FUTURE LAW
WORKING PAPERS 2024 • 6

universität innsbruck
Institut für Theorie und Zukunft des Rechts

MATTHIAS C. KETTEMANN • MALTE KRAMME
CLARA RAUCHEGGER • CAROLINE VOITHOFER
EDITORS

The Rights We Have Are Always On

MATTHIAS C. KETTEMANN
CAROLINE BÖCK

INNSBRUCK

Federal Ministry
Republic of Austria
European and International Affairs

VIENNA +30
OUR RIGHTS FUTURE

AUGUST 2024 • ZUKUNFTSRECHT@UIBK.AC.AT

The Future Law Working Papers were established in 2022 to offer a forum for cutting-edge research on legal topics connected to the challenges of the future. As the German Constitutional Court recently ruled, we have to act today to save the freedoms of tomorrow. Similarly, the Future Law Working Papers series hosts research that tackles difficult questions and provides challenging, and at times uncomfortable, answers, to the question of how to design good normative frameworks to ensure that rights and obligations are spread fairly within societies and between societies, in this generation and the next. The series is open for interdisciplinary papers with a normative twist and the editors encourage creative thinking. If you are interested in contributing, please send an email to the editors at zukunftsrecht@uibk.ac.at. Submissions are welcome in English and German.

The series is edited by senior current and affiliated members of the Department of Legal Theory and the Future of Law at the University of Innsbruck: Matthias C. Kettemann, Malte Kramme, Clara Rauchegger and Caroline Voithofer.

Founded in 2019 as the tenth department of the law faculty, the Department of Legal Theory and Future of Law at the University of Innsbruck (ITZR) investigates how law can make individuals as well as society, states as well as Europe "fit" for the future and if and how law has to change in order to meet future challenges. This includes the preservation of freedom spaces as well as natural resources in an intergenerational perspective, the safeguarding of societal cohesion in times of technologically fueled value change, the normative framing of sustainable digitization and digitized sustainability, and the breaking through of traditional legal structures of domination and thought with a view to rediscovering the emancipatory element of law against law.

Publisher:
Institut für Theorie und Zukunft des Rechts, Universität Innsbruck
Innrain 15, 6020 Innsbruck
Univ.-Prof. Mag. Dr. Matthias C. Kettemann, LL.M. (Harvard)
Univ.-Prof. Dr. Malte Kramme
Ass. Prof.in MMag.a Dr. Clara Rauchegger, LL.M. (Cambridge)
Univ.-Ass.in MMag.a Dr.in Caroline Voithofer

The Rights We Have Are Always On

Respecting, Protecting and Implementing Human Rights in the Age of Digital Transformation 30 Years after the Vienna Declaration and Programme of Action

Matthias C. Kettemann and Caroline Böck
University of Innsbruck

Note on funding:

This study was financially supported by the Austrian Federal Ministry of European and International Affairs. Any views and opinions presented in this document are solely those of the author and do not necessarily represent the official position of the Austrian Federal Ministry for European and International Affairs.

Federal Ministry
Republic of Austria
European and International Affairs

VIENNA +30
OUR RIGHTS FUTURE

Table of Contents

Introduction

Respecting, protecting and implementing human rights is always essential. But some years bear a special significance. One of these years was 2023. 75 years ago, the international community recognized that respect for, and protection and implementation of, human rights are the basis for freedom, justice and peace in the world and adopted the Universal Declaration of Human Rights. 30 years ago, in June 1993, the international community took one step further and, during the World Conference on Human Rights in Vienna, the first major human rights conference after the end of the Cold War adopted a common commitment to strengthening human rights around the world: the Vienna Declaration and Programme of Action. Then-UN Secretary-General Boutros Boutros-Ghali described the Vienna Declaration as a "new vision for global action in human rights protection". While the need for global action remains, the concrete visions have changed as much as the circumstances have.

Rather than a singular event, like the end of the Second World War or the end of the Cold War, it is a socio-economic and politico-cultural phenomenon that has brought, globally, changes to the way we live, work, communicate, decide: the digital transformation. The increased prevalence and use of digital tools in many facets of life has brought many advantages, but also substantial challenges. The most recent World Economic Forum Global Risks Perception Survey (2023-2024) counts three digitalization-related risks among its top 12, with “misinformation and disinformation” at the first place for short-term risks, and cyber insecurity at 4th place. As long-term risks (10 years), misinformation and disinformation, adverse outcomes of AI technologies and cyber insecurity are on position 5, 6 and 8, topped only by four weather- and ecosystem-related risks. [1]

Do these new risks, these interlinked and interconnected phenomena of digital transformation, and the new spaces in which national and global processes of societal self-determination take place, necessitate new human rights? The aim of this study is to show why calls for new human rights are unnecessary attempts to undermine global commitments. Rather, this is the time to focus on leveraging existing human rights and fine-tuning their application to the challenges of the digital age, to the presence of digital tools, and to reiterate the underlying human values in light of the growing role of automated decisions-making and AI. Just like the Vienna Declaration and Programme of Action, 30 years ago, shed a bright light on the need to recommit to a holistic understanding of human rights, this study shows how the digital transformation impacts *existing* human rights and how these human rights have to be applied and strengthened, rather than questioned, with regard to their role and relevance for the digital age.

[1] World Economic Forum, “The Global Risks Report 2024”, 19th ed. (2024), https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf, pp. 20 et seq.

Governments across the world must take decisive and deliberate action to safeguard human rights in light of substantial, but not unsurmountable, digital challenges in order to ensure that emerging digital societies and digital communication spaces become places where human rights and human security are ensured, and human development is supported.

1. Executive Summary

- Calls for *new* human rights are misguided. The substantial impact of digital transformation on individual development and societal evolution can be cushioned by existing human rights, interpreted in light of recent technological challenges.

- Human rights apply offline just as online. The current human rights corpus, adaptable and non-discriminatory, should be applied to online, hybrid and offline spaces equally.

- While all human rights apply online just as offline, the digital transformation has certain characteristics which raise specific human rights questions: Technology companies, for instance, now act as gatekeepers of information, influencing what content is seen and promoted. Their policies and decisions therefore impact freedom of expression and access to information, raising concerns about their power over public discourse. By applying human rights in a horizontal fashion, these phenomena can be countered.

- Yet, threats to “digital” human rights can also be public: The capacity for widespread digital surveillance by governments threatens the right to privacy and can have a chilling effect on freedom of expression and assembly.

- Hackers, cybercriminals, and non-state actors can infringe on individuals' rights to privacy and security through data breaches, cyber-attacks, and mis- and disinformation campaigns. Their transnational nature makes it challenging to counter their actions effectively.

- The creators of AI and machine learning technologies play a critical role in shaping digital communication environments. Biases in these technologies can lead to discrimination and inequality, affecting rights to equality and non-discrimination. Algorithmic recommender systems can perpetuate and amplify biases, leading to discriminatory outcomes. This can affect the

fairness of automated decisions in employment, justice, and access to services.

- Existing human rights need to be interpreted in light of new digital challenges, and new actors to keep pace with the rapid development of digital technologies. Time lags between technological developments and normative responses through, e.g. judicial developments, challenge the effective protection of rights in the digital sphere. However, this is not a fundamental problem. It can be countered by capacity-building and awareness-raising.

- The global nature of the digital environment necessitates international cooperation. However, disparities in regulation and enforcement capabilities between countries create gaps in human rights protection.

- With the critical role of digital technologies in accessing information, services, and public life, there is a growing recognition of the need to consider access to the Internet a fundamental human right, ensuring equitable access for all.

- Promoting digital inclusivity and accessibility is crucial to ensuring technologies that serve all demographics, including persons with disabilities and marginalized groups. International solidarity to ensure more equal and equitable access to technological progress between states (and within states) should be mainstreamed into all digital development policies.

- Data rights and privacy need reinforcement, balancing protection with the need for more data to assess human rights threats.

- Digital literacy is essential for navigating online spaces, necessitating educational programs.

- Internet access is a public good and fundamental right; thus, states must ensure its stability and continuous availability and refrain from state-mandated shutdowns or censorship.

- The time to refine the application of human rights in times of digital transformation is now. A key motivation must be to ensure intergenerational equity. The people of today have an obligation, based in human rights, towards the next generation(s) to ensure that their spheres of freedom are not violated. What we do today counts for the protection of human rights in the future.

2. The Premise: The Rights We Have Are Always On

How far-reaching is the ambit of current human rights protection? Can existing guarantees be applied to the digital age? Are our rights still "on" in the digital age? First, the concept of universality and its meaning as basic principle within human rights laws will be analyzed (2.1.). At the same time, calls for *new* human rights, specifically adapted to the digital age, have become louder in recent years. They are particularly attractive for capturing the *zeitgeist*. But are new human rights really necessary, or are such calls misguided (2.2.)?

2.1. Universality: We enjoy the same rights online as offline

Human dignity is at the foundation of human rights. The indivisibility, universality, interrelatedness and mutually dependent and reinforcing character of all human rights were guiding principles of the Vienna Declaration 30 years ago. Even earlier, the Universal Declaration of Human Rights (UDHR) of 1948 committed states to the "promotion of universal respect for and observance of human rights and fundamental freedoms", proclaiming a "common standard of achievement for all peoples and nations".

