MRS Journal of Multidisciplinary Research and Studies
ISSN *(Online) 3049-1398*
Vol-3, Iss-1 (January-2026)
Journal homepage: https://mrspublisher.com/journals

Digital Age Human Rights: Privacy, Surveillance, and Global Governance

Dr. Rachana Kumari[*]

Ph.D. (Amity Institute of Defence and Strategic Studies)

Corresponding Author: **Dr. Rachana Kumari** (Ph.D. (Amity Institute of Defence and Strategic Studies))

Received: 10 / 12 / 2025 | Accepted: 07 / 01 / 2026 | Published: 18 / 01 / 2026

Abstract: The digital age has redefined the meaning, scope, and protection of human rights. With unprecedented technological advancements, digital infrastructures now shape social interactions, economic systems, political governance, and personal autonomy. While such developments have empowered individuals and enhanced global connectivity, they have also generated new vulnerabilities, particularly concerning privacy, surveillance, data security, and algorithmic biases. This research paper examines the evolving human rights landscape in the digital era, focusing on the central issues of privacy violations, mass surveillance, digital authoritarianism, and the challenges of global governance. It draws upon international human rights frameworks, privacy theories, and global regulatory debates to explore how states, corporations, and transnational institutions negotiate power in digital spaces. The paper analyzes the tensions between national security and civil liberties, public welfare and personal autonomy, technological innovation and ethical constraints. It also investigates emerging global governance mechanisms, including GDPR, UN resolutions, AI ethics guidelines, and multilateral cyber norms. The study concludes by arguing that safeguarding human rights in the digital age requires stronger global cooperation, transparent governance models, human-centric technological design, and legally binding international standards that balance innovation with fundamental freedoms.

Keywords: *Digital human rights, privacy, surveillance, global governance, data protection, artificial intelligence, cyber law, digital authoritarianism, human rights law.*

Cite this article: Kumari, R. (2026). Digital Age Human Rights: Privacy, Surveillance, and Global Governance. *MRS Journal of Multidisciplinary Research and Studies, 3(1),34-37.*

Introduction

The twenty-first century is characterized by the unprecedented rise of digital technologies that permeate every dimension of human life. From communication and education to healthcare and governance, digital infrastructures have become inseparable from the basic functioning of global society. This digital transformation has facilitated empowerment, democratized information, and expanded opportunities for social inclusion. At the same time, however, it has also generated significant challenges concerning the protection of human rights, particularly the right to privacy, freedom of expression, data autonomy, and protection against arbitrary surveillance.

Human rights, traditionally understood within the framework of physical space and state-citizen relationships, now face complex reinterpretations in cyberspace. The rise of big data, artificial intelligence, biometric systems, and algorithmic governance has restructured the dynamics of power between individuals, corporations, and states. Questions emerge around who controls personal data, how it is processed, and to what extent surveillance—both overt and covert—is compatible with democratic values. These concerns are not limited to authoritarian regimes; they also manifest in liberal democracies where national security, counterterrorism, and technological competition often overshadow human rights considerations.

This research paper investigates the transformation of human rights in the digital age, with a particular focus on privacy, surveillance, and global governance structures. It explores the philosophical underpinnings of digital rights, the legal and regulatory gaps in existing systems, and the global struggle to develop coherent and enforceable governance mechanisms. Through an interdisciplinary lens, the paper aims to contribute to the ongoing discourse on how to protect human dignity and autonomy in an era dominated by datafication and pervasive technological control.

Privacy in the Digital Age: Concepts, Challenges, and Ethical Debates

Privacy, once understood as a physical boundary or the right to be left alone, has evolved into a multifaceted concept involving data ownership, informational self-determination, and digital autonomy. In the digital age, personal data has become a valuable commodity, often described as the “new oil” of the global economy. Every online activity—communication, financial transactions, social media engagement, movement tracking, or biometric authentication—generates data trails that can be collected, stored, analyzed, and monetized by corporations and governments.

