



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

ARTIFICIAL INTELLIGENCE AND THE RIGHT TO PRIVACY: ASSESSING THE ADEQUACY OF INDIA'S DIGITAL PERSONAL DATA PROTECTION ACT, 2023

-Vaniya Arzoo

ABSTRACT

Artificial Intelligence (AI) has become an integral part of modern governance, commerce, healthcare, finance, education, and law enforcement. AI systems rely heavily on the collection, processing, and analysis of personal data to generate predictions, automate decisions, and improve efficiency. While AI offers unprecedented opportunities for economic growth and technological advancement, it also poses significant threats to the fundamental right to privacy. In India, the enactment of the Digital Personal Data Protection Act, 2023 (DPDP Act, 2023) marks a major legislative milestone in regulating personal data. However, the growing sophistication of AI raises important legal questions regarding the adequacy of the Act in safeguarding individual privacy. This article critically examines the DPDP Act, 2023 from a legal perspective and evaluates whether it effectively addresses the privacy challenges posed by AI technologies. It concludes that although the Act establishes a comprehensive framework for personal data protection, significant legislative and regulatory gaps remain concerning algorithmic transparency, automated decision-making, biometric surveillance, and accountability.

INTRODUCTION

Artificial Intelligence has transformed the digital ecosystem by enabling machines to perform tasks traditionally requiring human intelligence. AI applications include facial recognition, predictive policing, recommendation systems, autonomous vehicles, healthcare diagnostics,

credit scoring, recruitment, and digital governance. These technologies process enormous quantities of personal information, making privacy protection increasingly complex. The right to privacy in India attained constitutional recognition through the landmark judgment of Justice K. S. Puttaswamy.¹ The Supreme Court unanimously declared privacy to be a fundamental right protected under Article 21 and other provisions of the Constitution.² The Court also emphasized informational privacy and recognized the State's obligation to protect citizens against unauthorized data collection and misuse. Following this constitutional mandate, Parliament enacted the Digital Personal Data Protection Act, 2023³ to regulate the processing of digital personal data. While the legislation represents a significant advancement in India's data protection framework, the rapid evolution of AI raises concerns about whether existing legal safeguards adequately address emerging privacy risks.

AI systems depend upon vast quantities of personal information collected through smartphones, social media platforms, banking systems, healthcare databases, surveillance cameras, and government records. Machine learning algorithms continuously process this information to improve decision-making capabilities. However, AI poses several privacy challenges:

1. Mass Data Collection: AI systems require extensive datasets for training. Organizations frequently collect personal information beyond what is necessary, increasing the risk of misuse.
2. Automated Decision-Making: AI increasingly makes decisions regarding employment, education, insurance, banking, and criminal justice without meaningful human intervention. Such decisions may adversely affect individuals without transparency or explanation.
3. Profiling: AI creates detailed behavioral profiles by combining multiple sources of personal information. Profiling enables organizations to predict preferences, financial status, political beliefs, or health conditions.

¹ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (India).

² The Indian Constitution, article 21.

³ Digital Personal Data Protection Act, No. 22 of 2023, Acts of Parliament, 2023 (India).

4. Facial Recognition and Surveillance: Governments and private entities increasingly deploy facial recognition systems capable of tracking individuals in public spaces, potentially undermining anonymity and freedom.⁴

5. Data Breaches: Large AI databases become attractive targets for cybercriminals, exposing sensitive personal information to unauthorized access.

6. Algorithmic Bias: AI systems trained on biased datasets may discriminate against marginalized communities, affecting equality and dignity.

These challenges demonstrate that privacy protection in the AI era extends beyond preventing unauthorized disclosure of data; it also requires regulating how algorithms collect, infer, analyze, and utilize personal information.

