International Journal of Research in Social Sciences
Vol. 16, Issue 5, May 2026,
ISSN: 2249-2496 Impact Factor: 7.081
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Human Rights Implications of Facial Recognition Technology: Towards a Global and Indian Legal Framework

Dr. Quemre Alam
Assistant Professor,
Patna Law College, Patna University, Patna, Bihar, India

Abstract
Facial Recognition Technology (FRT) has become a transformative innovation within digital governance, security, and commerce. While its rapid adoption enhances efficiency and service delivery, it also raises complex ethical and human rights concerns. This paper critically examines the implications of FRT within global and Indian legal frameworks through a doctrinal and comparative methodology. It analyses major human rights instruments such as the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), and regional regulatory frameworks including the European Union's General Data Protection Regulation (GDPR) and the Artificial Intelligence Act (2024). The study juxtaposes these global norms against India's evolving digital regulation, including the Digital Personal Data Protection Act (DPDP), 2023, and the jurisprudence of Justice K.S. Puttaswamy v. Union of India (2017). Findings reveal that India's biometric governance lacks adequate consent standards, algorithmic transparency, and oversight. The paper concludes that a rights-based approach rooted in proportionality, accountability, and public consultation is essential to reconcile technological advancement with fundamental human rights.
Keywords: Facial Recognition Technology, Human Rights, Privacy, Algorithmic Accountability, Regulation, India, AI Ethics

1. Introduction
Technological advancements in artificial intelligence and biometrics have redefined state and corporate surveillance capacities. Among these, Facial Recognition Technology (FRT) represents one of the most pervasive and controversial innovations. Its applications span from criminal investigations and border control to personal device authentication and e-commerce personalization. While these developments promise efficiency, the unchecked use of FRT undermines core human rights, particularly privacy, dignity, equality, and freedom of expression.
According to the United Nations High Commissioner for Human Rights (UNHCHR, 2021), mass surveillance via FRT threatens rights enshrined in the UDHR and ICCPR, specifically Articles 12, 17, and 19, which safeguard privacy and free expression. Furthermore, studies have shown that algorithmic bias often results in discriminatory outcomes against women, minorities, and marginalized groups (Fussey & Murray, 2019).
In India, the deployment of Automated Facial Recognition Systems (AFRS) and initiatives like DigiYatra reflect the increasing use of biometric technologies in governance. Despite the recognition of privacy as a fundamental right in Justice K.S. Puttaswamy v. Union of India (2017), India still lacks comprehensive legislation to regulate FRT. This paper argues for a balanced legal framework that harmonizes innovation with constitutional and international human rights guarantees.

2. Literature Review
2.1 Global Perspectives
Global academic discourse underscores the dual role of FRT as both a tool of efficiency and a potential mechanism for oppression. Calo (2019) emphasizes the need for ethical oversight in AI systems, while Whittaker et al. (2021) highlight the role of algorithmic transparency in protecting civil liberties. Fussey and Murray (2019) demonstrate how bias in FRT undermines the right to equality and non-discrimination under human rights law.
The European Union (EU) leads the regulatory frontier. Under the GDPR (2018), biometric data are classified as sensitive personal data, requiring explicit consent for lawful processing. The EU AI Act (2024) further introduces stringent restrictions on real-time facial recognition, mandating risk

assessments and human oversight. These measures illustrate a preventive, rights-based regulatory approach rooted in precaution and accountability.

2.2 Indian Perspectives

In contrast, India's legal landscape remains fragmented. Scholars such as Bhandari (2020) and Singh (2023) note that India's privacy jurisprudence, though constitutionally sound, suffers from weak legislative implementation. Civil society groups like the Internet Freedom Foundation (2023) criticize the opaque deployment of FRT in policing and public administration, where data collection often occurs without explicit consent or transparency.

2.3 Research Gap

Existing literature often isolates FRT's technical and ethical aspects without integrating a comparative human rights perspective. This study fills that gap by systematically comparing international standards and India's emerging regulatory framework, identifying pathways for harmonized, rights-based governance.

3. Methodology

This research employs a doctrinal and comparative legal methodology, focusing on the intersection of human rights and technology regulation.

3.1 Primary Sources

International frameworks: UDHR, ICCPR, GDPR, and the EU AI Act (2024).

Indian frameworks: Constitution of India, Puttaswamy v. Union of India (2017), and the DPDP Act (2023).

3.2 Secondary Sources

Academic journals, UN reports, and NGO analyses (Internet Freedom Foundation, UNESCO).

Comparative studies between the EU, US, and India regarding AI ethics and privacy governance.

The study applies normative analysis based on transparency, consent, accountability, and proportionality—core principles of international human rights law.

4. Results and Discussion

4.1 Global Regulatory Frameworks

European Union: A Rights-Driven Paradigm

The EU's regulatory regime sets a global benchmark for human rights–based governance. The GDPR (2018) classifies biometric data as "special category data," allowing processing only under strict consent or legal necessity. In Digital Rights Ireland Ltd v. Minister for Communications (2014), the ECJ emphasized that blanket data retention violates fundamental rights to privacy and data protection. The AI Act (2024) enhances these protections by designating real-time biometric identification as a "high-risk activity." It requires algorithmic impact assessments, human oversight, and documentation of training datasets to mitigate bias—thereby embedding ethical safeguards within the technological lifecycle.

