

Artificial Intelligence and the Right to Privacy in India: Emerging Legal Challenges and Regulatory Responses

Manya Srivastava¹

ABSTRACT

Artificial intelligence (AI) technology has revolutionized public administration, business, health care, and governance through big data analytics and automation. However, the success of such technological innovations is contingent on the ability to gather and analyze large quantities of information. Thus, there arise serious concerns about the right to privacy due to the potential for surveillance, profiling, monitoring, and automated decision-making. The constitutional status of the right to privacy in India was established by the Supreme Court in *Justice K.S. Puttaswamy v. Union of India*, which recognized privacy as an integral element of constitutional rights to dignity, liberty, and autonomy. In light of this context, the growing adoption of AI technology poses certain legal challenges in India.

This paper aims to discuss the development of privacy law and policy in India, identify privacy challenges posed by the use of AI technologies, and assess whether existing regulation is sufficient to deal with such challenges. Specifically, the article will examine India's recent Digital Personal Data Protection Act, 2023 and India AI Governance Guidelines.

KEYWORDS

Artificial Intelligence; Right to Privacy; Digital Personal Data Protection Act, 2023; Facial Recognition Technology; AI Governance

INTRODUCTION

Artificial intelligence has proven to be one of the most influential innovations of the twenty-first century in terms of its impact on governance, business operations, healthcare practices, educational processes, police investigations, and many other fields. AI algorithms have been shown to be capable of analyzing large amounts of data, detecting patterns and making forecasts, as well as automating decision-making procedures more efficiently than ever before.²

¹ Student at Faculty of Law, University of Allahabad, Uttar Pradesh.

² Akshaya R & Devadharshini VV, An Analysis on Artificial Intelligence and Data Privacy in India, 7 INDIAN JOURNAL 7(2) (2025).

Yet, the capabilities of AI algorithms depend on the availability of huge amounts of data. Personal data, biometrics, locational information, and online behavior are regularly used to refine the operation of AI algorithms. While such data-intensive development can provide many advantages, there are several ethical issues related to privacy, surveillance, and consent. The gathering of large amounts of personal data provides an opportunity for invasive profiling, algorithmic discrimination, illegal sharing of personal data, and constant tracking of people's activities without their knowledge or consent.³

The foregoing considerations take on added relevance within the context of the Indian constitution, whereby the Supreme Court, in *Justice K.S. Puttaswamy v. Union of India*,⁴ explicitly acknowledged the right to privacy as a fundamental right enshrined in Part III of the Constitution. Privacy was established as an inseparable component of human dignity, personal liberty, and individual autonomy, necessitating that any limitation imposed upon privacy be legally, necessarily, and proportionately justified. Against the backdrop of a technologically advanced era driven by artificial intelligence, this poses an essential legal and constitutional concern.

While India has made commendable strides toward the regulation of personal data, both with respect to the enactment of the Digital Personal Data Protection Act, 2023⁵ and implementation of various policies facilitating the ethical deployment of artificial intelligence technology, many uncertainties persist in light of whether the existing framework suffices to meet the novel challenges of AI-related privacy risks. The following discussion provides an examination of the constitutional aspects of privacy in India, as well as the emerging issues and current state of affairs in AI-related privacy protection.

CONSTITUTIONAL FOUNDATION OF PRIVACY IN INDIA

The foundation of privacy jurisprudence can be traced to *Kharak Singh v. State of Uttar Pradesh* (1962), where the Supreme Court invalidated intrusive domiciliary visits conducted under police surveillance regulations. Although the Court did not expressly recognise a right to privacy, the decision acknowledged that excessive State surveillance could infringe personal liberty under Article 21.⁶

³ Prashant Mali, AI and Data Privacy in India: Emerging Legal and Ethical Challenges, CYBER LAW CONSULTING (Sept. 11, 2024).

⁴ Justice KS Puttaswamy (Retd) v Union of India, (2017) 10 SCC 1.

⁵ The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India)

⁶ Kharak Singh v State of Uttar Pradesh, AIR 1963 SC 1295.