THE CONSTITUTIONAL RIGHT TO PRIVACY

The constitutional foundation of privacy law in India originates from the Supreme Court's decision in Justice K. S. Puttaswamy (Retd.) v. Union of India. The Court held that privacy is intrinsic to life and personal liberty under Article 21 and forms part of the freedoms guaranteed by Part III of the Constitution.⁵

The judgment identified three important aspects of privacy: Bodily privacy, Informational privacy, Decisional autonomy

The Court further held that any infringement of privacy must satisfy the following requirements: Legitimate State purpose, Necessity, Proportionality, Procedural safeguards

These constitutional principles serve as the benchmark for evaluating the DPDP Act, 2023.

OVERVIEW OF THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

The DPDP Act, 2023 governs the processing of digital personal data by both public and private entities.⁶

⁴ UNESCO, *Recommendation on the Ethics of Artificial Intelligence* (2021).overview

⁵ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (India).

⁶ Digital Personal Data Protection Act, No. 22 of 2023, Acts of Parliament, 2023 (India).

Its primary objectives include: protection of personal data, recognition of individual rights, regulation of data fiduciaries, promotion of responsible data processing, facilitation of the digital economy. Major features include Consent-Based Processing: Processing generally requires free, informed, specific, unconditional, and unambiguous consent.⁷

RIGHTS OF DATA PRINCIPALS

Individuals possess several statutory rights, including right to access information, Right to correction, Right to erasure, Right to grievance redressal, Right to nominate another person.⁸

DUTIES OF DATA FIDUCIARIES

Organizations processing personal data must ensure data security, notify breaches, delete unnecessary information, process data only for lawful purposes.^{9,10}

SIGNIFICANT DATA FIDUCIARIES

Entities processing substantial quantities of personal data may be designated Significant Data Fiduciaries and become subject to additional compliance obligations, including: appointment of Data Protection Officers, Independent data audits, Periodic impact assessments

DATA PROTECTION BOARD

The Act establishes the Data Protection Board of India for adjudication and enforcement. Although the Act introduces important privacy safeguards, several challenges arise when applied to AI technologies.

1. Consent Fatigue

The Act emphasizes consent as the primary legal basis for data processing. However, AI systems often involve lengthy privacy policies that users rarely understand. Consequently, consent may become merely formal rather than genuinely informed. In AI-driven environments, meaningful consent requires greater transparency regarding: types of algorithms used, purpose

⁷ Digital Personal Data Protection Act, 2023, Section 4–6.

⁸ Digital Personal Data Protection Act, 2023, Section 11–15.

⁹ Digital Personal Data Protection Act, 2023, Section 8–10.

¹⁰ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (India).

of profiling, automated decision-making, future data usage. The Act does not sufficiently mandate such disclosures.

2. Automated Decision-Making

One significant limitation is the absence of explicit regulation concerning automated decision-making. Many foreign jurisdictions provide individuals the right to object to automated decisions, to seek human review, and, to receive explanations. The DPDP Act does not expressly recognize these rights, leaving individuals vulnerable to opaque AI decisions affecting employment, education, healthcare, insurance, and financial services.

3. Algorithmic Transparency

AI systems often function as "black boxes," where even developers struggle to explain decision-making processes. The Act primarily regulates personal data processing rather than algorithmic accountability. It does not require: explainable AI, transparency reports, disclosure of training datasets, fairness assessments, or algorithmic auditing. Consequently, individuals may remain unaware of how AI reached decisions affecting their legal rights.

4. Profiling and Behavioural Analytics

AI enables extensive profiling by combining data from multiple platforms. Although profiling significantly impacts privacy, the Act contains no comprehensive legal framework regulating AI profiling. This creates opportunities for excessive surveillance, targeted manipulation, and discriminatory practices.

5. Government Exemptions

The DPDP Act grants broad exemptions permitting government agencies to process personal data under specified circumstances. While national security and public order constitute legitimate objectives, broad exemptions without sufficient judicial oversight may weaken constitutional privacy protections. Given increasing governmental use of AI-powered surveillance technologies, stronger procedural safeguards would enhance accountability.

