International Journal of Law Research, Education and Social Sciences

Open Access Journal – Copyright © 2026 – ISSN 3048-7501
Editor-in-Chief – Prof. (Dr.) Vageshwari Deswal; Publisher – Sakshi Batham

Artificial Intelligence and the Right to Privacy in India

Deshika T.K[a]

[a]JSS Law College, Mysuru, India

Received 11 June 2026; Accepted 11 July 2026; Published 14 July 2026

The rapid proliferation of artificial intelligence (AI) technologies in India presents profound challenges to the constitutional right to privacy, necessitating a comprehensive legal analysis of the existing regulatory framework and its adequacy in addressing emerging threats. This article examines the intersection of AI governance and privacy rights within the Indian legal landscape, tracing the constitutional evolution of privacy jurisprudence from the landmark decision in Justice K.S. Puttaswamy (Retd.) v Union of India (2017) to the enactment of the Digital Personal Data Protection Act 2023 and the India AI Governance Guidelines, 2025. The analysis explores how AI- driven technologies, including facial recognition systems, predictive policing algorithms, biometric surveillance through Aadhaar, and automated decision-making systems, create unprecedented threats to informational privacy, bodily integrity, and decisional autonomy. The article critically evaluates the adequacy of existing legislative mechanisms, identifying significant gaps in algorithmic accountability, consent frameworks for AI training data, and the absence of dedicated AI-specific legislation. Through comparative analysis with international regulatory approaches, particularly the European Union General Data Protection Regulation and the EU AI Act, this study highlights both convergence and divergence in privacy protection standards. The findings suggest that while India has made significant strides in establishing a data protection framework, substantial reforms are necessary to address the autonomous and predictive capabilities of AI systems, ensure meaningful consent, and establish robust institutional mechanisms for enforcement and oversight.

Keywords: *artificial intelligence, data protection, algorithmic accountability, surveillance, constitutional rights.*

INTRODUTION

The twenty-first century has witnessed an unprecedented transformation in the relationship between technology and individual rights. Artificial intelligence, as a general-purpose technology, has permeated virtually every domain of human activity, from healthcare diagnostics and criminal justice to financial services and social media platforms.[1] In India, this technological revolution has been accelerated by the government's ambitious Digital India initiative, which aims to transform the country into a digitally empowered society and knowledge economy.[2] However, this rapid digitalisation has simultaneously created new and formidable challenges to the fundamental right to privacy, which the Supreme Court of India unequivocally recognised as a constitutionally protected right in the landmark decision of Justice K.S. Puttaswamy (Retd.) v Union of India.[3]

The intersection of artificial intelligence and privacy rights presents unique and multifaceted challenges. AI systems, by their very nature, require vast quantities of data to function effectively, creating an inherent tension between technological advancement and individual privacy.[4] Machine learning algorithms process personal data at scales previously unimaginable, identifying patterns, making predictions, and generating insights that can profoundly affect individual lives, often without their knowledge or meaningful consent.[5] In the Indian context, this challenge is particularly acute given the country's massive population, its rapidly expanding digital economy, and the government's increasing reliance on technology-driven governance mechanisms.

The concerns are not merely theoretical. AI-powered facial recognition systems are being deployed across Indian cities for law enforcement and public safety purposes, often without

[1] Esmat Zaidan and Imad Antoine Ibrahim, 'AI Governance in a Complex and Rapidly Changing Regulatory Landscape: A Global Perspective' (2024) 11 Humanities and Social Sciences Communications <https://doi.org/10.1057/s41599-024-03560-x> accessed 10 June 2026
[2] *India AI Governance Guidelines* (Ministry of Electronics and Information Technology (MeitY), 2025)
[3] *Justice K S Puttaswamy (Retd) & Anr v Union of India & Ors* (2017) 10 SCC 1
[4] Changwu Huang et al., 'An Overview of Artificial Intelligence Ethics' (2022) (4)4 IEEE Transactions on Artificial Intelligence <https://doi.org/10.1109/tai.2022.3194503> accessed 10 June 2026
[5] Usha Tandon and Neeral Kumar Gupta, 'Informational Privacy in the Age of Artificial Intelligence: A Critical Analysis of India DPDP Act, 2023' (2025) 6(2) Legal Issues in the Digital Age <https://doi.org/10.17323/2713-2749.2025.2.87.117> accessed 10 June 2026

adequate legal frameworks or oversight mechanisms.[6] The Aadhaar system, the world's largest biometric identification programme, collects and processes the biometric data of over 1.3 billion Indians, creating a comprehensive digital identity infrastructure that raises significant surveillance concerns.[7] Predictive policing algorithms are being adopted by law enforcement agencies, potentially entrenching existing biases and discrimination.[8] These developments, occurring in a regulatory environment that is still adapting to the challenges of the digital age, underscore the urgency of a comprehensive legal analysis.