The UDHR paved the way for more than seventy treaties related to human rights. These include, for example, the International Covenant on Economic, Social and Cultural Rights (ICESCR) and the International Covenant on Civil and Political Rights (ICCPR) of 1966, which – together with the UDHR – are considered the International Bill of Human Rights, which enjoys universal application. The Vienna Declaration and Programme of Action (VDPA) reiterated the universality of human rights once again. The more than 170 UN member states present in Vienna reconfirmed their "solemn commitment […] to fulfill their obligations to promote universal respect for, and observance and protection of, all human rights and fundamental freedoms for all [...]. The universal nature of these rights and freedoms is beyond question."

2.2. *New* challenges – *new* human rights?

Do new challenges give rise to the need for new human rights? Not necessarily, and especially not when it comes to human rights: As the UN High Commissioner for Human Rights, Michelle Bachelet, concluded in a 2019 speech, new challenges do not necessitate new human rights, but, rather adapting "the way we use institutions and processes. [...] We can protect rights effectively only if we constantly fine-tune our

processes to find the right mix of interventions."[2] Constant fine-tuning is difficult, therefore the siren song of new human rights is understandable. But rather than giving in to the temptation of developing an International Bill of Rights 2.0, the following sections show how fine-tuning human rights in light of the challenges of digitalization can increase the effectivity of human rights protection in the digital age. To illustrate this point: Does it make more sense to call for a right to *digital dignity* or to digital services providers to adapt their terms of service to key rules of law standards based on a horizontal application of human rights?[3] But let us address the transformative challenges of digital transformations to human rights systematically.

3. The Framework: Digital Transformations and Human Rights

Traditionally, human rights catalogues bind states and enshrine obligations to respect, protect and implement human rights within their jurisdiction. In light of the growing role of private actors – as providers of much of the infrastructure and the communicative spaces of today's discourses – private actors have become increasingly important. They set rules and use automated decision-making systems to implement them. New players, like providers of digital services, social media companies, online marketplaces, disinformation actors, and bots, must therefore be integrated into the human rights discourse.

Like other transnational corporations that impact the enjoyment of human rights, digital platforms have human rights obligations. Historically, the normative instrument used with corporations was the *Ruggie Principles*, the *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*[4]. The ten Principles of the United Nations Global Compact also include a commitment for businesses to make sure they are not complicit in human rights abuses.[5]

[2] Keynote speech by *Michelle Bachelet*, "Human rights in the digital age - Can they make a difference?", 17 October 2019, New York, https://www.ohchr.org/en/speeches/2019/10/human-rights-digital-age.
[3] Compare for: *João Pedro Quintais* and others, "Using Terms and Conditions to apply Fundamental Rights to Content Moderation", German Law Journal 2023, pp. 1 et seq.
[4] *Human Rights Council,* Report of the Special Representative of the Secretary- General on the issue of human rights and transnational corporations and other business enterprises, John Ruggie - Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework (2011) A/HRC/17/31.
[5] *UN Secretary-General*, Intensification of efforts to eliminate all forms of violence against women and girls - Report of the Secretary-General (2022), A/77/302, marginal no. 26.

In spite of these commitments, major companies behind key social platforms such as Facebook, Instagram, X and TikTok have long been reluctant to implement human rights obligations effectively. As gatekeepers of information, they have the ability to

influence what content is seen and what is not for their billions of users. As they operate mainly for profit and are subject to relatively few (and only recent, and regional) regulations, they have been able to set rules and prioritize information governance with a view to increasing engagement and not, necessarily, societal values like social cohesion and societal resilience. Thus private decision can impact freedom of expression and access to information, raising concerns about their power over public discourse.

Regional legislative approaches regularly attempt to reduce this position of power by including e.g. transparency rules: This can firstly be seen in the Digital Strategy of the EU, which attempts to curb the power of large digital companies by imposing obligations on them that mitigate the negative effects of online communication and at the same time promote the implementation of fundamental rights. The EU's Digital Services Act (DSA), Digital Markets Act (DMA), Data Act, Data Governance Act and Artificial Intelligence Act (AIA) echo the main message of this study in that they provide few *new* substantive obligations but focus on transparency and compliance obligations. The DSA builds on existing human rights in a number of provisions as it requires platforms to consider fundamental rights in their moderation practices (Art. 14(4) DSA) or in the obligations to assess and mitigate risks they pose for these rights (Art. 34(1)(b), 35 DSA). The DMA prohibits various platform practices that have led to the current oligopoly of, and missing competition between, Big Tech companies. Finally, the AI Act contains provisions to safeguard human dignity and avoid discriminatory use of the technology, among others.[6] Following a possible reenactment of the General Data Protection Regulation's *Brussels Effect*[7], other jurisdictions have adopted similar approaches, inter alia the UK with its Online Safety Act 2023[8] or the APAC region.[9]

But it is not only platforms as private companies who aim to make a profit that are shaping the infrastructure under which online human rights are exercised today. New

[6] Cf. in more detail *Martin Müller and Matthias C. Kettemann*, "European Approaches to the Regulation of Digital Technologies", in: Hannes Werthner and others (eds.), Introduction to Digital Humanism (Vienna 2024), pp. 631-634.

[7] *Anu Bradford*, "The Brussels Effect: How the European Union Rules the World", OUP 2020.

[8] Cf. https://bills.parliament.uk/bills/3137. Different to the DSA, the Act contains "chat control" provision which may violate human rights law following ECtHR, Judgment of 13 February 2024, no. 33696/19, *Podchasov v. Russia*, see Thomas Claburn, "European Court of Human Rights declares backdoored encryption is illegal", https://www.theregister.com/2024/02/15/echr_backdoor_encryption.

[9] *Agne Kaarlep* and others, "Platform Regulation in APAC and the EU: A Comparative Overview", https://www.techpolicy.press/platform-regulation-in-apac-and-the-eu-a-comparative-overview.

forms of speech regulation[10] include powers of standard-setting organizations, like the non-profit organization ICANN and the non-governmental standard-setter IEEE, telecommunication companies as Internet Service Providers (ISPs) or auxiliary services on a technical level, such as DNS resolvers or content delivery networks. Their aim is – in contrast to the large digital corporations – by and large to promote a secure, stable and resilient Internet environment. Recent examples, such as a de facto blockage of extremist forum KiwiFarms through a withdrawal of the DNS resolver service by Cloudflare[11] or orders by the Cambodian government to ISPs to block news outlets before the national election in July 2023,[12] show how these technical infrastructure-level actors can affect freedom of speech. A new frontier of human rights, but one that showcases interferences with, and violations of, *existing* human rights.

Creators of AI and machine learning technologies play a critical role in shaping digital environments, thus influencing the enjoyment of human rights. Biases in these technologies can lead to discrimination and inequality, affecting rights to equality and non-discrimination. AI systems are trained with data that is often biased, which results in AI systems that reflect or even intensify these biases.[13] This is evident when one looks, for example, at the use of the AI system Northpointe's Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) in the U.S. criminal justice system for sentencing and parole hearings. Several studies show that this software has a racial bias, since it rates black convicts higher than non-black convicts even if the non-black convict is accused of more severe offenses.[14] Generative AI as the latest development step in AI development is considered to be a major disruptive force with substantial implications for several rights, including data protection, privacy and intellectual property rights.[15] Large Language Models (LLM) are trained with massive amount of tokenized data, such as Wikipedia, online archives of newspapers, but also private forums, like Reddit. The used data itself can contain biases or specific language patterns.[16]

[10] *Jack M. Balkin,* "Free speech in the algorithmic society: Big Data, Private Governance, and New School Speech Regulation", 51 UC Davis Law Review 1188.
[11] *Matthew Price*, "Blocking Kiwifarms", https://blog.cloudflare.com/kiwifarms-blocked.
[12] "RFA statement on Cambodian order to block online content", https://www.rfa.org/about/releases/rfa-statement-on-cambodian-order-to-block-online-content.
[13] *Bushra Kundi* and others, "Artificial Intelligence and Bias: A Scoping Review", Chapter 12, in: Christo El Morr, AI and Society, 2022; *Alfonso Min,* "Artificial Intelligence and Bias: Challenges, implications, and remedies", 2 Journal of Social Research 2023, pp. 3808 et seqq.; already: *Filippo A. Raso* and others, "Artificial Intelligence & Human Rights: Opportunities & Risks", Berkman Klein Center Research Publication No. 2018-6, p. 15. Cf. *Osonde Osoba and William Welser IV*, "An Intelligence in Our Image – The Risks of Bias and Errors in Artificial Intelligence", RAND Corporation 2017, pp. 13 et seqq.
[14] *Roberto Navigli* and others, "Biases in Large Language Models: Origins, Inventory, and Discussion", 15 Journal of Data and Information Quality 2023, pp. 1 et seqq.
[15] *Pamela Samuelson*, "Generative AI meets copyright" Science 381 (6654), p. 159.
[16] *Roberto Navigli* and others, "Biases in Large Language Models: Origins, Inventory, and Discussion", 15 Journal of Data and Information Quality 2023, pp. 1 et seqq.

