

Artificial Intelligence and Data Protection in India: A Legal Analysis under the Digital Personal Data Protection Act, 2023

Dr. Sarthak Agresar

Ansuyaben Balkrishna Parikh Law College, Kadi, India

sarthakagresar@gmail.com

Abstract

AI has swiftly been integrated into online systems of governance, business websites, financial services, medical systems, education technologies, and civic administration. Due to the reliance on data collection, analysis, inference, and reuse, the growth of AI systems has increased the discussion of privacy, surveillance, profiling, and data obscurity, automated decision-making, and accountability. These issues have gained particular significance in India following the recognition of privacy as a constitutional value in Justice K.S. Puttaswamy v. Union of India and the following adoption of the Digital Personal Data Protection Act, 2023. The paper is a systematic literature review of the scholarly work that has been published from 2014 to 2025 to assess how Indian law responds to the relationship between AI and personal data protection. Based on academic databases, legal databases, and official policy sources, the paper synthesizes literature regarding informational privacy, AI governance, consent, fiduciary obligations, children data, enforcement, and regulatory gaps. The discussion concludes that the Digital Personal Data Protection Act, 2023, represents a significant shift in the previous disjointed attitude of the Indian legislative system to the Information Technology Act and SPDI Rules in favor of a more systematic approach to lawful processing, principal rights, and the duty of data fiduciaries. Concurrently, the paper holds that the concerns related to AI, including its algorithmic opaqueness, inferential profiling, fairness, explainability, and automated harms, are met half-heartedly by the current statutory design. The paper finds that although the DPDP Act offers a structural framework for privacy protection in the era of AI, India will need more interpretive guidance, institutional capacity, and auxiliary governance practices to make AI innovation consistent with constitutional privacy and digital justice.

Keywords: Artificial Intelligence; Data Protection; India; Digital Personal Data Protection Act, 2023; Privacy; Legal Analysis.

Introduction

Artificial intelligence has transformed the interaction between technology, information, and law by ensuring that data mining, identifying patterns, predicting, and making decisions without human intervention are the key aspects of digital governance. However, in contrast to the previous types of

software that completed very specific and apparent tasks, modern AI systems can work with large amounts of personal data, draw probabilistic conclusions, categorize people, and assist or substitute human expertise in the fields of credit rating, employment, content regulation, law enforcement, health care diagnostics, and government services. This change brings about a great deal of efficiency, personalization, and innovation, yet also poses challenging legal issues. Personal information is no longer simply stored or transferred; modeled, recombined, profiled, and transformed into behavior, identity, and risk predictions. Consequently, the data protection law has taken center stage in the management of AI[1]. In India, these developments are especially legally pertinent due to the presence of the vast platform-based digital environment, the speed of the public digitization, the biometric identification facilities, the development of the fintech and the e-governmental infrastructure, and the increasing dependence of the state and the non-state sectors on the data-driven instruments. However, there has been no specific and thorough law in India for a number of years. The protection was diffused among sectoral norms, constitutional principles, and the Information Technology system, particularly, the Sensitive Personal Data or Information Rules, 2011. The importance of that older regime was limited. It gave more emphasis on information security and also on smaller sets of sensitive information than on an effective rights-based architecture of all digital personal data[2].

