SUPREMO AMICUS

VOLUME 40 | February, 2026 ISSN 2456-9704

ARTIFICIAL INTELLIGENCE AND PRIVACY IN INDIA: NAVIGATING THE FINE LINE BETWEEN INNOVATION AND FUNDAMENTAL RIGHTS

By *Gaurang Singh*
From *B. P. Singh Law College, Khanpur Satwan, Kaushambi, Prayagraj, Uttar Pradesh*

Abstract

India is witnessing a technological revolution with Artificial Intelligence (AI) penetrating diverse sectors, from healthcare and finance to governance and law enforcement. While AI promises efficiency, innovation, and economic growth, it raises unprecedented concerns regarding the protection of individual privacy and fundamental rights under the Indian Constitution. This article explores the intersection of AI and privacy laws in India, critically analyzing the adequacy of existing legal frameworks such as the Information Technology Act, 2000, and the Personal Data Protection Bill, 2019. Through case studies, judicial interventions, and comparative international perspectives, it argues that India must adopt a balanced regulatory approach that safeguards citizens' privacy without stifling technological progress. The article concludes with actionable recommendations for policymakers, emphasizing the need for transparency, accountability, and ethical AI deployment in harmony with constitutional guarantees.

Keywords

- Artificial Intelligence
- Privacy Law
- Fundamental Rights
- Data Protection
- India
- Ethical AI

Article Outline

I. Introduction
- Background: AI adoption in India
- Why privacy matters in AI era
- Research question / purpose

II. Conceptual Framework
- Definition of AI & Privacy
- Fundamental Rights under Indian Constitution (Article 21, 19, etc.)
- Global perspective: EU GDPR, US, etc.

III. Current Legal Landscape in India
- IT Act, 2000 (provisions related to data & privacy)
- Personal Data Protection Bill, 2019: Key highlights & gaps
- Judicial interpretations: Puttaswamy v. Union of India, etc.

IV. Challenges & Issues
- Mass data collection & surveillance
- Algorithmic bias & discrimination
- Consent & awareness issues
- Corporate vs government accountability

V. Case Studies & Comparative Analysis
- Real-life examples of AI misuse / privacy breach in India
- International case studies (EU, US)

VI. Policy & Regulatory Recommendations
- Balanced regulatory framework
- Ethical AI guidelines
- Transparency, accountability & public awareness
- Role of judiciary & legislature

VII. Conclusion
- Summarize findings
- Future outlook
- Call for responsible AI development

VOLUME 40 | February, 2026 ISSN 2456-9704

I. Introduction

Artificial Intelligence (AI) is no longer a futuristic concept; it has become an integral part of India's social, economic, and technological landscape. From healthcare diagnostics to predictive policing, AI-driven solutions are reshaping the way individuals interact with technology, businesses operate, and governments deliver services. While these developments promise efficiency, innovation, and economic growth, they also bring unprecedented challenges — chief among them, the protection of individual privacy. In an era where personal data is collected, analyzed, and stored at an unprecedented scale, the question arises: how can India balance rapid technological advancement with the fundamental right to privacy?

India's legal system has historically struggled to keep pace with technological innovations. Although the Information Technology Act, 2000 provides certain safeguards against cyber intrusions and unauthorized data access, it was not designed with AI in mind. More recently, the Personal Data Protection Bill, 2019, attempts to bridge this gap by laying down principles for the collection, storage, and processing of personal data. However, challenges remain, particularly concerning consent, algorithmic decision-making, and corporate accountability. Moreover, judicial interventions, most notably in Puttaswamy v. Union of India (2017), have recognized privacy as a fundamental right, yet the practical enforcement of this right in the context of AI is still evolving.

This article aims to explore the complex intersection of AI and privacy laws in India. It examines the current legal framework, identifies gaps and challenges, and offers actionable recommendations for policymakers, researchers, and industry stakeholders. By combining a socio-legal perspective with case studies and comparative international insights, this paper seeks to provide a roadmap for responsible and ethical AI deployment that aligns with India's constitutional values.

II. Conceptual Framework

To meaningfully discuss AI and privacy in India, it is essential to establish a conceptual framework that clarifies key terms and contextualizes the issues.

A. Artificial Intelligence (AI)

AI refers to computer systems capable of performing tasks that typically require human intelligence, including learning, reasoning, problem-solving, and decision-making. In the Indian context, AI applications span diverse sectors such as finance, education, healthcare, agriculture, and law enforcement. While AI has the potential to transform public service delivery and business operations, it also introduces risks related to data misuse, algorithmic bias, and surveillance.