Hackers, cybercriminals, and (non-)state actors can infringe on individuals' rights to privacy and security through data breaches, cyber-attacks, and follow-up disinformation campaigns.[17] Their transnational nature makes it challenging to regulate their actions effectively. In recent times, cyber-attacks are often linked with

orchestrated disinformation campaigns. Still the most prominent example where hacks and misinformation could be observed together is[18] the case of the Democratic National Committee hacked by the Russian Military Intelligence Agency (GRU). The group gained access to the entire database of opposition research on Donald Trump and leaked it for the use of misinformation campaigns.[19] However, this attack is far from the only one. In 2020 and 2022, serious cyber-attacks against the Austrian Federal Ministry for European and International Affairs were reported,[20] which were aimed at obtaining information and then utilizing it for misinformation purposes.

This trend can also be demonstrated statically: Publicly known cyber incidents have increased almost tenfold since the COVID-19 pandemic and the war of aggression by Russia in Ukraine and more than half of these incidents have been in the sector of state institutions and the political system.[21]

4. The Substance: Human Rights in the Digital Transformation

In the following section, different human rights, grouped into families, are presented in light of their challenges in the digital constellation. The discussion will show why there is no specific need for new human rights, because a modern interpretation of existing human rights guarantees is suitable to answer to challenges posed by technological developments.

[17] *James Shires, "*Windmills of the Mind: Higher-Order Forms of Disinformation in International Politics", 13th International Conference on Cyber Conflict 2021; *Christopher Whyte*, "Cyber conflict or democracy "hacked"? How cyber operations enhance information warfare", Journal of Cybersecurity 2020, pp. 1 et seqq.

[18] Cf. *Alexander Martin*, "Ransomware gang posts breast cancer patients' clinical photographs", https://therecord.media/ransomware-lehigh-valley-alphv-black-cat.

[19] *Robin Maria Valeria and Binneh Minteh,* "Cybercrime, Cyberterrorism and Information Warfare – Threats to Democracy, Governance and National Security", in R. Yahya and others, "Communicating Global Crises: Media, War, Climate and Politics" 2023; *Christopher Whyte*, "Cyber conflict or democracy "hacked"? How cyber operations enhance information warfare", Journal of Cybersecurity 2020, p. 1 et seqq.

[20] BMeiA, https://www.bmeia.gv.at/ministerium/presse/aktuelles/2020/02/cyberangriff-auf-das-aussenministerium-ist-beendet.

[21] See the dashboard of the EuRepoC project, https://eurepoc.eu/dashboard.

4.1. Human Dignity and Fundamental Rights

Right to Life

The right to life is the foundation of all human rights and is explicitly enshrined in various human rights instruments, such as Art. 3 UDHR, Art. 6 ICCPR, Art. 2 ECHR.[22] It obliges states to protect human life by national law, Art. 6 (2) ICCPR. In principle, human rights, such as the right to life, apply outside and inside armed conflicts, even

if they are supplemented in armed conflicts by the more specialized provisions of international humanitarian law.[23]

Research into the use of drones for military purposes has been ongoing since the 1960s.[24] Armed drones are used in large numbers by many countries today: The US, for example, has carried out at least 2,500 armed drone attacks in just a few years with the Predator MQ1 and Reaper MQ-9.[25] The development of these drones is ongoing. In the beginning, military bases near the battlefield were necessary to control these drones. For some time now, the drones can be controlled from thousands of kilometers away.[26]

Yet the development of technology has not stopped here. Although, until recently, control by a human was still necessary and thus a clear and direct criminal attribution to a subject liable to prosecution was possible, research into so-called Lethal Autonomous Weapon Systems (LAWS) is increasingly being driven forward. There is no consensus on the exact definition of these systems. However, the UN's Group of Governmental Experts on LAWS 2023 has undertaken a characterization of these systems: LAWS are characterized by the execution of lethal attacks in the absence of a human decision. The systems decide for themselves, for example on the basis of AI systems, how and where to carry out a lethal attack. A human only switches the system on or off if necessary.[27] This definition includes mines that have been in use for decades, but also the latest developments in the field of autonomous missile defence

[22] *Paul M. Taylor*. in Taylor (eds.)., "A Commentary on the ICCPR" (2020), Art. 6 ICCPR pp. 138 et seq.
[23] *International Court of Justice*, "Legality of the Threat or Use of Nuclear Weapons", Advisory Opinion of 8 July 1996, ICJ Reports, 1996, pp. 226 et seqq.
[24] *E.F. Byrne,* "Making Drones to Kill Civilians: Is it Ethical?", 147 Journal of Business Ethics 2018, pp. 81 et seqq.
[25] *Chris Woods,* "Sudden Justice: America's Secret Drone Wars" (2015) pp. 3 et seq.
[26] *Cf. Reuters*, "Explainer: What are the 'kamikaze drones' Russia is using in Ukraine?" https://www.reuters.com/world/europe/kamikaze-drones-what-are-weapons-russia-is-using-ukraine-2022-10-18.
[27] Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons System, Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects, CCW/GGE.1/2023/CRP.1, 10 March 2023.

systems as well as "kamikaze" drones that scan the ground independently and search for their target and weaponized autonomous land and sea vehicles.[28]

Such LAWS are capable of inflicting particularly great damage, and the absence of human intervention when it comes to the decision to kill people increases the reprehensibility of these weapon systems. This is especially true when civilians are harmed by these weapons.[29].The question now is whether human rights and therefore the right to life can be upheld when using this technology.

The protection of the right to life in international humanitarian law requires in all cases a constant proportionality test when deciding whether the killing of a person is justified in individual cases. In this context, it is difficult to imagine that LAWS, even with the use of artificial intelligence, can "decide" as a human being that a person poses a danger that justifies killing them. Rather, the argument is convincing that such a "decision" by LAWS is arbitrary in any case due to the differences to a human, reason-based decision and therefore jeopardizes the right to life. This assumption that human decisions are part of the exercise and limitation of human rights is also made clear by Art. 1 UDHR, which states: "All *human beings* are [...] endowed with reason and conscience". This makes it clear that human rights have people in mind when they are respected, but also when they are disregarded.[30] Thus, the use of LAWS entails a violation of the right to life that is already evident without the establishment of new human rights violations.

Technological developments in medicine represent another area when it comes to "new" threats to the right to life. For example, new therapeutic measures such as pre-implantation diagnostics are already having an impact on human rights, including the right to health and dignity. With the increase in the use of more data in medicine and the use of more powerful (quantum) technologies, the therapeutic approaches already in use will make it possible to recognize hereditary diseases earlier and more accurately than today. What can certainly be a relief for those affected is more problematic from a global perspective: With the targeted "selection" of unborn life, there is a risk of the successful implementation of social Darwinist theories. Even if the bioethical debate continues as medical progress continues, all these questions can be assessed under existing human rights law, namely the right to life and its basis in human dignity.[31]

[28] For a closer look https://disarmament.unoda.org/the-convention-on-certain-conventional-weapons/background-on-laws-in-the-ccw.

[29] *E.F. Byrne,* "Making Drones to Kill Civilians: Is it Ethical?", 147 Journal of Business Ethics 2018, pp. 81 et seqq.

[30] Consenting: *Christof Heyns*, "Autonomous weapons systems and human rights law", Presentation made at the informal expert meeting organized by the state parties to the Convention on Certain Conventional Weapons 13 – 16 May 2014.

[31] *Elizabeth Wicks*, "The Meaning of 'Life': Dignity and the Right to Life in International Human Rights Treaties", 12 Human Rights Law Review, 199, pp. 208 et seqq.

Dignity

Human Dignity is an underlying principle, or even a right, in numerous international human rights instruments such as the ICCPR, the UDHR and the ICESCR.[32] Within the ICCPR and the ICESCR, it is particularly broad and refers to the "inherent dignity and the equal and inalienable rights of all".

As new technologies question our understanding of dignity, one should bear in mind that dignity – even if referred to in numerous instances in the human rights discourse – does not seem to follow a common understanding.[33] What might be discouraging at a first glance, allows for the development of a conception of dignity fit for the digital age. AI is a case in point. AI is often used to sort and classify attributes and characteristics from datasets that do not take into account the interests and characteristics of the individual person. Organizations that use this AI-filtered data to determine a person's status as a victim (e.g. women at risk of domestic violence[34]) or the likelihood of re-offending (think of the Palantir software, for example[35]) in the case of predictive risk assessments are likely to violate the individual's right to human dignity, as the assessment is no longer based on the personal individual situation and merits.[36] This can lead to a de facto objectivization of a person, which violates their – existing – rights to the protection of their dignity.