This article seeks to address this lacuna by providing a thorough examination of the legal, constitutional, and policy dimensions of artificial intelligence and the right to privacy in India. It traces the constitutional evolution of privacy rights, analyses the specific privacy implications of various AI technologies, evaluates the adequacy of the existing legislative framework, including the Digital Personal Data Protection Act, 2023 (DPDP Act) and the India AI Governance Guidelines, 2025, and offers comparative perspectives from international regulatory approaches. The article concludes with recommendations for reform aimed at ensuring that India's legal framework is adequate to meet the challenges posed by the AI revolution while safeguarding the fundamental right to privacy.

CONSTITUTIONAL EVOLUTION OF PRIVACY RIGHTS IN INDIA

Pre-Puttaswamy Jurisprudence: The constitutional trajectory of the right to privacy in India has been neither linear nor straightforward. Unlike the Fourth Amendment to the United States Constitution, which expressly protects against unreasonable searches and seizures, the Indian Constitution does not contain an express right to privacy.[9] This absence of explicit textual protection led to decades of judicial uncertainty regarding the constitutional status of privacy rights.

---

[6] Imad A Basheer, 'Bias in the Algorithm: Issues Raised Due to Use of Facial Recognition in India' (2024) 10(1) Journal of Development Policy and Practice <https://doi.org/10.1177/24551333241283992> accessed 10 June 2026

[7] Ameya Bondre et al., 'Protecting Mental Health Data Privacy in India: The Case of Data Linkage with Aadhaar' (2021) 9(3) Global Health Science and Practice <https://www.ghspjournal.org/content/9/3/467> accessed 25 July 2026

[8] Navin Kumar, 'The Role of Artificial Intelligence in Criminal Investigations in India' (2025) 35(49) Journal of Legal Studies <https://doi.org/10.2478/jles-2025-0006> accessed 10 June 2026

[9] *M P Sharma & Ors v Satish Chandra, District Magistrate, Delhi, and Ors* (1954) SCR 1077

The early jurisprudence on privacy was characterised by an express denial of its constitutional protection. In M.P. Sharma v Satish Chandra, an eight-judge bench of the Supreme Court held that the right to privacy was not a fundamental right guaranteed by the Indian Constitution, reasoning that in the absence of a provision equivalent to the Fourth Amendment of the US Constitution, no such right could be read into the constitutional framework. This decision was followed by Kharak Singh v State of U.P.,[10] where a six-judge bench reiterated this position, holding that the right to privacy was not a guaranteed fundamental right, although Justice Subba Rao, in a lone dissent, presciently argued that privacy was implicit in the concept of ordered liberty.

However, the Supreme Court subsequently began to expand the scope of Article 21, which guarantees the right to life and personal liberty, to include rights not explicitly enumerated in the constitutional text. In Gobind v State of MP,[11] the Court recognised that the right to privacy, while not absolute, was a constitutionally protected right, at least insofar as it related to personal liberty. This expansion continued through a series of decisions, including PUCL v Union of India,[12] which addressed phone tapping and surveillance; District Registrar and Collector v Canara Bank,[13] which concerned the disclosure of bank records; Mr X v Hospital Z,[14] which dealt with the disclosure of medical records; and Selvi v State of Karnataka,[15] which addressed the admissibility of evidence obtained through invasive police interrogation techniques.

The Puttaswamy Decision: A Constitutional Watershed: The constitutional landscape was irrevocably transformed on 24 August 2017, when a nine-judge bench of the Supreme Court delivered its unanimous judgement in Justice K.S. Puttaswamy (Retd.) v Union of India.[16] This historic decision unequivocally declared that the right to privacy is a fundamental right protected under the Constitution, intrinsic to the right to life and personal liberty under Article 21, and also protected under Articles 14 and 19.

[10] *Kharak Singh v State of U P & Ors* (1964) 1 SCR 332
[11] *Gobind v State of Madhya Pradesh & Anr* (1975) 2 SCC 148
[12] *People's Union for Civil Liberties v Union of India & Anr* (1997) 1 SCC 301
[13] *District Registrar and Collector, Hyderabad & Anr v Canara Bank Etc* (2005) 1 SCC 496
[14] *Mr X v Hospital Z* (1998) 8 SCC 296
[15] *Smt Selvi & Ors v State of Karnataka* (2010) 7 SCC 263
[16] *Justice K S Puttaswamy (Retd) & Anr v Union of India & Ors* (2017) 10 SCC 1

The judgement explicitly overruled the earlier decisions in M.P. Sharma and Kharak Singh to the extent that they denied the existence of a fundamental right to privacy. Justice D.Y. Chandrachud, writing on behalf of Chief Justice J.S. Khehar and Justices R.K. Agarwal and S.A. Bobde, held that privacy is "a natural right that pre-exists the Constitution" and that the Constitution "merely recognises, rather than creates" this right. This assertion placed privacy in the same moral and philosophical category as liberty and equality, elevating it beyond the realm of statutory protection to the status of an inviolable constitutional guarantee.

