

Law and Policy Review (LPR)

Volume 3 Issue 2, Fall 2024

ISSN(P): 2076-5614, ISSN(E): 3007-4290

Homepage: <https://journals.umt.edu.pk/index.php/lpr>



Article QR



Title: From Bytes to Rights: Enforcing Digital Human Rights through International Law

Author (s): Showkat Ahmad Mir¹, Fouzia Khaliq², and Zeeshan Ashraf³


Affiliation (s): ¹Mohi-ud-Din Islamic University, Nerian Sharif, AJK, Pakistan
²Mirpur University of Science and Technology, New Mirpur City, Pakistan
³University of Southern Punjab, Multan, Pakistan

DOI: <https://doi.org/10.32350/lpr.32.06>

History: Received: October 29, 2023, Revised: September 03, 2024, Accepted: December 23, 2024,
Published: December 30, 2024

Citation: Mir, S. A., Khaliq, F., & Ashraf, Z. (2024). From bytes to rights: Enforcing digital human rights through international law. *Law and Policy Review*, 3(2), 97–116. <https://doi.org/10.32350/lpr.32.06>

Copyright: © The Authors

Licensing:  This article is open access and is distributed under the terms of [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/)

Conflict of Interest: Author(s) declared no conflict of interest



A publication of
School of Law and Policy
University of Management and Technology, Lahore, Pakistan

From Bytes to Rights: Enforcing Digital Human Rights through International Law

Showkat Ahmad Mir^{1*}, Fouzia Khaliq², and Zeeshan Ashraf³

¹Department of Law, Mohi-ud-Din Islamic University Nerian Sharif
Trarkhel Aj&K, Pakistan

²Mirpur University of Science and Technology,
New Mirpur City, Pakistan

³Department of Law, University of Southern Punjab, Multan, Pakistan.

Abstract

Digital human rights require careful definition and protection in the contemporary digital landscape. This research employs a jurisprudential analysis based on international law to clarify the evolving nature of digital human rights. Through a methodological approach encompassing a legal framework review, case study analysis, and policy recommendations, the intricate relationship between technology and human rights is examined. Key findings emphasize the importance of international law in protecting digital human rights while also identifying existing legal deficiencies and obstacles. The research further underscores the transformative potential, and associated risks, of artificial intelligence and machine learning. The conclusion presents a future-oriented perspective, advocating for international collaboration and substantial revisions to existing legal frameworks to promote a digital environment that respects human rights. The research also encourages further investigation into the ethical dimensions of emerging technologies, emphasizing the need for innovation guided by human rights principles.

Keywords: artificial intelligence, data governance, digital ecosystem, digital rights, human rights: international law, policy recommendations

Introduction

By the beginning of the 21st century, the world began embarking on digitalizing every aspect of our communication, work, education and social participation (Castells, 2011). With the rapid progress in information technology, there have been a myriad of changes in the way we live in the age of information technology, such as individuals, communities and

*Corresponding Author: mshowkat5@gmail.com

societies. Digital social media networks and e-commerce sites have fundamentally changed the way people interact in society and conduct business. With all the positives that this transition brought, it has also introduced some complexities and tribulations. With the extensive use of digital technologies, there has been an increase in privacy concerns, data protection dilemmas, and concerns about freedom of speech and access to information. Individuals tend to attribute their rights to the veil of the internet, which, in essence, largely results in the misuse and infringement of such rights (Singh, [2024](#)).

Additionally, the digital divide is creating ground for even increased inequality, as people without access to or understanding of technology are becoming increasingly marginalized. These examples reflect just a few of the distortions concerning how the Digital Era is affecting our societies. This shift has occurred alongside the same timeline as the timeline of evolving interpretations of human rights in response to new digital facets. The concept of digital human rights has emerged to address how technology intersects with society. This involves taking the standard human rights ideology and converting it to the digital world. It is not limited to digital platforms such as internet usage or other digital platforms' rights to freedom of expression or privacy; it is also extended to the right to access the internet or to obtain technical proficiency (Mariniello, [2022](#)).

The purpose of digital human rights is to ensure that everyone can benefit from the advancements of the digital revolution while ensuring that technology upholds and protects fundamental human rights. The right to privacy is necessary in today's world, in which personal information about each individual is collected in enormous quantities to intrusively keep an eternal watch on them (West, [2018](#)). Similarly, digital forums are becoming a major medium for public debate, political activity, and freedom of speech, all of which must be protected. With respect to international law, its power in the digital domain is indispensable. Designed essentially to control interstate conduct and interstate relations at the international level (Shaw, [2008](#)), its significance increases further each day on our path to deep digitization. The time is now ripe to recognize the central role that international law plays in maintaining order, protecting rights, settling disputes in cyberspace, and guiding the application and interpretation of legal standards in this new realm of cyberspace.