Health

The right to health is the economic, social, and cultural right to a universal minimum standard of health to which all individuals are entitled. The right is guaranteed in Art. 25 UDHR, Art. 16 ICESCR and Art. 24 ECHR, among others. Art. 12 ICESCR states that everyone has the right "to the enjoyment of the highest attainable standard of physical and mental health".[37]

---

[32] *Christina Binder* in Donath, Heger, Malkmus, Bayrak (eds.), "Der Schutz des Individuums durch das Recht - Festschrift für Rainer Hofmann zum 70. Geburtstag" (2023), p. 228.

[33] Extensively discussed by *Christopher McCrudden*, "Human Dignity and Judicial Interpretation of Human Rights", 19 European Journal of International Law, p. 697-712.

[34] For example, the VioGén protocol in Spain, which includes an algorithm that evaluates the risk that victims of domestic violence are going to be attacked again by their partners or ex-partners. For a critical view, cf. *Algorithm Watch*, "In Spain, the VioGén algorithm attempts to forecast gender violence" https://algorithmwatch.org/en/viogen-algorithm-gender-violence/.

[35] On the human rights violations committed by Palantir, cf. *Amnesty International*, Palantir Technologies Contracts Raise Human Rights Concerns before NYSE Direct Listing, https://www.amnestyusa.org/press-releases/palantirs-contracts-with-ice-raise-human-rights-concerns-around-direct-listing.

[36] *European Commission*, Commission Staff Working Document "Impact Assessment Accompanying the Proposal for an Artificial Intelligence Act", SWD(2021) 84 final, pp. 17 et seq.

[37] *Tony Anders*, "A human right to health?", 23 Third World Quarterly 2002, p. 199.

Digital technologies are not only in conflict with human rights, they are also capable of promoting human rights. This can be the case in the area of health promotion. By improving predictions, optimizing processes and resource allocation and personalizing services, the use of AI can lead to socially and environmentally beneficial outcomes in the healthcare sector. The use of AI systems in healthcare can help solve complex problems for the common good, such as alleviating the shortage of nursing staff. In combination with robotics and the Internet of Things (IoT), AI systems are increasingly gaining the potential to take on complex tasks that go far beyond human capabilities.[38] This has already been demonstrated during the COVID-19 pandemic, when AI systems were being used, for example, in the quest for vaccines, in disease detection via pattern recognition using medical imagery, in calculating probabilities of infection, or in emergency response with robots replacing humans for high-exposure tasks in hospitals.[39] Such developments lead to the improvement of the standard of physical and mental health by combating diseases more effectively or making care in general possible at all. In this respect, new technologies even have the potential to further promote the right to health. This also shows that there is no need for new human rights, but that digital technologies offer a new way of interpreting the right to health.

Rights of the child

Digital transformation presents several unique challenges for the rights of children and young people, one of which is the heightened risk of online exploitation and abuse. The proliferation of digital platforms has unfortunately facilitated access for predators to engage in harmful activities like cybergrooming, cyberbullying, sexual exploitation, and inappropriate content distribution.[40] These dangers pose a significant threat to the safety and well-being of children, violating their rights as outlined in the United Nations Convention on the Rights of the Child, particularly the right to protection from harm. To combat this, robust online safety measures and regulatory frameworks are essential. Governments, in collaboration with technology companies, must enforce stringent online safety laws and policies, including age verification systems, monitoring and reporting mechanisms for abuse, and stringent privacy protections for children. Furthermore, education and awareness programs for

[38] *European Commission*, Commission Staff Working Document "Impact Assessment Accompanying the Proposal for an Artificial Intelligence Act", SWD(2021) 84 final, pp. 3 et seq.
[39] *OECD*, "Using artificial intelligence to detect, respond and recover from COVID-19", https://ora.ox.ac.uk/objects/uuid:ac36d8d5-cd59-4871-ab30-7925b6714243.
[40] In detail on these phenomena: *Committee on the Rights of the Childs,* General comment No. 25 (2021) on children's rights in relation to the digital environment, CRC/C/GC/25.

children, parents, and educators about online risks and safety practices are crucial in empowering and protecting young people in the digital world.[41]

On a positive side, children should profit from quick, fair and easy access to digital education and resources. The shift towards digital learning platforms can exacerbate educational inequalities, particularly affecting those from lower socio-economic backgrounds or rural areas, who may lack access to necessary technology and connectivity.[42] This digital divide undermines the right to education. To address this, it is imperative to implement policies and programs that ensure all children have equal access to digital learning tools.[43] This includes providing affordable or free Internet access and digital devices to disadvantaged students, integrating digital literacy into the educational curriculum, and training teachers to effectively use and teach with digital technologies. Additionally, public-private partnerships can be leveraged to support the deployment of digital infrastructure and resources in underserved communities.

Digital Inclusion

Societally marginalized groups, such as older persons or persons with disabilities, enjoy the same human rights as everyone else, but they experience a number of challenges when it comes to the full realization of them.[44] Of particular importance in connection with new technologies at the level of the Council of Europe is Art. 23 of the European Social Charter (ESC), which directly addresses the rights of older persons. It states that older people must be able to access resources that enable them to live a decent life and play an active role in public, social and cultural life. In addition, they must be able to obtain certain services and information in a simple and accessible way.[45] The principle of human dignity described above calls for similar rights for older people. Similar special access and inclusion rights can be found in the area of persons with disabilities. Thus, Art. 19 of the Convention on the Rights of Persons with Disabilities (CRPD) reserves the right of these persons to be integrated into society; Art. 21 CRPD contains information access rights, which, according to Art. 24 CRPD, apply especially in the field of education, which has received a strong boost in the field of digitalization since the COVID-19 pandemic.[46]

---

[41] These requirements correspond to the results of the Plenipotentiary Conference of the International Telecommunication Union (Bucharest, 2022), https://www.itu.int/en/council/Documents/basic-texts-2023/RES-179-E.pdf.

[42] *Committee on the Rights of the Childs,* General comment No. 25 (2021) on children's rights in relation to the digital environment, CRC/C/GC/25, marginal no. 99 et seqq.

[43] Derived from the objective of ibid, marginal no. 7.

[44] Cf. eg. *Human Rights Council,* The human rights of older persons, 27 September 2013, A/HRC/RES/24/20.

[45] *József Hajdú*, "Dignity of elderly persons and digitalized social care", pp. 573 et seq. in Zoran Pavlović, Yearbook Human Rights Protection # 3.

[46] *Inka Bormann* and others, "COVID-19 and its effects: On the risk of social inequality through digitalization and the loss of trust in three European education systems" 20 European Educational Research

Inclusion of marginalized groups, such as older people and persons with disabilities, can be promoted through the use of age-appropriate and easy-to-understand technology so that these human rights are safeguarded. Such technology could also enable older people and people with disabilities to be better integrated into social structures by making it easier for them to stay in touch with friends, family and acquaintances through the use of digital platforms or to learn how to carry out administrative procedures digitally. However, empirical studies currently show that health, social and economic factors are sources of inequalities in the access to new digital technologies.[47] Given the cost of digital technologies, such as smartphones and virtual reality headset, the rise in popularity of digital technologies may contribute to widening inequalities,[48] especially for older people, who are more often socio-economically disadvantaged and have few financial resources.

Besides that, older adults are often less autonomous and experienced in using new technologies. The COVID-19 pandemic has intensified this trend, as technical progress has grown sharply in many areas during that time. For example, some services and the receipt of information, for example in the areas of health and care, which are important for older people, are now possible only digitally.[49] Empirical research in this area shows that the difference between young and older people, as well as people with disabilities, in accessing and dealing with technological developments has widened in the last decade even further.[50] The additional physical disabilities that have hardly been taken into account in the development of new technologies, such as virtual reality hardware, make such technological developments almost unusable for older people and persons with disabilities.[51]

These developments are in conflict with the human rights to access and inclusion of marginalized groups, which are particularly protected under existing human rights law. This, too, is an example of how negative effects of technological developments on existing human rights do not have to lead to calls for new human rights.

Journal 2021, p. 610; *Ksenia Skobeltsina*, "Education Systems Management in Critical Situations: Potential Risks of Digitalization", pp. 739 et seqq., XIV International Scientific Conference "INTERAGROMASH 2021" 2021.

[47] *Laura Robinson* and others, "Digital inequalities 2.0: legacy inequalities in the information age", First Monday 2020, p. 7.

[48] *Vincent Paquin* and others, "Time to Think "Meta": A Critical Viewpoint on the Risks and Benefits of Virtual Worlds for Mental Health" JMIR Serious Games (2023), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9944144/.

[49] *Barbara Mikołajczyk*, "Universal human rights instruments and digital literacy of older persons", 27 The International Journal of Human Rights 2023, pp. 403 et seqq.

[50] See *Suzanne Smythe and Sherry Breshears*, "Complicating Access: Digital Inequality and Adult Learning in a Public-Access Computing Space", 29 The Canadian Journal for the Study of Adult Education 2017, p. 67 for further details.

[51] *Ben Egliston* and *Marcus Carter*, "Critical questions for Facebook's virtual reality: data, power and the metaverse", Internet Policy Review 2021 p. 4.

