International Journal of Law
www.lawjournals.org
ISSN: 2455-2194
Received: 30-08-2025, Accepted: 29-09-2025, Published: 13-10-2025
Volume 11, Issue 10, 2025, Page No. 22-24

A critical analysis of the digital personal data protection Act, 2023

Dr. Srinivas Katkuri
Department of Law, Osmania University, Hyderabad, Telangana, India

Abstract
This commentary critically examines the Digital Personal Data Protection Act, 2023 (DPDPA), focusing on its implications for privacy rights, regulatory frameworks, and the overall landscape of data protection in India. The DPDPA represents a significant shift in the Indian legal framework, aiming to align with international standards while addressing local concerns about data privacy and security. Key provisions, such as consent requirements, data processing obligations, and the establishment of a Data Protection Authority, are analyzed in detail. The commentary further explores potential challenges in implementation, the balance between innovation and regulation, and the role of stakeholders in fostering a culture of data protection. By situating the DPDPA within the broader context of global data protection trends, this work aims to provide insights into its effectiveness and future trajectory in safeguarding individual privacy rights in the digital age.

Keywords: Digital personal data protection act, data privacy, regulatory framework, consent management, data protection authority, data

Introduction
The Digital Personal Data Protection Act, 2023 (DPDPA) is a landmark legislation in India's legal and regulatory landscape, representing the culmination of years of policy discussions, legal debates, and global influences on data protection and privacy. Its journey has been shaped by the changing dynamics of technology, increasing concerns over data privacy, and the need for India to align itself with international standards in protecting personal data. Here is a paraphrased analysis of the evolution of the DPDPA, capturing the key milestones and developments leading to its enactment.

Need for Data Protection
The need for a formal data protection law in India began gaining attention in the early 2000s, driven by the growth of the internet and the increased exchange of personal data through online services. However, it wasn't until the 2017 landmark Supreme Court judgment in Justice K.S. Puttaswamy v. Union of India that the right to privacy was formally recognized as a fundamental right under the Indian Constitution. This judgment highlighted the necessity for a legal framework that would safeguard individuals' personal data against misuse, thereby accelerating efforts to develop comprehensive data protection legislation (Garg, 2024) [3].

Drafting of the Personal Data Protection Bill, 2019
The Indian government commissioned a committee led by retired Supreme Court Justice B.N. Srikrishna to draft a data protection law, which led to the Personal Data Protection Bill, 2018. This bill introduced concepts like data fiduciaries and rights, drawing inspiration from the EU's GDPR. However, it sparked debates on exemptions, consent, and data localization. A revised version, the Personal Data Protection Bill, 2019 was introduced.

Prolonged Parliamentary Scrutiny and Delays
The Personal Data Protection Bill, 2019 underwent extensive review by a Joint Parliamentary Committee, leading to significant changes and a renaming as the Data Protection Bill. Despite political complexities and administrative delays, the bill aimed to create a comprehensive legal framework for both personal and non-personal data.

Withdrawal of the 2019 Bill
In August 2022, the government made a surprising move by withdrawing the Personal Data Protection Bill, 2019, citing the need for a more comprehensive and forward-looking legislation. This decision, though unexpected, was seen as a response to the growing realization that the 2019 bill, despite its extensive provisions, did not adequately address the complexities of the modern digital economy and emerging technologies like artificial intelligence (AI) and blockchain.

Global Influences and India's Unique Approach
India's data protection law, DPDPA, is influenced by global developments like GDPR and the country's unique socio-political landscape. It requires explicit consent and data minimization, while focusing on data localization and government exemptions. The law addresses the massive scale of personal data processing within India and by foreign entities.