The law enforcement of privacy jurisprudence by the Supreme Court created the constitutional basis of a more robust legal system. In Justice K.S. Puttaswamy (Retd.) v. Union of India, the Court acknowledged the existence of privacy as a value constitutionally attached to dignity, liberty, and autonomy and specifically stated that information privacy was an urgent issue in the digital era. It was also highlighted in the judgment that the threat to privacy can be caused not only by the State, but also by non-state actors, which preconditions laying a doctrinal foundation on the broad-scaled data protection law[3]. This constitutional moment redefined privacy as something diffuse into a normative standard that digital governance and data-driven technologies, such as AI, should be held. The Digital Personal Data Protection Act, 2023, was the most significant Indian legislative reaction to this issue. The Act gives a guideline on how digital personal data should be processed in a way that acknowledges the right of individuals to safeguard their personal data and the necessity of processing such data for a legitimate purpose. It presents the notions of notice, consent, lawful use, data fiduciary, rights of data principal, obligations related to children's data, redress of grievances, and penalties. Towards the end of 2025, the framework was also shifted towards operationalization with the announcement of the Digital Personal Data Protection Rules, 2025, and the formation of the Data Protection Board of India[4]. Nonetheless, the adoption of a general data protection law will not necessarily address the special legal issues of AI. AI systems are usually opaque processing chains, inferential analytics, automated scoring, data repurposing, and structural

imbalance between data subjects and data processors. An all-consent model would not be sufficient in situations where people are unable to comprehend the downstream implications of algorithmic processing with any meaningfulness. Likewise, general tasks of security and lawful processing might not be able to answer questions of prejudice, elucidation, human control, or the lawfulness of machine-produced inferences[5]. Therefore, the connection between AI regulation and the law of data protection is an issue requiring a high level of scholarly interest. The current paper presents a systematic literature review of the literature published in the period between 2014 and 2025 on the topic of artificial intelligence and data protection in India. It is not merely an attempt to summarize the previous scholarship but a way to interpret it in terms of the doctrinal perspective of the Digital Personal Data Protection Act, 2023. The paper poses the question of whether the existing framework in India has offered sufficient legal foundation for the regulation of AI-based personal data processing and where the key gaps still lie. The integration of the SLR methodology with the doctrinal legal argument helps the study add to the better comprehension of the advantages and disadvantages of the emerging digital rights framework in India[6].

Legal and Conceptual Background

The evolving definition of privacy in the digital sphere should be the starting point in the legal analysis of AI and data protection in India. Conventional privacy law tended to be preoccupied with the secrets, intrusion, or unauthorized disclosure. In the AI era, though, privacy is advanced to the management of information streams, metadata, patterns of behaviour, profiles of inferences, and the structure of digital decisions themselves[7]. AI systems do not merely take the data provided by people; they can make inferences of new knowledge out of seemingly trivial data and make foretelling decisions that influence opportunities, treatment, and freedom. Therefore, the issue is not whether data are gathered with permission, but whether the data processing structures can be consistent with dignity, fairness, and the law.

The Indian law discourse on privacy took time to get a constitutional clarification. Before the DPDP framework, the most visible regulatory foundation of the operations of the private sector in respect of handling a group of sensitive personal information was the Information Technology Act, 2000, and the SPDI Rules, 2011[8]. These regulations demanded privacy policies, consent to collection and disclosure in some situations, and reasonable security measures. However, they were smaller and conceptually less expansive than current comprehensive legislation on data protection and not created to address the nuances of the reality of AI-driven personal data ecosystems. They failed to offer a complete framework of data subject rights in general, governance of purpose, institutional enforcement, or algorithmic harms. The constitutional change occurred in Puttaswamy, at which the Supreme Court provided that privacy is

a primary constitutional value per Articles 14, 19, and 21. More importantly, the ruling identified informational privacy as a core of liberty in the technologically networked society. The Court was sensitive to the risks of aggregation, surveillance, and the growing ability of the state and non-state actors to control personal information. This jurisprudence has become important to the governance of AI since it does not view privacy only as a unilateral command over discrete data, but as a structural precondition of autonomy and of democratic citizenship. Any legal framework processing AI ought to be interpreted through the prism of constitutional proportionality, legitimate purpose, and individual dignity protection[9].

The role of data governance was also recognized in the policy discourse of AI in India. The National Strategy of Artificial Intelligence by NITI Aayog pointed at the potential transformative role of AI in various sectors, at the same time noting some concerns regarding the accessibility of data, privacy, and regulatory protection. According to the strategy, the ambitions of India in AI would need strong structures of data protection and standards-based governance. This is how the policy of innovation and the regulation of privacy are connected: data protection is not only an inhibitor of AI, but a constituent part of trustworthy AI systems[10].