4.2. Civil and Political, Economic, Social and Cultural Rights

Freedom of expression

The right to freedom of expression is the "cornerstone"[52] to the formation of democratic societies and as such protected by all human rights instruments such as Art. 19 UDHR, Art. 19 ICCPR or Art. 4 ECHR. Apart from the freedom to express and hold one's own opinion, as established in Art. 19(1) ICCPR, commonly four pillars of the freedom of expression are distinguished: the right to hold an opinion, to impart information, to seek and receive information and the freedom of the media.[53]

This right is being put to the test by the use of digital technologies such as social media. This can be seen in hybrid conflicts, for example, in which social media has often been used for information operations[54] in recent years.[55] Less developed countries such as Pakistan are also exposed to this modern approach to conducting conflicts: In recent years in particular, (social) media has been used by political opponents, such as India, and non-state actors to divide social cohesion and unity and at the same time create resentment among the population, leading to further challenges for politics, the economy and society as a whole.[56] The threat to freedom of opinion posed by social media and thus technical developments is evident. [57]

Disinformation poses a particular threat that undermines the inclusivity of democratic institutions, for example. As has been shown in practice, some cases of disinformation lead not only to online but also to offline acts of violence. However, disinformation is in many cases permissible for reasons of freedom of expression. At the same time, Art. 19(3) ICCPR, for example, enables UN member states to restrict freedom of expression for various reasons. This opens up several possibilities for dealing with disinformation.[58]

---

[52] *IACtHR*, Advisory Opinion OC-5/85 of 13 November 1985 marginal no. 70 (Compulsory Membership in an Association Prescribed by Law for the Practice of Journalism).

[53] *Nicola Wenzel*, "Opinion and Expression, Freedom of, International Protection" in Peters/Wolfrum (eds.), MPEPIL, marginal no. 13 et seqq.

[54] *Office of the Director of National Intelligence*, Background to "Assessing Russian Activities and Intentions in Recent US Elections: The Analytic process and Cyber Incident Attribution" (2017), https://dataspace.princeton.edu/handle/88435/dsp01k930c052b?mode=full.

[55] *Nathalie Van Raemdonck and Trisha Meyer*, "Why disinformation is here to stay. A socio-technical analysis of disinformation as a hybrid threat", pp. 57 et seqq., in Luigi Lonardo, Addressing Hybrid threats, 2024.

[56] *Noor Ul Amin and Babrak Niaz*, "Media and Hybrid War: Political influence and Disinformation", 15 Journal of Education & Humanities Research (JEHR) 2023, Issues 1.

[57] *Irene Khan*, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression", A/78/288.

[58] *Matthias C. Kettemann* and *Caroline Böck*, "Krisen, Wahlen, Regeln: 2024 digital gestalten" (forthcoming).

In order to enable users to recognize disinformation more quickly and comprehensively, it is particularly important to promote skills in the areas of media, information and digital literacy. Education and facts alone will not combat the phenomenon, as disinformation campaigns are based on controversial topics, emotionalized discourse, fear and confusion. The causes of these problems therefore often lie in current social or environmental challenges that need to be mitigated in their own right.

Finally, platform operators must contribute: Platforms should set up mechanisms to recognize and label harmful campaigns and enforce their own terms of use more effectively. Platforms could be encouraged to incentivize users to help them report disinformation. Promoting public-private partnerships and involving users in content moderation can also help in the fight against disinformation. The use of artificial intelligence trained to recognize disinformation in accordance with platform guidelines and national laws can also make a valuable contribution. The process can be accelerated by working closely with reputable fact-checking organizations that focus on verifying the accuracy and credibility of content. Calls for a new right to truth

online are thus of little help. Rather, a variety of measures are necessary to prevent the phenomenon of disinformation and to safeguard democratic values.

Democracy and democratic decision-making

Democracy is regarded at UN level as a form of government that provides a stable foundation for the effective implementation of human rights.[59] This connection is explicitly mentioned in the VDPA and the member states are urged to continuously implement measures to promote democracy in order to simultaneously promote human rights.[60]

Free, equal, secret and independent elections and democratic decision-making processes are of fundamental importance from a democratic and, as a result, a human rights perspective. Targeted disinformation campaigns are used in particular to influence elections and wage wars,[61] with major negative effects for social cohesion, political decision making and the economy.[62] Undermining democratic processes becomes all the easier when digital disinformation actors use AI systems to create lies,

[59] *Office of the High Commissioner for Human Rights*, "About democracy and human rights", https://www.ohchr.org/en/about-democracy-and-human-rights.
[60] VDPA marginal no. 8 et seq., 66, https://www.ohchr.org/en/instruments-mechanisms/instruments. vienna-declaration-and-programme-action.
[61] *OECD, "*Disinformation and Russia's war of aggression against Ukraine - Threats and governance response" from 3 November 2022, https://www.oecd.org/ukraine-hub/policy-responses/disinformation-and-russia-s-
war-of-aggression-against-ukraine-37186bde.
[62] *Noor Ul Amin and Babrak Niaz*, "Media and Hybrid War: Political influence and Disinformation", 15 Journal of Education & Humanities Research (JEHR) 2023, Issue 1.

synthetic images and artificial images.[63] Even if the techniques used are not subliminal, for certain categories of vulnerable subjects, in particular children, these might have the same adverse manipulative effects if their mental health, age or credulity are exploited in harmful ways.[64] As the AI application areas develop, these (mis)uses and risks are likely to increase, especially since the introduction of generative AI.[65] Generative AI has significant potential for misuse in the form of disinformation. This is due to the ability to create deceptively authentic video material in a matter of seconds, which can then be used to spread deepfakes and misinformation globally.[66]

The integrity of existing information ecosystems is threatened by the use of such technologies.[67] However, this example also demonstrates that protecting existing human rights in the digital age can be achieved by implementing countermeasures, as described in the area of freedom of expression.

Racism, racial discrimination, xenophobia, and related intolerance

In the face of digital transformation, one of the key challenges in combating racism, racial discrimination, xenophobia, and related intolerance is the rapid spread of hate speech and extremist ideologies through digital platforms.[68] The Internet, especially social media, provides a vast, easily accessible stage where harmful narratives can be disseminated widely, exacerbating racial tensions and prejudices. To effectively address this issue, there is a crucial need not for the enactment of new human rights and principles but for the rigorous enforcement of existing legal frameworks that prohibit hate speech and racial discrimination. These laws must be applied stringently in digital contexts, ensuring that online platforms are not exempt from responsibilities upheld in other media. Alongside this, increasing the transparency of online platforms is essential. Platforms should be required to disclose how they monitor and moderate content, including their efforts to detect and remove hate speech. This transparency,

[63] *European Commission*, Commission Staff Working Document Impact Assessment Accompanying the Proposal for an Artificial Intelligence Act, SWD(2021) 84 final, p. 17 et seq.
[64] *Anna-Lisa Vollmer*, "Children conform, adults resist: A robot group induced peer pressure on normative social conformity", 3 Science Robotics of 15 August 2018, Issue 21.
[65] *Cathleen Berger* and others, "EU-Wahlen 2024: Wie wir resilienter gegen Desinformationskampagnen auf sozialen Plattformen werden", https://www.hiig.de/publication/dezentralisierung-als-demokratisierung.
[66] *Matthias C. Kettemann and Caroline Böck*, "Mapping the future of digital technologies", REGROUP Paper (forthcoming).
[67] *Mohamed R. Shoaib* and others, "Deepfakes, Misinformation, and Disinformation in the Era of Frontier AI, Generative AI, and Large AI Models" International Conference on Computer and Applications (ICCA) 2023, p. 1; *Emilio Ferrara*, "GenAI against humanity: nefarious applications of generative artificial intelligence and large language models" Journal of Computational Social Science 2024.
[68] *Ariadna Matamoros-Fernández and Johan Farkas*, "Racism, Hate Speech, and Social Media: A Systematic Review and Critique, Special Issue: Nationalisms and Racisms on Digital Media" (2022) https://journals.sagepub.com/toc/tvna/22/2.

combined with the active enforcement of existing laws, would create a more accountable and less hostile online environment.[69]

Profiling-based advertising algorithms might disproportionately direct certain financial or housing ads to specific ethnic groups, impacting their access to services and opportunities.[70] Yet AI-based systems are also used in the public sector. The "Toeslagenaffaire" has seen Dutch tax authorities use information about people's nationality in a discriminatory manner in an AI system for years to obtain child benefits repayments, especially from migrant families.[71] Most of the European member state tax authorities use AI-based tax systems that check citizens' tax returns automatically, for example "the systeem risico indicatie (SyRI) and eKasa". These are also at risk due to existing biases in their algorithms to create such unfair and discriminatory results

as in the "Toeslagenaffaire".[72] To counter this, there needs to be a robust framework of oversight and accountability for digital marketing practices as well as regulation in the field of the use of AI systems in the public sector[73] – but no new rights. By addressing the underlying issues in digital marketing and the use of AI in the public sector, we can mitigate its role in perpetuating racial discrimination and work towards a more equitable world.[74]

Privacy

Emerging technologies present significant challenges to the right to data protection. While there is no specific mentioning of data protection, most human rights jurisprudence and scholarship find it covered through the right to privacy, as stipulated e.g. in Art. 12 UDHR, Art. 17 ICCPR or Art. 8 ECHR. One prominent challenge to the right to data protection is the widespread collection and processing of personal data by both private and public entities. In the digital era, vast amounts of personal information are constantly gathered, often without explicit consent or sufficient transparency. This practice can lead to privacy invasions and the potential misuse of data.[75] To address this issue, it is essential to enforce existing privacy laws and

[69] *Matthias C. Kettemann* and others, "Menschenrechte im Digitalen - Wie wir Freiheit im digitalen Raum sichern. Handlungsoptionen für die Bundesregierung", pp. 11 et seq., https://library.fes.de/pdf-files/a-p-b/19746.pdf.