The Court conceptualised privacy across three interconnected dimensions: bodily privacy, informational privacy, and decisional autonomy. Bodily privacy protects individuals from intrusive physical interventions and surveillance. Informational privacy safeguards control over personal data and the right to determine how personal information is collected, used, and disseminated. Decisional autonomy protects intimate personal choices relating to marriage, sexuality, procreation, and family life. This tripartite framework has profound implications for the regulation of AI technologies, which often implicate all three dimensions simultaneously.

The Proportionality Framework: The Puttaswamy judgement established a rigorous threefold test for evaluating any state interference with the right to privacy: legality; legitimate state aim, and proportionality. Under the legality requirement, any restriction on privacy must be authorised by law. The legitimate state aim requirement mandates that the intrusion must serve a recognised public purpose. The proportionality test requires that the means adopted must be rationally connected to the objective and represent the least restrictive means of achieving the legitimate aim.

Justice Sanjay Kishan Kaul, in his separate concurring opinion, added a fourth element: procedural safeguards against abuse. This addition echoes Article 21's central requirement of having a "procedure established by law" and reinforces the principle that even constitutionally permissible restrictions on privacy must be accompanied by adequate safeguards to prevent arbitrary exercise of power.

The proportionality framework established in Puttaswamy has become the controlling analytical tool for evaluating state actions involving large-scale data collection and surveillance.[17] Its application to AI governance is particularly significant, as it requires that any deployment of AI technologies that impacts privacy must satisfy the tests of legality, necessity, and proportionality. This framework provides a constitutional foundation for challenging AI systems that collect, process, or utilise personal data without adequate safeguards or proportionate justification.

ARTIFICIAL INTELLIGENCE TECHNOLOGIES AND PRIVACY IMPLICATIONS

Defining AI in the Indian Context: Artificial intelligence, broadly defined, refers to computational systems designed to perform tasks that typically require human intelligence, including learning, reasoning, problem-solving, and decision-making.[18] In the Indian context, AI encompasses a wide range of technologies, from natural language processing and computer vision to machine learning algorithms and neural networks. The National Strategy for Artificial Intelligence, released by NITI Aayog in 2018, identified five priority sectors for AI deployment in India: healthcare, agriculture, education, smart cities, and smart mobility.

The privacy implications of AI are multifaceted and context-dependent. AI systems typically require large datasets for training, which often include personal data. The algorithms process this data to identify patterns and generate predictions, which can then be used to make decisions that affect individual lives. The "black box" nature of many AI systems, particularly deep learning models, creates additional challenges, as the decision-making processes may be opaque even to the developers who created them.[19]

Data Collection and Processing Challenges: The fundamental privacy challenge posed by AI lies in the data collection and processing required for its functioning. AI systems operate on the principle that more data leads to better performance, creating powerful incentives for extensive data collection.[20] In India, where digital adoption has been accelerating rapidly, the

[17] Prateek Bagra, 'Right to Privacy as a Fundamental Right in India: An Analysis of the Puttaswamy Judgement' (*Record of Law,* 03 December 2025) <https://recordoflaw.in/right-to-privacy-as-a-fundamental-right-in-india-an-analysis-of-the-puttaswamy-judgment/> accessed 10 June 2026
[18] *NATIONAL STRATEGY FOR ARTIFICIAL INTELLIGENCE #AIFORALL* (NITI Aayog, 2018)
[19] Ameet Datta et al., 'Data privacy considerations surrounding AI use in India' (*Law.Asia,* 02 April 2025) <https://law.asia/ai-and-data-protection/> accessed 10 June 2026
[20] *Handbook on Data Protection and Privacy for Developers of Artificial Intelligence (AI) in India* (NASSCOM, 2026)

volume of personal data generated by individuals through their interactions with digital services, social media platforms, and government databases is growing exponentially.