A major challenge is the asymmetry of knowledge and power between individuals and digital corporations. Users rarely understand the extent of data collected or the implications of consenting to terms and conditions embedded in lengthy legal agreements. Surveillance capitalism, a term coined by Shoshana

Zuboff, describes this system in which corporations commodify personal data to predict and influence human behavior. Such practices raise ethical concerns regarding autonomy, manipulation, and the erosion of individual agency.

Another central issue is the blurring of boundaries between personal and public spheres. Smartphones, smart homes, wearable devices, and social networks create an ecosystem where individuals constantly disclose personal information, consciously or unconsciously. This increases vulnerability to data breaches, identity theft, profiling, and algorithmic discrimination. Moreover, digital privacy intersects with socio-economic inequalities. Marginalized populations often have less control over their data and face greater risks of surveillance and exploitation.

Legal frameworks such as the European Union’s General Data Protection Regulation (GDPR) represent attempts to restore control to individuals through rights like data portability, consent, and the “right to be forgotten.” However, such regulations remain regionally limited and insufficient to address global data flows. The fragmented nature of global digital governance means that privacy protections vary widely across countries, exposing individuals to inconsistent and sometimes exploitative practices. Overall, privacy in the digital age requires new philosophical and legal frameworks that recognize the centrality of data to human dignity and social participation.

Surveillance in the Digital Era: State Power, Corporate Monitoring, and Digital Authoritarianism

Surveillance is not a new phenomenon, but digital technologies have dramatically expanded its scale, sophistication, and invisibility. Government surveillance, initially justified for national security and crime prevention, now operates through advanced tools such as facial recognition, biometric databases, artificial intelligence analytics, and mass metadata collection. Revelations by whistle-blowers, including Edward Snowden, exposed the extent to which intelligence agencies conduct mass surveillance not only on suspected criminals but on ordinary citizens worldwide.

The digital infrastructure allows states to monitor communication patterns, track movement, and profile individuals in ways that were previously unimaginable. This raises crucial questions about the balance between national security and civil liberties. While governments argue that surveillance is necessary to combat terrorism, cybercrime, and political extremism, critics highlight the erosion of personal freedom, the threat of self-censorship, and the chilling effect on democratic participation.

Surveillance is not limited to state actors; private corporations also engage in extensive data monitoring. Technology companies track user behavior to personalize advertisements, curate content, and optimize user engagement. Although such surveillance is often presented as benign or beneficial, it contributes to behavioral manipulation, targeted political campaigns, and the creation of echo chambers that polarize public discourse.

In authoritarian regimes, surveillance technologies are deployed to suppress dissent, control political opposition, and monitor ethnic or religious minorities. China’s “social credit system” and extensive use of facial recognition in Xinjiang are among the most cited examples of digital authoritarianism. Such models are increasingly exported to other countries, perpetuating a global trend of technologically enabled authoritarian control. This raises concerns about a future where surveillance becomes normalized and human rights protections are weakened in favor of state power and corporate interests.

Artificial Intelligence, Algorithms, and Human Rights

Artificial intelligence (AI) and machine learning algorithms have introduced a new dimension to human rights debates. While AI can enhance efficiency, improve governance, and support decision-making, it can also reinforce biases, undermine fairness, and violate human dignity. Algorithms trained on biased datasets may discriminate in areas such as employment, credit scoring, policing, healthcare, and judicial decisions. Such biases often disproportionately affect marginalized communities, exacerbating social inequalities.

Predictive policing tools, for instance, use data-driven models to identify areas or individuals likely to commit crimes. Critics argue that such technologies perpetuate racial profiling and criminalize poverty. Similarly, algorithmic decision-making in welfare systems may unfairly deny benefits to vulnerable populations based on opaque data analytics.

AI also raises concerns about transparency and accountability. Automated systems often operate as “black boxes,” making it difficult for individuals to challenge decisions or understand how data is being used. This undermines the right to due process and the principle of equality before the law.