Additionally, it also plays a role in adapting existing legal norms and creating new ones to address challenges arising from developing new technologies. At the foreign level, existing international treaties and conventions on human rights, such as the International Covenant on Civil and Political Rights (ICCPR), also constitute an important basis for recognizing and implementing digital human rights. Article 17 of the ICCPR safeguards privacy rights, which, in today's context, protect individuals from unrestrained data collection and surveillance in digital environments (Oh, [2024](#)). In parallel, Article 19, which protects the freedom of expression, now includes within its regulative arm the current areas, such as those that are taking place in social media, to ensure that people have one fundamental right to express their views freely over the internet. However, applying those traditional legal tools in a digital world can be full of complexities and uncertainties requiring new understandings or sometimes all new laws.

Moreover, digital technologies worldwide and noncentralized aspects present new challenges for the application of international law (Alubaidi, [2023](#)). This study aims to identify the role of international law in protecting digital human rights, examine the problems and gaps in current legal frameworks and suggest how this function can be improved for international law to better protect digital human rights. This subject matter is very important given that digital technology advancement is fast and has increasingly broad penetration in our daily lives. For those with a decorous interest in directing how we shape our future, which is technology-enriched yet human rights-respecting, ensuring, and advancing, it is critical to understand how international law and digital human rights interact.

Research Methodology

Using multiple methods, the research looks at digital human rights through an international law lens. It explains how the researchers went about doing the study in the hopes that others, too, could do the same. The first step in the work consisted of a thorough analysis of already issued written materials, the establishment of existing academic papers and the analysis of real cases. This allows researchers to understand how digital human rights evolve and how international law guarantees these rights. The ongoing transformation of digital human rights has also been discussed in recent academic papers in this paper. The researchers then looked at several case studies from around the world that demonstrated how digital human rights

laws actually work. This explained how international law protects people in real life and where we need to improve to safeguard digital rights.

The paper reviewed the literature and case studies, examined existing rules, and presented new ones. It looks at existing laws to determine how these rules can handle the massive changes brought about by computers and the internet. The researcher based their ideas on making the digital world fair and respectful of human rights. They also tried to guess what might happen to digital rights in the future, especially with new tools such as artificial intelligence and computer programs that learn by themselves. Researchers have considered how laws might need to change as technology continues to grow. To fully understand these complex ideas, they used qualitative research methods to look at how technology and human rights connect. The paper carefully discusses the right and wrong ways to use new technology, how it changes society, and what it means for people's rights. This gave them a big picture of digital rights. This study blended various research methods: reading previous research, studying real cases, checking current rules, anticipating future trends, and understanding complex relationships between people and technology. Researchers have focused on fairness, equal treatment, and human dignity while studying how digital rights fit with international laws that continue to change.

The Digital Ecosystem and Human Rights

The digital realm can be conceptualized as a complex, interconnected network encompassing individuals, groups, institutions, and enabling technologies that operate collaboratively within an online environment. Analogous to a dynamic ecosystem, this digital space has undergone continuous evolution, with diverse digital entities flourishing and adapting over time, all adhering to the protocols governing the Worldwide Web (Lee & Levins, [2023](#)). The growth and maintenance of this system are dependent on the consistent flow of information; specifically, each interaction, be it between human users or computational systems, involves the generation and utilization of data. This information helps many sectors work better, such as schools, stores, governments, and hospitals. When we use all this information properly, more work is done, new ideas grow, and more people can help their communities (Clavero & Benlloch-Dualde, [2019](#)). The digital world goes beyond regular maps and connects everyone everywhere. This means that people can learn new things easily and work with others far away, making large groups of friends online. People use social media to talk

to each other all around the world, share what they think, and work together on large projects.

However, the digital world also has some problems. When much information is collected and stored, people worry about keeping their secrets safe. As Mayer-Schönberger (2009) explains, when private information stays stored forever as "digital folders," it gives too much power to the groups that keep this information (Merino et al., [2023](#)). Additionally, computer programs that make decisions sometimes treat people unfairly because they learn from unfair information. For example, these programs might not pick people fairly for jobs, loans, or following rules. However, digital tools affect our rights in both good and bad ways. On the good side, digital tools help people speak freely and share information, as affirmed by the UN General Assembly in 2011. These tools also help people join their community, vote, and enjoy their culture (Chadha, [2024](#)).

