Journal of International Research and Multidisciplinary Innovation

Data Privacy Challenges in the Age of Artificial Intelligence Under India's Digital Personal Data Protection Act, 2023

Author: Gaurav Yadav

Affiliation: Mahatma Gandhi Kashi Vidyapeeth, Varanasi

Email: gauravyadav62@gmail.in

Submitted to: Journal of International Research & Multidisciplinary Innovation (JIRMI)

Date: 10 January 2026

ABSTRACT

The Digital Personal Data Protection Act, 2023 (DPDP Act) is India's first comprehensive privacy law, which has long been lacking in regulatory coverage under the ad hoc provisions of the Information Technology Act, 2000. However, the legislation was designed with a wider intent — to be a general data-protection measure, rather than a direct response to the governance issues of AI. The paper argues that the Act's architecture presents four structural lacuna in relation to AI-specific privacy issues: firstly, the legal nature of inferences drawn by AI about individuals is not defined; secondly, there is no statutory right to be excluded from AI-informed decisions; thirdly, duties of Data Fiduciaries for algorithmic transparency are weak, and fourthly, the general exemptions for State instrumentalities are incongruous with the proportionality principle required by the Supreme Court's right-to-privacy judgment. Analogously, the paper maps some specific amendments and ancillary legislation to the DPDP Act that could help it become relevant and useful for the era of AI without stifling India's growth goals.

JIRMI

Journal of International Research and Multidisciplinary Innovation

Keywords: DPDP Act 2023, Artificial Intelligence, Data Privacy, Algorithmic Accountability, GDPR, Automated Decision-Making, Data Fiduciary, India, Data Protection Board.

I. INTRODUCTION

It's not comfortable, asking a general statute to do specialised work and that is exactly what you're doing here. India's Digital Personal Data Protection Act, 2023 is a well-crafted privacy law, but not one that was designed for machine learning pipelines and recommender systems. So we have a law that doesn't really mean much, but it is a law that covers some of the most important technology of our generation: the fuel (personal data) that is driving it.

This is important because AI-powered data processing is not just a 'big data' or 'fast data' version of previous methods. It's a different kind of quality. An AI system trained on location, purchases and browsing history can accurately predict a person's health status, political opinion, or financial issues, information the person did not reveal to them, nor did they provide to the platform. No matter how robust, the consent provisions in the DPDP Act will not be able to prevent harms that occurred after the initial data collection, and not reasonably anticipated at the time of consent.

This paper is presented in five parts. Part II provides a short constitutional and legislative history of the DPDP Act. Part III presents the identified privacy risks that the Act will have to address through AI. Part IV considers those risks in the context of the provisions of the Act as they now exist. EU law is used as a comparative framework in Part V. Targeted recommendations are laid out in Part VI.

II. LEGISLATIVE AND CONSTITUTIONAL BACKGROUND

After two withdrawn bills, a Joint Parliamentary Committee review, the DPDP Act was enacted on 11 August 2023, following a legislative journey since the Justice B.N. Srikrishna Committee's report in 2018. The last law is significantly slimmer than its predecessors, with the data portability, localisation of data for sensitive categories and separate regulation of non-personal data either deleted or left to be addressed by future laws.

The main directive principle of the Act is the nine-judge interpretation of the Constitution by the *Supreme Court in Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1*, which declared privacy as a fundamental right including the right to control one's personal data. That ruling creates a proportionality test for any state action that interferes with privacy, and directly affects the blanket exceptions the DPDP Act provides government bodies for their action under Section 17. Whether those exemptions pass the proportionality check will be put before the courts in the future.

From the institutional point of view, the Act introduces a Data Protection Board of India (DPBI) which has adjudicatory powers, particularly designates Data Fiduciaries as the main duty bearers, and introduces a sub-category of Significant Data Fiduciaries (SDFs) with enhanced obligations such as Data Protection Impact Assessments (DPIAs) and third-party audits. These are good starting points. It's the absence of something that is in the Act about AI that is the issue.

III. HOW AI CREATES PRIVACY CHALLENGES CONVENTIONAL LAW CANNOT ABSORB

A. The Inference Problem

AI models of today don't just work with data that people give them—they produce data about people. Train a model on seemingly trivial data and it will generate inferences of health, sexuality, political opinion and financial stress that are often more accurate than self-reported data. These assumptions are personal information in all respects; they concern a specific individual and could impact an individual's life. However, they have never been collected, never agreed to and, according to a narrow interpretation of the DPDP Act's definition of “personal data”, may not even clearly be covered by the Act.

This is the aggregation problem in "algorithm" attire. The damage isn't in any single data point, but rather in the result of many points, processed through a statistical model. Consent for one use (e.g. a supermarket loyalty scheme) has nothing to do with the inference drawn at the other end of the pipeline (e.g. a pregnancy prediction for advertising timing).