The DPDP Act defines "processing" to include "any automated operation or set of operations performed on digital personal data," which captures the vast majority of AI-related data operations.[21] However, the Act's reliance on consent as the primary basis for processing creates significant challenges in the AI context, where data may be collected for one purpose but subsequently used to train algorithms for entirely different applications.[22] The practice of scraping publicly available data from the internet to train AI models, which has become widespread among technology companies, operates in a legal grey area under the DPDP Act.[23]

Algorithms, Decision-Making and Profiling: AI-powered decision-making systems present particular challenges to informational privacy and decisional autonomy. These systems can make or influence decisions affecting individuals in critical domains such as employment, credit, healthcare, and criminal justice.[24] In India, the use of AI in credit scoring, loan approval, and insurance underwriting has raised concerns about algorithmic bias and discrimination, particularly against marginalised communities.[25]

The concept of profiling, whereby AI systems analyse personal data to create detailed individual profiles, poses a direct threat to privacy.[26] Such profiles can reveal sensitive information about individuals, including their political views, health conditions, sexual orientation, and personal relationships, often without the individual's knowledge or consent. The DPDP Act does not contain specific provisions addressing automated profiling or AI-driven decision-making, a

[21] Digital Personal Data Protection Act 2023
[22] Paarth Naithani, 'Analysis of India Digital Personal Data Protection Act, 2023' (2025) 67(5) International Journal of Law and Management <https://doi.org/10.1108/ijlma-05-2024-0174> accessed 10 June 2026
[23] Gopika Nair, 'DPDP draws the consent line for AI, but industry still sees grey zones' *The Financial Express* (28 November 2025) <https://www.financialexpress.com/business/news/dpdp-draws-the-consent-line-for-ai-but-industry-still-sees-grey-zones/4058774/> accessed 10 June 2026
[24] Helena Machado et al., 'Publics views on ethical challenges of artificial intelligence: a scoping review' (2023) 5 AI and Ethics <https://doi.org/10.1007/s43681-023-00387-1> accessed 10 June 2026
[25] Hifajatali Sayyed, 'Artificial intelligence and criminal liability in India: exploring legal implications and challenges' (2024) 10(1) Cogent Social Sciences <https://www.tandfonline.com/doi/full/10.1080/23311886.2024.2343195> accessed 10 June 2026
[26] Sakiko Fukuda-Parr and Elizabeth Gibbons, 'Emerging Consensus on 'Ethical AI': Human Rights Critique of Stakeholder Guidelines' (2021) 12(S6) Global Policy <https://doi.org/10.1111/1758-5899.12965> accessed 10 June 2026

significant lacuna compared to international frameworks such as the GDPR, which provides specific protections against decisions based solely on automated processing.[27]

THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023: A CRITICAL ANALYSIS

Overview and Legislative Context: The enactment of the Digital Personal Data Protection Act, 2023 represents a watershed moment in India's data protection landscape.[28] Enacted on 11 August 2023 after more than five years of deliberation and multiple iterations of draft legislation, the DPDP Act establishes India's first comprehensive legal framework for the collection, processing, storage, and protection of personal data.[29] The Act was conceived as a response to the constitutional mandate articulated in the Puttaswamy judgement, which called for the development of a robust data protection framework to safeguard informational privacy.

The DPDP Act applies to the processing of digital personal data within India and, significantly, to processing carried out outside India if such processing relates to offering goods or services to data principals in India.[30] This extraterritorial scope reflects the global nature of data flows and the recognition that privacy protection must extend beyond national boundaries. The Act establishes a consent-based regulatory regime, requiring data fiduciaries to obtain the consent of data principals before processing their personal data, subject to certain exceptions for legitimate uses.

Consent and Notice Requirements: The DPDP Act places significant emphasis on consent as the primary lawful basis for processing personal data. Section 4 requires that before processing personal data, a data fiduciary must provide data principals with a notice specifying the purpose of data collection and the rights available to them. The Act requires that consent must be "free, specific, informed, unconditional, unambiguous," and given through a clear affirmative action.

---

[27] General Data Protection Regulation 2016
[28] Subhajit Saha and Surjashis Mukhopadhyay, 'A New Age of Data Privacy Laws in India: Review of Digital Personal Data Protection Act, 2023' (2024) 10(1) International Journal of Law and Social Sciences <https://doi.org/10.60143/ijls.v10.i1.2024.114> accessed 10 June 2026
[29] Aashi Dixit, 'DATA PROTECTION IN INDIA AFTER THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023: A CRITICAL EVALUATION OF PRIVACY AND STATE POWER' (2026) 6(1) Indian Journal of Legal Review <https://ijlr.iledu.in/wp-content/uploads/2026/01/V6I114.pdf> accessed 10 June 2026
[30] Digital personal Data Protection Act 2023

However, the application of these consent requirements to AI systems presents several challenges. The "black box" nature of many AI systems makes it difficult to provide meaningful notice about how data will be processed. When data is used to train machine learning models, the specific purpose of processing may be difficult to define at the time of collection, as the insights generated by the algorithm may be unpredictable. Furthermore, the DPDP Act provision for "legitimate uses" allows data processing without consent in certain circumstances, including for compliance with legal obligations and the performance of statutory functions by government agencies, creating potential avenues for surveillance-oriented data processing.