Introduction of the DPDPA, 2023
The government quickly moved to draft a new bill, resulting in the Digital Personal Data Protection Bill, 2022, which was introduced for public consultation. This version significantly simplified the earlier drafts by focusing solely on personal data, leaving the regulation of non-personal data for a separate legislative process. The Digital Personal Data Protection Act, 2023 (DPDPA) was finally enacted in August 2023, marking the culmination of nearly six years of legislative effort. However, the Act has also attracted criticisms, especially concerning the exemptions it provides and the extent to which it empowers the government

1. Scope and Application

The Act applies to the processing of digital personal data collected within India, whether in digital or non-digital forms (Government of India, 2023 [2], sec. 3). It also applies to the processing of data by foreign entities if it concerns the offering of goods or services to individuals within India. However, it exempts personal or domestic data processing, as well as publicly available personal data (Government of India, 2023, sec. 3). This scope appropriately reflects the evolving digital landscape but may require expansion. Given the increasing sophistication of cybercrime, even domestic or publicly available data could be exploited for harmful purposes. Therefore, future amendments might consider regulating the usage of such data to safeguard against identity theft or other abuses.

2. Definitions

The Act introduces critical definitions, including those of "Data Fiduciary," "Data Processor," and "Data Principal" (Government of India, 2023 [2], sec. 2). These definitions align the DPDPA with global standards, such as the General Data Protection Regulation (GDPR) in the European Union. An important addition is the "Consent Manager," who acts as a mediator in managing the data principal's consent (Government of India, 2023 [2], sec. 2). While this is a positive step, further clarification on the Consent Manager's accountability and qualifications could enhance the system's robustness. For example, defining minimum technical and ethical standards for Consent Managers would ensure higher trust in data transactions.

3. Consent Mechanism

The Act emphasizes the importance of obtaining explicit, informed consent from data principals (Government of India, 2023 [2], sec. 6). Consent must be specific and unambiguous, and the data principal must be able to withdraw consent at any time. This aligns with global best practices in data protection.

However, a potential area of concern is the balance between consent withdrawal and the operational needs of data fiduciaries. The Act allows data fiduciaries to continue processing data when necessary for fulfilling contractual obligations (Government of India, 2023 [2], sec. 6(5)). To mitigate misuse, the Act could benefit from more detailed guidance on how fiduciaries should handle such scenarios. In particular, clearer rules on the limits of "contractual necessity" could prevent overreach by corporations.

4. Obligations of Data Fiduciaries

The Act places significant responsibilities on data fiduciaries, including ensuring the accuracy, security, and erasure of personal data (Government of India, 2023 [2], sec. 8). It also mandates the appointment of Data Protection Officers and Data Auditors for "Significant Data Fiduciaries" (Government of India, 2023 [2], sec. 10).

Although these provisions align with international standards, their successful implementation will depend heavily on the operational capacity of fiduciaries. Small and medium enterprises (SMEs) may struggle to comply with these obligations due to resource constraints. To address this, the government could introduce tiered obligations, with lighter requirements for SMEs and more stringent ones for larger corporations or those dealing with sensitive personal data.

5. Processing of Children's Data

The Act offers special protections for children's data, requiring the consent of parents or lawful guardians for its processing (Government of India, 2023, sec. 9). Additionally, the Act prohibits tracking, behavioral monitoring, and targeted advertising for children.

While this is commendable, there are concerns about the definition of "child," which the Act sets at 18 years. Many countries adopt a lower age threshold, typically 13 or 16, for certain data processing activities (Martin, 2022) [4]. A more flexible approach could be introduced, with different levels of protection for younger and older minors. This would allow greater autonomy for teenagers in managing their digital presence while ensuring younger children are protected from exploitation.

6. Data Breach and Security Obligations

Data fiduciaries are required to notify both the Data Protection Board of India and the affected data principal in the event of a data breach (Government of India, 2023, sec. 8(6)). This is a key feature of the Act that mirrors practices seen in other jurisdictions.

However, there is no explicit timeline for breach notifications, which could undermine the effectiveness of this provision. Specifying a clear time frame, such as 72 hours, would ensure timely disclosure and allow individuals to take protective actions. In addition, imposing stricter penalties for delays in reporting breaches could serve as a deterrent to fiduciaries who may otherwise underreport such incidents.