JIRMI

Journal of International Research and Multidisciplinary Innovation

B. Automated Decisions and the Absence of Human Judgment

What used to take a human being to decide is now increasingly decided or greatly influenced by the algorithmic systems such as loan approval, shortlisting jobs, granting bail and allocating beds in hospitals. It's not simply the use of the data that's an issue, but what happens to the person when data about them is fed into a black box model that yields a consequential output that a person has no reasonable chance of understanding or contesting. The DPDP Act does not provide a right of explanation and no right to human review. Under current Indian law, an individual who is rejected by an AI-based credit-scoring algorithm does not have a legal right to know the reasons behind the rejection.

C. The Opacity of Machine Learning Systems

Privacy law is based on a disclosure model – the disclosure of what is being collected, why it is being collected and how it is being used. All three pillars of that model are threatened by AI. The information gathered could be less significant than what is derived from it. The intent given at collection may have little to do with the final use downstream. But, in the technical sense, the operations of a deep neural network may be "how" unknowable even to the model operators. It is not possible to have a transparent notice that provides a description of the output, which is an emergent property of the training process itself, prior to the training of the model.

IV. THE DPDP ACT THROUGH AN AI LENS

A. Consent and Its Limits

Section 6 of the Act stipulates that consent must be free, specific, informed and unambiguous. These words are the correct ones. The challenge is that uses of AI processing often exceed the purposes for which the data is collected and may not have been foreseen by the data principal or the data fiduciary. The Act does not clarify if the use of personal data for training a model is considered a new purpose – one needing new consent – or whether it is within the scope of the original consent. This interpretation loophole isn't insignificant: it is what could make the difference between millions of Indians being able to have any say in how their data contributes to the artificial intelligence systems that have become a significant part of their lives.

JIRMI

Journal of International Research and Multidisciplinary Innovation

B. Rights of Data Principals

The Act provides four rights: to information (Section 11); to correction and erasure (Section 12); to grievance redressal (Section 13); and the right to nomination (Section 14). The right to erasure is a sensitive, especially in an AI environment. After personal information is used to train a model, the personal information is not removed from the model's learned parameters by deleting the personal information. The Act doesn't address this technical fact: where the right to erasure is triggered, it may not be enforceable in practice, for reasons of technicality.

It is more significant what the Act does not say. There is no right to explanation for automated decision-making, no right to object to profiling, and no right to data portability. These are not frills; they are the real tools by which people can really have some control in a setting in which data about them is constantly generated and used by systems they cannot see.

C. Significant Data Fiduciaries and DPIAs

The most promising AI-governance tool in the Act is the so-called SDF framework under Section 10. The Act introduces, at least, the structure for substantive accountability, by giving the Central Government the power to designate large data processors as SDFs and to mandate them to carry out DPIAs and algorithmic audits. The issue is that there is missing scaffolding. The Act does not prescribe the content of a DPIA, the methods to be used by the auditors or how the result of the audit should be communicated. That detail – which needs to be conveyed through rules under Section 40 – can lead to the DPIA mandate becoming a “tick the box” exercise rather than a true risk assessment task.

D. The Section 17 Problem

The Central Government may exempt State instrumentalities from all or any of the provisions of this Act, on the grounds of national security and public order considerations. This is important as the Indian government is also one of the largest data generators in the country (Aadhaar, National Population Register, sectoral databases) and is a developer of AI systems for governance. It would be difficult to reconcile the requirement for proportionality safeguards and parliamentary oversight in government AI deployments, that the Supreme Court gave in Puttaswamy, with an Act that can be disapplied through executive notification without providing any rationale for such an exception.

JIRMI

Journal of International Research and Multidisciplinary Innovation

V. WHAT THE EU FRAMEWORK OFFERS

The GDPR is the most referenced comparative reference for Indian data protection legislation, which has been in effect since 2018. It grants a right not to be subject to decisions based on automated processing "where there are significant effects" (Article 22), which is a right that is not provided for in the DPDP Act. The DPIA provisions of the DPDP Act are much more methodologically specific than those in Article 35 that apply to SDF. But the GDPR's accountability framework – the requirement to maintain records of processing activities, appoint a DPO and have strong powers of supervisory bodies – has created its own brand of enforcement practice, a lesson for Indian policymakers to learn, and not copy wholesale.