B. Privacy

Privacy is the right of individuals to control access to their personal information and protect themselves from unwarranted intrusion. Recognized as a fundamental right under Article 21 of the Indian Constitution, privacy is crucial in safeguarding human dignity and autonomy. In the context of AI, privacy concerns extend beyond traditional notions of secrecy, encompassing data collection, algorithmic profiling, and automated decision-making.

C. The Intersection of AI and Privacy

The convergence of AI and personal data collection creates unique legal and ethical challenges. Unlike conventional technology, AI systems often operate as "black boxes", making it difficult for users to understand how their data is processed or decisions are made.

This opacity raises questions about accountability, consent, and legal enforceability. Internationally, frameworks like the European Union's General Data Protection Regulation (GDPR) emphasize

transparency, data minimization, and user control, providing lessons for India's evolving regulatory landscape.

III. Current Legal Landscape in India

India's legal framework governing AI and privacy is evolving but faces significant challenges in keeping pace with technological advancements. The main pillars of this landscape are the Information Technology Act, 2000 (IT Act), the Personal Data Protection Bill, 2019 (PDP Bill), and judicial interpretations of the fundamental right to privacy.

A. Information Technology Act, 2000

The IT Act, 2000, was India's first comprehensive attempt to regulate electronic communication, data storage, and cybercrime. Key provisions related to data protection include:

- ★ Section 43A: Mandates compensation for negligence in handling sensitive personal data or information.
- ★ Reasonable Security Practices & Procedures: Organizations collecting sensitive personal data must implement safeguards.

Limitations:

- ★ The IT Act was drafted in an era when AI and machine learning were largely nascent; it does not address automated decision-making, algorithmic bias, or the opaque nature of AI systems.
- ★ Definitions of sensitive data are limited and may not cover modern AI data collection practices such as behavioral profiling or biometric analytics.

B. Personal Data Protection Bill, 2019

The PDP Bill represents India's most significant step towards comprehensive data protection. It draws inspiration from the European Union's GDPR, aiming to give individuals greater control over personal data. Key features include:

- ★ Data Principal Rights: Right to access, correction, and erasure of personal data.
- ★ Consent Requirement: Organizations must obtain informed consent before collecting or processing personal data.
- ★ Data Fiduciary Obligations: Entities processing data must follow principles of purpose limitation, storage limitation, and accountability.

Challenges in AI Context:

- ★ AI systems often process large datasets with minimal human intervention, making informed consent difficult to implement.
- ★ Algorithmic decision-making may lead to profiling or discrimination without clear transparency.
- ★ Enforcement mechanisms are still under development; the Data Protection Authority has yet to be established.

C. Judicial Interpretations

The Supreme Court of India, in Justice K.S. Puttaswamy v. Union of India (2017), recognized privacy as a fundamental right under Article 21. This landmark judgment laid the foundation for future legal discourse on AI and privacy:

- ★ Reasonable Expectation of Privacy: Citizens have a right to control their personal information.
- ★ Balancing Test: Any restriction on privacy must be lawful, necessary, and proportionate.

Application to AI:

- ★ Automated systems and mass data collection programs, such as the Aadhaar scheme, have faced scrutiny for potential privacy violations.
- ★ Courts emphasize that technological advancement cannot override constitutional safeguards, reinforcing the need for regulatory frameworks tailored to AI.

D. Comparative Perspective

While India's legal framework is evolving, countries like the EU, USA, and Singapore have adopted AI-specific guidelines and privacy regulations:

★ EU GDPR: Strong focus on transparency, accountability, and rights of automated decision-making.

★ USA: Sectoral approach, emphasizing self-regulation with limited federal oversight.

★ Singapore Model AI Governance Framework: Voluntary principles for ethical AI deployment.

India's challenge lies in adapting existing laws to AI realities while protecting citizens' fundamental rights.

Summary of this section:

➢ IT Act provides basic safeguards but is outdated for AI.

➢ PDP Bill introduces comprehensive data protection but faces implementation challenges.

➢ Judicial recognition of privacy strengthens citizens' rights.

➢ International frameworks offer lessons for India's evolving AI privacy laws.

IV. Challenges & Issues in AI and Privacy in India

While Artificial Intelligence (AI) offers transformative potential, it simultaneously introduces complex challenges that strain existing legal frameworks and raise ethical concerns. The primary challenges in India can be categorized as follows:

A. Mass Data Collection & Surveillance

AI systems rely on large datasets to function effectively. In India, initiatives such as Aadhaar, e-governance projects, and digital health records involve collection of sensitive personal information at scale. While these programs aim to improve efficiency, they pose several privacy risks:

★ Unauthorized access: Data breaches may expose millions of citizens' personal information.