The new digital tools, born from innovative ideas and the needs of society, can collect much information and help make choices, but this creates new problems related to people's rights. Privacy becomes more difficult to protect in the digital world. When governments and companies collect and study private information, it affects people's secrets. Additionally, when computers make choices by themselves, they might not treat everyone fairly. If these computers learn from unfair information, they might make things worse for some groups of people (Barocas & Selbst, [2016](#)). This could mean that some people do not have fair chances at jobs, schools, or other important things. The digital world also has new types of bullying and mean behavior. Online bullying and harassment make it difficult for people to feel safe and free (Trigo et al., [2024](#)). Additionally, when some people cannot use digital tools—the 'digital divide'—it is not fair to them. Since digital tools matter so much now, people who cannot use them might feel left out. In the end, while digital tools can help protect people's rights, they also create major problems that need to be fixed.

Understanding Digital Human Rights

Like regular rights, digital human rights protect people's freedom in the digital world, which in turn safeguards their rights in the physical world. These special rights help people stay free and safe when they use computers, phones, and the internet. As more people use digital tools every day,

ensuring that their rights are upheld in this new technological world is crucial. Digital human rights include many types of protection. People have the right to keep their information private online, express their opinions freely on the internet, use online tools, stay safe from others watching them, and be treated fairly by computer programs. For example, digital privacy means keeping one's personal information safe from others who might take it or use it without asking. In our world today, where much information is collected and studied, this freedom helps people stay safe and respected online (Solove, [2008](#)). Another important right allows people to share their thoughts online freely. This means that everyone can write their ideas and find information on the internet without others stopping them unfairly.

Digital human rights matter because they help everyone use digital tools fairly and safely. These rights tell us how to make and use technology in ways that help people while keeping them safe and free. We can better understand digital human rights by considering them normal rights that work in the technological world. These rights come in different types: civil, political, economic, social, and cultural. Civil rights in the digital world mean keeping your privacy online and saying what you think freely. Political rights mean that one can use technology to help make decisions, such as by voting online or asking the government to change things. Economic rights ensure that everyone can use digital tools and find jobs online fairly. Social rights help people learn online and obtain health care through computers.

Cultural rights also matter in the digital world. These rights allow people to share their culture online and save important cultural things in digital form. Special computer codes, called encryption, protect digital privacy by keeping online messages safe from others who should not see them (Lekić, [2024](#)). Additionally, social media helps people share their thoughts freely and work together to make things better. Digital human rights work the same way as regular human rights—they belong to everyone. It does not matter where someone lives, what they look like, what language they speak, or what they believe in. These rights work together like puzzle pieces; when one right works well, it helps the other rights work better too.

International Law and Human Rights

International law works like a big rulebook that guides countries in how to behave with each other and with people (Shaw, [2008](#)). This rulebook has

grown over time and now includes rules about how countries should treat their people and protect their rights. International law comes from two main places: treaties and customary international law. Treaties are written promises between countries that tell them what they must and must not do; these promises are sometimes called conventions or agreements. Customary international law refers to rules that countries follow because they believe it is their responsibility to do so. These basic rules appear in the special book of the International Court of Justice. This court belongs to the United Nations and helps solve problems between countries. It also provides advice about laws when other parts of the United Nations ask for help.

All big legal systems in the world, including international law, follow some basic rules that everyone agrees are good. Judges' decisions and what smart people write about the law help everyone understand these rules better. The rules concerning human rights around the world changed substantially after the United Nations wrote the Universal Declaration of Human Rights in 1948. This special paper tells countries how to protect people's rights and freedoms. It makes countries promise to respect these rights and help people use them. The most important rules concerning human rights appear in special agreements, such as the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social, and Cultural Rights. These rules also exist in customary international law; for example, no country can hurt people through torture. The rules also say that everyone must be treated fairly. Human rights and international law work together closely. International law includes a special part called international human rights law, which focuses on protecting people and groups (Ortynskiy, [2024](#)). This means that human rights belong to everyone in the world, regardless of where they live, what country they come from, or what rules their country uses. Many different tools help protect human rights around the world. Each tool does something special to ensure that people's rights remain safe everywhere.

The Proclamation of the Universal Declaration of Human Rights (UDHR)

The UDHR, ratified by the UN General Assembly in 1948, served as a seminal charter in modern human rights law after World War II. It is a universal blueprint for individuals and nations, advocating that every human is born equal in dignity and rights (United Nations, 1948). While not legally binding, its principles have been incorporated into subsequent treaties and

national constitutions. The UDHR's 30 articles delineate a comprehensive set of rights, including civil, political, economic, and social entitlements, that still echo its relevance in today's digital landscape.