The concept was further developed in *Gobind v. State of Madhya Pradesh* (1975), where the Court moved closer to recognising privacy as a constitutionally protected interest. While observing that privacy is not absolute, it accepted that individual freedom and personal liberty encompass privacy interests subject to reasonable restrictions.⁷

The turning point came in *Justice K.S. Puttaswamy v. Union of India* (2017) where a nine-member constitution bench of the Supreme Court declared that the right to privacy is a fundamental right. It was stated that privacy was inherent to life and liberty under Article 21 and it was associated with concepts such as dignity, autonomy, and freedom. Notably, the judgement also highlighted that due to technology and digital economy there was an increased threat to invasion of privacy via data collection, monitoring, and profiling of individuals. The judgement stressed that for the restriction on right to privacy there had to be conditions of legality, legitimacy of state action, necessity, and proportionality.⁸

The impact of Puttaswamy is not limited to conventional views on privacy. By identifying the importance of informational privacy in the constitution, the decision set a crucial normative standard for analyzing new technologies such as artificial intelligence. Since AI technologies are highly dependent on the gathering and processing of personal information, constitutional values mentioned in Puttaswamy become key factors that determine if any technological innovation violates fundamental constitutional rights. The evolution of privacy legislation provides a constitutional basis against which modern discussions on AI regulations should be made.⁹

AI AND EMERGING PRIVACY CHALLENGES

There has been a fast pace at which artificial intelligence is being adopted by governing bodies in relation to business, medicine, financial institutions, and public administration.¹⁰ In this regard, AI relies heavily on massive amounts of data gathered, analyzed, and processed in order to create solutions to problems that may arise. This has made the use of AI a matter of concern since data collection and surveillance are becoming increasingly relevant due to the

⁷ *Gobind v State of Madhya Pradesh*, (1975) 2 SCC 148.

⁸ *Puttaswamy*, *supra* note X, at 2.

⁹ *Puttaswamy*, *supra* note X, at 2.

¹⁰ Press Information Bureau, Ministry of Information and Broadcasting, Govt. of India, *Transforming India with AI, THE PRESS INFORMATION BUREAU* (Dec. 30, 2025), <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2209737®=3&lang=1>.

advancement in artificial intelligence. There are, therefore, serious threats posed to the constitutionally guaranteed right to privacy.¹¹

A. Large-scale data gathering and profiling

AI models depend on data-driven processes to enhance their learning abilities. They keep collecting and analysing data about the behaviour, habits, location, purchases, preferences, and other aspects of people's lives, online and offline. In many cases, the data collected is sufficient for creating highly comprehensive digital portraits of the person that could expose their most intimate life moments.¹²

The problem related to profiling goes far beyond just collecting data from the user. AI models could make assumptions about their sensitive characteristics, make predictions about future behaviour, or even classify them without even notifying. Therefore, the growing prevalence of profiling could affect personal autonomy by making people targets for advertising, manipulations, or discrimination.¹³

B. AI Training Data and Problems of Informed Consent

The functioning of AI technologies requires big amounts of data to undergo further training and refinement. Personal data obtained for one purpose or another is being used again as a resource for creating AI software, which triggers problems related to informed consent. The problem is that data is aggregated and re-used by various players in the market, which makes people lose control over its use.¹⁴

C. Automating Decisions

With the help of artificial intelligence, decisions are automated in many areas like employment, financial markets, insurance, and public administration. These decisions are made through opaque methods which cannot be comprehended by individuals or disputed easily by them. This is a problem when it comes to accountability and information privacy.¹⁵

¹¹ AKSHAYA R. & DEVADHARSHINI V.V., *supra* note 1.

¹² PRASHANT MALI, *supra* note 2

¹³ Anurati Dasgupta & Ruchika Sharma, *Artificial Intelligence and Data Protection: Legal Challenges and the Need for a Robust Framework in India*, 13(11) IJCRT(2025).

¹⁴ *AI Training Data under India's DPDP Regime: Compliance Challenges and Strategies*, KHURANA & KHURANA (2025), <https://www.khuranaandkhurana.com/ai-training-data-under-india-s-dpdp-regime-compliance-challenges-and-strategies>.

¹⁵ DASGUPTA & SHARMA, *supra* note 10.