★ Mass surveillance: Continuous monitoring can lead to a surveillance state if adequate safeguards are not in place.

★ Chilling effect: Awareness of pervasive monitoring can deter individuals from exercising freedoms of expression and association.

B. Algorithmic Bias & Discrimination

AI systems learn patterns from historical data. In India, biased or incomplete datasets may lead to algorithmic discrimination, disproportionately affecting marginalized groups:

★ Examples include loan approvals, job recruitment, and predictive policing algorithms.

★ Bias may be inadvertent (reflecting historical inequalities) or structural (embedded in system design).

★ Existing Indian laws do not specifically address accountability for AI-induced discrimination.

C. Consent & Awareness Issues

A cornerstone of data protection is informed consent. In the Indian context, however:

★ Many users do not fully understand how their data is collected or used by AI applications.

★ Consent forms are often complex, legalistic, or buried in terms and conditions.

★ AI systems may process personal data in ways unforeseen by users, undermining the very principle of consent.

D. Corporate vs Government Accountability

The deployment of AI involves multiple stakeholders — private companies, government agencies, and intermediaries. Key issues include:

★ Ambiguity in liability: If an AI system misuses data or causes harm, it is unclear who is responsible.

★ Regulatory gaps: There is no comprehensive enforcement mechanism to hold corporations or government bodies accountable.
★ Profit-driven vs rights-driven priorities: Corporates may prioritize efficiency and profit over citizen privacy, while government agencies may prioritize surveillance or administrative efficiency.

E. Transparency & Explainability

AI systems are often "black boxes", producing decisions without clarity on underlying reasoning. This lack of transparency presents serious concerns:

★ Citizens cannot challenge or understand decisions affecting them, such as AI-based credit scoring or law enforcement profiling.
★ Lack of explainability hinders judicial review and accountability, undermining fundamental rights.

Summary of Challenges

1. Mass data collection threatens individual privacy and may enable surveillance.
2. Algorithmic bias risks discrimination and perpetuates societal inequities.
3. Consent and awareness gaps limit meaningful control over personal data.
4. Ambiguous accountability leaves victims without remedies.
5. Opaque AI systems prevent transparency, challenging legal and ethical norms.

India's current legal framework partially addresses these concerns, but AI-specific regulations, ethical guidelines, and robust enforcement mechanisms remain urgently needed.

V. Case Studies & Comparative Analysis

To understand the real-world implications of AI and privacy laws in India, it is essential to examine practical examples and international perspectives. These case studies illustrate the challenges and provide lessons for effective regulation.

A. Indian Case Studies

1. Aadhaar Data Breaches

The Aadhaar system, India's biometric identification initiative, has faced multiple data security incidents. Personal information, including Aadhaar numbers, addresses, and fingerprints, was reportedly leaked online due to vulnerabilities in system security.

➔ Issue: Large-scale collection of sensitive personal data without robust safeguards.
➔ Implication: Citizens' fundamental right to privacy was compromised, sparking judicial scrutiny in the Puttaswamy case.

2. AI in Law Enforcement

Predictive policing tools have been piloted in several Indian states to forecast crime hotspots. However, concerns regarding algorithmic bias and lack of transparency have emerged:

➔ Historical crime data may reinforce social prejudices, disproportionately targeting marginalized communities.
➔ Decisions made by AI systems without human oversight raise questions about accountability and legality.

3. Health Data During COVID-19

AI-driven apps for contact tracing and vaccination monitoring collected sensitive health and location data. While crucial for public health, these initiatives revealed gaps in consent mechanisms and data protection compliance.

➔ Citizens often lacked clarity on who accessed their data and for how long it would be stored.
➔ Highlights the tension between public interest and individual privacy rights.

B. International Comparative Analysis

1. European Union – GDPR & AI

The EU's General Data Protection Regulation (GDPR) sets a global benchmark for data protection:

➔ Strong emphasis on transparency, accountability, and user consent.

- ➔ Includes rights to explanation for automated decisions, directly addressing AI's black-box problem.
- ➔ Offers India valuable lessons on balancing innovation with privacy.

2. United States – Sectoral Approach

The US uses a sector-specific approach rather than comprehensive legislation:

- ➔ Certain sectors like healthcare (HIPAA) or finance have strict rules.
- ➔ AI regulation is mostly voluntary or industry-driven, highlighting a trade-off between innovation flexibility and data protection certainty.

3. Singapore – Model AI Governance Framework

Singapore provides a voluntary framework for ethical AI deployment:

- ➔ Emphasizes fairness, transparency, and human oversight.
- ➔ Encourages organizations to adopt best practices before legal mandates are introduced.