Rights to Data Principals: The DPDP Act confers several rights on data principals, including the right to access information about the processing of their data, the right to correction and erasure, and the right to grievance redressal. These rights are significant for AI governance, as they potentially enable individuals to challenge AI-driven decisions that affect them and to demand transparency about how their data is being used.

However, the Act rights framework has notable limitations in the AI context. The right to erasure, while valuable, may be technically challenging to exercise in the context of AI systems, where personal data used to train algorithms may be difficult to separate from the model itself.[31] The Act does not explicitly provide for a "right to explanation" regarding AI-driven decisions, nor does it require human review of automated decisions that significantly affect individuals. These omissions stand in contrast to the GDPR, which provides specific protections in this regard under Article 22.

Government Exemptions and Surveillance Concerns: Perhaps the most contentious aspect of the DPDP Act, from a privacy perspective, is the breadth of exemptions granted to government entities. Section 17(2)(a) exempts the processing of personal data by the state for "any function which is necessary or expedient for national security or for reasons arising out of sovereignty and integrity of India."[32] Section 17(2)(b) provides a similar exemption for the

[31] Ajay Kumar Bisht and Neeruganti Shanmuka Sreenivasulu, 'Information Privacy Rights in India: A Study of the Digital Personal Data Protection Act, 2023' in Jaydip Sen (ed), *Data Privacy: Techniques, Applications, and Standards* (IntechOpen 2025)
[32] Digital Personal Data Protection Act 2023, s 17(2)(a)

processing of personal data for compliance with any law or for the performance of any statutory function.[33]

These exemptions have raised significant concerns about the potential for unchecked state surveillance. Critics argue that the broad language of these provisions could be invoked to justify mass surveillance programmes, profiling of individuals, and the creation of comprehensive databases of citizens' personal information, all without adequate judicial oversight or proportionality checks. The lack of an independent, judicially insulated data protection authority compounds these concerns, as the Data Protection Board of India established under the Act is an executive body rather than an independent regulatory commission.

THE INDIA AI GOVERNANCE GUIDELINES, 2025

Overview and Philosophy: The release of the India AI Governance Guidelines in November 2025 by the Ministry of Electronics and Information Technology (MeitY) represents India's first comprehensive framework for responsible AI development and deployment. Unlike the DPDP Act, which is binding legislation, the Guidelines are voluntary, adopting what has been described as a "techno-legal governance architecture" that emphasises accountability, transparency, and innovation-friendly regulation.[34]

The Guidelines' guiding philosophy of "innovation over restraint" reflects an attempt to balance the promotion of AI innovation with the protection of constitutional rights, including privacy. While this approach has merit in fostering a vibrant AI ecosystem, the voluntary nature of the Guidelines raises questions about their effectiveness in safeguarding privacy, particularly when voluntary compliance has proven insufficient in other jurisdictions.

Key Principles: The India AI Governance Guidelines establish several principles relevant to privacy protection. These include requirements for transparency in AI systems, including disclosure when users are interacting with AI or AI-generated content. The Guidelines explicitly link AI governance to the DPDP Act, requiring AI actors to embed privacy into their design and deployment processes. They emphasise the importance of purpose limitation, consent, and data

[33] Digital Personal Data Protection Act 2023, s 17(2)(b)
[34] 'Regulating The Machine Mind: AI, Privacy, And Intellectual Property Under India 2025 AI Governance Guidelines' (*Mondaq,* 26 November 2025) <https://www.mondaq.com/india/new-technology/1709856> accessed 10 June 2026

minimisation in AI development. The Guidelines also address the treatment of "publicly available" data in AI training, noting that the scope of this concept "remains unclear when applied to AI training." They suggest that further guidance or legislative changes may be required to address questions around consent, purpose limitation, and whether research or legitimate-use exceptions can support AI development.

Accountability and Compliance: The Guidelines recommend that persons involved in developing or deploying AI systems in India comply with all applicable laws, including those relating to information technology, data protection, copyright, and consumer protection. They call for the adoption of voluntary measures relating to privacy, security, fairness, inclusivity, non-discrimination, and transparency. The Guidelines also recommend the creation of grievance redressal mechanisms for reporting AI-related harms and the publication of transparency reports evaluating the risk of harm.

