Paper from Hayley Ramsay-Jones to E. Tendayi Achiume, U.N. Special Rapporteur on Contemporary Forms of Racism, Racial Discrimination, Xenophobia and Related Intolerance (Oct. 17, 2019), <https://www.ohchr.org/sites/default/files/Documents/Issues/Racism/SR/Call/campaigntostopkillerrobots.pdf> [<https://perma.cc/DZ3U-AZ8V>].

137. Finnemore & Hollis, *supra* note 1, at 440.

development stages of technology by studying the impact the technology itself can have and the impact that the making of the technology can have on individuals and on society. The fact that Finnemore and Hollis explicitly add “or inactivity” to the definition of a regulative norm is particularly important, as it rules out any passive behavior of corporations vis-à-vis human rights.<sup>138</sup> A proposed norm requiring States and non-state actors to do a “human rights check” during the design and development process of software and hardware should ideally also include a mechanism for verifying that these requirements are met. Section III will propose how to approach such a norm.

### III. PROPOSING A NORM ON HUMAN RIGHTS IN TECHNOLOGY

Human rights have always been an agenda point in international law, yet the preceding overview has shown that simply mentioning human rights or only focusing on specific human rights is insufficient to offer the necessary guardrails for an appropriate use of technology. For that reason, this final Section concentrates on how to close this gap by proposing a principle as a type of norm that requires State and non-state actors who are involved in developing technology to have due respect for human rights from the earliest stages of the development process. This is where by-design thinking comes in.

#### A. *By-Design Thinking*

Ann Cavoukian was one of the authors advocating for privacy-by-design, introducing by-design thinking into the world of cyber security governance.<sup>139</sup> The models originating from computer science showing how to apply security-by-design to build more secure software, followed.<sup>140</sup> In international cyber

---

138. *See id.* (focusing on processes for constructing cybersecurity norms without addressing corporate behavior regarding human rights).

139. ANN CAVOUKIAN, *PRIVACY BY DESIGN - THE 7 FOUNDATIONAL PRINCIPLES: IMPLEMENTATION AND MAPPING OF FAIR INFORMATION PRACTICES* ¶¶ 7–8 (2011).

140. *See* Lee A. Bygrave, *Security by Design: Aspirations and Realities in a Regulatory Context*, 8 OSLO L. REV. 126, 130 (2022); *see also* Cristina Del Real et al., *Shielding Software Systems: A Comparison of Security by Design and Privacy by Design Based on a Systematic Literature Review*, *COMPUT. L. & SEC. REV.*, Apr. 2024, at 1, 2 (2024).

security, it was the GCSC that brought by-design thinking into the discussion about the stability of cyberspace by recommending that State and non-state actors do not tamper with products and services in development and production.<sup>141</sup> Even if the latter is specified to only those tampering efforts that would substantially impair the stability of cyberspace, the GCSC putting its weight behind this recommendation as a norm is a clear sign that this is a debate worth having. Other efforts to bring this approach to international cyber security were made in relation to the debates on encryption and the creation of so-called backdoors into commercial communication devices.<sup>142</sup>

By-design thinking as such is not new. However, it is a new concept to use this type of reasoning to build protective characteristics into technology by moving the attention to human rights to the earliest stage of creation. Software engineers refer to this method as “shifting to the left” when they speak of introducing security features into new software by design.<sup>143</sup> Before the design of a new technology is fully complete and before it enters the development stage, designers should consider human rights to help them decide which particular characteristics and functionalities should be included in the design. This approach proactively prevents harm rather than repairs any harmful effects or compensates for any financial, material, physical, or psychological damage caused after the fact. This proactive consideration prevents human rights from becoming a mere afterthought and instead makes them a priority.

### *B. The Addressees of the Norm*

Embracing human rights by design means that in practice, everyone who is involved in the design of new technology should consider what the impact of this new technology could be on human rights. Though international law typically only addresses States, there is no limitation on which audiences are relevant in the creation and implementation of norms or principles. Earlier attempts to introduce norms, such as the aforementioned Digital

---

141. Glob. Comm’n on the Stability of Cyberspace, *supra* note 4, at 8.

142. MICROSOFT, *supra* note 4.

143. Arina Kudriavtseva & Olga Gadyatskaya, Secure Software Development Methodologies: A Multivocal Literature Review 1 (July 4, 2023) (unpublished manuscript) <https://arxiv.org/pdf/2211.16987> [<https://perma.cc/9SQW-QFZ2>].