[70] *Muhammad Ali*, "Measuring and Mitigating Bias and Harm in Personalized Advertising" RecSys '21: Proceedings of the 15th ACM Conference on Recommender Systems 2021, pp. 869 et seqq.

[71] *David Hadwick and Shimeng Lan,* "Lessons to Be Learned from the Dutch Childcare Allowance Scandal: A Comparative Review of Algorithmic Governance by Tax Administrations in the Netherlands, France and Germany" 13 World tax journal 2021, pp. 609 et seqq.

[72] *David Hadwick,* "Behind the One-Way Mirror: Reviewing the Legality of EU Tax Algorithmic Governance" 31 ec Tax Review 2022, pp. 184 et seqq.

[73] UN General Assembly resolution 2106 (XX), A/RES/2106 (XX).

[74] *Susanne Lilian Gössl*, "Recommender Systems and Discrimination", pp. 13 et seqq, in Genovesi and others (eds.) Recommender Systems: Legal and Ethical Issues (2023).

[75] These issues remain even after landmark legislation such as the EU's General Data Protection Regulation, cf. *Matt Burgess*, "How the GDPR is failing", https://www.wired.co.uk/article/gdpr-2022.

international human rights standards that emphasize consent, data minimization, and purpose limitation in data processing. Data protection authorities should rigorously monitor and enforce compliance, ensuring that data collection practices are transparent and respect individuals' privacy rights. Moreover, individuals should be empowered with knowledge and tools to manage their data privacy, including clear options to opt out of data collection and the right to access and control their personal information.

Technologies such as facial recognition, location tracking, and mass data collection have the potential to create a surveillance environment that infringes upon the right to privacy. The application of existing human rights law is crucial in this context. Any surveillance measures must adhere to the principles of legality, necessity, and proportionality as outlined in human rights norms. There should be robust legal safeguards and oversight mechanisms, including judicial review, to ensure that surveillance practices do not exceed what is permissible under international human rights law. Moreover, some technology should be prohibited when it is clear that its use cannot be justified under human rights law.[76] Transparency from governments regarding the extent and purpose of surveillance is also essential. By upholding these

principles, the potential privacy infringements in the digital age can be mitigated, safeguarding the right to privacy in an increasingly interconnected world. The enactment of new human rights is therefore obsolete.

Cultural rights

Digital transformation poses several challenges for cultural rights such as the preferential representation of certain traditions. The dominance of certain languages and cultures in digital content and platforms can lead to the marginalization of less dominant cultures and languages. This undermines the diversity of cultural expressions and the right of individuals to participate in cultural life.[77] To counter this with regard to digitalization, it is crucial to promote and protect cultural diversity in the digital sphere. This can be achieved by supporting the creation and dissemination of digital content in diverse languages and from various cultural backgrounds. Policies and programs should be designed to encourage and fund the digital representation of minority and indigenous cultures, ensuring their visibility and accessibility online. These have to be based on the existing human rights to cultural rights; new rights are not necessary.

[76] Art. 5 Proposal for a Regulation of the European Parliament and the European Council laying down harmonized rules on artificial intelligence, COM(2021) 206 final.

[77] *UNESCO*, "The 2005 Convention on the Protection and Promotion of the Diversity of Cultural Expressions" (2016 adapted), CLT-2016/WS/7.

Digital literacy

Digital transformation introduces the challenge of a widening digital literacy gap, which can create and exacerbate social inequalities. As technology rapidly evolves, a significant portion of the population – particularly older adults, individuals in rural areas, and those from lower socio-economic backgrounds – often lacks the necessary skills to effectively engage with digital tools. This gap impedes their ability to access information, services, and opportunities in the digital age, infringing on their rights to education and information, as stipulated in Art.s 13 ICESCR and 19 ICCPR respectively. To bridge this digital literacy divide, it is vital to implement comprehensive, inclusive digital education programs. These programs should be tailored to meet the diverse needs of different population segments, ensuring that all individuals, regardless of age, location, or economic status, have the opportunity to acquire essential digital skills. Furthermore, public-private partnerships can be leveraged to provide resources and infrastructure for digital education, making technology more accessible and fostering a more inclusive digital society.

Another challenge is the need for continuous adaptation and learning in response to the ever-changing digital landscape, which is integral to lifelong learning. The rapid pace of technological innovation requires ongoing education and skill development to remain relevant in the workforce and society. This necessity poses a challenge, particularly for those already in the workforce or in later stages of life, who may find it difficult to access or adapt to new forms of learning. Upholding the right to lifelong

learning from Art. 13(2)(d) ICESCR, as emphasized in the 2016 UNESCO Recommendation on Adult Learning and Education[78], necessitates policies and programs that support continuous digital education and training. Governments, in collaboration with educational institutions and industry, should develop flexible, accessible learning platforms and programs that cater to the needs of adult learners and workers. These initiatives should focus not only on imparting technical skills but also on fostering an adaptive mindset and the ability to learn new digital competencies. By prioritizing lifelong learning in the digital domain, we can ensure that all individuals are equipped to navigate and contribute to the digital world throughout their lives. The conclusion is the same: There is no need for new human rights, rather a need for effective actions to combat the infringement of the existing human rights.

[78] *UNESCO Institute for Lifelong Learning,* "Recommendation on adult learning and education", UIL/2016/PI/H/31.

4.3. Governance, Equality and Solidarity

Discrimination and violence against women and girls

Digital transformation has led to new forms of discrimination and violence, as mentioned above, against marginalized groups such as women and girls, including the amplification of gender-based violence online. Cyber harassment, image-based abuse, and gendered disinformation campaigns disproportionately target women and girls, creating an environment of intimidation and fear that can deter their participation in digital life and infringe upon their right to freedom of expression. This online violence can have real-world repercussions, leading to psychological trauma, harm to reputation, and physical violence.[79] To counter this, existing human rights laws that protect against discrimination and violence must be enforced within digital spaces, states the Report of the Secretary-General: "States have obligations to ensure that both State and non-State agents refrain from engaging in any act of discrimination or violence against women and girls, including due diligence obligations to prevent, investigate and punish acts of violence against women committed by private companies, such as Internet intermediaries".[80]

Another challenge is the rise in the use of digital platforms for human trafficking and sexual exploitation, which increasingly operate via hidden corners of the Internet. This includes the distribution of non-consensual imagery and the facilitation of sex trafficking. These digital platforms can unfortunately provide anonymity and a broad reach for perpetrators.[81] Tackling this challenge cannot be done by just changing the law, such as creating a new human right. Those practices already infringe existing human rights such as the freedom from discrimination as well as violence against women and girls but also their right to life and human dignity.[82] Women and children are particularly affected by technology-facilitated violence, which is reflected in some studies. For example, around 90% of the women surveyed in a Korean study say they have already experienced online harassment at least once.[83]

[79] *UNESCO, "*UNESCO's Global Survey on Online Violence against Women Journalists", https://www.unesco.org/en/articles/unescos-global-survey-online-violence-against-women-journalists.
[80] *UN Secretary-General*, "Intensification of efforts to eliminate all forms of violence against women and girls", Report of the Secretary-General (2022), A/77/302.
[81] *Europol*, "Exploiting isolation: Offenders and victims of online child sexual abuse during the COVID-19 pandemic "(2020) https://www.europol.europa.eu/cms/sites/default/files/documents/europol_covid_report-cse_jun2020v.3_0.pdf.
[82] *Simmons BA* and others, "The Global Diffusion of Law: Transnational Crime and the Case of Human Trafficking" 72.2 International Organization 2018, pp. 249 et seqq.
[83] *UN Women*, https://www.unwomen.org/en/what-we-do/ending-violence-against-women/facts-and-figures#83915, keyword: Technology-facilitated violence against women and girls.

There is a need for strengthening international cooperation to monitor and police the digital spaces used for such exploitation.[84] Especially the cybersecurity agenda must be extended to trafficking in human beings in the digital landscape, providing clear and uniform definitions and stiff penalties for digital forms of exploitation and abuse. This is especially necessary to protect women and children, since out of ten victims of human trafficking, four are women and two are girls. They are exposed to sexual exploitation, especially in the online sector.[85] Moreover, there needs to be an emphasis on the creation and implementation of technology tools that can detect and prevent the dissemination of exploitative content.