The emphasis on techno-legal solutions, including privacy-enhancing technologies, machine unlearning capabilities, algorithmic auditing systems, and automated bias detection mechanisms, reflects a recognition that traditional regulatory approaches may be insufficient for governing AI systems. However, the voluntary nature of these recommendations and the absence of enforcement mechanisms limit their practical impact.

SPECIFIC AI-DRIVEN PRIVACY CHALLENGES

Facial Recognition Technology: The deployment of Facial Recognition Technology (FRT) in India represents one of the most direct intersections of AI and privacy concerns. Indian Railways has announced plans to install FRT-based video surveillance systems in 983 railway stations across the country. Law enforcement agencies in multiple states have adopted FRT for criminal identification and surveillance purposes.

The privacy implications of FRT are profound. Unlike other forms of identification, facial recognition operates without the knowledge or consent of the subject, creating a pervasive surveillance environment that fundamentally alters the nature of public spaces.[35] Research has consistently demonstrated significant racial and gender biases in facial recognition algorithms,

[35] Shivangi Narayan, 'CCTVs and the Criminal City' (2023) 21(4) Surveillance & Society <https://doi.org/10.24908/ss.v21i4.15779> accessed 10 June 2026

with higher error rates for women, people of colour, and individuals with darker skin tones. In the Indian context, these biases could disproportionately affect already marginalised communities, raising concerns about both privacy and equality.

The deployment of FRT in India lacks a comprehensive legal framework. There is no specific legislation governing the use of facial recognition by either the state or private entities, and the existing legal framework, including the IT Act and the DPDP Act, does not adequately address the unique privacy challenges posed by this technology. The Puttaswamy proportionality test, while providing a constitutional standard, has not been systematically applied to FRT deployments.

The Aadhaar System and Biometric Surveillance: The Aadhaar system, which assigns a unique 12-digit identification number to Indian residents based on their biometric and demographic data, is the world's largest biometric identification programme, covering over 1.3 billion individuals. While the Supreme Court upheld the constitutional validity of the Aadhaar Act in the second Puttaswamy decision (2018), it significantly limited its scope, holding that Aadhaar could not be mandatory for bank accounts and mobile phones, and that private entities could not be compelled to use Aadhaar.[36]

The integration of Aadhaar with artificial intelligence creates significant privacy concerns. The linkage of biometric data with other databases and the use of AI algorithms to analyse this comprehensive dataset raise the spectre of mass surveillance.[37] The potential for the creation of detailed profiles of individuals based on their interactions with government services, financial institutions, and healthcare providers poses a direct threat to informational privacy.

Predictive Policing and Algorithmic Justice: The adoption of predictive policing algorithms by Indian law enforcement agencies presents significant privacy and equality concerns. These systems analyse historical crime data and other variables to predict where crimes are likely to occur or who is likely to commit them, informing the deployment of police resources.

---

[36] *Justice K S Puttaswamy (Retd) v union of India* (2019) 1 SCC 1

[37] Dr Sangeeta Mahapatra, 'Digital Surveillance and the Threat to Civil Liberties in India' (*German Institute for Global and Area Studies*, 03 November 2021) <https://www.giga-hamburg.de/en/publications/giga-focus/digital-surveillance-and-the-threat-to-civil-liberties-in-india> accessed 10 June 2026

The privacy implications are substantial. Predictive policing relies on the collection and analysis of vast quantities of personal data, including data from social media, surveillance systems, and criminal records. The predictive nature of these systems means that individuals may be subjected to increased police attention based not on their conduct but on algorithmic predictions, potentially infringing on their privacy and liberty without any suspicion of wrongdoing.

Research has demonstrated that predictive policing algorithms tend to reinforce and amplify existing biases in policing data, leading to the disproportionate surveillance and targeting of minority communities. In India, where caste-based and religious discrimination remain significant social issues, the deployment of biased algorithms could exacerbate existing inequalities and violate not only privacy rights but also the right to equality under Article 14.

AI in Healthcare and the Aadhaar-PHI Nexus: The intersection of AI and healthcare in India raises particular concerns about the privacy of sensitive Personal Health Information (PHI).[38] The increasing digitisation of health records, the growth of telemedicine, and the deployment of AI diagnostic tools require the processing of highly sensitive health data.[39] The linkage of health data with Aadhaar creates the potential for comprehensive health profiles that could be used for purposes beyond healthcare delivery.