7. Rights of Data Principals

The Act grants data principals several rights, including the right to access information about their personal data, correct inaccuracies, and request its erasure (Government of India, 2023, secs. 11, 12). These rights are integral to empowering individuals in a data-driven society.

One enhancement could involve broadening the scope of data portability. While the Act allows for correction and erasure, it could go further by requiring data fiduciaries to provide data in a format that allows individuals to transfer it to other platforms (Burman, 2023) [1]. This would align India's regulations with global data portability standards, such as those under GDPR, and promote competition and innovation.

8. Penalties and Compliance Mechanisms

The Act prescribes severe penalties for non-compliance, with fines reaching up to ₹250 crores (approximately $30 million USD) for severe breaches (Government of India, 2023, sec. 33). This sends a strong message to organizations about the importance of data protection.

Nevertheless, the penalty regime could be further refined to ensure proportionality. Currently, penalties are tied to the breach's gravity and duration, but the financial capacity of the data fiduciary should also be considered. This would prevent disproportionately large fines for smaller businesses and ensure that penalties are an effective deterrent for larger corporations.

9. Exemptions and Government Powers

One of the most controversial aspects of the Act is the broad exemptions granted to the government and its instrumentalities. The state is allowed to process personal

data without consent for reasons such as national security, public order, and the prevention of crime (Government of India, 2023 [2], sec. 17). Additionally, the government is empowered to restrict data transfers to foreign countries (Government of India, 2023 [2], sec. 16).

While national security concerns are valid, these exemptions raise questions about potential misuse. To build public trust, these provisions should be accompanied by robust safeguards, including judicial oversight and transparency mechanisms. A balanced approach would ensure that the state's actions are both effective and accountable.

10. Data Protection Board of India

The establishment of the Data Protection Board of India (DPBI) is a central feature of the Act. The Board is empowered to inquire into breaches, issue penalties, and mediate disputes between data principals and fiduciaries (Government of India, 2023 [2], sec. 18).

The DPBI is designed to function as an independent body, which is essential for maintaining public trust. However, concerns remain about the extent of government influence over appointments to the Board. To enhance its credibility, the appointment process for the Board's members should be transparent and involve multiple stakeholders, including representatives from civil society and industry.

11. Appeals and Dispute Resolution

The Act provides mechanisms for appeals against decisions of the DPBI, including through an Appellate Tribunal (Government of India, 2023, sec. 29). Additionally, it encourages alternative dispute resolution methods, such as mediation, for resolving data-related disputes (Government of India, 2023, sec. 31).

While these provisions are progressive, their effectiveness will depend on the capacity of the legal system to handle the expected volume of data-related disputes. Ensuring that the judiciary is equipped to handle complex data issues is essential for the successful implementation of these provisions.

Conclusion

The Digital Personal Data Protection Act, 2023 represents a major milestone in India's legal landscape, bringing the country closer to global standards of data protection. However, the Act is not without its challenges, particularly regarding its exemptions, enforcement mechanisms, and the balancing of individual rights with state interests.

Future amendments should focus on refining the Act's provisions to ensure it can address emerging challenges in the digital economy. This could include incorporating more detailed guidelines on the handling of emerging technologies, such as artificial intelligence, and strengthening oversight mechanisms to protect individuals' rights more effectively.

In conclusion, the DPDPA sets a strong foundation, but ongoing monitoring and iterative improvements will be necessary to ensure its long-term success in protecting personal data in India's rapidly evolving digital environment.

References

1. Burman A. Understanding India's new data protection law. Carnegie Endowment for International Peace, 2023.
2. Government of India. The Digital Personal Data Protection Act, Legislative Department, Ministry of Law and Justice, 2023.
3. Garg M. The Indian Puttaswamy judgments: Privacy rights at stake in the pursuit of social security. Oxford Human Rights Hub, 2024.
4. Martin B. Privacy in a programmed platform: How the General Data Protection Regulation applies to the metaverse. Harvard Journal of Law & Technology,2022:36(1).