Geneva Convention and the Siemens Charter of Trust,<sup>144</sup> also addressed corporations because part of the international cyber security infrastructure is owned by private companies.<sup>145</sup>

There are three reasons for addressing States as well as companies. First, States can be involved in the design and development of new technologies just as much as companies because (1) State authorities have in-house engineers developing, for example, new algorithms for creating more efficient workflows or (2) a State authority contracts a company or a developer to deliver a new product with the certain functionalities. Second, cases such as the Dutch child benefits scandal have shown that when State authorities start using technology for services to citizens and end up causing harm to citizens, individuals lose trust in government, which is hard to repair.<sup>146</sup> The more governments rely on technology for their services to citizens, and that technology causes harm, the higher the risk that a lack of trust in technology will merge with a lack of trust in governments. Both types of trust will continue to go hand in hand. Potentially, this could work in the opposite direction as well: when governments use technology in their services to citizens that respects human rights, citizens' trust in governments may increase. Third, States can develop rules and policies and create incentives for companies to create more secure technology that includes a stronger consideration for human rights. In a carrot-and-stick approach, States could also develop disincentives in case companies do not follow the norm.

Inevitably, the approach to address corporations besides States will remind scholars of the so-called Ruggie principles.<sup>147</sup> However, these principles of corporate responsibility to respect human rights have a different aim, as the primary objective is to call upon corporations to improve poor working conditions for their staff.<sup>148</sup> The aim of the proposed norm on human rights in technology is to call upon corporations to improve the way they

---

144. MICROSOFT, *supra* note 4; *Charter of Trust Principles*, *supra* note 90.

145. Finnemore & Hollis, *supra* note 1, at 460.

146. *See* discussion *supra* Section II(D).

147. U.N. Off. of the High Comm'r, *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*, U.N. Doc. HR/PUB/11/04 (2011).

148. *Id.* at 1.

take human rights into account while developing products that can have an adverse effect on individuals through the way that they are designed or through the way that they are used. Nevertheless, some of the Ruggie principles are formulated in such general fashion that the proposed norm could be seen as a *lex specialis* of principle thirteen on the human rights impacts of companies' activities, operations, products, or services.<sup>149</sup>

C. *Who Is Protected by the Norm?*

When proposing a new norm on protecting human rights, the question is obviously *whose* human rights? That is a relevant question because when discussing the impact of harmful technology, the attention goes directly to the user. This is especially true when we consider traditional by-design thinking, which is typically defined as user-focused.<sup>150</sup> However, it is not always clear who the user precisely is—is it the individual who is actively hitting the buttons and using the technology, or is it everyone who is affected positively or negatively by the technology? Does one need to be aware of the fact that a decision affecting them was made by technology and not by a human to be called a user?

In view of the fundamental aim of the proposed norm – namely, protecting individuals from harm caused by technology – it is a logical choice to expand the definition of user to *anyone who can reasonably be expected to be affected by technology*. Since making a prediction into the future about the impact of technology has its limits, the addition of “reasonable” is of essential importance here. In practice, this means that the impact that the software or hardware could have must be assessed at the time the software or hardware is being designed and developed. Further criteria for such human rights impact assessment should include what is already known in terms of the effects of a particular technology. For example, if no scientific research would exist on the effects of social media on the mental health of teenagers, the relationship between the two would hardly be taken into consideration. At the same time, such criteria could act as a call to researchers to conduct more in-depth studies into the effects of the technology on individuals as well as on society.

---

149. *Id.* at 14.

150. *Id.*

#### IV. CONCLUDING ON A NEW NORM

This Paper first focused on the pacing problem in governing technology while ensuring respect for human rights that may be at risk because of the way technology is created or the way it functions. The objective of this Paper was to find a way to solve or mitigate the pacing problem and to ensure respect for human rights in the design and development of technology. This solution would have to combine a way to foresee the impact of a new technology with a form of governance that regulates problems we do not know exist yet.

