OPEN ACCESS Freely available online

IJSSAI International Journal of Social Sciences and Artistic Innovations

Issue 4
Volume 5
ISSN 2737-5293
International Journal of Social Sciences and Artistic Innovations

Review

Digital Rights and Ethical Dilemmas in Adopting Emerging Technologies: Implications for International Relations and Global Norms

Minji Park

Teda International School, Tianjin 300457, China; 2009parkminji@naver.com

Received: Sep 06, 2025; **Revised:** Sep 21, 2025; **Accepted:** Oct 25, 2025; **Published:** Nov 03. 2025

Abstract: The global proliferation of digital technologies has enabled unprecedented connectivity and innovation, yet it has also introduced challenges to human rights and ethical dilemmas, affecting international relations and global norms. Therefore, the manner in which digital technologies are used for surveillance, censorship, and repression by state and non-state actors is examined, and the implications for fundamental human rights are investigated in this review article. Digital rights violations and ethical dilemmas influence the execution of international relations and diplomacy. The digital tools are weaponized for power projection and control, increasing geopolitical tensions, eroding trust between nations, and fragmenting global governance. The struggle over digital norms, data sovereignty, and technological standards has been observed in contemporary diplomacy, necessitating a re-evaluation of international legal frameworks and the establishment of robust global ethical guidelines to safeguard human rights in employing emerging technologies.

Keywords: Digital rights, Ethical dilemmas, Emerging technologies, Surveillance, Censorship, Repression, Human rights, International relations, Diplomacy, Global norms, Cyber warfare, Data governance

1. Introduction

The digital revolution is characterized by the ubiquity of emerging technologies, including the Internet, artificial intelligence (AI), and large-scale data analytics, which considerably enhance surveillance capabilities and fundamentally reshape the global society. While offering immense opportunities for economic growth, social interaction, and access to information, technological advancements have concurrently presented ethical dilemmas and challenges to human rights. Such a dual nature of emerging technologies enhances the progress and efficiency in the social and global system, but at the same time, is repurposed for control, oppression, and coercion (Feldstein, 2019). This issue necessitates an in-depth review of how digital technologies exploit surveillance, censorship, and repression, and detailing how these practices affect human rights globally, international relations, and the development of global norms.

The weaponization of digital technologies and their antithetical use to human rights has become a source of tension and a determining feature of contemporary international relations. Nations and, increasingly, non-state actors, such as multinational corporations, non-governmental organizations (NGOs), terrorist groups, religious organizations, and transnational advocacy networks, are employing diverse digital tools to monitor citizens, suppress dissent, control information flows, and even influence political processes beyond borders. This can be a growing schism between nations that prioritize digital freedom and human rights, and state control and digital sovereignty. The resulting contestation over digital norms and governance frameworks affects diplomatic interactions, shapes alliances, and raises fundamental questions about the future of a free and open use of technologies.

The influences of digital rights abuses are not confined to domestic boundaries but affect global society from multiple perspectives:

- Erosion of trust and increased geopolitical tensions: Nations engaging in digital repression face international condemnation, leading to diplomatic friction and a decline in trust. This exacerbates geopolitical tensions and hinders cooperation on other global issues.
- Transnational repression and extraterritorial reach: Digital technologies extend a state's repressive tactics beyond their physical borders, targeting dissidents, activists, and journalists in other countries, challenging diplomatic relations and national sovereignty.

- Fragmentation of global norms and governance: The lack of agreed-upon global norms for digital behavior and human rights in cyberspace fragments global society, where different nations adhere to conflicting principles. This makes it difficult to forge a global consensus on data governance and cyber warfare.
- Impact on multilateral diplomacy: State and non-state actors increasingly grapple with digital rights issues, but struggle to reach consensus due to their interests and interpretations of human rights and ethical problems. This undermines the effectiveness of multilateral diplomacy.

This article delineates the framework of digital rights and the ethical dilemmas presented by emerging technologies. Then, the mechanisms through which surveillance, censorship, and repression are executed using digital tools are analyzed. Based on the previous research results, the direct and indirect influences of the practices on international relations and diplomacy are discussed, based on empirical evidence and recent developments. Then, the efforts and challenges in establishing global norms and governance frameworks are discussed, and related recommendations are proposed for safeguarding digital rights and fostering a stable and rights-respecting international digital environment.

