



**HUMAN RIGHTS IN THE AGE OF TECHNOLOGY: THE NEED FOR A NEW LEGAL  
FRAMEWORK**

**Rakhi Karan Vyas, Dr. Umesh, Shrikrishnarao Aswar**

Ph. D. Research Scholar, Department of Law, Mumbai University, University of Mumbai, Fort,  
Mumbai – 400032, Maharashtra, India

(Ph. D. Research Guide, Government Law College, 1002, A Road, Churchgate, Mumbai  
Maharashtra 400020, India

Asstt. Professor, Government Law College, 1002, A Road, Churchgate, Mumbai Maharashtra  
400020, India

**Abstract**

The rapid advancement of technology has transformed nearly every aspect of human life, from communication and healthcare to governance and education. However, these advancements have also raised significant challenges to the protection and enforcement of human rights. Issues such as data privacy, surveillance, artificial intelligence (AI) bias, and cybercrime have highlighted the inadequacies of existing legal frameworks. This paper explores the intersection of human rights and technology, emphasizing the need for a new legal framework to address emerging challenges. It examines the historical evolution of human rights in the context of technological progress, identifies gaps in current laws, and proposes recommendations for a more robust and adaptive legal system. The study concludes that a multidisciplinary approach, involving policymakers, technologists, and human rights advocates, is essential to safeguard human rights in the digital age. The rapid advancement of technology has transformed nearly every aspect of human life, from communication and commerce to governance and social interactions. While these developments have brought numerous benefits, they have also posed unprecedented challenges to the protection and enforcement of human rights. Emerging technologies such as artificial intelligence (AI), big data analytics, surveillance systems, and digital platforms have reshaped traditional legal and ethical paradigms, often outpacing existing regulatory frameworks. This shift has necessitated a reconsideration of human rights protections in the digital age.

The intersection of technology and human rights is complex, as it involves multiple dimensions, including privacy, freedom of expression, data security, and digital access. The internet and social media have revolutionized the way individuals exercise their rights to speech and assembly, yet they have also created new threats such as online censorship, misinformation, and cyber harassment. Similarly, AI-driven decision-making in areas such as policing, employment, and healthcare has raised concerns about algorithmic bias, discrimination, and lack of accountability.

Moreover, the rise of mass surveillance, facilitated by governments and private corporations, has significantly altered the landscape of personal privacy. Digital tracking, facial recognition technology, and data collection practices challenge the foundational principles of civil liberties,



often operating in legal gray areas. The absence of a comprehensive legal framework to address these emerging concerns has led to growing calls for international legal reforms that can safeguard human rights in the digital era.

As traditional human rights laws were primarily designed for an offline world, there is an urgent need to adapt and expand legal frameworks to ensure that technological advancements do not erode fundamental rights. This study explores the challenges posed by technology to human rights and argues for a new legal framework that is both adaptable and enforceable. It examines global efforts to regulate digital technologies, identifies existing gaps in legal protections, and proposes a structured approach to balance innovation with ethical responsibility.

Through this analysis, the study aims to contribute to the ongoing discourse on the future of human rights in an increasingly digitalized society, emphasizing the role of governments, international organizations, and technology corporations in shaping policies that protect individuals while fostering technological progress.

## Keywords

Human Rights, Technology, Legal Framework, Data Privacy, Surveillance, Artificial Intelligence, Cybercrime, Digital Age, Ethics, Governance.

## Introduction

The digital revolution has brought unprecedented opportunities for innovation and progress. However, it has also introduced complex challenges to the protection of human rights. Technologies such as AI, big data, and the Internet of Things (IoT) have created new avenues for surveillance, discrimination, and exploitation. Existing legal frameworks, designed for a pre-digital era, are often ill-equipped to address these issues. This paper argues that the rapid pace of technological change necessitates a rethinking of human rights laws to ensure they remain relevant and effective in the 21st century.