In a poignant summary added to her 2021 report on Racial and Xenophobic Discrimination and the Use of Digital Technologies in Border and Immigration Enforcement, Special Rapporteur Achiume stated that “[I]n some cases, discrimination and exclusion occur in the absence of explicit animus, but as a result of the pursuit of bureaucratic and humanitarian efficiency without the necessary human rights safeguards.”<sup>151</sup>

This message can count for many other examples than the use of digital technologies in a border and immigration setting. It is not necessarily with intent that technology is designed, developed, or used in a discriminatory or otherwise rights-violating way. It is, however, the lack of focus on these rights that eats away at their protection. The international community requires stronger human rights guardrails to guide decision-making on all institutional and organizational levels. Working with principles as a type of norm could function well in a setting that already relies heavily on norms but that needs clearer guidance for decision-making in the cyberspace realm.

Combining this reasoning with the reasoning behind the by-design approach can lead to a newly formulated principle that is wide enough to work in a number of circumstances, standing the test of time and the advancement of technology but also remaining sharp enough to make a difference. That difference lies in making State and non-state actors who are involved in the design and development of new technology think about what their product will mean for individuals and for society. The proposed norm is the following:

State and non-state actors who are planning to design and develop new technology should exercise due consideration

---

151. Achiume, *supra* note 5, ¶ 7.

for the reasonably expected impact that this technology could have on individuals and on society by assessing already during the design phase and throughout the development process, the human rights that could reasonably be affected considering the state of the art of technology and the state of society at the moment of assessment.

In view of the described by-design approach, the proposed norm calls upon actors involved to consider the impact of their product in the earliest stages of the design and development process. In the planning phase, when it may not be crystal clear yet what a new technology could look like, designers must consider the impact that the technology will have on individual people and the international community. Ideally, this question should be answered by individuals from different levels of the actor's organization and from different backgrounds (ethnic, cultural, disciplinary, etc.) in order to bring a diverse set of opinions to the table. Preferably, the question should be asked throughout the whole design and development process as new functionalities or characteristics are added to the technology and a clearer view emerges on what the impact may or may not be.

It is important to assess the impact of the technology not only on individuals but also on society. First, individuals of different ages, sexes, and backgrounds could be affected differently, hence the need for a range of opinions speaking out on the potential effects of the technology. Second, researchers should study the effect on individuals or groups alongside but separate from the effect on society. Besides the decaying levels of societal trust in technology, there could also be crumbling trust in governments, in private companies, or even in the deepening of the digital divide.

No one can predict all the impacts that a new technology will have. However, designers, developers, and scholars can study any potential impact through dynamic tests and the evaluation of set criteria. A first criteria should naturally be the current state of the art in technology at the time of the assessment. Depending on how widespread the use of that particular technology is, how accessible it is for all groups in society, and what the known risks already are, designers, developers, and scholars can evaluate how likely it is that the technology will have adverse effects. Second, the current state of technology as used in society could play a significant role in making an accurate assessment on the

reasonably expected impact. Obviously, this criterion is more difficult to evaluate than the state of the art of technology. It focuses on what current trends in technology are – either in general, or for a particular type of technology, such as social media – and how these trends are perceived by society. The combination of both criteria should offer a comprehensive view on the likelihood of any adverse effects of the planned technology on human rights.

The human rights that could reasonably be affected are intentionally not specified in the proposed norm in order to not restrict the norm’s functioning. The goal of the norm is to assess the impact on human rights in general, intentionally not limiting that impact to a particular human right.

The purpose of the norm is comparable to a best-efforts obligation. The actors involved in the design and development of new technology can only be made to assess the reasonably expected impact to the best of their abilities considering the state of the art of technology and the state of society at that time. The word “reasonably” is the operative word in the text of the norm since not all impacts can be predicted. Depending on the employment of the technology in practice and depending on the state of society, rights could be affected that were not envisioned to be affected in the first place.

Finding a mechanism to look into the future and evaluate the impact a new technology may have on individuals and on society and combining it with a mechanism that governs unknown problems seems an impossible challenge. This Article proposes implementing a human rights impact assessment at the earliest stages of the design and development of new technology as a potential way forward.