*Page 1193 - 1202* **DOI:** *https://doij.org/10.10000/IJLMH.119695*

# INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

**Volume 8 | Issue 3**

**2025**

# Safeguarding or Surrendering Privacy?: Examining the Impact of India's DPDPA 2023

**OM UPADHYAYA**[1]

## ABSTRACT

*This paper critically examines the Digital Personal Data Protection Act, 2023 (DPDPA), a landmark legislative attempt by India to safeguard citizens' privacy in an increasingly digital world. Rooted in the constitutional affirmation of privacy as a fundamental right in K.S. Puttaswamy v. Union of India (2017), the DPDPA aims to regulate the collection, storage, and processing of personal data. While the Act introduces foundational concepts such as data fiduciaries, consent managers, and rights for data principals—including access, correction, and erasure of data—it simultaneously raises serious concerns regarding the dilution of consent, broad government exemptions, and limited enforcement powers.*

*The paper explores the Act's limitations, particularly the problematic provision of "deemed consent" and the sweeping powers granted to the central government, which many critics argue threaten the autonomy and privacy of individuals. A comparative analysis with global data protection laws such as the EU's General Data Protection Regulation (GDPR) and California's Consumer Privacy Act (CCPA) reveals that India's framework lacks several essential features including independent oversight, robust user rights like data portability, and explicit restrictions on state surveillance.*

*Further, the absence of mandates for data localization, vague definitions such as "public interest," and insufficient safeguards against algorithmic profiling and biometric misuse highlight the Act's inability to fully address modern privacy threats posed by artificial intelligence and surveillance capitalism. The paper underscores the need for public digital literacy, judicial vigilance, and civil society participation to make the DPDPA effective.*

*Ultimately, while the DPDPA is a step forward in India's digital privacy landscape, it is fraught with compromises that prioritize state and corporate interests over individual rights. The success of India's data protection regime hinges on continued reform and judicial interpretation that aligns with constitutional values and evolving global standards.*

[1] Author is a Law student in India

 [ISSN 2581-5369]

## I. THE EVOLUTION OF PRIVACY IN INDIA

In recent years, the concept of privacy has evolved significantly in India, especially in the context of growing digitalization and the increasing amount of personal data being generated and stored online. One of the landmark moments in this evolution was the Supreme Court's decision in *K.S. Puttaswamy v. Union of India (2017)*, which established the fundamental right to privacy as part of the right to life and personal liberty under Article 21 of the Indian Constitution. This judgment highlighted the importance of privacy in an era of technological advancement, where the boundaries of personal information were being increasingly blurred by both state surveillance and private actors.

- **The Puttaswamy Judgment and Its Impact**

The Puttaswamy case was pivotal in setting the stage for a more comprehensive approach to data protection and informational privacy. The judgment recognized that informational privacy was integral to an individual's dignity and autonomy. The Court stated that the right to privacy is not absolute and can be restricted on the basis of legality, necessity, and proportionality. This reasoning laid the foundation for a legal framework to protect personal data, particularly in an environment characterized by rapid technological advancements and the proliferation of online platforms. The judgment also emphasized that privacy is a key determinant of an individual's freedom, urging the government to adopt a robust data protection regime.

- **The Need for a Data Protection Framework**

Following the Puttaswamy judgment, the Government of India realized the urgency of introducing a robust data protection law. This led to the formation of the Committee of Experts, chaired by Justice B.N. Srikrishna, to draft a data protection law. The recommendations of this committee culminated in the introduction of the Personal Data Protection Bill. The bill aimed to regulate the collection, processing, and storage of personal data by both government and private entities. It was seen as a significant step toward safeguarding the privacy of individuals in a rapidly evolving digital landscape.

However, despite the advances in the bill, it faced criticism for several reasons. A major concern was the broad exemptions granted to the government, which critics argued could allow unchecked surveillance and data collection by the state. In response to these concerns, the bill was revised multiple times. The final version of the bill, known as the *Digital Personal Data Protection Act, 2023 (DPDPA)*, was passed in 2023. While it is a step forward

 [ISSN 2581-5369]

in ensuring better data protection, it still falls short of the expectations set by the Puttaswamy judgment in several respects.

- **Shortcomings of the DPDPA**

While the DPDPA introduces several important provisions aimed at securing data privacy, it does not adequately address the challenges posed by the ever-evolving digital threats. The Act does not offer sufficient clarity on issues like cross-border data flow and the enforcement of data protection principles in the face of rapidly changing technological practices. Critics argue that the Act's provisions still grant the government broad powers to exempt itself from certain obligations, which undermines the core principles of transparency and accountability in data processing.

Moreover, the absence of specific provisions addressing the protection of sensitive personal data in the context of emerging technologies, such as artificial intelligence and facial recognition, makes it less effective in responding to current and future challenges. As noted by legal scholar Kaur (2024), earlier frameworks like the Information Technology Act, 2000 were inadequate in addressing the complexities of modern digital threats. This is why stronger, more dynamic protections are needed to ensure that the privacy of individuals is maintained in the face of ever-evolving technological advancements.