United States: Fragmented but Evolving

The US lacks a comprehensive federal data protection law. Instead, regulation is decentralized across states. The Illinois Biometric Information Privacy Act (BIPA, 2008) mandates explicit consent for facial data collection and provides individuals with legal remedies. In ACLU v. Clearview AI (2020), the unauthorized scraping of facial images was held to violate privacy rights. Similarly, the California Consumer Privacy Act (CCPA, 2018) and the California Privacy Rights Act (CPRA, 2023) reinforce consumer data rights through access and deletion provisions.

United Nations and Global Mechanisms

The UNHCHR (2021) report, The Right to Privacy in the Digital Age, underscores that indiscriminate FRT use contravenes Articles 12 and 19 of the UDHR and ICCPR. Similarly, the UNESCO (2021) Recommendation on the Ethics of Artificial Intelligence advocates for algorithmic transparency, proportionality, and human oversight—principles that remain central to this study's analysis.

4.2 Indian Legal and Constitutional Framework

Constitutional Safeguards

In Justice K.S. Puttaswamy v. Union of India (2017), the Supreme Court declared privacy a fundamental right intrinsic to human dignity and liberty. However, India's FRT ecosystem operates

largely outside this judicial framework. Projects like AFRS and DigiYatra lack statutory oversight, raising questions about legality and proportionality.

Digital Personal Data Protection Act, 2023

The DPDP Act, 2023 marks progress toward a structured data protection regime. Yet, its provisions under Section 17 grant broad exemptions to the state, undermining individual safeguards. Without an independent Data Protection Authority, enforcement remains weak, particularly in contexts of biometric and algorithmic surveillance.

Operational Gaps

Civil society audits reveal that most FRT deployments in India operate without impact assessments or public consultations (Internet Freedom Foundation, 2023). Algorithmic bias remains unaddressed, leading to potential violations of equality under Article 14 of the Constitution.

4.3 Comparative Assessment

Aspect	European Union	United States	India
Legal Status of FRT	High-risk (AI Act)	State-level laws	No specific law
Privacy Protection	Comprehensive (GDPR)	Fragmented	DPDP Act with exemptions
Oversight Authority	Data Protection Authorities	Courts and state agencies	None independent
Algorithmic Transparency	Mandated	Voluntary	Absent
Public Consultation	Mandatory	Limited	None

The EU's rights-centric approach contrasts sharply with India's state-exempted model, highlighting the need for explicit statutory mechanisms ensuring transparency, proportionality, and judicial oversight.

4.4 Human Rights and Societal Implications

FRT's human rights implications extend beyond privacy. Surveillance in public spaces risks chilling dissent and assembly, violating Article 19(1)(a) and 19(1)(b) of the Indian Constitution. Algorithmic errors can reinforce social hierarchies, perpetuating caste and gender bias contrary to Article 14 guarantees of equality.

While FRT can enhance governance efficiency and law enforcement precision, its potential misuse could transform democratic societies into surveillance states. Thus, embedding human rights by design is essential for legitimate technological governance.

5. Conclusion and Policy Implications

FRT stands at the intersection of innovation and intrusion. Effective regulation must balance technological progress with constitutional and human rights safeguards. India's policy direction should rest on four pillars:

1. Transparency and Accountability: Mandatory algorithmic audits, bias testing, and public reporting.
2. Consent and Oversight: Enact a dedicated Facial Recognition Regulation Bill requiring judicial authorization for public surveillance.
3. Institutional Autonomy: Establish an independent Data Protection Authority with enforcement powers.
4. Public Participation: Ensure inclusive consultations involving civil society and digital rights experts.

Adopting a rights-based regulatory architecture aligned with global norms will ensure that FRT serves human dignity rather than undermines it.

Author Contributions and Declarations

Author Contributions: The author solely conceived, researched, and drafted this manuscript.
Conflict of Interest: The author declares no conflict of interest.
Ethical Approval: Not applicable.

References (APA 7th Edition)

Bhandari, V. (2020). *Surveillance and privacy in India: Legal and policy challenges. Indian Journal of Law and Technology*, 16(2), 45–67.

Calo, R. (2019). *Artificial intelligence policy: A primer and roadmap. UC Davis Law Review*, 51(2), 399–436.
European Union. (2018). *General Data Protection Regulation (GDPR). Official Journal of the European Union*, L119, 1–88.
Fussey, P., & Murray, D. (2019). *Independent report on the London Metropolitan Police's live facial recognition trials.* Essex Human Rights Centre.
Internet Freedom Foundation. (2023). *Automated facial recognition in India: A human rights* analysis. https://internetfreedom.in
Singh, P. (2023*). Regulating AI and biometric technologies in India. Journal of Policy and Governance, 12(3),* 115–132.
United Nations High Commissioner for Human Rights. (2021). *The right to privacy in the digital age.* United Nations.
UNESCO. (2021). *Recommendation on the ethics of artificial intelligence*. UNESCO.
Whittaker, M., Alper, M., Crawford, K., & Barocas, S. (2021). *AI Now Report 2021: Algorithmic accountability and human rights*. New York University.