The Digital Personal Data Protection Act, 2023, has to be interpreted on this constitutional and policy backdrop. The Act is relevant to digital personal data, such as personal data obtained in a digital format and data obtained offline and subsequently digitized, as well as extraterritorial in that processing pertains to the provision of goods or services in India. Its design is based on legal processing, particularly consent and some legitimate purposes; data fiduciary obligations; data principal rights; special duties concerning the data of children; notice of breaches; and an enforcement system based on penalties. Even though the Act does not specifically present itself as an AI law, it is closely applicable to AI systems as long as they rely on digital personal data, behavioral analytics, or data-intensive automation[10].

The 2025 Rules and notifications also suggest a shift in legislative aspiration to institutional implementation. Of special importance are the announcements of the DPDP Rules, 2025 and the creation of the Data Protection Board as it is proposed that the Indian data protection regime will turn into a working and not only a declarative one. This is significant to the researcher who is investigating the years up to 2025 since it is the last year of the first complete legislative cycle, which is the constitutional recognition of a statute enactment and the first implementation of the law[12]. Theoretically, five are the most crucial AI-related issues that overlap with the DPDP framework. First, AI relies on large-scale data processing and, in many cases, on repackaging or combining information from several sources. Second, AI systems are capable of generating non-transparent and inexplicable results, undermining meaningful

notice and consent. Third, AI poses risks of inferential privacy losses, in which new personal information is constructed based on existing information. Fourth, AI may promote discrimination or unfair classification by using biased training data or model design. Fifth, AI makes responsibility more difficult as decisions can be spread among developers, deployers, vendors, and platform operators. These facts imply that a general data protection law can give only a partial solution. The key legal issue is whether the DPDP framework can be construed in a way to regulate these harms, or whether there is a need to have extra sector-specific and AI-specific regulations[11].