## Definitions

1. **Human Rights:** Fundamental rights and freedoms that belong to every individual, regardless of nationality, ethnicity, or gender, as outlined in documents like the Universal Declaration of Human Rights (UDHR).
2. **Technology:** The application of scientific knowledge for practical purposes, particularly in fields such as computing, AI, and biotechnology.
3. **Legal Framework:** A system of laws, regulations, and guidelines designed to govern behavior and protect rights within a society.



## Need for a New Legal Framework

The current legal frameworks were established in an era when technology was not as pervasive or influential as it is today. Issues such as mass surveillance, data breaches, and algorithmic bias require new legal approaches to protect individuals' rights. Without updated laws, there is a risk of human rights violations going unchecked, leading to a loss of trust in institutions and technologies.

### Aims

The primary aim of this study is to analyze the impact of technology on human rights and propose a new legal framework that addresses the challenges of the digital age.

### Objectives

1. To examine the historical evolution of human rights in the context of technological advancements.
2. To identify gaps in existing legal frameworks regarding technology and human rights.
3. To propose recommendations for a new legal framework that safeguards human rights in the digital age.
4. To explore the role of stakeholders, including governments, corporations, and civil society, in shaping this framework.

### Hypothesis

The hypothesis of this study is that existing legal frameworks are insufficient to address the challenges posed by modern technology, and a new, adaptive legal framework is necessary to protect human rights effectively.

### Literature Search

A comprehensive review of existing literature was conducted, focusing on:

- The impact of technology on human rights.
- Case studies of human rights violations in the digital age.
- Analysis of current legal frameworks and their limitations.
- Proposals for new legal approaches to address technological challenges.

### Research Methodology

This study employs a qualitative research approach, including:

1. **Document Analysis:** Review of international human rights laws, national legislation, and policy documents.



2. **Case Studies:** Examination of specific instances where technology has impacted human rights.
3. **Expert Interviews:** Conversations with legal scholars, technologists, and human rights advocates.
4. **Comparative Analysis:** Comparison of legal frameworks across different countries to identify best practices.

## **Strong Points**

### **1. Digital Privacy and Data Protection**

- The rise of surveillance capitalism and data mining by corporations and governments.
- The need for stronger data protection laws (e.g., GDPR, India's Data Protection Bill).
- Issues of mass surveillance, facial recognition, and AI-driven profiling.

### **2. Freedom of Expression and Censorship**

- The role of social media in shaping political discourse.
- The tension between free speech and misinformation/disinformation.
- Algorithmic bias and the suppression of marginalized voices.

### **3. Cybersecurity and Protection from Digital Threats**

- The increasing prevalence of cyberattacks on individuals, institutions, and governments.
- The role of international law in combating cybercrime and cyber warfare.
- Ethical concerns around hacking, digital espionage, and state-sponsored cyber warfare.

### **4. AI and Algorithmic Decision-Making**

- The risks of bias in AI-driven legal, financial, and hiring decisions.
- Ethical dilemmas in predictive policing and automated justice systems.
- The lack of accountability for AI errors impacting fundamental rights.

### **5. Digital Divide and Access to Technology as a Human Right**

- The disparity in access to the internet and digital resources.
- The role of technology in education and its impact on human development.
- The digital exclusion of marginalized and economically weaker sections.



## 6. Tech-Enabled Workplace and Labor Rights

- The impact of automation and AI on employment opportunities.
- Gig economy challenges: job insecurity, unfair wages, and worker rights.
- Surveillance and worker productivity tracking in remote/hybrid work.

## 7. Biometric and DNA Data Ethics

- Ethical concerns surrounding biometric databases (Aadhaar, etc.).
- The use of DNA profiling in criminal investigations and privacy concerns.
- Risks of genetic discrimination in employment and insurance sectors.