D. Algorithmic Discrimination

Artificial intelligence is often seen as unbiased and neutral technology. In actuality, however, the efficacy of an AI system is only as good as its training data. When historical discrimination, social injustice, or incomplete data underlie an AI's training data, then the results obtained from that system are likely to perpetuate discrimination or even amplify it.¹⁶

Algorithmic discrimination can have an impact on various decisions related to employment, education, credit, health care, and public services. Without even knowing what makes for their discrimination or exclusion, people might find themselves facing adverse consequences. From a privacy point of view, algorithmic discrimination reduces one's capability to exert control over the use of personal information.¹⁷

E. Facial Recognition Technology and Mass Surveillance

One of the most debated uses of artificial intelligence technology has been the use of facial recognition technology. Through the analysis of biometric facial characteristics, these technologies make it possible to identify, track, and monitor individuals in real-time. Police forces and other authorities are making increasing use of facial recognition technology as an effective means of security, investigations, and surveillance.¹⁸

The use of facial recognition technology poses serious issues related to privacy. As compared to traditional methods of surveillance, facial recognition makes it possible to conduct surveillance without necessitating the participation or cooperation of the subject involved. The threat posed by mass surveillance using biometric data becomes particularly worrying under these circumstances.¹⁹

Given the recognition by the Supreme Court that privacy is a fundamental right, these kinds of activities are very crucial constitutionally speaking. Constant biometric monitoring will have an intimidating effect on freedom of speech, assembly, and even movement. The increased use of facial recognition technology brings about the dire need for adequate legal protection that strikes a balance between the need to secure one's safety and their fundamental rights.²⁰

¹⁶ DASGUPTA & SHARMA, *supra* note 10.

¹⁷ AKSHAYA R. & DEVADHARSHINI V.V., *supra* note 1.

¹⁸ Sritrisha S., *Facial Recognition Technology and the Right to Privacy in India: A Constitutional and Regulatory Analysis*, 7(4) IJLLR (2025).

¹⁹ Mohita Yadav & Arti Sharma, *Facial Recognition Technology in India: Socio-Legal Debates on Privacy and Human Rights*, IJSET (2025).

²⁰ SRITRISHA S., *supra* note 15.

REGULATORY RESPONSE IN INDIA

Realising the emerging significance of protecting privacy and developing technology responsibly, several regulatory steps have been taken in India in order to protect privacy in the digital age. Most notably, some of these steps include passing of the Digital Personal Data Protection Act, 2023 (DPDP Act) and adoption of ethical policy frameworks for artificial intelligence. However, one cannot fail to notice that there still exists the need for assessing the adequacy of such regulatory response in the light of challenges posed by AI technologies.

A. Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 acts as the central piece of legislation dealing with the processing of digital personal data in India.²¹ The Act follows the principle of consent-based data processing, provides rights for data principals, and places an obligation on data fiduciaries for ensuring data protection and processing of personal data in a lawful manner. Despite the fact that it helps in protecting informational privacy rights, this Act regulates mainly the process of data processing rather than AI technology itself.

Nonetheless, the DPDP Act is more inclined towards regulating personal data rather than addressing issues related to the utilization of artificial intelligence itself. Though the Act deals with issues relating to data processing, it does not cover areas like algorithmic decision-making, AI-based profiling, explainability, etc.²² Apart from data protection laws, there have been increasing efforts by the Indian government towards fostering the growth of ethical and trustworthy use of AI in India. India's AI Governance Guidelines²³ encourage the implementation of responsible practices for the use of AI technologies while ensuring innovation, transparency, safety, accountability, and trust. The guidelines aim at ensuring that the use of AI is aligned with the constitutional principles and interests of the society.

One aspect of this governance approach is the focus on risk management and responsible innovation. There are various concerns surrounding issues such as bias, transparency, security,

²¹ DPDP Act, 2023.

²² Akshaya R and Devadharshini VV (n 1).