Methodology

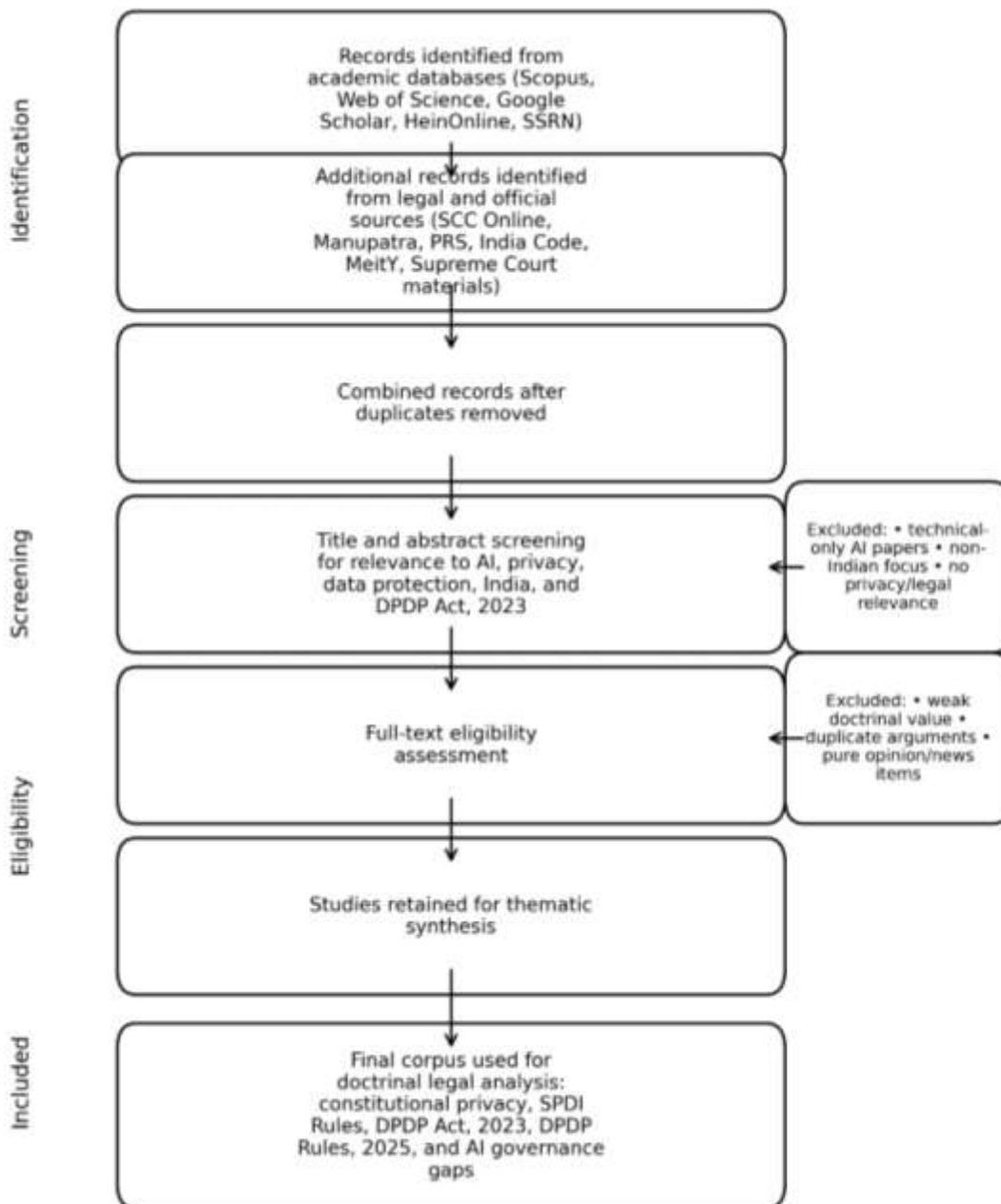
The research design of this paper is a systematic literature review design together with doctrinal legal analysis. The SLR methodology was chosen since the field of research is at the crossroads of legal, public policy, technology governance, and digital rights, and it is vital to integrate the work on the topic across various fields of knowledge instead of using a purely narrative review. The doctrinal part is included due to the purpose of the paper, which is not only to list themes in the literature but also to draw their implications under the Digital Personal Data Protection Act, 2023, and other Indian legal sources[13].

It was set that the review period would be done between 2014 and 2025. This time frame was selected in order to represent the maturation of Indian digital governance discourses, the emergence of AI discussion, the constitutionalizing of privacy, and the passage and early enforcement of the DPDP regime. Even though there are older resources on the law of privacy, the given time frame provides analytical consistency as it draws attention to the decade when AI became a key governance concern, and data protection became a policy focus in India. Multidisciplinary academic and legal databases, such as Scopus, Web of Science, Google Scholar, HeinOnline, SSRN, SCC Online, Manupatra, and official repositories related to the topic, including India Code, MeitY, PRS Legislative Research, and Supreme Court materials, were used as sources. The search terms were a combination of Artificial Intelligence, AI governance, privacy, data protection, personal data, India, Digital Personal Data Protection Act, DPDP Act, informational privacy, automated decision-making, and profiling. Additional searches were made using the terms Puttaswamy, SPDI Rules, and Data Protection Board to include doctrinal and institutional facets[14].

Screening was based on PRISMA-style logic, but the current paper is conceptual, not empirical in its presentation of count-based review measures. During the identification phase, data in the academic, legal, and official databases were collected. In the second phase, there was the elimination of duplicate records. At the third stage, titles were filtered to remove obviously irrelevant literature, including extremely

technical AI engineering papers that did not contain a legal or data governance aspect[15]. The fourth stage involved the evaluation of abstracts and executive summaries on the relevance to AI, personal data, privacy, and the Indian legal context. Finally, complete texts were sorted and kept when they had some meaning to one or more research questions. The integration of government notifications, statutory texts, and significant judicial materials as primary legal sources was introduced instead of being considered secondary literature.