Data governance

In the digital age, the term data governance is being used more and more frequently. This refers to the utilization and sharing of large data sets, for example in the healthcare sector. In the era of big data and the Internet of Things (IoT), vast amounts of personal data are constantly being gathered, often without the explicit consent or knowledge of individuals.[86]

To address these concerns, robust data governance frameworks that prioritize privacy rights are essential. Such frameworks should enforce principles of data minimization, transparency, and consent, ensuring that personal data is collected and used in a manner that respects individual privacy. Additionally, international cooperation is crucial to regulate cross-border data flows and harmonize privacy standards, safeguarding data protection rights in a globally interconnected digital landscape. Many international organizations have already recognized this and have

therefore developed guidelines and principles: The OECD has adopted a Recommendation on Health Data Governance that aims to enable the use of health data in a proportionate and human rights-friendly manner.[87]

Another challenge is the risk of surveillance and data misuse by both state and non-state actors. The severity of this challenge is increased by the use and the ongoing

development of late-generation AI models that allow for more intensive and extensive electronic analysis.[88] Law enforcement authorities (LEAs) and security and intelligence agencies (SIAs) use algorithmic surveillance already in different areas such as

[84] *Viola Rentzsch*, "Human Trafficking 2.0 – The Impact of New Technologies", 2021, pp. 62 et seqq.
[85] *UN Women*, https://www.unwomen.org/en/what-we-do/ending-violence-against-women/facts-and-figures#83915, keyword: Trafficking in women.
[86] *Ibrahim Alhassan* and others, Data governance activities: an analysis of the literature (2016) https://www.tandfonline.com/doi/full/10.1080/12460125.2016.1187397.
[87] *OECD*, "Recommendation of the Council on Health Data Governance"*,* OECD/LEGAL/0433 (2019).
[88] *Eleni Kosta,* "Algorithmic state surveillance: Challenging the notion of agency in human rights", 16 Regulation & Governance 2020, pp. 212 et seqq.

predictive policing, risk profiling, and pre-emptive surveillance.[89] The pervasive tracking and profiling capabilities enabled by advanced digital technologies can lead to intrusive surveillance, affecting the rights to privacy and freedom of expression but also discrimination rights as well as the right to life and dignity.[90]

This challenge is compounded by the lack of adequate legal safeguards and oversight mechanisms in many jurisdictions. The most important legal challenge in this context is the lack of unified legal standards that ensure evidence-based decision-making while introducing, next to a legality test, a necessity and proportionality test of the use of digital surveillance technologies.[91] In this context, it is also necessary to establish firm legal regulations in connection with data collection, storage, access and analysis.[92] However, a mere legality check is not sufficient. As the cases of the CJEU[93] and the ECtHR[94] in the EU show, such a comprehensive test of proportionality is already necessary, taking into account existing human rights. An extension of human rights is therefore not necessary in this case. Rather, measures must be taken under the existing legal framework to mitigate the restriction of privacy, dignity and discrimination rights.[95]

Disabilities

Digital transformation presents unique challenges for individuals with disabilities, one of which is the accessibility of digital content and interfaces. Many digital services, websites, and applications are not designed with accessibility in mind, thereby excluding those with visual, auditory, motor, or cognitive impairments.[96] This lack of accessibility hinders the ability of disabled individuals to participate fully in the digital economy, education, and social life. The United Nations Convention on the Rights of

Persons with Disabilities (UNCRPD)[97] mandates that states ensure that persons with disabilities can access information and communication technologies on an equal basis

[89] Ibid.
[90] *M. Ziewitz*, "Governing Algorithms: Myth, Mess, and Methods", 41 *Science, Technology, & Human Values* 2016, pp. 3 et seqq.
[91] *Akarsh Venkatasubramanian*, "The Human Rights Challenges of Digital COVID-19 Surveillance", 22 Health Human Rights 2020, p. 79 et seqq.
[92] Ibid.
[93] See for example *CJEU*, Judgement of 16 December 2008, Ref. no. C-73/07, *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy*.
[94] See for example *ECtHR*, Judgement of 12 January 2016, App. No. 37138/14, *Szabó and Vissy v Hungary*, pp. 23, 73.
[95] *Zlatan Meškić and Darko Samardžić*, "The strict necessity test on data protection by the CJEU: A proportionality test to face the challenges at the beginning of a new digital era in the midst of security concerns", Croatian Yearbook of European Law & Policy 2017, p. 133 et seqq.
[96] *Ben Egliston* and *Marcus Carter*, "Critical questions for Facebook's virtual reality: data, power and the metaverse", Internet Policy Review 2021, p. 4.
[97] *UN General Assembly*, The Convention on the Rights of Persons with Disabilities and its Optional Protocol (2006), A/RES/61/106.

with others according to Art. 21 UNCRPD. To overcome this challenge, there must be a concerted effort to enforce and expand accessibility guidelines for digital content, incentivize the development of assistive technologies, and rigorously implement accessibility standards in both the public and private sectors. UNESCO has developed guidelines to provide companies and countries with a strategy on how to achieve digital inclusion in the context of the UN Disability Inclusion strategy.[98]

Another challenge is the digital skills gap that disproportionately affects individuals with disabilities. Often, there is a lack of tailored educational resources to equip those with disabilities with the necessary skills to navigate and utilize digital technologies effectively.[99] This gap can lead to reduced employment opportunities and social isolation in an increasingly digital world. The right to education and work, as articulated in the UNCRPD, provides a foundation to combat this issue. States and educational institutions should provide customized training and educational programs that are designed to meet diverse learning needs and incorporate assistive technologies. By doing so, individuals with disabilities can acquire the digital competencies required to thrive in the digital age, thereby ensuring their right to education and employment is fulfilled in the context of digital transformation.

4.4. A Right to the Internet?

There is generally no need to develop new human rights due to technological innovations of the last but also the next decades. The existing human rights framework represents a firm basis to master the challenges of the digital age. Instead, concrete measures should be implemented based on the existing human rights framework. However, is there perhaps one exception to this rule? Given the unparalleled possibilities connected to 'being connected to' the Internet: Do we need a right to the Internet as a new human right or can we develop if from existing human rights, keeping with the theme of this study?

Even if new rights emerge, they often emerge bottom-up without the involvement of legislators. The *right to the Internet*, e.g., is a catalyst for the exercise of other human rights. However, the realization of this right to Internet access is not yet complete and there are still major differences between countries. In Germany, for example, a positive right to the Internet exists for all citizens and residents, derived from the right to a minimum subsistence level, which represents an expression of human dignity.[100]

[98] *UN Secretary General*, Secretary-General's report on the implementation of the UN Disability Inclusion Strategy (2022) https://www.un.org/sites/un2.un.org/files/undis_sg_report_2022_english.pdf.
[99] Ibid p. 18.
[100] *German Constitutional Court,* Judgement of 27 February 2008, Ref. no. 1 BvR 370/07, marginal no. 171; *German Federal Court of Justice*, Judgement of 24. January 2013, Ref. No. III ZR 98/12.

Furthermore, the implementation of this right by companies poses a challenge, as states must rely on private companies to build the necessary digital infrastructure. This harbors additional risks for citizens.

The right to the Internet can be seen as a relatively new right whose development has not yet been finalized. The right to the Internet can be made up of two different dimensions: the right to access the Internet (infrastructural dimension) and the right to access the Internet in relation to its content (content dimension).[101] Furthermore, the right has two directions of protection: States have a negative obligation not to interfere with the right to the Internet, i.e. not to restrict access to the Internet or access to content on the Internet, which shows the close link between the right to the Internet and other communication rights. As already shown, this right is being violated in part by several states. The right to the Internet also includes a positive obligation on states to provide a communications infrastructure that enables people to access the Internet and Internet content.[102]

The right to the Internet is not explicitly codified in international law.[103] Neither the ICCPR nor the ICESCR explicitly mention it. However, as the use of the Internet is a key to participation in a society and can be crucial for the exercise of other fundamental rights, it can be assumed that the right to the Internet exists on the basis of other fundamental rights.[104] Art. 19 (2) of the Covenant can be interpreted in this way. It protects communication technologies by guaranteeing the expression of opinion through "any [...] media of [one's] choice". Although the Human Rights Committee in its General Comment No. 34 on Article 19[105] confirms its defensive dimension, it also stresses its performative dimension. International law is characterized by soft language: "States parties should take all necessary steps to foster the independence of these new media and to ensure access of individuals thereto."[106] The ECtHR has acknowledged this view in the last years in its judgments.[107]

To summarize this, the right to the Internet is a fairly new right, but a right that exists nonetheless. It didn't need to be created ex nunc, but has evolved organically at the intersection of existing rights.