The ICCPR: Legal Cornerstone

Established in 1966 and effective in 1976, the ICCPR extends the UDHR principles into binding legal norms. Part of the "International Bill of Rights," this covenant details provisions from the right to life to freedom of thought in its six sections and 53 articles (Scheinin, [2003](#)). Despite its foundational role, implementing the ICCPR remains a complex task, often requiring collaborative efforts from states (Joseph & Castan, [2013](#)).

The CRC: A Comprehensive Framework for Child Rights

The CRC, ratified in 1989, is the most universally accepted human rights treaty, focusing on a child's holistic well-being. It enumerates an extensive set of civil, cultural, economic, health, political, and social rights for children globally. Four core principles, housed within Articles 2, 3, 6, and 12, underpin the CRC and guide its interpretation. Furthermore, the Convention urges nations to protect children in today's expansive digital world and is overseen by the Committee on the Rights of the Child (Papadopoulos, [2023](#)).

Interplay of International Law and Digital Human Rights

The advent of the digital epoch presents novel legal complexities and ethical dilemmas, profoundly influencing human rights. As global interconnectedness intensifies, with digital tools becoming integral to diverse facets of existence, robust international legal mechanisms become imperative for safeguarding digital human rights (Florek & Eroglu, [2019](#)). Digital human rights refer to a continuum of entitlements to freedom of expression, access to information, privacy, freedom from discrimination, and participation in cultural and scientific progress. Even though these rights are not new, the crisis of technologically pervasive contemporary society endows them with new significance (Cerf, [2012](#)). The assumption of international law about its pivotal function in safeguarding these rights in the digital sphere is also emphasized. In Chapter 4, this research examined individual fundamental rights documents—namely, the UDHR, ICCPR, CRC, and CEDAW—as important parts of this action. These legal instruments delineate state responsibilities regarding three interconnected

aspects of digital human rights: no hate, no harassment, just respect, protection, and fulfillment within the digital realm. (Shelton, [2015](#)).

Governments respect human rights by abstaining from actions that may violate digital human rights. Infringements may include coercive software installed on users' computers, which engages in intrusive surveillance, virtual censorship of digital content, or unwarranted restrictions on access to technology (Deibert & Rohozinski, [2010](#)). Moreover, states must protect individuals from invasions of their digital human rights by actors of different organizations or nonstate actors. Online platforms can also be held accountable for (some of) their actions that infringe on user rights in a regulatory sense (Gasser et al., [2015](#)). Finally, states must actively promote the enjoyment of digital human rights. This means taking steps to promote digital literacy, investing in accessible technological infrastructure, and creating legal and policy frameworks that promote an online environment that supports universal human values (UNICEF, [n.d.](#)).

International law is the cornerstone upon which the development and governance of online human rights are based. Provisions in the digital domain are available for instruments such as the UDHR, ICCPR, CRC, and CEDAW. These rules are, however, useful in solving digital human rights issues, depending on the national setting and emerging global norms (Erol, [2023](#)). However, there is a very real and central challenge, which is in the interpretation and realization of these legal texts into the reality of these fast-developing but also very practical digital technologies. While we have shown these instruments to be adaptive, their predigital (re)construction could render them ill-equipped to grapple with digitally specific problems. This means that our global standards will have to be constantly met and updated to take into account the creativity and invention of technology. Furthermore, the realization of these rights can be dependent on different levels of national technological, regulatory, and political capacity. However, owing to domestic legal implementation policy incorporation as well as the local institutional capability and willingness to concretize human rights, many states that conventionally ratify international human rights treaties need help to enforce them (Donoho, [2001](#)).

Lessons from Applications and Observances of Digital Human Rights

The interplay of international legal provisions concerning online human liberties is evident in numerous cases. The European Court of Human

Rights' decision in *Delfi AS v. Estonia* (2015), which affirmed the responsibility of internet service providers to regulate harmful speech on their platforms, exemplifies the application of fundamental human rights principles in the digital context. Similarly, *Schrems v. Data Protection Commissioner* (2015) demonstrated how extensive data transfers violated privacy standards, prompting the Court of Justice of the European Union to invalidate existing data protection agreements between the EU and the US, thereby reshaping data protection law for both jurisdictions (*Schrems v. Data Prot. Comm'r*, 2015). In the context of developing economies, Brazil's *Marco Civil da internet* (Moncau & Arguelhes, 2014) illustrates how national legislation can integrate global human rights norms while addressing local digital governance challenges. This law safeguards net neutrality and user privacy while also establishing a participatory governance framework for internet oversight, demonstrating a model for the domestic implementation of digital human rights principles (Moncau & Arguelhes, 2020).