Figure 1.



Inclusion criteria included English-language materials published since 2014 and also included substantial content on AI, algorithmic systems, privacy, personal data, surveillance, data protection, or digital governance in India. Articles in peer-reviewed journals, book chapters, conference papers, official policy reports, legal commentary, legislative documents, and judicial documents were also incorporated when they directly shed light on the Indian legal situation[16]. The exclusion criteria eliminated redundant studies, purely journalistic articles, documents that contained no substantive legal or analytical information, and articles that had no significant connection to India or data protection law.

Upon selection, the material was coded into the general thematic categories: constitutional privacy and informational autonomy; pre-DPDP legal regulation; AI-specific privacy risks; consent and lawful

processing under the DPDP Act; rights and duties under the Act; children's data and high-risk contexts; enforcement and institutional design; and regulatory gaps in respect to algorithmic accountability[17]. This thematic synthesis enabled the analysis of the literature not as individual texts but as a component of a larger jurisprudential and policy dialogue. The last interpretive step then evaluated the extent to which the DPDP framework can accommodate AI-related concerns and how its existing wording can be underspecified. The methodological appropriateness of this hybrid approach to a legal study is that the adequacy of statutes cannot be quantified by textual reading alone. It should also be put to the test with the issues of scholarship. On the other hand, the literature on AI ethics and governance should be based on the real characteristics of Indian law. The current approach thus aims at achieving a moderate compromise between normative legal interpretation and systematic scholarly review.

Findings and Legal Analysis

The literature reviewed shows a wide agreement that AI amplifies the traditional privacy issues and gives rise to additional legal vulnerabilities. In the materials surveyed, AI is not only described as a tool that allows working with personal data faster, but as a socio-technical system capable of predicting traits, behavior, organizing opportunities, and mediating access to resources. The transformation poses a more serious legal issue than traditional data abuse. Autonomy and fairness can be compromised even in situations where there is no direct disclosure, but there is widespread profiling, predicting behavior, and non-transparent categorization. The literature thus considers the protection of data as a preliminary, but not a comprehensive, regulatory reaction to AI[18].

The first significant discovery is that Indian scholarship views AI governance more and more through the constitutional logic of Puttaswamy. The acknowledgement of informational privacy and its sensitivity to data aggregation in the judgment has placed it as a pivotal interpretative reference point of AI-related legal discourses. More often than not, researchers believe that AI systems should not be judged based on their efficiency or economic innovation but on their ability to comply with dignity, decisional freedom, and democratic accountability. Such constitutional framing matters as it implies that AI regulation in India cannot be confined to compliance checklists as such; instead, it must be linked to substantive rights.

The second observation is that the pre-DPDP legal regime was generally viewed as inefficient in data-intensive AI settings. The SPDI Rules were a pioneering effort to be prescriptive about how some types of personal information are processed by the private sector, although the literature observes that they had little scope, inconsistent enforcement rationale, and did not reflect the modern digital architecture. They were not programmed to be persistent, large-scale, inferential, and automated in processing data. Such a

lacuna in the previous paradigm serves to justify why the DPDP Act is considered in the literature as a structural break and not a small amendment of laws.

The third conclusion is that the DPDP Act, 2023, leads to a much better situation regarding the legal environment since it establishes a better vocabulary of rights and duties. The fact that the Act acknowledges the existence of data principals and data fiduciaries, the consent-based design, its redressal of grievances, and its penalties framework all create a more consistent legal framework governing digital personal data than one ever existed in India. These provisions establish minimum obligations in AI systems that receive or process digital personal information, which have direct relevance. Specifically, the Act can be interpreted as advocating legality, purpose discipline, user awareness, and fiduciary responsibility in AI-enabled settings[19].