## II. OVERVIEW OF THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

The *Digital Personal Data Protection Act (DPDPA), 2023* represents a crucial development in India's legal framework for personal data protection. The Act introduces several fundamental concepts, including Personal Data, which refers to any information that can identify an individual. A Data Fiduciary is defined as an entity that determines the purpose and manner of processing personal data, and a Consent Manager is a third-party entity responsible for managing and obtaining consent from data principals for the processing of their personal data (Ministry of Electronics and Information Technology, 2023).

The DPDPA grants several rights to Data Principals—the individuals whose personal data is collected. These rights include the right to access, correct, and erase their data. The Act also enshrines key data protection principles such as purpose limitation (data must be collected for specific, legitimate purposes), data minimization (only necessary data should be collected), and storage limitation (data should not be kept longer than necessary) (Ministry of Electronics and Information Technology, 2023).

However, the Act includes broad exemptions, particularly for government agencies, allowing them to bypass certain provisions in the interest of national security, public order, and law enforcement. This has raised concerns about the balance between privacy and state interests. Additionally, the Act lacks robust enforcement mechanisms, relying on self-regulation by data fiduciaries, which could undermine its practical effectiveness in protecting individuals' privacy rights *(Kaur, 2024)*.

While the DPDPA 2023 lays the groundwork for stronger data protection in India, it also reflects compromises that may limit its full potential. The Act presents both opportunities for enhanced privacy and challenges related to enforcement and state exceptions.

## III. CRITICAL ANALYSIS OF DPDPA 2023

- **Consent Framework: Robust or Redundant?**

Consent is the cornerstone of modern data protection frameworks, ensuring that individuals maintain control over their personal information. While the Digital Personal Data Protection Act recognizes consent as a precondition for data processing, the concept of "deemed consent" considerably weakens this protection. Under the Act, deemed consent is assumed for activities related to public interest, state functions, or medical emergencies, allowing data fiduciaries to process personal data without seeking explicit permission from individuals *(Thapa, 2024)*.

This approach starkly contrasts with the *General Data Protection Regulation (GDPR)* of the European Union, where consent must be freely given, specific, informed, and unambiguous (GDPR.eu, 2024). The dilution of consent under the DPDPA not only undermines individual autonomy but also risks normalizing unauthorized data collection. By broadening the categories under which deemed consent is acceptable, the DPDPA introduces a loophole that may be exploited, weakening the integrity of privacy protections in India.

- **Government Exemptions and Surveillance Risks**

One of the most controversial aspects of the DPDPA is the vast discretionary power it grants the central government. The Act allows the government to exempt any of its agencies from compliance with key provisions, citing vague and broad grounds like national security, public order, and friendly relations with foreign states (Chaudhary & Chaudhari, 2025).

These wide exemptions echo the concerns raised by the Supreme Court in the landmark Puttaswamy judgment (K.S. Puttaswamy v. Union of India, 2017), where the Court warned against unchecked surveillance practices. The DPDPA’s exemption mechanism appears to bypass the principle of proportionality—an essential safeguard against state overreach.

Without stringent checks and balances, these provisions may facilitate mass surveillance under the guise of public interest, thereby eroding trust in the state's data handling practices.

- **Comparison with GDPR and CCPA: A Missed Opportunity**

When compared globally, the DPDPA lags behind the standards set by the GDPR and the California Consumer Privacy Act (CCPA). The GDPR enforces a strong, consent-based model and grants comprehensive rights such as data portability, the right to object to processing, and the appointment of independent supervisory authorities (GDPR Text, 2024). Meanwhile, the CCPA empowers consumers with rights to opt-out of data sales, request data deletion, and access collected information (CCPA, State of California Department of Justice, 2024).

India's DPDPA lacks several of these features. It neither mandates privacy by design obligations—where privacy is embedded in system architecture from inception—nor establishes truly independent enforcement bodies. Moreover, unlike the CCPA, the DPDPA does not grant consumers the specific right to opt-out of the sale of their data, missing an important tool for consumer empowerment (Singh, 2024).

In essence, the DPDPA represents a significant legislative step but falls short of leveraging global best practices to build a truly citizen-centric privacy regime.

- **Limited Data Principal Rights**

The DPDPA acknowledges some essential rights for Data Principals, such as the right to access, correct, and request the erasure of their personal data. However, critical rights like data portability the ability to transfer one's data between service providers and the right to object to data processing are conspicuously absent (Saha & Mukhopadhyay, 2024).

The lack of a right to object particularly limits an individual's agency, making it difficult to refuse or challenge unwanted data processing activities. Without portability, users are locked into service ecosystems, making market competition weaker and reducing users' ability to seek better, privacy-respecting alternatives.

In comparison, GDPR grants a clear right to object, even for legitimate interests pursued by controllers, emphasizing the individual's supremacy over their data (GDPR Article 21, 2024). India's DPDPA thus only partially empowers users, leaving significant gaps in individual control over personal data.