2. Digital Rights and Emerging Ethical Dilemmas

Digital rights refer to the human rights in the digital environment, particularly concerning online activities, data collection, and access to digital information. These rights are generally understood as extensions of existing human rights frameworks, as those enshrined in the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR) (United Nations, 1948). Digital rights include the following components:

- Freedom of expression online: The right to seek, receive, and impart information and ideas through any media, regardless of frontiers, including the Internet.
- Right to privacy: The right to be free from arbitrary interference with one's privacy, family, home, or correspondence, extending to online data and communications.
- Freedom of assembly and association online: The ability to organize and participate in peaceful online gatherings and to form associations.
- Right to access information: The ability to access the Internet and information online without undue restrictions.
- Right to due process and non-discrimination: Ensuring that digital tools and their applications do not lead to arbitrary or discriminatory outcomes.

The ethical dilemmas are posed by emerging technologies as they arise from their potential to infringe upon digital rights. AI, big data analytics, and advanced networking capabilities (e.g., 5G) present complex opportunities and risks. For instance, while AI enhances public services, surveillance using AI leads to mass monitoring without consent. Big data is useful for targeted advertising, but can be weaponized for profiling and discrimination (Mendoza, 2022). As a result, ethical considerations must be taken about its design, deployment, and governance (Floridi, 2021). The dual nature of the emerging technologies indicates that a tool developed for benign purposes is easily repurposed for surveillance or repression, posing challenges for policymakers and human rights advocates.

3. Surveillance, Censorship, and Repression Using Digital Technologies

3.1. Surveillance

Emerging technologies might be used by state and non-state actors to monitor, control, and suppress populations. For example, digital surveillance excels traditional monitoring methods but enables pervasive, often imperceptible, and deeply intrusive oversight. Emerging technologies also enable mass data collection and analytics. Governments can collect vast amounts of data from a plethora of sources, including internet service providers, telecommunication companies, social media platforms, public closed-circuit television (CCTV) cameras integrated with facial recognition capability, smart sensors, and personal devices such as smartphones and wearable devices. AI and big data analytics can be utilized to process this data, identify patterns, track movements, analyze communications, and predict behaviors (Padden, 2023). The sheer volume of massive data makes surveillance feasible on a national scale.

When facial recognition technology is integrated into networks, individuals are recognized and tracked in real-time identification in public places. This technology can be used to identify protestors, monitor public gatherings, and enforce social control. Its widespread deployment raises serious concerns about privacy and freedom of assembly (Human Rights Watch, 2019). In addition, mobile phones and internet-connected devices constantly transmit location data, which enables tracking the movements of individuals, identifying their associates, and monitoring their activities, often without consent or judicial oversight. Leveraging

recent technologies, sophisticated malware and hacking tools (e.g., Pegasus spyware) are used to infiltrate personal devices to extract data, monitor communications, and even remotely control devices. These tools are supplied by private companies to governments, creating a lucrative market for surveillance technology (Tumber and Waisbord, 2017). In authoritarian regimes, digital data can be integrated into social credit systems to evaluate citizens' behavior based on a range of criteria. This leads to the construction of pervasive digital control, restricting access to services, travel, and employment (World Economic Forum, 2025).

3.2. Censorship

Digital technologies are also used as a censorship tool on an unprecedented and sophisticated scale. National firewalls and sophisticated filtering technologies can be used to block access to websites, social media platforms, and online content that are undesirable or considered threatening to state control. These systems are dynamic, adapting to new circumvention methods (Roberts *et al.*, 2018). Governments can compel social media companies and internet service providers to remove specific content, accounts, or applications through legal frameworks and informal pressure, or direct coercion. Such platform governance forces private companies to be arbiters of online speech, often under state pressure (Volokh, 2025). AI-powered algorithms are widely used to automatically detect and remove content. However, human oversight occurs in using such algorithms, leading to legitimate removal of harmful content and arbitrary suppression of dissenting voices. Search algorithms can also be manipulated to deprioritize or hide certain information. Disinformation and propaganda are also serious problems beyond blocking information. Nations can actively use digital platforms to spread propaganda, create false narratives, and sow disinformation to manipulate public opinion and discredit critics (Radsch, 2022). This blurs the lines between legitimate information and state-sponsored falsehoods.