International organizations, including the United Nations, UNESCO, and the OECD, have begun developing ethical guidelines for AI governance. These frameworks emphasize principles such as fairness, transparency, accountability, and human oversight. However, ethical guidelines alone are insufficient; legally binding regulations are needed to ensure that AI systems respect human rights. The challenge lies in regulating rapidly evolving technologies while encouraging innovation and economic development.

Cybersecurity, Data Protection, and Human Rights

Cybersecurity has emerged as a critical concern in the digital age. Cyberattacks, hacking, ransomware, and data breaches threaten not only economic stability and national security but also individual rights. When personal data is compromised, individuals lose control over sensitive information related to their identity, financial status, health, or personal behavior.

Data breaches at major corporations, government agencies, and financial institutions highlight the vulnerability of digital infrastructures. Inadequate cybersecurity measures can lead to mass violations of privacy, identity theft, and long-term psychological and financial harm. Vulnerabilities in digital systems disproportionately affect individuals who rely on online platforms for social services, banking, and communication.

At the same time, cybersecurity policies must be balanced with human rights considerations. Overly restrictive laws may limit freedom of expression, enable censorship, or justify intrusive surveillance. The challenge is to develop cybersecurity frameworks that protect both national interests and human dignity.

Global Governance and International Human Rights Frameworks

Global governance in the digital age remains fragmented, inconsistent, and often reactive rather than proactive. The rapid pace of technological innovation has outstripped the ability of international law to regulate digital space effectively. Existing human rights frameworks, such as the Universal Declaration of Human Rights (UDHR), International Covenant on Civil and Political Rights (ICCPR), and regional human rights conventions, provide general protections that can be extended to digital rights. However, they lack explicit provisions for emerging digital challenges.

The European Union's GDPR is currently the most comprehensive data protection law globally, setting high standards for privacy, consent, and data security. Its extraterritorial applicability influences global data practices, encouraging other regions to adopt similar frameworks. However, many countries lack robust data protection laws, and international corporations exploit jurisdictional gaps to weaken compliance.

The United Nations has initiated efforts to develop global norms for cyberspace, including resolutions on digital privacy, internet governance forums, and discussions on cybercrime treaties. However, consensus remains difficult due to geopolitical tensions, differing national interests, and competing visions of digital governance. Democracies generally support a free and open internet, while authoritarian states advocate for "cyber sovereignty," emphasizing state control over digital infrastructure.

Multi-stakeholder governance models that involve states, private corporations, civil society organizations, and international institutions represent a promising approach. Such models promote collaboration, transparency, and shared responsibility. Yet, their effectiveness depends on political will, resource allocation, and inclusive participation.

Digital Rights as Human Rights: Conceptual and Legal Evolution

The recognition of digital rights as an extension of human rights reflects a broader understanding of human dignity in a connected world. Digital rights include the right to privacy, access to information, freedom of expression online, data autonomy, protection from algorithmic discrimination, and the right to a secure digital environment. These rights are essential for participation in modern society, economic empowerment, and democratic engagement.

Courts in various jurisdictions have begun interpreting existing rights to include digital dimensions. For instance, the "right to be forgotten" allows individuals to request the removal of outdated or inaccurate personal information from the internet. The recognition of internet access as a fundamental right in some countries highlights its importance for social inclusion and economic opportunity.

However, challenges remain in translating digital rights into enforceable legal norms. Conflicts between national laws, cross-border data flows, and corporate policies create legal uncertainty. Many digital platforms operate beyond the jurisdiction of national legal systems, complicating accountability mechanisms. Strengthening digital rights therefore requires both national reforms and international cooperation.

The Future of Human Rights in an Increasingly Digitalized World

The future of human rights in the digital age depends on how societies balance innovation with ethical considerations and regulatory safeguards. Rapid advancements in AI, quantum computing, biotechnology, and virtual reality will introduce new complexities. For instance, brain-computer interfaces challenge traditional notions of mental privacy, while biometric surveillance blurs the boundary between physical and digital identities.

