

“Intersection of Artificial Intelligence and Privacy Rights in India: Legal Challenges and the Way Forward”

Yashwant Shailendra Soni
LL.M. Student,
Mahatma Gandhi Kashi Vidyapeeth,
Varanasi

Abstract

This research paper explores the evolving intersection between Artificial Intelligence (AI) and the constitutionally guaranteed right to privacy in India. As AI technologies become increasingly embedded in governance, policing, healthcare, and financial services, the scale and complexity of data processing raise serious concerns regarding surveillance, profiling, and discrimination. While the Supreme Court’s decision in *Justice K.S. Puttaswamy v Union of India*¹ enshrined privacy as a fundamental right, India’s legal framework lacks the nuance and depth required to regulate AI-driven decision-making. This paper critically evaluates existing regulatory gaps, draws comparative insights from jurisdictions like the EU and the United States, and advocates for a comprehensive, rights-based AI legal framework tailored to India’s democratic and constitutional ethos.

Keywords: Artificial Intelligence, Privacy Rights, Surveillance, Algorithmic Bias, Fundamental Rights, AI Governance, Legal Reform

Introduction

Artificial Intelligence (AI), once a speculative technological promise, has rapidly evolved into a powerful tool reshaping governance, healthcare, law enforcement, and consumer markets. In India, AI technologies are already being used in Aadhaar-based public welfare verification, real-time fraud detection in fintech platforms, and automated facial recognition systems in metropolitan policing. While these applications offer efficiency and scalability, they raise concerns over autonomy, consent, and the risk of technological overreach.

The recognition of “the right to privacy as a fundamental right under Article 21 of the Indian Constitution in Puttaswamy” marked a significant shift in Indian constitutional jurisprudence. Yet, despite this judicial landmark, India’s regulatory framework remains ill-equipped to address the unique challenges posed by AI. This paper aims to critically assess these lacunae and suggest a rights-compatible roadmap for AI governance.

¹ Justice K.S. Puttaswamy v Union of India (2017) 10 SCC 1.

Constitutional and Statutory Framework

The Supreme Court in *Justice K.S. Puttaswamy v Union of India*² held that the right to privacy is intrinsic to human dignity and a core component of the right to life and personal liberty under Article 21 of the Constitution¹. It emphasized informational self-determination and applied the proportionality test to evaluate state interventions.

However, statutes like the *Information Technology Act, 2000*³ and its associated rules remain ill-suited to regulate emerging threats posed by AI, such as real-time biometric surveillance and algorithmic profiling. These instruments lack clarity on AI-specific harms, fail to define automated decision-making, and offer little guidance on transparency or accountability. The regulatory vacuum exposes citizens to unchecked surveillance and unaccountable data processing, particularly by private actors using opaque AI systems.

Jurisprudential and Regulatory Challenges

AI's intersection with privacy and fundamental rights raises the following key concerns:

- 1. Opaque Algorithmic Governance:** AI models often operate as “black boxes,” making it difficult for users and even developers to understand the logic behind specific outcomes. This violates principles of natural justice, such as “audi alteram partem (right to be heard), as individuals affected by AI decisions cannot effectively challenge them.”⁴
- 2. Consent and Purpose Limitation:** AI systems harvest data in ways that undermine genuine consent. Long, complex privacy policies make informed consent meaningless. Moreover, the use of personal data often extends beyond the original purpose, violating core data protection norms.⁵
- 3. Profiling, Bias, and Discrimination:** AI models trained on biased data perpetuate historical inequalities, particularly affecting marginalized groups. For example, caste- or religion-based disparities may be embedded in predictive policing tools or hiring algorithms.⁶
- 4. Mass Surveillance and Chilling Effect:** Facial recognition and predictive policing technologies are already being deployed by Indian authorities without clear legal mandates. The lack of transparency and accountability creates a chilling effect, deterring dissent and democratic participation.⁷

² Ibid

³ Information Technology Act 2000

⁴ Sandra Wachter, Brent Mittelstadt and Chris Russell, ‘Why Fairness Cannot Be Automated’ (2021) 13(3) Harvard Journal of Law & Technology

⁵ Digital Personal Data Protection Bill, 2023 (Draft)

⁶ Suresh Venkatasubramanian, ‘Algorithmic Bias and Justice’ in Ethics in AI (Oxford, 2021)

⁷ Internet Freedom Foundation, ‘Project Panoptic’ (2022)

Comparative International Legal Landscape

- 1. European Union:** The General Data Protection Regulation (GDPR) and the proposed EU Artificial Intelligence Act exemplify a rights-based approach. They mandate risk-based classification, transparency, human-in-the-loop decision-making, and accountability.⁸
- 2. United States:** Though lacking a comprehensive federal AI law, the U.S. has sector-specific statutes like the California Consumer Privacy Act (CCPA).⁹ While these promote consumer autonomy, they remain fragmented and insufficient for nationwide AI governance.
- 3. Global Normative Instruments:** The OECD's AI Principles¹⁰ and UNESCO's Ethics Recommendation¹¹ advocate for fairness, accountability, and transparency in AI design. Though non-binding, these guidelines reflect international consensus on ethical AI deployment.

Legislative Imperatives for India

India must enact sui generis legislation that incorporates:

- **Algorithmic Explainability and Interpretability:** Essential for ensuring procedural fairness and contestability.
- **Accountability of AI Developers and Deployers:** Legal liability for harms resulting from negligence or bias.
- **Human Oversight and Audit Trails:** High-risk decisions should be subject to human review.
- **Strong Data Fiduciary Obligations:** Tailored to AI's inferential and dynamic nature.
- **Civil Remedies and Regulatory Enforcement:** Empower users and regulators to act against AI-induced rights violations.

Recommendations

To ensure AI is deployed responsibly and ethically within India's democratic framework:

- Enact a dedicated AI law guided by risk classification and rights-based principles.
- Mandate algorithmic transparency, regular audits, and public reporting for high-risk AI.
- Establish a specialized AI regulatory authority.
- Encourage multi-stakeholder collaboration technologists, jurists, civil society, and industry.
- Promote AI literacy and data rights awareness among the public.

⁸ European Commission, Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) COM/2021/206 final.

⁹ California Consumer Privacy Act, 2018 (CCPA), Cal. Civ. Code § 1798.100 et seq.

¹⁰ OECD, 'OECD Principles on Artificial Intelligence' (2019).

¹¹ UNESCO, 'Recommendation on the Ethics of Artificial Intelligence' (2021).

Conclusion

Artificial Intelligence has the potential to transform society, but its unregulated deployment risks undermining individual freedoms and democratic values. The current legal framework in India is insufficient to address the multifaceted challenges posed by AI. A robust, rights-based, and transparent regulatory architecture is imperative. India must look toward global best practices while ensuring its laws remain rooted in constitutional morality. Only through a proactive and thoughtful approach can AI serve the public good without compromising fundamental rights.