3.3. Repression

Digital technologies are also used to facilitate various forms of repression, often amplifying their effect and reach. State-sponsored actors or proxies might conduct online harassment campaigns, publishing private information and intimidation tactics against activists, journalists, and dissidents, aiming to silence them or drive them offline (Zhuravskaya *et al.*, 2020). Cyberattacks can be executed to disrupt critical services, target opposition websites, or temporarily shut down internet access, using internet kill switches, to prevent organizations from communicating with each other (Lubis et al., 2025). The integration of surveillance data with legal or administrative systems enables the automation of the identification and punishment of individuals based on their digital footprint, potentially without adequate due process. Several nations are actively exporting their surveillance and censorship technologies and models of digital governance to other nations, particularly developing nations, often as part of broader aid or infrastructure projects. This raises concerns about the global proliferation of digital repression (Freedom House, 2023).

4. Influences on International Relations and Diplomacy

4.1. Erosion of Trust and Increased Geopolitical Tensions

Widespread digital rights abuses undermine trust in bilateral and multilateral relations between nations. When one nation engages in mass surveillance of its citizens or extends surveillance capabilities beyond its borders, it generates suspicion and resentment from other nations (Domazet and Dinić, 2022). The ongoing geopolitical competition between the United States of America and China presents an example of disputes over digital security and human rights. The US has openly condemned China's use of surveillance technologies (e.g., in Xinjiang) and its broader censorship apparatus, leading to sanctions on Chinese tech companies (e.g., Huawei, Hikvision) and export controls on advanced semiconductors (Eichensehr, 2022). This has heightened trade tensions, technological decoupling efforts, and a broader breakdown of trust in diplomatic engagements where technology is an important agenda item. Concerns over data security and potential nation backdoors in 5G networks, for example, have led to diplomatic pressure on allies to avoid Chinese vendors, shaping international technology alliances.

The revelations surrounding the use of Pegasus spyware by various governments against journalists, human rights defenders, and even heads of state have caused significant diplomatic crises. Countries whose officials or citizens are targeted have lodged formal protests, recalled ambassadors, and initiated investigations, directly straining bilateral relations and exposing the vulnerabilities of digital diplomacy (The Guardian, 2021). These incidents reveal a lack of adherence to established norms of non-interference and national sovereignty in the digital domain.

4.2. Transnational Repression and Extraterritorial Reach

Digital technologies enable nations to overcome geographical limitations, extending their repressive reach to target individuals abroad. This creates a new dimension of international relations, where a nation's domestic policies on digital control can directly

impact the sovereignty of other nations. Authoritarian regimes increasingly use digital means to harass, intimidate, and even abduct dissidents and activists living in other countries through cyberstalking, phishing attacks, and weaponizing social media to spread disinformation about exiles (Maizland, 2022). These actions undermine the sovereignty of host nations and strain diplomatic relations, forcing host governments to respond and protect their citizens and residents. Diplomatic protests and the expulsion of foreign agents can ensue and escalate tensions. The flow of data on a global scale, combined with national demands for access to servers located in other nations, creates complex legal and diplomatic challenges. Nations often assert "data sovereignty," demanding that data of their citizens be stored in their territories and subject to their laws. This might conflict with the surveillance laws of different nations and complicate global legal cooperation, leading to diplomatic stalemates over data access requests (Electronic Privacy Information Center, 2025).

4.3. Fragmentation of Global Norms and Governance

The rapid technological advancement requires the development of global norms and legal frameworks for governing cyberspace. A lack of global norms and legal frameworks requires different nations to develop diverse approaches to digital rights to avoid the fragmentation of global governance. The debate over digital rights reflects an ideological divide in international relations. While several nations advocate for a splinternet model, where national sovereignty extends fully to the digital realm, allowing for extensive censorship and surveillance, others pursue an "open, free, and secure internet," emphasizing human rights and multi-stakeholder governance (Seo and Thorson, 2017). This difference hinders the establishment of global standards for digital behavior, cybersecurity, and data protection.