But even the literature and the analysis of the doctrines indicate that there is a limit to this improvement. The connection between consent and AI opacity is one of the key issues. The minimum intelligibility in consent under the law of data protection presupposes that the persons can comprehend what information is gathered, why, and with what effects. This assumption is frequently complicated by AI systems since downstream processing can be dynamic, inferential, and challenging to define using the common language of notice. A data principal could be aware of the fact that data are being gathered, but still fail to realize how such data can be utilized to score, recommend, target, or predict. Therefore, as the DPDP framework reinforces the consent and notice, the legal adequacy of these tools becomes less solid in the case of complex AI systems.

The other key observation is that of inferential privacy and profiling. Most of the literature underlines the point that AI systems do not just generate value through the utilization of the revealed personal data, but generate new personal knowledge based on the patterns and correlations. This poses a doctrinal challenge, since data protection laws tend to apply to identifiable data that are directly obtained or processed, but AI harms can be caused by inferred attributes, risk scores or behavioral categories. The DPDP Act is definitely applicable where such inferences are still associated with identifiable persons and are based on digital personal data, but the law does not explicitly work out an advanced model of inferential harms, algorithmic rating, or automatic decision protection. It is one of the best in which the legal analysis has found a partial but incomplete match between the general data protection law and AI governance.

The problem of fairness and discrimination is also preempted in the reviewed literature. The systems of AI can reproduce and increase historical bias by providing biased datasets, having broken proxies, or unclear optimization goals. In India, this threat overlaps with social inequalities, and automated systems can be detrimental in employment, credit, insurance, education, welfare targeting, and law enforcement

situations. The DPDP Act is indirectly fair in that it brings obligations to lawful processing and protection of data principals, but is not an anti-discrimination or algorithmic fairness law. Consequently, numerous harms of fairness will have to be upheld by constitutional equality, sectoral regulation, consumer protection, or AI-specific regulations in the future, and not by the DPDP text itself.

The literature also adds that children's data should be given special consideration in AI ecosystems. The personal data and duties of children in the DPDP Act are thus quite applicable to educational technologies, social media settings, gaming systems, and recommendation architectures where children are particularly susceptible. In this case, the Act plays a significant protective role in that it indicates that some types of data processing require extra attention. However, the literature also indicates that the implementation is going to be a challenge in cases where age assurance, platform design, and AI-mediated personalization are hard to control in real-time.

Another theme is that of enforcement and institutional capacity. The introduction of the Data Protection Board and the announcement of the Rules in 2025 suggest that India is shifting from the field of theoretical legislation design to practice. This is a significant advancement since enforcement institutions play a crucial role in the law of data protection. In the absence of available complaint mechanisms, investigative competence, and well-defined procedural standards, even well-written rights may continue to be formal as opposed to being effective. The AI governance literature repeatedly emphasizes that accountability cannot rely purely on ex post punishment, but also it must have preventive compliance, documentation, risk assessment, and institutional monitoring. In this case, the DPDP framework provides a preliminary framework, but with room to be elaborated in the future.

In general, the results indicate that the DPDP Act, 2023, needs to be interpreted as a privacy law at its core, but not as a full-fledged AI regulation code. It deals with many of the conditions of data-processing under which AI is applied, but it does not fully govern all the normative issues AI develops. Its most powerful strength has been to formalize a rights-based legal architecture of digital personal data. Its greatest AI vulnerability, however, is that it lacks a focused and systematic discussion regarding the explainability of algorithms, inferential profiling, automated decision review, or fairness-by-design requirements.