The EU AI Act, which was approved in June 2024, creates a second level of regulation for AI systems. It categorizes AI applications based on risk, mandates conformity assessments and post-market monitoring for high-risk applications (such as those used in credit scoring, employment, education and law enforcement), and requires operators to keep technical documentation sufficiently developed for regulatory review. The importance for India is not that it should replicate this system, but that the EU experience has proven how inadequate a general data protection law, no matter how well drafted, can be to regulate AI uses. An instrument for AI governance that is not specific to any sector or at least a dedicated Chapter for AI in the DPDP is needed at some point.

VI. RECOMMENDATIONS

The DPDP Act could be much more effective as an AI governance tool if four targeted interventions were made.

The definition of personal data in Section 2 should be changed to explicitly cover data obtained or inferred from automated systems on the basis of data that was not personal data. This fills the gap in the inference without changing the structure of the Act.

Second, a new provision of this kind, modelled on but simpler to GDPR Article 22, should enable data principals to know when a ‘significant decision' impacting on them has been taken primarily using automated systems and to seek clarification about that decision from a human. To keep the

compliance burden proportionate to the scope of "significant" should be defined to include decisions that have material impact on legal rights, financial situation, employment, or access to government services.

Third, the Central Government must impose substantive DPIA requirements on the deployment of SDFs by means of its rule-making authority under Section 40. The standards should include an evaluation of discriminatory risk, sufficient description of the functioning of the model for regulatory review, and a monitoring plan following deployment. The DPBI should be provided (at a minimum) with the audit reports.

Fourthly, there should be minimum requirements for Section 17 exemptions, including time limitation, notification of the DPBI, and an independent oversight mechanism, if not the DPBI itself. It does not limit the legitimate powers of the State; it puts these powers on a minimum level of accountability, which corresponds to the requirement of proportionality in the constitution.

VII. CONCLUSION

The DPDP Act is not the end of the solution, but it's a good beginning. The basic architecture of consent-based processing, a tiered fiduciary structure and a separate adjudicatory board offers a viable structure. It does not give a clear account of how that foundation is applied to systems that produce personal data based on other data, make consequential decisions without human input and are built in ways that are by design hard to explain or inspect.

These are not fringe situations. They outline the everyday use of AI systems that are already successfully deployed on a large scale in Indian banking, healthcare, government service delivery and e-commerce. The law is missing and the impact is growing. The recommendations contained in this paper are one-off, with no suggestions to overhaul the Act, however their impact would have a positive effect on the balance and would be meaningful for the data principals the Act is designed to serve. The question is whether the Parliament and Executive will take any action on it and what kind of a digital society India wants to construct.

JIRMI

Journal of International Research and Multidisciplinary Innovation

REFERENCES

A. Primary Sources

1.Digital Personal Data Protection Act, 2023 (No. 22 of 2023), Ministry of Electronics and Information Technology, Government of India.

2.Information Technology Act, 2000 (No. 21 of 2000), Government of India.

3.Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (Supreme Court of India).

4.Regulation (EU) 2016/679 (General Data Protection Regulation), OJ L 119/1, 4 May 2016.

5.Regulation (EU) 2024/1689 (EU AI Act), OJ L 2024/1689, 12 July 2024.

6.IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

B. Secondary Sources

7.Justice B.N. Srikrishna Committee, 'A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians' (Ministry of Electronics and Information Technology, 2018).

8.Joint Parliamentary Committee, Report on the Personal Data Protection Bill, 2019 (Lok Sabha Secretariat, December 2021).

9.NITI Aayog, 'Responsible AI for All: Adopting the Framework' (2022).

10.Meha Agarwal and Anubhav Pandey, 'The DPDP Act 2023: An Assessment of India's Data Protection Architecture' (2024) 36(1) National Law School of India Review 45.

11.Sandra Wachter, Brent Mittelstadt and Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the GDPR' (2017) 7(2) International Data Privacy Law 76.

12.Mike Ananny and Kate Crawford, 'Seeing without Knowing: Limitations of the Transparency Ideal and its Application to Algorithmic Accountability' (2018) 20(3) New Media & Society 973.

JIRMI

Journal of International Research and Multidisciplinary Innovation

13.Prateek Waghre, 'India's Draft Digital Data Protection Bill: An Analysis' (Internet Freedom Foundation, Working Paper No. 1/2022).

14.Paul Schwartz and Karl-Nikolaus Peifer, 'Transatlantic Data Privacy Law' (2017) 106(1) Georgetown Law Journal 115.

15.Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power (Profile Books 2019).

16.AI Now Institute, 'AI Now Report 2023' (AI Now Institute, 2023) <https://ainowinstitute.org>.

17.World Economic Forum, 'Data-Driven AI: Responsible Data Governance for the AI Economy' (WEF White Paper, 2023).

18.Brenda Leong and Patrick Hall, 'Artificial Intelligence and Data Privacy: Four Problems and Four Solutions' (Future of Privacy Forum, 2020).