Discussions on digital human rights have been conducted in the UN General Assembly, Human Rights Council, and other multilateral bodies, without elusive consensus. Western countries adopt robust protections for the freedom of expression and privacy, while authoritarian countries emphasize control and stability. Such differences in norms delay or derail global agreements on issues ranging from cybercrime to the responsible use of AI in warfare. The differences or competition over digital norms are not purely ideological but economic and strategic. Nations are competing to set global technical standards (e.g., for 5G, AI ethics), which enables privilege for companies and embeds in governance models. This leads to the formation of "technological alliances" and "standardization blocs," which fragment the global system along digital lines.

4.4. Impact on Multilateral Diplomacy

Digital rights abuses directly affect the efficacy and nature of multilateral diplomacy. Digital espionage and surveillance undermine trust in multilateral cooperation. Delegations may be wary of discussing sensitive information if they fear their communications are compromised, hindering open dialogue and effective problem-solving (Tumber and Waisbord, 2017). Digital rights, cybersecurity, and internet governance have been referred to in the multilateral agenda. This has led to the creation of various diplomatic forums and expert groups (e.g., UN Group of Governmental Experts on cybersecurity) to address complex technical and ethical issues. However, progress has been limited due to the divergent national interests mentioned earlier.

While digital platforms offer new tools for public diplomacy, the spread of disinformation and the ability of nations to manipulate online information complicate diplomatic efforts. Governments must contend with online campaigns, often fueled by foreign actors, which undermine their diplomatic messages and shape public opinion in target countries (Chauhan et al., 2025). The ability to control the narrative online, or counter false narratives, is a critical diplomatic tactic nowadays.

5. Results and Discussion

The pervasive use of digital technologies for surveillance, censorship, and repression has changed the dynamics of international relations and created a complex interplay of power, trust, and normative contestation.

5.1. Shifting Power Dynamics

The ability to control information, monitor populations, and leverage cutting-edge digital tools forms a new power in the global system. Nations with advanced cyber capabilities and pervasive surveillance infrastructures have more influence and control domestically and externally. Digital power has become as critical as traditional military or economic power, enabling coercive diplomacy and shaping geopolitical alignments. For instance, China, which has heavily invested in developing and exporting its digital authoritarian models, is shaping the digital future of developing nations, creating a new sphere of influence (Freedom House, 2023).

5.2. Fragmented and Contested Digital Order

A lack of unified global approaches to digital rights and governance has fragmented the digital order. Tensions have emerged between the protection of human rights and the prioritization of digital sovereignty and national control. Such tensions manifest in various forms. Different nations are enacting different laws on data privacy, content moderation, and cybersecurity, creating legal and operational complexities for international businesses and fostering regulatory arbitrage. Concerns over digital security and human rights have driven efforts towards "decoupling" in the technology sector, particularly between the US and China. This leads to parallel digital ecosystems, potentially hindering global innovation and increasing costs, while reflecting a deeper distrust in international relations. Digital rights and cybersecurity concerns are increasingly influencing alliance structures. Nations that share democratic values and concerns regarding digital authoritarianism are forming coalitions to collectively address these challenges, while authoritarian nations find common ground in promoting digital sovereignty and control.

5.3. Diplomacy for Human Rights and International Law

The digital rights abuses pose questions for global human rights. Existing frameworks are adaptable, but their application to the digital sphere is challenging, regarding extraterritorial violations and the role of private tech companies. The debate over the creation of new international digital rights or the extension of existing ones (United Nations General Assembly, 2020) highlights the need for stricter regulations and closer cooperation. These needs also affect diplomacy, which presents the challenge of digital rights violations. The positive potential of digital technologies to foster global cooperation must be harnessed in tandem with efforts to mitigate their risks.

