Volume - 7 (2026)
Special Issue - 1 (January)
RESEARCH HUB
International Peer-Reviewed Multidisciplinary E-Journal
ISSN 2582-9173
Website : www.researchhub.org.in/research-hub !! Email : researchhubjournal@gmail.com

THE EVOLVING RELATIONSHIP BETWEEN TECHNOLOGY, LAW, AND HUMAN RIGHTS

Dr. Sanjay P. Dhok
Associate Professor
Sant Gadge Maharaj Mahavidyalaya, Hingna, Dist. Nagpur

Crossref DOI - https://doi.org/10.63665/rh.v7i1.32

Abstract :

Modern technology has rapidly changed societies, creating new opportunities while also raising serious concerns for human rights. This paper explores how law and human rights interact with technological development, emphasizing the need for legal systems to continuously adapt to new innovations. It examines key technologies such as artificial intelligence, digital surveillance, social media, biometric identification, and the Internet of Things, and evaluates their impact on fundamental rights including privacy, freedom of expression, equality, and security.

The study highlights major human rights challenges in the digital age, including large-scale data collection, algorithmic bias, online censorship, and unequal access to technology. While these advancements can empower individuals and improve access to information, they can also threaten personal freedoms if not properly regulated. The paper reviews existing international and regional legal frameworks and ethical guidelines, identifying gaps that limit their effectiveness.

Finally, the paper stresses the importance of proactive regulation, responsible innovation, and international cooperation to address emerging risks from technologies such as blockchain, quantum computing, and deepfake media. It supports a human rights–based approach that balances technological progress with the protection of human dignity, arguing that safeguarding rights in the digital age is essential for a fair, transparent, and inclusive society.

Keywords : Human Rights, Digital Technology, Privacy, Legal frameworks, international law.

Introduction :

Technology has consistently shaped the course of human civilization, serving as a catalyst for progress while simultaneously generating complex legal and ethical challenges. From early innovations such as the printing press to contemporary developments including artificial intelligence (AI), digital surveillance, and global data networks, technological change has profoundly altered social structures, economic systems, and the exercise of individual rights. In the modern era, technology is deeply embedded in everyday life, making it essential

to examine how legal systems can respond effectively to innovation while safeguarding human dignity, privacy, equality, and freedom.

The relationship between law, technology, and human rights is dynamic and interdependent. Legal systems exist to regulate behavior, ensure accountability, and protect fundamental rights, yet technological advancement frequently outpaces legal reform. This disparity creates regulatory gaps, forcing societies to reconsider established legal principles such as privacy, freedom of expression, equality before the law, and state responsibility. As emerging technologies blur traditional boundaries of jurisdiction and accountability, the challenge of aligning innovation with justice becomes increasingly urgent.

Historical experience demonstrates that technological revolutions invariably demand legal adaptation. The invention of the printing press in the fifteenth century expanded access to information and weakened centralized authority, giving rise to early debates on censorship and freedom of expression. Similarly, the industrial revolution transformed labor relations and living conditions, prompting the development of labor laws to address exploitation, unsafe working environments, and child labor. These examples illustrate that law evolves in response to social and technological change, reinforcing the need for flexible and responsive legal frameworks.

In the late twentieth and early twenty-first centuries, digital technologies such as the internet, mobile devices, and cloud computing created unprecedented global connectivity. While these developments enhanced communication, economic opportunity, and access to information, they also introduced new risks, including cybercrime, mass surveillance, data exploitation, and cross-border regulatory conflicts. The emergence of artificial intelligence and automated decision-making systems further challenges traditional legal notions of liability, transparency, and fairness. Understanding the interaction between law and technology is therefore essential to ensure that technological advancement serves human welfare rather than undermining fundamental rights.

The Role Of Law In Regulating Technology :

Law plays a central role in shaping the development and use of technology by establishing norms, assigning responsibility, and protecting individual and collective rights. Governments, international organizations, and private actors must navigate significant regulatory challenges arising from the speed, scale, and global reach of technological innovation.