To protect human rights in this evolving environment, several principles must guide future governance. First, human-centric technological design must prioritize dignity, fairness, and autonomy. Second, transparency and accountability must be embedded in digital systems, ensuring individuals can understand and challenge algorithmic decisions. Third, global cooperation is essential, as digital technologies transcend national borders and require harmonized standards.

Educational initiatives and digital literacy programs can empower individuals to navigate the digital world responsibly. At the institutional level, independent oversight bodies can monitor compliance, investigate abuses, and enforce regulations. Ultimately, the digital age presents both opportunities and risks. With thoughtful governance, ethical innovation, and strong legal protections, human rights can be preserved and enhanced in the twenty-first century.

Conclusion

The digital age has profoundly reshaped the meaning and practice of human rights. While technological innovations have transformed society in positive ways, they have also created new vulnerabilities related to privacy, surveillance, data autonomy, and digital participation. This research paper has explored these challenges and examined the evolving global governance mechanisms designed to address them.

The central argument is that human rights protection in the digital age requires a holistic approach that integrates legal, ethical, technological, and political perspectives. Privacy must be recognized as an essential component of human dignity, and surveillance practices—whether by states or corporations—must be bounded by transparency, accountability, and democratic oversight. Global governance structures must evolve to address cross-border data flows, regulate AI, and ensure consistent standards for digital rights.

As technology continues to advance, the need for robust international cooperation becomes even more critical. The future of human rights will depend on our collective ability to harness the benefits of the digital age while safeguarding fundamental freedoms. Ensuring that digital technologies empower rather than exploit individuals is essential for building an inclusive, just, and human-centered global society.

References:

1. Andrejevic, M. (2014). *Surveillance and alienation in the online economy*. Surveillance & Society, 12(3), 381–397.
2. Article 19. (2018). *Privacy and freedom of expression in the digital age*. Article 19 Policy Brief.
3. Bradshaw, S., & DeNardis, L. (2019). *The governance of cybersecurity*. Journal of Cyber Policy, 4(1), 1–15.

4. Cohen, J. E. (2019). *Between truth and power: The legal constructions of informational capitalism*. Oxford University Press.
5. Creemers, R. (2018). *China's social credit system: An evolving practice of control*. SSRN Electronic Journal.
6. DeNardis, L. (2020). *The Internet in everything: Freedom and security in a world with no off switch*. Yale University Press.
7. European Union. (2018). *General Data Protection Regulation* (GDPR), Regulation (EU) 2016/679.
8. Gillespie, T. (2018). *Custodians of the Internet: Platforms, content moderation, and the hidden decisions that shape social media*. Yale University Press.
9. Greenleaf, G. (2021). Global data privacy laws 2021: *153 national laws & many bills*. Privacy Laws & Business International Report, 170, 10–13.
10. Human Rights Council. (2014). *The right to privacy in the digital age*. United Nations General Assembly, A/HRC/27/37.
11. Kerr, I., & Earle, J. (2013). *Prediction, preemption, presumption: How big data threatens big-picture privacy*. Stanford Law Review Online, 66, 65–72.
12. Kurbalija, J. (2016). *An introduction to Internet governance* (7th ed.). DiploFoundation.
13. La Rue, F. (2013). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*. United Nations, A/HRC/23/40.
14. Lyon, D. (2018). *The culture of surveillance: Watching as a way of life*. Polity Press.
15. MacKinnon, R. (2012). *Consent of the networked: The worldwide struggle for Internet freedom*. Basic Books.
16. Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Harvard University Press.
17. Snowden, E. (2019). *Permanent record*. Metropolitan Books.
18. Solove, D. J. (2021). *The privacy paradox and the future of privacy regulation*. UCLA Law Review, 68(4), 1230–1292.
19. UNESCO. (2021). *Recommendation on the ethics of artificial intelligence*. United Nations Educational, Scientific and Cultural Organization.
20. Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.