Discussion

The debate that has been raised against the reviewed literature is not that the DPDP Act is not adequate per se, but that its adequacy is contingent. The Act is a significant institutional development in the case of traditional types of digital data processing. In AI-intensive ecosystems, however, it is only a baseline layer, as opposed to a full regulatory solution. This is a critical difference. It would be analytically

erroneous to consider the Act irrelevant to AI or to think that it answers all AI governance concerns. The more convincing argument is the fact that the Act offers the required privacy base where more specific AI norms should be established.

It is also due to the fact that AI regulation necessarily starts with lawful data governance, and this is one reason why the Act is so foundational. Personally dependent AI systems must have a justifiable legal ground for collection, usage, storage, transfer, protection, and access control. The DPDP framework, in this regard, bridges a gap that has existed in Indian law for a long time. It renders constitutional privacy into a legislative paradigm of rights, trusts, and bureaucratic protection. It also conveys a wider normative message that technological innovation should not leave a legal and responsible processing. However, according to the literature, AI law is not exhausted by privacy law alone. As an example, meaningful consent will be strained in the case of non-transparent relevant processing logic or when it changes post-collection. Likewise, unjust results can be achieved even in the case of a completely legal data collection, provided that algorithmic outputs are prejudiced or inexplicable. The AI legal implications are thus greater than data protection in its limited context. These are procedural fairness, contestability, auditability, discrimination control, transparency standards, and human oversight. The current DPDP framework only reflects these to a partial extent.

In light of reform, there are several implications. To begin with, India would gain the authoritative interpretive direction on the application of DPDP obligations to AI-based profiling, predictive analytics, and recommender systems. This guidance may clarify how notice, consent, constriction of purpose, and fiduciary obligation would work in situations of dynamic processing and model-based processing. Second, in financial, health, education, employment, and public administration sectors, sector-specific regulators ought to incorporate DPDP principles into AI regulation. Third, institutional practice must shift to preventive compliance techniques, such as documentation standards, privacy impact assessments, and internal accountability procedures of high-risk automated processing. Fourth, Indian law might eventually need to have additional norms addressing automated decision-making, algorithmic explainability, or redress rights when AI has a material impact on people.

The influence of AI governance on constitutional values and the interaction between AI governance and constitutional values are particularly critical issues. Since Puttaswamy prioritizes the dignity and informational autonomy as core to privacy, future application of the DPDP Act should not be interpreted narrowly, focusing on compliance with the checkbox consent. The law is to be interpreted by the courts, regulators, and policymakers in a sensitive way to structural power asymmetries, the obscurity of machine systems, and the social implications of datafied decision-making. This would make data protection

consistent with the more constitutional goal of protecting individual freedom in a digitally mediated society.

This direction is also backed by the overall policy trend. The Indian policy discourse on AI has always acknowledged that sustainable AI implementation requires that the people have trust in it, that it is standardized, and that it has a strong governance framework. In that respect, enhanced data protection is not anti-innovative. To the contrary, it will render AI ecosystems more acceptable, predictable, and legitimate. India has to grapple with, however, not whether she is to pursue innovation or rights, but how she can establish a system where technological advancement is responsible to constitutional democracy.

Conclusion

The paper aimed to review the artificial intelligence and data protection in India with a systematic literature review to 2014-2025 and a doctrinal study focusing on the Digital Personal Data Protection Act, 2023. The review reveals that it is impossible to make sense of the legal role of AI in India outside of the emergence of informational privacy as a constitutional issue, the constraints of the previous SPDI-based regime, and the subsequent establishment of a specific statutory framework of digital personal data. Under that historical and doctrinal meaning, the DPDP Act is a significant legal step. It transforms privacy into a concept that is much more fragmented and sectoral into a more coherent system of rights, obligations, and enforcement within the context of the digital era. Simultaneously, the paper concludes that AI brings about types of risks that can be partially absorbed by the general data protection law. AI systems interfere with the presumptions of meaningful consent, produce inferential harms that is not self-evident data disclosure, complicate transparency, and expose risks of unjust or discriminatory results. The DPDP Act also concerns the legality of digital personal data processing and provides a robust base architecture of accountability, although it is not yet a complete normative framework of algorithmic governance. The legal account of the relationship between AI and data protection can then be regarded as being layered: data protection is not only sufficient, but also necessary, for reliable AI.