C. Lessons for India

- ➔ Indian law must evolve to integrate AI-specific provisions, drawing from GDPR and Singapore frameworks.
- ➔ Transparency and explainability should be mandatory in AI systems affecting citizens.
- ➔ Robust enforcement mechanisms are essential to ensure corporate and government accountability.
- ➔ Ethical AI principles must be embedded in policy, balancing innovation and fundamental rights.

Summary of this section:

- ➔ Real-life Indian examples highlight practical privacy risks.
- ➔ International frameworks provide guidelines and lessons for India.
- ➔ Case studies strengthen the argument for AI-specific legal reforms and ethical AI deployment.

VI. Policy & Regulatory Recommendations

Based on the analysis of India's current legal framework, challenges, and comparative international practices, this article proposes the following recommendations for policymakers, regulators, and organizations deploying AI:

A. Develop AI-Specific Legal Provisions

- ➔ India's IT Act and PDP Bill must include explicit provisions addressing AI-based decision-making, algorithmic transparency, and accountability.
- ➔ Legal recognition of algorithmic bias as a violation of fundamental rights can create enforceable standards.
- ➔ Introduce mandatory impact assessments for AI systems affecting citizens' rights.

B. Strengthen Consent and Transparency Mechanisms

- ➔ Ensure that data collection for AI is based on informed and granular consent, not buried in generic terms.
- ➔ Adopt standards for explainable AI, allowing individuals to understand how automated decisions affecting them are made.
- ➔ Encourage periodic audits by independent bodies to verify compliance with privacy norms.

C. Establish a Robust Regulatory Authority

- ➔ Create a dedicated Data Protection and AI Authority to oversee AI deployments, enforce regulations, and handle grievances.
- ➔ Authority should have powers to investigate data breaches, algorithmic discrimination, and misuse of AI in governance or commerce.
- ➔ Encourage collaboration with academic and civil society experts for continuous policy updates.

D. Promote Ethical AI Deployment

- ➔ Embed ethical guidelines in all AI applications: fairness, non-discrimination, accountability, and respect for fundamental rights.
- ➔ Encourage organizations to adopt voluntary ethical frameworks (similar to Singapore's Model AI Governance Framework) until binding legislation is established.
- ➔ Provide incentives for responsible AI practices, including certifications and public recognition.

E. Public Awareness and Capacity Building

- ➔ Educate citizens about privacy rights, consent, and AI impacts.
- ➔ Train regulators, judiciary, and law enforcement on AI's technical and legal challenges.
- ➔ Support interdisciplinary research combining law, technology, and ethics to inform policy evolution.

F. International Collaboration

- ➔ Engage with international bodies to harmonize AI and privacy standards, ensuring that India's AI ecosystem is globally competitive yet rights-compliant.
- ➔ Learn from GDPR, US sectoral approach, and Singapore's model to create context-specific regulations that reflect India's socio-legal realities.

Summary of Recommendations:

1. AI-specific legal provisions to ensure accountability and fairness.
2. Stronger consent, transparency, and explainability standards.
3. A dedicated regulatory authority for AI and data protection.
4. Ethical AI deployment embedded in policy and corporate practice.
5. Public awareness and capacity-building initiatives.
6. International collaboration to align with best practices while safeguarding Indian citizens' rights.

VII. Conclusion

Artificial Intelligence is reshaping India's socio-economic landscape, offering transformative opportunities across governance, healthcare, finance, and education. However, the rapid adoption of AI also presents unprecedented challenges to the fundamental right to privacy, exposing gaps in the current legal and regulatory framework. While the IT Act, 2000 provides foundational safeguards and the Personal Data Protection Bill, 2019 attempts to strengthen privacy protections, neither fully addresses the unique risks posed by AI-driven decision-making, algorithmic bias, and mass data collection.

Through case studies, judicial interpretations, and comparative international analysis, this article has highlighted the urgent need for a balanced, proactive, and ethical approach to AI governance in India. Implementing AI-specific legal provisions, enhancing consent and transparency mechanisms, establishing a robust regulatory authority, promoting ethical deployment, and building public awareness are all crucial steps to ensure that technological innovation does not come at the cost of citizens' rights.

India stands at a crossroads: it can embrace AI responsibly, safeguarding privacy while fostering innovation, or risk undermining constitutional guarantees in the rush toward technological advancement. This article advocates for a rights-conscious, evidence-based, and forward-looking framework, ensuring that AI contributes to inclusive development without compromising the dignity and autonomy of India's citizens.

*****