Obstacles and Lacunae: Scrutinizing the Difficulties and Shortcomings in Upholding Electronic Human Rights

With its continuous innovations, digital technology presents a dual nature. It empowers individuals, democratizes information, and reduces geographical barriers, yet simultaneously outpaces regulatory frameworks, posing substantial challenges for governing bodies (Lee, 2024). Rapid technological developments, such as machine learning, blockchain, and quantum computing, expand technological possibilities while creating ambiguous legal territories where existing laws seem obsolete. This disparity between technological advancement and legal adaptation is not simply a matter of time; it is a profound divide that generates ethical dilemmas and moral risks (Tufekci, 2017). Legal delays inadvertently create exploitable loopholes, rendering citizens vulnerable to digital rights infringements, including unwarranted surveillance, data breaches, and online harassment (Solove, 2008). The intricacies of international law allow for diverse interpretations, a problem amplified in the context of digital human rights. While international legal instruments provide a foundational structure, implementation remains the responsibility of individual states (Lytvynenko & Skoblyk, 2024). These divergent interpretations frequently result in fragmented regulations that deviate significantly from original international norms (Chimni, 2017).

Furthermore, the unique cultural, political, and social contexts of each nation add complexity. Different nations may prioritize different digital human rights, resulting in substantial variations, from robust data protection in some European countries to more permissive approaches to privacy elsewhere (Natamiharja & Setiawan, [2024](#)). These disparities represent concrete differences that affect the daily experiences of internet users, contributing to digital inequality and influencing global information flows (Natamiharja & Setiawan, [2024](#)). While international law provides theoretical frameworks, its efficacy is often compromised by weak enforcement mechanisms, particularly with respect to digital human rights (Simmons, [2009](#)). The absence of a central internet governing authority diminishes accountability, making it difficult to hold violators responsible. Countries with poor human rights records often lack incentives to adhere to international norms. In these instances, international sanctions or diplomatic pressure become the primary recourse, yet both demonstrate limited effectiveness (Weber & Gunnarson, [2013](#)). Even with existing national laws, enforcement often remains inadequate due to resource limitations or a lack of political will. Protecting digital human rights is a complex undertaking fraught with challenges, including technological complexities, diverse legal interpretations, and enforcement deficiencies. However, every complex situation presents solutions. Technological complexity should motivate the creation of equally nuanced and adaptable laws (Biswa, [2023](#)). Divergent interpretations necessitate dialog focused on harmonization while respecting diversity. Enforcement gaps should encourage the strengthening of national and international accountability mechanisms (Reis et al., [2024](#)).

Future of Digital Human Rights and International Law

Digital human rights exist at the intersection of technology and law, a complex domain that resists simple categorization or prediction (Wagner et al., [2023](#)). Humanity stands at a critical juncture, where technological forces threaten established values of human dignity and rights. The Law of Accelerating Returns posits that technological progress is exponential, not linear (Alexeyev, [2024](#)). Therefore, international law must exhibit similar adaptability and flexibility to accommodate the evolving landscape of digital innovation (Susskind & Susskind, [2015](#)). Legal codification may transition from static texts to dynamic, adaptive algorithms. This is not mere speculation; the emergence of “smart contracts” and the use of machine

learning in judicial processes demonstrate this trend. However, this raises concerns about transparency and accountability in algorithmic governance (Chau & Livermore, [2024](#)). The future may also feature decentralized, cryptographically secured digital identities (Smethurst, [2023](#)). This paradigm shift would decentralize human rights, necessitating the restructuring of international law. Artificial intelligence and biotechnology present unique ethical dilemmas. From the legal status of sentient AI to the rights of genetically modified organisms, the definition of a “right-bearing entity” is expanding. International law must adapt to encompass these nontraditional entities, guided by a cosmopolitan ethic that transcends anthropocentric limitations (Singer, [2011](#)). Digital human rights are no longer a secondary concern; they are central to the social contract of the Information Age (Sunstein, [2001](#)). International law must evolve from preserving the status quo to promoting progressive change. Challenges abound, yet so do opportunities. The future is not predetermined but shaped by present choices. Legal scholars, ethicists, and global citizens must ensure that the future of digital human rights is a narrative of human achievement, not a dystopian account.