---

[101] *Matthias C. Kettemann,* "Menschenrechte im Multistakeholder-Zeitalter: Mehr Demokratie für das Internet?," Zeitschrift für Menschenrechte 2016, pp. 24 et seq.
[102] Ibid.
[103] *Johann-Christoph Woltag*, "Internet" in Peters/Wolfrum (eds.) MPEPIL marginal no. 31.
[104] *Matthias C. Kettemann,* "Das Internetgrundrecht zwischen Völkerrecht, Staatsrecht und Europarecht (I)", Völkerrechtsblog of 7. October 2015, https://voelkerrechtsblog.org/das-recht-auf-internet-zwischen-voelkerrecht-staatsrecht-und-europarecht/.
[105] *UN Human Rights Committee*, General comment No. 34 Article 19: Freedoms of opinion and expression, CCPR /C/GC/34, eg. p. 13. *UN Human Right s Committee*, General comment No. 34 Article 19: Freedoms of opinion and expression, CCPR /C/GC/34, eg. p. 13. Human rights in the digital age - Can they make a difference?", https://www.ohchr.org/en/speeches/2019/10/human-rights-digital-age .
[106] *UN Human Rights Committee*, General comment No. 34 Article 19: Freedoms of opinion and expression, CCPR /C/GC/34, eg. p. 13, Para. 15, Geneva, 11-29 July 2011.
[107] *ETCHR*, Judgement of 18 December 2012, App no. 3111/10, *Yildirim v. Turkey*, § 54.

5. Conclusions

- There is no need to create new human rights.
- Existing catalogs of human rights can and must be reinterpreted progressively and applied consistently in order to respond to the challenges of the digital constellation.
- In human rights terms, there is no 'online' and no 'offline' world, just the one world, in which human dignity and activity is protected by human rights. Given the importance of digital technology, access to the Internet and its content is covered by a right to Internet access, which some jurisdictions recognize as an independent right and others, just as effectively, see as emanating from existing human rights, interpreted with a view to digital challenges.
- In the digital environment, it is no longer just states that have the power to legislate, but digital companies, such as Meta, exercise regulatory power over their users - especially on social platforms. To a large extent, they determine the rules of conduct, for example via their community guidelines, and through automated content governance systems which contents is shared and seen.
- This power should be checked, not by new human rights but rather by a horizontal application of existing human rights and increased obligations on platforms regarding their internal rules, algorithms and decision-making procedures. The new European digital rules show one way forward.
- With a view to the effective exercise of all human rights in the digital constellation, solidarity and cooperation must also be promoted to ensure that no society, and no individuals, are left behind.
- Technological developments pose particular challenges for marginalized groups, such as older people and people with disabilities. States, and platforms, need to ensure that their human rights can also be fully realized.
- It is becoming increasingly clear that digital literacy is an essential skill for navigating online spaces.

6. Recommendations

The rights we have are always on. Their protective ambit and impact, however, is challenged by new actors that influence the way how we exercise rights online, by the tools we use and by new frontiers of human interaction that require us to revisit assumptions about how human rights can function as guardrails of human development in times of digital change.

(1) Leverage the existing human rights corpus 30 years after the Vienna Declaration and Programme of Action: There is no need for new human rights. Existing human rights can be adapted to protect us in times of digitalization. The extant human rights corpus, characterized by its adaptability, interpretive precedents, and non-discriminatory principles, is adequately equipped to protect individuals in digital communication spaces. The emphasis should therefore be on the full implementation of these rights in the digital age, rather than on the creation of new rights, which could complicate the legal landscape and potentially dilute the protections intended by the current framework.

(2) Focus on the Actors: New actors have emerged over the last decade, who have a particular influence on how we exercise human rights in the digital age. Large digital companies control our everyday use of technological innovations not only in the area of software, for example on social platforms, but also in terms of hardware. This gives them a strong position of power, which is to a certain extent comparable to the power exercised by a state over its citizens. The interpretation of human rights must therefore be reconfigured. The question of accountability of these companies must be asked at the international level: a horizontalization effect of human rights so that digital companies are also responsible to a certain extent for upholding certain human rights seems plausible. This approach taken by the EU through the Digital Services Act and Digital Markets Act, as well as the AI Act, can be recommended globally. Coupling human rights obligations with transparency and procedural obligations, and a risk assessment coupled with disclosure obligations and mitigation duties, seems to strike a good balance between a company's rights and societal needs.

(3) Take a multi-stakeholder approach to common problems: It is clear that an approach is needed that brings all the key players to the table to tackle these multiple, complex risks that cross cultures, national boundaries and legal jurisdictions.[108] This includes the involvement of states, individuals, private companies, civil society and technical standard setters in various formats of varying geometry at regional and UN levels. The debate on how to best safeguard human rights in times of digital transformation is only beginning – and it must be forcefully led. One example of good

[108] Keynote speech by *Michelle Bachelet*, "Human rights in the digital age - Can they make a difference?", 17 October 2019, New York, https://www.ohchr.org/en/speeches/2019/10/human-rights-digital-age.

practice can be the Internet Governance Forum, an annual international meeting under UN auspices to discuss, but not decide on, current challenges the Internet faces. Such a global forum on human rights in the digital world would be helpful.[109]

(4) Focus on intergenerational equity: As we navigate through the rapid advancements in technology, it becomes crucial to establish policies that ensure these innovations do not come at the expense of future rights, that is the rights of future generations. For instance, environmental degradation and digital waste could significantly hinder the quality of life and access to digital resources for future generations. Therefore, integrating the concept of intergenerational equity into digital transformation policies means advocating for sustainable practices, such as green technology and the ethical as well as human rights-based use of artificial intelligence, which do not compromise the ability of future generations to meet their needs.

(5) Ensure international solidarity: In the digital age, international solidarity is indispensable for bridging the global divide and fostering a more inclusive digital transformation. Technological advancements must benefit all of humanity, rather than increasing existing inequalities, especially in intersectional dimensions. The digital divide, which refers to the gap between those with easy access to digital technology and those without, poses a significant threat to the realization of human rights globally. Collaborative efforts are needed to ensure equitable access to technology, knowledge sharing, and capacity building across borders based on policies that prioritize the needs of the most vulnerable and marginalized communities, ensuring that the digital transformation leads to empowerment and inclusion, rather than exclusion.

(6) Promote digital inclusivity and accessibility: A key priority for the protection of human rights in the digital age is the promotion of digital inclusivity and accessibility, ensuring that digital technologies are accessible to all, including persons with disabilities, marginalized communities, and those in remote areas. A human rights approach sensitive to the challenges of the digital age must emphasize the development and implementation of inclusive technologies and digital services that accommodate the full spectrum of human diversity.

(7) Regulate AI's impact on human rights: The use of Artificial Intelligence raises several human rights issues that have become increasingly pressing as AI technologies are becoming more pervasive in society. AI systems can perpetuate and amplify existing biases present in their training data, leading to discriminatory outcomes against certain groups, based on race, gender, ethnicity, or socio-economic status. The use of AI in political campaigning and electoral processes raises issues concerning

[109] *Matthias C. Kettemann*, in Chris Piallat (eds.) Der Wert der Digitalisierung (2021), p. 347; *Michael Zürn* and others, 14 Zeitschrift für Internationale Beziehungen 2007, pp. 154 et seqq.

transparency, accountability, and the manipulation of democratic decision-making. AI-driven personalization on social media platforms can influence voters and polarize public opinion, impacting individuals' rights to freely participate in their government and public affairs.

(8) Safeguard data rights, but collect and analyze more data: UN member states need to reinforce the right to privacy and data protection in the digital age with robust legal frameworks for private actors that regulate data collection, processing, and sharing. These frameworks should be designed to prevent unlawful surveillance and to protect individuals from privacy breaches. At the same time, member states need to collect and analyze more data to make human rights threats assessment empirically grounded. We have too little reliable data about those who do not use the Internet, about the use of the Internet by people with immigrant backgrounds and about those who have (often multiple and intersecting) experiences of discrimination and exclusion.

(9) Strengthen digital literacy and engage in capacity-building: UN member states need to recognize digital literacy as a fundamental skill necessary for the effective exercise of human rights online. They should start and intensify comprehensive educational programs that equip individuals with the knowledge to navigate digital spaces safely and responsibly.

(10) Safeguarding "the Internet", but not for the Internet's sake: Internet access is a public good, a fundamental right and the backbone of digitalization. Therefore, states have to commit to keeping the Internet 'on', just like human rights are always on. Too many states use Internet access as a policy tool, threat and weapon in the political arsenal. This endangers the stability of the global Internet.

(11) Leverage good practices in digital human rights protection: Digital transformation touches all states. UN members across different jurisdictions should increase cooperation to develop good practices and share lessons learned. This includes learning from regional governance approaches, like Europe's digital regulation package of 2024, including the Digital Services and Markets Acts, the Media Freedom Act, the Data Act, the Data Governance Act and the AI Act.

(12) Ensure a comprehensive human rights framework for the digital future: As the UN's Summit of the Future and the UN Global Digital Compact draw nearer, stakeholders should advocate for the integration of comprehensive human rights frameworks into digital governance. They should call upon UN member states to commit more resources to the protection of human rights online, including Internet access and freedom of expression, privacy, and data protection, as gateway rights, aligned with existing international human rights treaties and standards.