6. Cross-Border Data Transfers

AI development often involves multinational cloud infrastructure and international datasets. The Act allows cross-border transfers except to restricted jurisdictions notified by the Central Government. While this facilitates technological innovation, stronger international privacy standards and interoperability mechanisms remain necessary.

7. Children's Data

The Act introduces enhanced protections for children's personal data. However, AI-powered educational platforms, gaming applications, and social media increasingly collect behavioural information from minors. Future regulations should specifically address AI-based profiling of children.

COMPARATIVE PERSPECTIVE

International legal frameworks provide useful guidance for strengthening India's AI governance. The General Data Protection Regulation (GDPR) contains stronger protections relating to automated decision-making under Article 22. Individuals have the right not to be subject solely to automated decisions producing legal or similarly significant effects. Similarly, the EU Artificial Intelligence Act adopts a risk-based regulatory framework, classifying AI systems according to their potential impact and imposing stringent obligations on high-risk applications. Compared with these frameworks, India's DPDP Act remains largely technology-neutral and does not comprehensively regulate AI-specific risks.

JUDICIAL DEVELOPMENTS

Indian courts increasingly recognize informational privacy as essential to constitutional democracy. The Supreme Court has consistently emphasized that technological advancement cannot override constitutional guarantees. The principles established in **Puttaswamy** require future AI regulation to balance innovation with transparency, accountability, proportionality, fairness, and protection of human **dignity**. These constitutional values should guide judicial interpretation of the DPDP Act.

CHALLENGES IN IMPLEMENTATION

Several practical challenges may affect the effectiveness of the Act: limited public awareness regarding data rights, shortage of AI regulatory expertise, rapid technological evolution,

difficulties in enforcing cross-border obligations, limited algorithmic transparency, inadequate mechanisms for AI accountability, broad governmental exemptions, lack of specialized AI oversight institutions, without robust implementation, statutory rights may remain largely theoretical.

RECOMMENDATIONS

To strengthen privacy protection in the AI era, India should consider the following reforms:

1. Enact dedicated AI legislation complementing the DPDP Act.
2. Introduce explicit rights against fully automated decision-making.
3. Mandate explainable AI for high-risk applications.
4. Require periodic algorithmic impact assessments.
5. Strengthen regulation of biometric surveillance technologies.
6. Narrow government exemptions through greater judicial oversight.
7. Establish an independent AI Regulatory Authority.
8. Promote privacy-by-design and ethical AI standards.
9. Introduce stronger accountability for AI developers and deployers.
10. Harmonize Indian law with emerging international AI governance frameworks while preserving constitutional protections.

CONCLUSION

Artificial Intelligence represents one of the most transformative technological developments of the twenty-first century. Its ability to process massive volumes of personal information creates unprecedented opportunities for innovation but simultaneously threatens informational privacy, autonomy, equality, and human dignity.

The Digital Personal Data Protection Act, 2023 is a landmark legislative initiative that establishes a foundational framework for personal data protection in India. By recognizing consent, imposing obligations on data fiduciaries, and creating institutional mechanisms for enforcement, the Act advances the constitutional vision articulated in *Puttaswamy*. Nevertheless, the legislation was designed primarily as a data protection statute rather than a comprehensive AI governance framework. It does not adequately regulate automated decision-making, algorithmic transparency, AI-driven profiling, or explainability, nor does it provide

sufficient safeguards against large-scale surveillance and opaque algorithmic practices. As AI systems become increasingly embedded in public administration and private decision-making, India's legal framework must evolve beyond traditional data protection principles. A comprehensive regulatory approach that integrates constitutional values, technological accountability, ethical AI standards, and robust enforcement mechanisms is essential. Strengthening the DPDP Act through AI-specific reforms will enable India to foster technological innovation while preserving the fundamental right to privacy, ensuring that the advancement of artificial intelligence remains consistent with the rule of law and the constitutional commitment to individual liberty and human dignity.