Conclusion

This scholarly expedition into the interplay of digital human rights and international law in the ever-growing digital era dominated by artificial intelligence (AI) and machine learning seeks to capture the complex and nuanced relationship between the two areas through the lens of both AI and human rights. Advances in digitization have radically revolutionized the human rights landscape. The first few chapters examined the digital ecosystem, unraveling the intertwined relationship between digital technologies and human rights. This engendered a better understanding of the digital human rights lexicon itself and then a detailed interrogation of the international law framework and its leading role in protecting these rights. The subsequent chapters addressed the nexus of international law and digital human rights with existing legal frameworks and focused on international law's important role in responding to them. A rigorous analysis of global case studies is performed (for example, *Delfi AS v. Ukraine*). This study analyzed the successes and failures in enforcing digital human rights, revealing legal gaps and where work can still be done in *Estonia, Schrems v. working with the Data Protection Commissioner Torsten Igelstrom (of ATAS)* and *Brazil's Marco Civil da internet*. This analysis informed the

policy recommendations presented and foresaw a digital ecosystem that respects and upholds rights. This research provides major insights for policymakers, legal professionals, and academics. It offers a comprehensive analysis of the digital ecosystem followed by a sound evaluation of existing legal architecture to guide policy development rooted in justice, equity and human dignity. This study contributes to our understanding of the complex relationship between digital technologies and human rights and illuminates key aspects of the digital human rights landscape, suggesting a comprehensive approach from within international law to better protect human rights within the digital context. On the basis of the research's meticulous data, policy recommendations are indispensable for policymakers to prescribe how to advance forward-thinking policies rooted in digital reality to create a future in which digital human rights are respected and protected.

Recommendations

On the basis of the analysis presented in this research, the following modifications to existing legal frameworks are recommended to protect digital human rights effectively:

Strengthening Existing International Frameworks: Provisions relevant to digital human rights exist in existing human rights treaties such as the ICCPR and UDHR; however, these need strengthened interpretation and application in a digital context. State rights need to be clarified to protect against violations by nonstate actors (corporations, online platforms) and assist individuals in enjoying digital rights (such as through digital literacy initiatives and affordable access to infrastructure).

Addressing the challenges of AI and algorithmic decision-making: There are many troubling implications for algorithmic systems and AI use related to bias, transparency and accountability. This is why international cooperation is essential for establishing ethical guidelines and regulatory frameworks that govern the development and deployment of AI in such a way that these systems do not, by default, contribute to or worsen existing inequalities and respect fundamental human rights. This included redress mechanisms when algorithmic systems did result in human rights violations.

Improving Data Protection and Privacy: International legal instruments must be strengthened to address the challenges engendered by the vast

collection and use of personal data in the digital age. This encompasses synchronized data protection standards between jurisdictions, encouragement of data minimization principles, and better individual control over personal data. Moreover, although the notion of global data stewardship could be bold, it is worth investigating further as a possible route for better international collaboration to occur in data protection.

Recommendations for Worldwide Synergy and Collective Accountability

Making a human rights-respecting digital ecosystem means close cooperation and shared responsibility globally. The following are recommended:

Enhanced International Collaboration: To effectively develop and implement consistent standards and mechanisms for protecting digital human rights, the present state of play calls for intensified international and domestic cooperation between international organizations, governments and civil society. We also work at fostering dialog around diverging interpretations of international law and encouraging the harmonization of national legislation.

Promoting Digital Literacy and Inclusion: Digital literacy can be valuable only if the digital divide is bridged. Digital literacy should become the focus of international initiatives seeking to promote equitable access to technology and the internet and the development of inclusive digital infrastructure at both the regional and international levels.

Future Research

In a path toward a fast-forwarding digital side, enhancing a research space that vibrates with the maturing digital world has become imperative. Future questions should cross the complex feedback of emerging technologies, such as quantum computing and the Internet of Things (IoT), into digital human rights, explore unseen fiefdoms and anticipate legal remedies. Furthermore, a significant inquiry into the ethical intricacies buried in the development of AI and machine learning technologies and their consequences for social unity and personal freedoms will prompt endless follow-up questions. This requires us to critically analyze the ethical use of these technologies, creating an innovative research environment motivated by the human rights ethos. As such, this manuscript progressively unfolds as a fundamental exploration of how the international law vista facilitates the exercise of digital human rights. It breathes life into the

possibility of a world where digital human rights are legally protected and enshrined globally through the meticulous examination of current law-making and future policy advocacy. In the vanguard of a digital revolution, if such a future waits to be found, it will surely be accessed only through collaborative tenacity and a rejection of tolerance in the face of a betrayal of the sacred rights of members of our community—our fellow human beings—and a fundamental betrayal of our founding principles of justice, equity, and human dignity.