International Legal Frameworks :

International human rights instruments provide a foundational framework for addressing technological challenges. The Universal Declaration of Human Rights (UDHR) affirms essential rights such as equality, privacy, and freedom of expression, which remain relevant in digital environments. Although the UDHR is not legally binding, it has informed binding treaties such as the International Covenant on Civil and Political Rights (ICCPR), which obligates states to protect privacy and free expression even as technology evolves.

The Budapest Convention on Cybercrime represents the first international effort to address offenses committed through digital means, including hacking and unauthorized access to data. While the Convention promotes international cooperation, it also raises concerns regarding privacy and proportionality. The United Nations Guiding Principles on Business and Human Rights emphasize that private corporations, particularly technology companies, have a responsibility to respect human rights, conduct due diligence, and provide remedies for harm.

The European Union's General Data Protection Regulation (GDPR) has emerged as one of the most influential data protection regimes globally. By strengthening consent requirements, enhancing user control, and imposing strict compliance obligations, the GDPR demonstrates how legal regulation can shape corporate behavior and empower individuals in the digital age.

Domestic Laws and National Approaches :

National responses to technological regulation vary according to political values, economic priorities, and governance models. The United States relies on a sector-specific regulatory approach, with laws such as the California Consumer Privacy Act (CCPA) addressing consumer data while broader federal privacy legislation remains absent. The European Union adopts a rights-based model through the GDPR, providing comprehensive protections with extraterritorial reach.

China's regulatory framework emphasizes state control, data localization, and extensive surveillance, reflecting a governance model that prioritizes security and political stability over individual privacy. India has proposed comprehensive data protection legislation inspired by the GDPR, aiming to enhance individual rights and data security, though implementation challenges persist.

Challenges in Legal Regulation :

Despite the existence of legal frameworks, effective regulation faces significant obstacles. Digital activities transcend national borders, complicating jurisdiction and enforcement. Legal systems often struggle to keep pace with rapid technological change, particularly in areas such as artificial intelligence, biometrics, and automated surveillance. Governments must balance national security interests with civil liberties, as illustrated by debates surrounding encryption, data retention, and surveillance powers.

Global inequalities in technological capacity and regulatory strength can result in digital colonialism, where powerful states or corporations impose norms on weaker regions. Moreover, ethical dilemmas—such as autonomous weapons and algorithmic decision-making—frequently fall outside existing legal categories, highlighting the limits of traditional regulation.

Adaptive Legal Frameworks :

To address these challenges, legal systems must be adaptable, inclusive, and grounded in fundamental rights. Regulation should be principle-oriented rather than overly prescriptive, enabling flexibility in response to innovation. Inclusive policymaking that considers

marginalized communities and developing nations is essential, as is international cooperation to harmonize standards and share best practices.

Key Technologies Impacting Human Rights :

Technological innovation has transformed nearly every aspect of modern life, generating both opportunities and risks for human rights.

Digital Surveillance and Privacy :

Digital surveillance involves the systematic collection and analysis of data to monitor individuals and populations. Governments justify surveillance for purposes such as national security and crime prevention, while corporations employ data analytics for marketing and profit. However, extensive monitoring threatens the right to privacy and undermines personal autonomy.

Revelations concerning mass surveillance programs exposed the scale of state monitoring and sparked global debate. Excessive surveillance can discourage political dissent, activism, and free expression, thereby weakening democratic participation. Corporate data exploitation further compounds these risks by enabling profiling, behavioral tracking, and discriminatory practices, often without meaningful consent or transparency.

Artificial Intelligence and Automation :

Artificial intelligence systems are increasingly deployed in policing, recruitment, credit assessment, healthcare, and judicial processes. While AI offers efficiency and innovation, it also raises serious human rights concerns. Algorithms trained on biased or incomplete data may reproduce and amplify social inequalities, resulting in discriminatory outcomes in employment, law enforcement, and access to services.