²³ Ministry of Electronics and Information Technology, Govt. of India, *India AI Governance Guidelines*, THE INDIAAI MISSION (Nov. 5, 2025), <https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/nov/doc2025115685601.pdf>.

fairness, and privacy. Therefore, the governance approach encourages stakeholders to implement strategies aimed at mitigating risks associated with the use of AI technologies.²⁴

B. Limitations of the Current Framework

Nevertheless, India's regulatory regime continues to be disjointed. The DPDP Act is geared towards resolving problems associated with data protection, whereas AI governance principles mainly serve as guidelines and lack enforceable legal backing. This makes it difficult to adequately regulate matters related to algorithmic decisions, algorithmic accountability, biometric surveillance, and explainability. The current framework thus only partially addresses the privacy issues arising from the use of AI technology.

REGULATORY GAP AND THE NEED FOR REFORM

Even with progress made on data protection laws and AI regulation, the present regulatory regime in India appears incapable of dealing with some of the intricate privacy threats posed by AI technology. While the DPDP Act 2023 enhances the protection of personal data and sets out accountability provisions for data fiduciaries, it fails to establish a legislative structure that addresses the AI-specific challenges.²⁵ As such, there persist regulatory shortcomings in the area.

For one, there is no separate AI law in place. Unlike conventional data processing operations, AI possesses the ability to learn, predict, profile, and make decisions independently. These capabilities pose threats that exceed what can be addressed using only data protection measures. But, the current regulatory regime has been unable to recognize AI regulatory needs and treat them as distinct from data governance needs.²⁶

Another problem is linked to the absence of explainability obligations. Modern people are becoming more vulnerable to the consequences of automated or computer-aided decisions made in areas related to job positions, banking, medical services, and administrative decisions. However, none of the modern laws ensure the right of individuals to obtain an explanation on the logic of AI decision-making processes.²⁷

²⁴*Decoding the India AI Governance Guidelines*, SAIKRISHNA & ASSOCIATES (2025), <https://www.saikrishnaassociates.com/decoding-the-india-ai-governance-guidelines>.

²⁵ DASGUPTA & SHARMA, *supra* note 10.

²⁶ AKSHAYA R. & DEVADHARSHINI V.V., *supra* note 1.

²⁷ DASGUPTA & SHARMA, *supra* note 10.

Problems arise due to the insufficient regulation of profiling and automated decision-making. Automated decision-making is often associated with an analysis of user behaviour and data to predict needs or risks and manipulate individuals. Although such technology increases effectiveness, the use of profiling technologies poses significant threats to privacy and even discrimination.²⁸

Concern is especially pronounced with regard to facial recognition technology and biometric surveillance. In spite of the lack of a specific legal framework regulating its use, there have been significant advances in the deployment of these technologies by government authorities and law enforcement agencies. Considering the highly sensitive nature of biometric data, the lack of any legal safeguard in this regard poses serious issues relating to the proportionality and necessity of such measures, as well as their constitutional validity.²⁹

India needs to formulate a more holistic and risk-focused legal approach in regulating artificial intelligence. Such an approach would necessarily require that a legal framework be devised that takes into account certain obligations and guarantees of transparency and accountability, as well as safeguards against discrimination. At the same time, there need to be stronger protections of biometric information and other forms of sensitive personal information. Moreover, individuals should be afforded certain legal rights relating to automated decision-making processes.³⁰

CONCLUSION

The growing application of AI in government, business, and administration has drastically changed how personal information is gathered, processed, and applied. Although AI systems contribute greatly to increased efficiency, innovation, and decision-making, they have raised some very serious issues regarding the use of personal information.

Under Indian constitutional law, particularly after *Justice K.S. Puttaswamy v. Union of India*, privacy can be considered a fundamental right. Privacy has been defined in connection with dignity, autonomy, and liberty. But the emergence of new technological innovations based on the application of AI has revealed weaknesses in the current system. While the Digital Personal

²⁸ PRASHANT MALI, *supra* note 2.

²⁹ MOHITA YADAV & ARTI SHARMA, *supra* note 16.

³⁰ MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY, *supra* note 22.

Data Protection Act, 2023 and India AI Governance Guidelines provide important means for protecting privacy interests, there are several gaps in these regulations.

For technology to remain within constitutional values, India needs to transcend its focus on merely dealing with data and implement an all-encompassing governance model for artificial intelligence. A good AI governance model should ensure transparency, accountability, and protection against any misuse while respecting individuals' rights in the digital world.