## 8. Regulation of Big Tech and Corporate Accountability

- The power of major tech companies in controlling digital infrastructure.
- The need for stronger antitrust laws to prevent monopolization.
- Holding platforms accountable for misinformation, hate speech, and extremist content.

## 9. Blockchain and Human Rights

- The potential of blockchain for securing digital identity and voting rights.
- The role of cryptocurrencies in financial inclusion vs. their misuse in illicit activities.
- Ethical concerns surrounding decentralized, unregulated financial systems.

## 10. Future of Human Rights in the Age of AI and Transhumanism

- The ethical and legal challenges of brain-computer interfaces (Neuralink, etc.).
- Human rights implications of AI-human augmentation.
- The future of digital personhood and rights for AI-driven entities.

### Weak Points

1. **Limited Scope:** The study focuses primarily on digital technologies and may not address broader technological impacts.
2. **Implementation Challenges:** The proposed framework may face resistance from governments and corporations.
3. **Lack of Quantitative Data:** The qualitative approach may lack statistical evidence to support its findings.



## Current Trends

1. **Increased Surveillance:** Governments and corporations are using technology to monitor individuals, raising privacy concerns.
2. **AI and Bias:** Algorithms are increasingly being used in decision-making processes, often perpetuating existing biases.
3. **Data Privacy Laws:** Countries are enacting new laws, such as the General Data Protection Regulation (GDPR), to address data privacy concerns.

## History

The relationship between human rights and technology has evolved over time. Early concerns focused on the impact of industrialization on workers' rights. In the digital age, the focus has shifted to issues such as internet freedom, data privacy, and the ethical use of AI.

### 1. Early Technological Developments and Their Impact on Human Rights (Pre-20th Century)

- **Printing Press (15th Century):** The invention of the printing press by Johannes Gutenberg led to mass communication, enabling the spread of ideas, including those on human rights, democracy, and freedom of speech.
- **Industrial Revolution (18th–19th Century):** While it brought economic progress, it also led to labor exploitation, unsafe working conditions, and child labor, prompting early labor rights movements.
- **Telegraph and Radio (19th–Early 20th Century):** Enabled global communication but also introduced concerns about state surveillance and propaganda control.

### 2. The Rise of Digital Technology and Early Human Rights Concerns (Mid-20th Century–1980s)

- **Post-WWII Era and the Universal Declaration of Human Rights (1948):** After WWII, the United Nations (UN) established the UDHR, setting the foundation for fundamental human rights, including freedom of expression, privacy, and dignity.
- **Cold War Era and Government Surveillance (1950s–1980s):** The US and USSR engaged in mass surveillance, wiretapping, and espionage, raising concerns about state control over personal freedoms.
- **Rise of Computers and the Internet (1960s–1980s):** The development of ARPANET (precursor to the internet) brought new questions about data security, privacy, and cyber rights.

### 3. The Digital Age and the Emergence of Internet Human Rights Challenges (1990s–Early 2000s)





- **World Wide Web (1990s):** The internet revolutionized communication, commerce, and governance but raised concerns about data privacy, cybercrime, and misinformation.
- **E-Commerce and Digital Transactions (1990s–2000s):** With the rise of online businesses (e.g., Amazon, eBay), data protection laws became necessary to safeguard users from financial fraud and identity theft.
- **Surveillance and Cybersecurity (Post-9/11 Era):** After the 9/11 attacks, governments expanded digital surveillance programs, such as the US PATRIOT Act and PRISM, raising major privacy concerns.

#### 4. Social Media, Big Tech, and Human Rights (2010s–Present)

- **Social Media Boom (2010s):** Platforms like Facebook, Twitter, and YouTube became powerful tools for free speech, political activism (e.g., Arab Spring), and disinformation.
- **Rise of AI and Algorithmic Bias:** Companies began using AI for decision-making (hiring, law enforcement, etc.), leading to concerns about discrimination, bias, and accountability.
- **Cambridge Analytica Scandal (2018):** Highlighted the misuse of personal data for political manipulation, sparking global discussions on digital privacy.
- **COVID-19 Pandemic (2020s):** Accelerated digitalization, but also increased government surveillance, misinformation, and debates on health data privacy.