Transparency is another critical issue. When AI systems influence decisions affecting liberty or livelihood, individuals must be able to understand and challenge those decisions. Opaque or "black-box" models undermine accountability and due process. Additionally, automation threatens economic and labor rights by displacing workers and exacerbating inequality.

Deepfake Technology :

Deepfakes involve the creation of realistic but fabricated audio or visual content. This technology poses serious risks to privacy, reputation, and democratic integrity. High-profile incidents involving manipulated political videos, election interference, and misuse against public figures illustrate the potential for harm. Although legal frameworks specifically addressing deepfakes remain underdeveloped, existing laws on defamation, privacy, and cyber harassment are increasingly applied to such cases.

Social Media and Freedom of Expression :

Social media platforms have democratized communication and enabled large-scale

civic mobilization. At the same time, they have facilitated the spread of misinformation, hate speech, and online harassment. Content moderation practices raise difficult questions about censorship, platform responsibility, and freedom of expression. Algorithmic amplification of polarizing content further complicates efforts to balance free speech with public safety.

Biometric Technologies :

Biometric technologies such as facial recognition, fingerprint scanning, and retinal imaging are widely used for identification and security. Biometric data is highly sensitive and irreversible, making misuse particularly harmful. Facial recognition systems have been shown to exhibit racial and gender bias, leading to false identification and disproportionate harm to marginalized communities. The widespread deployment of biometric surveillance in public spaces also raises concerns about repression and loss of anonymity.

Internet of Things (IoT) :

The Internet of Things refers to networks of interconnected devices that continuously collect and exchange data. While IoT enhances convenience and efficiency, it also increases risks to privacy and security. Weak security standards expose users to hacking and surveillance, while unequal access to digital infrastructure deepens social and economic divides.

Human Rights Challenges In The Digital Age :

Privacy and Data Protection :

Privacy is central to human dignity and autonomy and is protected under international human rights law. In the digital age, massive data collection by governments and corporations often occurs without informed consent, exposing individuals to surveillance, profiling, and misuse. Data breaches and cyberattacks further threaten personal security. The misuse of personal data for political manipulation, as demonstrated by high-profile scandals, highlights the vulnerability of democratic processes.

Freedom of Expression :

Freedom of expression is essential for democratic governance and public accountability. Digital technologies have expanded opportunities for expression but also enabled new forms of censorship and repression. Internet shutdowns, platform bans, and online harassment disproportionately affect journalists, activists, and political opponents, particularly in authoritarian contexts.

Equality and Non-Discrimination :

Digital systems must uphold the principle of equality, yet algorithmic bias and unequal access often perpetuate discrimination. The digital divide excludes marginalized populations from education, employment, and civic participation. Online abuse and gender-based violence further undermine equality and safety in digital spaces.

Access to Information and Inclusion :

Access to reliable information is critical for informed decision-making and participation. Censorship, infrastructure gaps, poverty, and language barriers restrict access and reinforce existing inequalities. Inclusive digital policies are necessary to ensure that technological benefits are equitably distributed.

Security and Safety :

While technology can enhance security, it also introduces new threats such as cybercrime, identity theft, ransomware attacks, and cyber warfare. Digital tools may be used for intimidation, surveillance, and repression, undermining both individual and national security.

Legal And Ethical Frameworks :

Addressing the human rights implications of technology requires robust legal and ethical frameworks guiding governments, corporations, and technologists.

International instruments such as the UDHR, ICCPR, and European Convention on Human Rights provide foundational principles applicable to digital contexts. The UN Guiding Principles on Business and Human Rights emphasize corporate accountability, while the Budapest Convention facilitates cooperation against cybercrime. Emerging initiatives such as the Global Digital Compact seek to establish shared principles for digital governance.