Conflict of Interest

The author of the manuscript has no financial or non-financial conflict of interest in the subject matter or materials discussed in this manuscript.

Data Availability Statement

Data availability is not applicable as no new data was created.

Funding Details

No funding has been received for this research.

References

- Alexeyev, G. V. (2024). 1. Metatheory and classification of digital human rights and freedoms. *Theoretical and Applied Jurisprudence*, 2, 24–36. <https://doi.org/10.22394/2686-7834-2024-2-24-36>
- Alubaidi, A. (2023). Challenges to implementing the international digital law to protect digital rights. *Journal of Law and Sustainable Development*, 11(5), Article e554. <https://doi.org/10.55908/sdgs.v11i5.554>
- Barocas, S., & Selbst, A. D. (2016). Big data's disparate impact. *California Law Review*, 104, 671–732.
- Biswa, A. (2024). International human rights law: Enforcement mechanisms and challenges in a globalized world. In *International Journal for Research Publication and Seminar*, 15(2), 157–163. <https://doi.org/10.36676/jrps.v15.i2.20>
- Castells, M. (2011). *The rise of the network society*. John Wiley & sons.

- Cerf, V. G. (2012, January 4). Internet access is not a human right. *New York Times*. <https://www.nytimes.com/2012/01/05/opinion/internet-access-is-not-a-human-right.html>
- Chadha, K. (2024). 3. Bias and fairness in artificial intelligence: Methods and mitigation strategies. *International Journal for Research Publication and Seminar*, 15(3), 36–49. <https://doi.org/10.36676/jrps.v15.i3.1425>
- Chau, B. K., & Livermore, M. A. (2024). Computational legal studies comes of age. *European Journal of Empirical Legal Studies*, 1(1), 89–104. <https://doi.org/10.62355/ejels.19684>
- Chimni, B. S. (2017). *International law and world order*. Cambridge University Press.
- Clavero, S. B., & Benlloch-Dualde, J. (2019, October, 23–25). *eSGarden: A European initiative to incorporate ICT in schools* [Paper presentation]. In Proceedings 5th CARPE Conference: Horizon Europe and beyond. València, Spain.
- Deibert, R., & Rohozinski, R. (2010). Liberation vs. control: The future of cyberspace. *J. Democracy*, 21(4), 43–57. <https://doi.org/10.1353/jod.2010.0010>
- Delfi As v. Estonia, 2015 ECHR 586 (2015).
- Donoho, D. L. (2001). Autonomy, self-governance, and the margin of appreciation: Developing a jurisprudence of diversity within universal human rights. *Emory International Law Review*, 15, 391–466.
- Erol, M. U. (2023). An international human rights law perspective on the impact of digitalization on the Alevi community. *Journal of Alevism-Bektashism Studies*, 28, 147–171. <https://doi.org/10.24082/2023.abked.424>
- Florek, I., & Eroglu, S. E. (2019). The need for protection of human rights in cyberspace. *Journal of Modern Science*, 42(3), 27–36.
- Gasser, U., Budish, R., & West, S. (2015). *Multistakeholder as governance groups: Observations from case studies*. Harvard Library. <http://nrs.harvard.edu/urn-3:HUL.InstRepos:dash.current.terms-of-use#OAP>

- Joseph, S., & Castan, M. (2022). *International covenant on civil and political rights (ICCPR)*. Oxford University Press
- Lee, L. (2024). *Enhancing financial inclusion and regulatory challenges: A critical analysis of digital banks and alternative lenders through digital platforms, machine learning, and large language models integration*. ArXiv Preprint <https://doi.org/10.48550/arXiv.2404.11898>
- Lee, M., & Levins, M. (2023). The history of the global evolution of digitally connected families 1990-2022. *Studies in Technology Enhanced Learning*, 3(3), 1–23. <https://doi.org/10.21428/8c225f6e.f14d2707>
- Lekić, S. (2024). The impact of digital technologies on the cultural rights of deaf and hard-of-hearing people. *Eudaimonia-Journal for Legal, Political and Social Theory and Philosophy*, 8(1), 55–83. https://doi.org/10.51204/ivrs_24103a
- Lytvynenko, E. V., & Skoblyk, M. A. T. (2024). Peculiarities of ensuring human rights in the conditions of digital transformation. *Analytical and Comparative Jurisprudence*, 3, 369–373. <https://doi.org/10.24144/2788-6018.2024.03.63>
- Mariniello, M. (2022). Digital inequality. In M. Mariniello (Ed.), *Digital economic policy: The economics of digital markets from a European Union perspective* (pp. 309–328). Oxford Academic Press.
- Merino, M. J. M., Plúa, J. N. C., Anchundia, J. C. H., & Gutiérrez, J. A. V. (2023). Information security in the world of digital business. *Journal TechInnovation*, 2(1), 85–91. <https://doi.org/10.47230/journal.techinnovation.v2.n1.2023.85-91>
- Moncau, L. F. M., & Arguelhes, D. W. (2020). The marco civil da internet and digital constitutionalism. In G. Frosio (Ed.), *Oxford handbook of online intermediary liability* (pp. 190–213). Oxford Academic Press.
- Natamiharja, R., & Setiawan, I. (2024). Guarding privacy in the digital age: A comparative analysis of data protection strategies in Indonesia and France. *Jambe Law Journal*, 7(1), 233–251. <https://doi.org/10.22437/home.v7i1.349>