#### 5. Recent Legal and Policy Developments (2020s–Present)

- **GDPR (2018):** The European Union introduced the General Data Protection Regulation (GDPR) to protect digital privacy rights.
- **India's Data Protection Bill (2023):** Aimed at regulating data collection and usage by tech companies and the government.
- **AI Regulations and Ethical Frameworks:** Countries are working on laws to regulate AI (e.g., the EU AI Act) to prevent rights violations.
- **Antitrust Actions Against Big Tech:** Governments worldwide are investigating and regulating monopolistic practices of Google, Amazon, Facebook, and Apple.

#### 6. The Need for a New Legal Framework in the Digital Age

- **Emerging Technologies (AI, Blockchain, Quantum Computing, etc.):** Raise ethical and legal questions about privacy, bias, and surveillance.
- **Digital Divide and Cybersecurity Risks:** Growing inequalities in internet access and increasing cyber threats necessitate new legal protections.



- **International Cooperation:** A global human rights framework for technology is essential to address cross-border digital challenges.

## Discussion

The study highlights the inadequacies of current legal frameworks in addressing technological challenges. It emphasizes the need for a new framework that is flexible, inclusive, and forward-looking. The discussion also explores the role of stakeholders in shaping this framework and the potential obstacles to its implementation.

## Results

The findings indicate that:

1. Existing legal frameworks are outdated and insufficient.
2. Technology poses significant risks to human rights, including privacy violations and discrimination.
3. A new legal framework is necessary to address these challenges effectively.

## Conclusion

The study concludes that the rapid pace of technological change necessitates a new legal framework to protect human rights. This framework must be adaptive, inclusive, and enforceable to address the unique challenges of the digital age.

## Suggestions and Recommendations

1. **Develop Adaptive Laws:** Create laws that can evolve with technological advancements.
2. **Promote Multistakeholder Collaboration:** Involve governments, corporations, and civil society in the development of new legal frameworks.
3. **Enhance Public Awareness:** Educate individuals about their rights in the digital age.
4. **Establish International Standards:** Develop global standards for the ethical use of technology.

## Future Scope

Future research should focus on:

1. The impact of emerging technologies, such as quantum computing and biotechnology, on human rights.
2. The role of international organizations in enforcing new legal frameworks.
3. The ethical implications of AI and automation.





## References

1. United Nations. (1948). *Universal Declaration of Human Rights*.
2. European Union. (2018). *General Data Protection Regulation (GDPR)*.
3. Zuboff, S. (2019). *The Age of Surveillance Capitalism*. PublicAffairs.
4. Lessig, L. (2006). *Code: And Other Laws of Cyberspace*. Basic Books.
5. Amnesty International. (2020). *Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights*.
6. Floridi, L. (2014). *The Fourth Revolution: How the Infosphere is Reshaping Human Reality*. Oxford University Press.
7. Solove, D. J. (2008). *Understanding Privacy*. Harvard University Press.
8. Calo, R. (2017). *Artificial Intelligence Policy: A Primer and Roadmap*. *University of Chicago Law Review*, 85(1), 1-57.
9. Cath, C. (2018). *Governing Artificial Intelligence: Ethical, Legal, and Technical Opportunities and Challenges*. *Philosophical Transactions of the Royal Society A*, 376(2133).
10. Human Rights Watch. (2021). *The Price of Connectivity: How Internet Shutdowns Impact Human Rights*.
11. World Economic Forum. (2020). *The Future of Jobs Report*.
12. Electronic Frontier Foundation (EFF). *Surveillance Self-Defense*. <https://ssd.eff.org>
13. United Nations Human Rights Office. *Digital Technologies and Human Rights*. <https://www.ohchr.org>