Digital technologies escalate diplomatic crises, as seen in the immediate global reactions to cyberattacks or large-scale internet shutdowns, so diplomats must engage in "cyber diplomacy" to de-escalate tensions and negotiate norms of behavior in cyberspace. To address diplomatic challenges in the digital space, governments need to promote their values and counter foreign disinformation campaigns, employing digital tools in public diplomacy (Servaes, 2012). Despite such challenges, global problems, including digital rights abuses, can be addressed through solutions such as multilateral forums and discussions on norms, capacity building, and technical cooperation. In such activities, tech companies, civil society organizations, and academic experts must participate and play influential roles, engaging governments and international organizations in digital diplomacy.

6. Conclusion

The ethical dilemmas stemming from emerging digital technologies are observed in digital surveillance, censorship, and repression of human rights. These practices present profound and intricate influences on the global political landscape and shape international relations and the development (or fragmentation) of global norms. The weaponization of digital tools erodes trust between nations, worsens geopolitical rivalries, and leads to transnational repression, which directly challenges national sovereignty. The ideological conflicts over digital rights between advocates of an open internet and proponents of state-controlled digital spaces demand coordinated global governance, as it fuels the emergence of a 'splinternet' marked by divergent technological and normative standards. The solutions affect how nations interact, cooperate, and even perceive each other in the digital realm.

These challenges necessitate a re-evaluation of traditional nationcraft. Diplomats must become adept at addressing complex technical issues, countering disinformation campaigns, and negotiating norms for cyberspace in an environment characterized by mistrust and divergent interests. The imperative to safeguard human rights in the digital age requires a robust and collective international response. Therefore, it is necessary to develop and enforce globally universally accepted norms for national behavior in cyberspace, particularly regarding surveillance, censorship, and cyberattacks on civilian infrastructure. This requires bridging the ideological divide between "digital sovereignty" and "human rights" -centered nations. Effective mechanisms are necessary to hold nations and private companies accountable for digital rights violations, through international legal frameworks, sanctions, or robust due diligence requirements for tech exports. Investment should be made in global digital literacy programs to empower citizens to assess online information and protect their digital rights. Simultaneously building digital resilience in vulnerable nations is essential to counter foreign interference and safeguard critical infrastructure. To foster genuine multi-stakeholder participation (governments, civil society, academia, and the private sector) in internet governance, diverse perspectives must be considered in shaping the future of the digital world. In addition, open-source technologies must be provided to enhance privacy and security and offer the support and protection of human rights activists, journalists, and activists who can be targets of digital repression.

The rapid adoption of emerging technologies presents a profound challenge, such as digital rights and ethical governance, although it is an accelerator of global progress. Geopolitical competition with technological adoption outpaces the establishment of necessary global norms, leading to significant ethical and security risks, particularly concerning human rights and sovereignty. To ensure democratic values and responsible technological development, the global society needs to cooperate for concrete and

accountable policies. Countries must form a treaty or a memorandum of understanding to enable immediate and reciprocal technical and investigative aid for power grids and health systems. The responsibility for drafting and enforcing such agreements accompanies technical coordination by a UN agency such as the International Telecommunication Union (ITU), and essential support from private companies. Governments must enact legislation and develop measurable indicators for critical infrastructure incidents, which require that all emerging technologies procured, deployed, or exported for public sector use undergo an independent digital rights impact assessment (DRIA) before their deployment. Assessments based on such legislation and indicators must be conducted to define ethical criteria and periodically review technology ethics. Related research on necessary policies must be extensively conducted in the future. By adopting generalized principles and actionable, measurable, and accountable policy proposals, the global society must proactively manage the ethical complexities of emerging technologies, reinforce global norms, and secure digital rights for a stable and fair future.

Funding: This research did not receive external funding.

Data Availability Statement: The data of this study are available from the corresponding author upon reasonable request.