The most compelling finding that is made in the literature is that India currently has an underlying privacy law that can be used to regulate AI, yet such a pillar must be reinforced by interpretation, institutional reform, and additional governance provisions. The announcement of the DPDP Rules and the establishment of the Data Protection Board by 2025 indicate that implementation has started, yet the effectiveness of the long-term success of the regime will be determined by its ability to react to real-life AI applications. But normatively, the future of AI regulation in India must be pegged on the constitutional values expressed in Puttaswamy: dignity, liberty, autonomy, and safeguarding against capricious

violations of personal life. The Digital Personal Data Protection Act, 2023, is a necessary step toward the same direction. But with the increase in the strength and deeper integration of AI systems into the governance and markets, Indian law will have to shift away from a model of minimalist compliance to a more robust model of transparency, contestability, fairness, and human-focused accountability. It is only at that point that data protection can be used as not only a legal protection against abuse, but as a value system of democratic and rights-observant AI governance.

References

- [1]. Committee of Experts under the Chairmanship of Justice B. N. Srikrishna. (2018). *A free and fair digital economy: Protecting privacy, empowering Indians*. Government of India.
- [2]. Deshpande, S. (2023). *Data privacy in India: Technical and legal perspective*. SSRN. <https://doi.org/10.2139/ssrn.4420148>
- [3]. Government of India. (2011). *The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011*. India Code.
- [4]. Government of India. (2023). *The Digital Personal Data Protection Act, 2023 (No. 22 of 2023)*. Ministry of Electronics and Information Technology.
- [5]. Government of India. (2025, January 3). *Notification under the Digital Personal Data Protection Act, 2023*. Ministry of Electronics and Information Technology, Gazette of India.
- [6]. Government of India. (2025, November 13). *Notification establishing the Data Protection Board of India*. Ministry of Electronics and Information Technology, Gazette of India.
- [7]. Government of India. (2025, November 14). *Digital Personal Data Protection Rules, 2025*. Ministry of Electronics and Information Technology, Gazette of India.
- [8]. Joshi, D. (2024). AI governance in India: Law, policy and political economy. *Policy Design and Practice*.
- [9]. Justice K. S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors., Writ Petition (Civil) No. 494 of 2012, Supreme Court of India (2018).
- [10]. Kanipakam, S. (2019). Law and regulation of artificial intelligence in India. In *Legal technology and the new sharing economy* (Springer).
- [11]. Khanna, V. (2025). Examining the significance of the Digital Personal Data Protection Act, 2023 in India's healthcare privacy framework. *Israel Journal of Health Policy Research*.
- [12]. Koul, S. (2025). Stakeholders' understanding of data privacy: Implications for digital governance and legal protection in India. *Cogent Social Sciences*.
- [13]. NITI Aayog. (2018). *National strategy for artificial intelligence*. Government of India.

- [14]. NITI Aayog. (2022). *Responsible AI for All: Adopting the framework—A use case approach on facial recognition technology*. Government of India.
- [15]. PRS Legislative Research. (2023). *The Digital Personal Data Protection Bill, 2023: Bill summary*. PRS Legislative Research.
- [16]. PRS Legislative Research. (2023). *The Digital Personal Data Protection Bill, 2023*. PRS Legislative Research.
- [17]. Sayyed, H. (2024). Artificial intelligence and criminal liability in India. *Cogent Social Sciences*.
- [18]. Saxena, A. (2025). Data privacy and protection issues in artificial intelligence: An Indian legal perspective. SSRN.
- [19]. Tripathi, K. (2020). Protecting privacy in the era of artificial intelligence. SSRN.