At the national and regional levels, laws such as the GDPR and similar data protection regimes reflect growing recognition of digital rights. Ethical standards complement legal rules, particularly in areas where legislation lags behind innovation. Responsible AI development prioritizes transparency, fairness, accountability, and human-centric design, as promoted by initiatives like the IEEE Global Ethics framework.

However, regulatory efforts face challenges including rapid technological change, cross-border enforcement difficulties, competing interests between privacy and security, and insufficient oversight. Effective governance requires multistakeholder collaboration, integration of human rights into technological design, and accessible remedies for rights violations**.**

Citizens' Duties And Responsibilities :

Citizens play a crucial role in protecting human rights in the digital environment. Their responsibilities include remaining informed about technological impacts, developing digital literacy, respecting the rights of others, and participating in democratic processes. Responsible behavior involves reporting cybercrime and misinformation, safeguarding personal data, and advocating for ethical technology use.

Citizens also bear legal and ethical liabilities. They must avoid illegal activities such as hacking or spreading harmful content and take responsibility for the accuracy of information they share. Community support and respectful online conduct contribute to a safer digital ecosystem.

Germany provides a notable example through laws such as the Network Enforcement Act (NetzDG) and the Federal Data Protection Act, which emphasize both platform

accountability and individual responsibility. Citizens are encouraged to report illegal content and protect personal data, reinforcing a culture of shared responsibility.

Conclusion :

Balancing law, technology, and human rights is one of the defining challenges of the twenty-first century. Technological innovation offers significant benefits in health, education, and economic development, yet it also threatens privacy, freedom, equality, and security. Ensuring that technological progress respects human rights requires a proactive, interdisciplinary approach involving legal reform, ethical standards, technological design, and civil society engagement.

Governments and institutions bear primary responsibility, but citizens also play a vital role through responsible use, awareness, and participation. Flexible legal frameworks, strong ethical principles, international cooperation, and active civic involvement are essential to achieving the Sustainable Development Goals and fostering a rights-respecting digital future. Ultimately, a human-centered, rights-based approach grounded in transparency, accountability, and respect for dignity is necessary to ensure that technology empowers rather than exploits humanity.

References :

- European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). *Official Journal of the European Union.* 2016; L119:1–88.
- United Nations Human Rights Office of the High Commissioner. *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework.* United Nations; 2011.
- Council of Europe. *European Convention on Human Rights.* 1950.
- Kuner C, Bygrave LA, Docksey C, editors. *The GDPR: A Commentary.* Oxford: Oxford University Press; 2017.
- Schneier B. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World.* New York: W. W. Norton & Company; 2015.
- Zuboff S. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.* New York: PublicAffairs; 2019.
- Bryson JJ. Artificial intelligence and human rights. In: *The Oxford Handbook of Ethics of Artificial Intelligence.* Oxford: Oxford University Press; 2018.
- Mann S, Ferenbok J. New media and the paparazzi: The politics of digital surveillance. *Media, Culture & Society.* 2013;35(1):37–54.
- Sharma S. Regulation of social media in India: A human rights perspective. *Science, Technology & Society.* 2022;27(1):45–63.
- Pillai K, Menon R. Biometric systems and privacy concerns in India. *Indian Journal of Information Security.* 2019;5(3):78–85.
- Das G. The impact of the Information Technology Act, 2000 on privacy rights in

India. *Law Journal of India.* 2018;18(2):210–225.

- Verma P. Challenges to implementing data protection laws in India. *International Journal of Cyber Law.* 2020;14(1):45–59.
- Kumar P. Data privacy and protection law in India: Challenges and opportunities. *International Journal of Law and Management.* 2020;62(3):233–248.
- Sinha A. Digital surveillance and privacy rights in India. *Indian Journal of Law.* 2021;12(4):145–160.
- Reddy M. Artificial intelligence and human rights: An Indian perspective. *Journal of Technology Law and Policy.* 2019;24(2):101–118.