Research has highlighted concerns about the potential for discrimination based on AI-processed health data, including denial of insurance coverage, employment discrimination, and stigmatisation of individuals with mental health conditions. The DPDP Act protections for personal data apply to health data, but the Act exemptions for government processing and the absence of specific provisions for health-related AI systems leave significant gaps in protection.[40]

COMPARATIVE INTERNATIONAL PERSPECTIVES

[38] Dipika Jain, 'Regulation of Digital Healthcare in India: Ethical and Legal Challenges' (2023) 11(6) Healthcare <https://doi.org/10.3390/healthcare11060911> accessed 10 June 2026
[39] Krishnan Ganapathy, 'Artificial Intelligence and Healthcare Regulatory and Legal Concerns' (2021) 6(2) Telehealth and Medicine Today <https://doi.org/10.30953/tmt.v6.252> accessed 10 June 2026
[40] Digital Personal Data Protection Act 2023

European Union: The GDPR and the AI Act: The European Union provides the most comprehensive framework for addressing the intersection of AI and privacy through its twin regulatory instruments: the General Data Protection Regulation (GDPR) and the AI Act.[41]

The GDPR, which came into effect in May 2018, establishes a robust framework for the protection of personal data, with specific provisions relevant to AI systems.[42] Article 22 of the GDPR provides individuals with the right not to be subject to decisions based solely on automated processing, including profiling, which produces legal effects or similarly significantly affects them.[43] This provision directly addresses one of the key gaps in the DPDP Act. The GDPR also requires data protection impact assessments for processing that is likely to result in a high risk to individuals' rights and freedoms, providing a proactive mechanism for addressing privacy risks associated with AI systems.

The EU AI Act, which came into force in 2024, represents the world's first comprehensive AI-specific legislation.[44] It adopts a risk-based approach, classifying AI systems into four categories: unacceptable risk (prohibited), high risk (subject to strict requirements), limited risk (subject to transparency obligations), and minimal risk (no specific requirements). High-risk AI systems, which include those used in law enforcement, employment, and critical infrastructure, are subject to requirements for data governance, transparency, human oversight, and accuracy.

Comparative Assessment: The comparison between the Indian and European approaches reveals significant divergences. India DPDP Act, while establishing important data protection principles, lacks the AI-specific provisions found in the GDPR and the EU AI Act. The absence of a provision equivalent to Article 22 GDPR, the lack of mandatory algorithmic impact assessments, and the absence of a risk classification system for AI technologies represent significant gaps in India's regulatory framework.

Furthermore, the breadth of government exemptions in the DPDP Act stands in contrast to the GDPR more limited exemptions. The absence of an independent regulatory authority, equivalent to the European Data Protection Authorities, raises concerns about the effectiveness of

[41] General Data Protection Regulation 2016; Artificial Intelligence Act 2024
[42] General Data Protection Regulation 2016
[43] General Data Protection Regulation 2016, art 22
[44] Artificial Intelligence Act 2024

enforcement. The voluntary nature of the India AI Governance Guidelines further differentiates the Indian approach from the EU binding regulatory framework.

However, India's approach also has certain advantages. The emphasis on "innovation over restraint" in the AI Governance Guidelines may foster greater technological development and deployment. The techno-legal approach, which encourages the use of privacy-enhancing technologies alongside regulatory measures, may prove more adaptable to the rapidly evolving AI landscape.

Other Comparative Perspectives: Beyond the European Union, several other jurisdictions have adopted noteworthy approaches to AI governance and privacy. The United States has adopted a sector-specific approach, with different regulatory frameworks applying to AI in healthcare, finance, and law enforcement.[45] While there is no comprehensive federal data protection law, the California Consumer Privacy Act (CCPA) provides significant privacy protection and has been influential in shaping the national debate.

China has adopted a comprehensive approach to AI governance through the Personal Information Protection Law (PIPL), the Data Security Law, and specific regulations on algorithmic recommendation systems and deep synthesis technologies.[46] China's approach is notable for its emphasis on data localisation and government access to data, which stands in tension with its strong individual privacy protections.

The United Kingdom, having exited the EU, is developing its own AI regulatory framework through the AI Safety Institute and a context-specific, principles-based approach. Japan and Singapore have adopted lighter-touch regulatory approaches that emphasise industry self-regulation and voluntary codes of conduct.[47] These diverse approaches provide valuable

[45] K Pavithra and M Aravind Kumar, 'The Legal Landscape of Ai in India: Existing Frameworks and Future Regulatory Needs' (2025) 17(5I) Journal of Research and Development <https://doi.org/10.5281/zenodo.15805702> accessed 10 June 2026

[46] Chao Wang et al., 'Privacy Protection in Using Artificial Intelligence for Healthcare: Chinese Regulation in Comparative Perspective' (2022) 10(10) Healthcare <https://doi.org/10.3390/healthcare10101878> accessed 10 June 2026

[47] Tahereh Saheb and Tayebeh Saheb, 'Mapping Ethical Artificial Intelligence Policy Landscape: A Mixed Method Analysis' (2024) 30 Science and Engineering Ethics <https://doi.org/10.1007/s11948-024-00472-6> accessed 10 June 2026

comparative perspectives for India's evolving regulatory framework, suggesting that there is no single model for balancing AI innovation with privacy protection.