Conflicts of Interest: The author declares no conflict of interest

References

1. Chauhan, S.S., Sahay, N., & Marwah, R. (2025). The Influence of Digital Diplomacy on Traditional Diplomatic Practices: Transforming Roles and Functions through Social Media. *South India Journal of Social Sciences*, *23*, 1–4. https://doi.org/10.62656/SIJSS.v23i4.2024
2. Domazet, S.S., & Dinić, S.S. (2022). International Legal Aspects of Mass Surveillance and Implications on Privacy. *Kultura Polisa*, *19*, 79–9713. https://doi.org/10.51738/Kpolisa2022.19.1r.5dd
3. Eichensehr, L. (2022). United States Pressures China Over Human Rights Abuses. *American Journal of International Law*, 433–438. Available online: https://www.law.virginia.edu/scholarship/publication/kristen-eichensehr/1573406 (accessed on July 29, 2025).
4. Feldstein, S. (2019). Findings and Three Key Insights. In *The Global Expansion of AI Surveillance*; Washington, DC, USA: Carnegie Endowment for International Peace; pp. 7–10.
5. Floridi, L. (2021). Mapping the Ethics of Algorithms. In *The Ethics of AI*; Oxford, UK: Oxford University Press.
6. Freedom House. (2023). Freedom on the Net 2023: The Repressive Power of AI. Freedom House, Washington, DC, USA. Available online: https://freedomhouse.org/sites/default/files/2023-10/Freedom-on-the-net-2023-DigitalBooklet.pdf (accessed on July 29, 2025).
7. Human Rights Watch. (2019). China's Algorithms of Repression: Reverse Engineering a Xinjiang Police Database. Available online: https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass (accessed on July 29, 2025).
8. Lubis, M., Safitra, M.F., Fakhrurroja, H., & Muttaqin, A.N. (2025). Guarding Our Vital Systems: A Metric for Critical Infrastructure Cyber Resilience. *Sensors*, *25*, 4545. https://doi.org/10.3390/s25154545
9. Maizland, L. (2022). China's Repression of Uyghurs in Xinjiang. Available online: https://www.cfr.org/backgrounder/china-xinjiang-uyghurs-muslims-repression-genocide-human-rights (accessed on July 29, 2025).
10. Mendoza, C. (2022). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. *Church, Communication and Culture*, *7*, 452–455. https://doi.org/10.1080/23753234.2022.2086891
11. Padden, M. (2023). The transformation of surveillance in the digitalisation discourse of the OECD: A brief genealogy. *Internet Policy Review, 12*(3), 1720. https://doi.org/10.14763/2023.3.1720
12. Radsch, C. (2022). AI and Disinformation: State-Aligned Information Operations and the Distortion of the Public Sphere. OSCE, Vienna, Austria. Available online: https://dx.doi.org/10.2139/ssrn.4192038 (accessed on September 29, 2025).
13. Seo, H., & Thorson, S. (2017). Network Approach to Regime Type and Global Internet Connectedness. *Journal of Global Information Technology Management, 20*, 141–155. https://doi.org/10.1080/1097198X.2017.1354597
14. Servaes, J. (2012). Public Diplomacy: Soft power and public diplomacy: The new frontier for public relations and international communication between the US and China. *Public Relations Review, 38*, 643–651. https://doi.org/10.1016/j.pubrev.2012.07.002
15. The Guardian. (2021). The Pegasus Project: Surveillance. Available online: https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus (accessed on July 29, 2025).
16. Tumber, H., & Waisbord, S. (2017). The Media and Human Rights: Mapping the Field. In *The Routledge Companion to Media and Human Rights*; Tumber, H., & Waisbord, S., Eds.; London, UK: Routledge, pp.1–14.
17. United Nations General Assembly. (2020). The right to privacy in the digital age: resolution / adopted by the General Assembly. Available online: https://digitallibrary.un.org/record/3896430?v=pdf (accessed on July 29, 2025).

18. United Nations. (1948). Universal Declaration of Human Rights. Available online: https://www.un.org/en/development/desa/population/migration/generalassembly/docs/globalcompact/A_RES_217(III).pdf (accessed on July 29, 2025).
19. Volokh, E. (2025). The Future of Government Pressure on Social Media Platforms. *Journal of Free Speech Law*, *6*, 403–422. Available online: https://www.journaloffreespeechlaw.org/volokh6.pdf (accessed on July 29, 2025).
20. World Economic Forum. (2025). Global Cybersecurity Outlook 2025. Available online: https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf (accessed on July 29, 2025).
21. Zhuravskaya, E., Petrova, M., & Enikolopov, R. (2020). Political Effects of the Internet and Social Media. *Annual Review of Economics*, *12*, 415–438. https://doi.org/10.1146/annurev-economics-081919-050239