- Oh, S. J. (2024). A study on the main issues of privacy rights in the digital age. *Myongii Law*, 22(2), 45–76. <https://doi.org/10.53066/mlr.2024.22.2.45>
- Ortynskiy, V. (2024). Regarding compliance with national standards for ensuring individual rights to protection in accordance with international standards. *Law*, 11(41), 1–7. <https://doi.org/10.23939/law2024.41.001>
- Papadopoulos, I. (2023). *Children's rights and methodologies*. In I. Papadopoulos (Ed.), *The criminalisation of unaccompanied migrant minors voices from the detention processes in Greece* (pp. 13–28). Bristol University Press.
- Reis, O., Eneh, N. E., Ehimuan, B., Anyanwu, A., Olorunsogo, T., & Abrahams, T. O. (2024). Privacy law challenges in the digital age: A global review of legislation and enforcement. *International Journal of Applied Research in Social Sciences*, 6(1), 73–88. <https://doi.org/10.51594/ijarss.v6i1.733>
- Scheinin, M. (2004). The human rights committee and freedom of religion or belief. In T. Lindholm, W. C. Durham, & B. Tahzib-Lie (Eds.), *Facilitating freedom of religion or belief: A deskbook* (pp. 189–202). Brill.
- Schrems v. Data Prot. Comm’r, 2015 ECR 650 (2015).
- Shaw, M. (2008). *International law*. Cambridge University Press.
- Shelton, D. (2015). *Remedies in international human rights law*. Oxford University Press.
- Simmons, B. A. (2009). *Mobilizing for human rights: International law in domestic politics*. Cambridge University Press.
- Singer, P. (2011). *The expanding circle: Ethics, evolution, and moral progress*. Princeton University Press.
- Singh, B. (2024). Cherish data privacy and human rights in the digital age: Harmonizing innovation and individual autonomy. In M. Pucelj & R. Bohinc (Eds.), *Balancing human rights, social responsibility, and digital ethics* (pp. 199–226). IGI Global.

- Smethurst, R. (2023, June 11–16). *Digital identity wallets and their semantic contradictions* [Paper presentation]. Thirty-first European Conference on Information Systems. Kristiansand, Norway.
- Solove, D. J. (2008). *Understanding privacy*. Harvard University Press.
- Sunstein, C. R. (2001). *Republic.com: Cass Sustein*. Princeton University Press.
- Susskind, R. E., & Susskind, D. (2015). *The future of the professions: How technology will transform the work of human experts*. Oxford University Press.
- Trigo, A., Stein, N., & Belfo, F. P. (2024). Strategies to improve fairness in artificial intelligence: A systematic literature review. *Education for Information*, 40(3), 323–346. <https://doi.org/10.3233/EFI-240045>
- Tufekci, Z. (2017). *Twitter and tear gas: The power and fragility of networked protest*. Yale University Press.
- UNICEF. (n.d.). *Convention on the rights of the child*. Retrieved July 22, 2024, from <https://www.unicef.org/child-rights-convention>
- Wagner, B., Sanchez, A., Sekwenz, M. T., Dideriksen, S. A. T., & Murray-Rust, D. S. (2023). *The politics of digital (human) rights*. Oxford Research Encyclopedia of International Studies. <https://doi.org/10.1093/acrefore/9780190846626.013.694>
- Weber, R. H., & Gunnarson, R. S. (2013). A constitutional solution for internet governance. *Science and Technology Law Review*, 14(1), 1–71.
- West, D. M. (2018). *The future of work: Robots, AI, and automation*. Brookings Institution Press.