RECOMMENDATIONS FOR REFORM

Based on the analysis conducted in this article, the following recommendations are proposed for strengthening India's legal framework for addressing the intersection of AI and privacy:

Enactment of AI-Specific Legislation: India should enact dedicated AI legislation that addresses the unique challenges posed by artificial intelligence systems. This legislation should establish a risk-based classification system for AI technologies, with enhanced requirements and oversight for high-risk applications, particularly those affecting privacy and fundamental rights. The legislation should mandate algorithmic impact assessments for AI systems that process personal data or make decisions affecting individuals' rights and interests.

Strengthening the DPDP Act: The DPDP Act should be amended to address AI-specific challenges. This should include the introduction of provisions equivalent to Article 22 GDPR, requiring human review of significant decisions based solely on automated processing.[48] The Act should also include specific provisions addressing algorithmic profiling, the right to explanation for AI-driven decisions, and enhanced protections for sensitive data processed by AI systems.

Institutional Reform: The Data Protection Board of India should be reconstituted as an independent, judicially insulated regulatory authority with the power to investigate, adjudicate, and impose meaningful sanctions for privacy violations. This would align India's data protection enforcement mechanisms with international best practices and ensure effective oversight of both state and private actors' use of AI technologies.

Narrowing Government Exemptions: The breadth of government exemptions under the DPDP Act should be significantly narrowed. Any processing of personal data by the state for national security or public order purposes should be subject to strict necessity and proportionality requirements, with independent judicial oversight.[49] This would ensure that the exemptions do not become instruments of unchecked mass surveillance.

[48] General Data Protection Regulation 2016, art 22
[49] *Justice K S Puttaswamy (Retd) & Anr v Union of India & Ors* (2017) 10 SCC 1

Promoting Privacy-Enhancing Technologies: The government should promote the development and deployment of Privacy-Enhancing Technologies (PETs) for AI systems. This should include support for research and development in areas such as federated learning, differential privacy, and homomorphic encryption, which enable the use of AI without compromising individual privacy. Incentives for the adoption of privacy-by-design principles in AI development should be established.

Addressing Algorithmic Bias: Specific provisions should be enacted to address algorithmic bias and discrimination. This should include requirements for regular auditing of AI systems for bias, mandatory reporting of significant discriminatory outcomes, and the establishment of remedial mechanisms for individuals affected by biased algorithmic decisions.

Enhancing Transparency and Accountability: AI developers and deployers should be required to maintain comprehensive records of their AI systems, including training data sources, algorithmic design choices, and deployment contexts. Transparency reports should be mandated for high-risk AI systems, and affected individuals should have the right to access meaningful information about how AI systems make decisions affecting them.

CONCLUSION

The intersection of artificial intelligence and the right to privacy in India presents one of the most significant legal and constitutional challenges of the contemporary era. The constitutional recognition of privacy as a fundamental right in the Puttaswamy decision established a robust foundation for privacy protection, while the DPDP Act and the India AI Governance Guidelines represent important steps towards developing a comprehensive regulatory framework. However, as this article has demonstrated, significant gaps remain in India's legal framework for addressing the privacy implications of AI technologies.

The challenges are multifaceted and require a comprehensive response. The autonomous and predictive capabilities of AI systems create privacy threats that existing data protection frameworks, designed for traditional data processing models, are ill-equipped to address. The breadth of government exemptions in the DPDP Act, the voluntary nature of the AI Governance Guidelines, the absence of an independent regulatory authority, and the lack of AI-specific legislation all represent significant vulnerabilities in India's privacy protection architecture.

The comparative analysis with international approaches, particularly the European Union GDPR and AI Act, suggests that India has much to learn from the regulatory experiences of other jurisdictions, while also recognising the unique challenges and opportunities of the Indian context. The recommendations proposed in this article, ranging from the enactment of dedicated AI legislation to institutional reform and the promotion of privacy-enhancing technologies, provide a roadmap for strengthening India's legal framework.

Ultimately, the challenge is not merely legal or technical but fundamentally constitutional. The Puttaswamy judgement recognised that privacy is "intrinsic to life and liberty" and "central to the exercise of human freedoms." Ensuring that this constitutional vision is realised in the age of artificial intelligence will require sustained commitment from legislators, regulators, the judiciary, civil society, and the technology industry. The choices made today will determine whether AI becomes an instrument of empowerment or a tool of surveillance, and whether the right to privacy remains a living constitutional guarantee or a paper promise in an increasingly algorithmic world.