- **Weak Enforcement Mechanisms**

Another area of concern is the enforcement model proposed under the DPDPA. The Data

 [ISSN 2581-5369]

Protection Board of India, established under the Act, is endowed primarily with adjudicatory powers rather than regulatory functions (Ministry of Electronics and Information Technology, 2023).

Unlike GDPR's Data Protection Authorities—which are autonomous, adequately funded, and empowered to conduct audits and impose heavy penalties—the Indian Board appears more reactive than proactive (Saurabh, 2024). Its close administrative link to the central government raises concerns about executive interference and reduces public confidence in its independence.

Without an independent enforcement agency actively monitoring compliance and deterring violations through substantial penalties, the DPDPA's ability to genuinely protect data principals remains questionable.

- **Absence of Data Localization Mandates**

Earlier drafts of India's data protection laws (such as the 2018 draft) included strong data localization requirements, which mandated that certain categories of personal data must be stored on servers located within India. However, the DPDPA 2023 relaxes these requirements by allowing cross-border data transfers to countries that the government deems safe (Ministry of Electronics and Information Technology, 2023).

While cross-border data flow facilitates global commerce, the absence of strict localization measures can expose Indian citizens' data to foreign jurisdictions and surveillance frameworks, potentially compromising national security and individual privacy. This change prioritizes ease of business operations for multinational corporations over robust data sovereignty, weakening the country's strategic control over its citizens' personal data.

- **Ambiguous Definitions and Lack of Accountability**

One of the critical flaws in the DPDPA is its reliance on vague and undefined terms such as "public interest," "legitimate use," and "fair and reasonable processing." These undefined expressions leave substantial room for subjective interpretation, leading to inconsistent application and potential misuse (Thapa, 2024).

Legal scholars emphasize that clear, narrowly tailored definitions are crucial in data protection laws to prevent abuse and ensure accountability. In the absence of precise definitions, government agencies and private companies might exploit these ambiguities to justify questionable data processing practices, effectively bypassing the necessary privacy safeguards.

 [ISSN 2581-5369]

## IV. CONTEMPORARY CHALLENGES AND FUTURE OUTLOOK

- **Emerging Technologies and Privacy Threats**

The rapid advancement of emerging technologies such as artificial intelligence (AI), facial recognition, and surveillance capitalism has created complex challenges to the protection of personal data. Automated profiling, behavioral prediction, and decision-making by AI systems introduce serious risks of discrimination, bias, and loss of autonomy. Despite recognizing "personal data" and "consent" as core elements, the Digital Personal Data Protection Act, 2023 (DPDPA)does not adequately regulate algorithmic processing. Scholars like Dalal & Richa (2025) point out that DPDPA lacks specific provisions to govern AI-driven profiling, unlike the General Data Protection Regulation (GDPR), which gives individuals the right not to be subject to decisions based solely on automated processing that significantly affects them.

Similarly, technologies like facial recognition can easily lead to mass surveillance if unchecked. The DPDPA remains silent on the governance of biometric data beyond general "reasonable safeguards," leaving citizens vulnerable to intrusive technologies increasingly used by both private and government actors.

- **Public Awareness and Digital Literacy**

For any privacy legislation to be truly effective, citizens must be aware of their rights and enforcement mechanisms. As noted by Banerjee (2024), digital literacy in India remains uneven, with large portions of the rural and semi-urban population lacking awareness of privacy rights. Although DPDPA provides for the appointment of a "Consent Manager" to assist individuals, no detailed framework ensures that these mechanisms will be user-friendly or accessible in regional languages.

In comparison to jurisdictions like the European Union, where GDPR mandates robust public information campaigns, India's DPDPA does not yet outline strong public engagement strategies. Without aggressive efforts in digital education and outreach, the ambitious rights enshrined under the Act may remain theoretical.

- **Global Trade and Data Flows**

Global trade increasingly hinges on trusted data exchange. India, with its vibrant IT and e-commerce sectors, needs strong privacy safeguards to maintain its competitive edge in cross-border services. India's efforts to attain "adequacy status" under GDPR allowing seamless data transfers with the EU could be jeopardized by the broad government exemptions and lack of independent oversight under DPDPA. Sharma (2024) warns that weak enforcement

mechanisms may create barriers to foreign investment and impact the export of IT services and digital goods.

The earlier versions of India's data protection proposals, including the 2019 Personal Data Protection Bill (PDPB), mandated strict data localization requiring critical personal data to be stored only in India. However, under the DPDPA 2023, this requirement was diluted. Cross-border transfers are permitted to countries "notified" by the central government, raising concerns about insufficient protections against foreign surveillance and lack of reciprocal standards.

- **Legal Amendments and Changes in the Act**

The DPDPA 2023 differs significantly from the earlier drafts, notably the Personal Data Protection Bill, 2019. Several crucial legal shifts were introduced:

- Removal of Data Localization: The earlier strict data localization mandates were relaxed, signaling a softer approach to global business demands but raising sovereignty concerns.
- Government Exemptions: The earlier drafts had limited exemptions for state agencies. DPDPA allows the central government to exempt any instrumentality of the state from the provisions of the Act on grounds such as national security, public order, or relations with foreign states.
- Simplified Data Principal Rights: Rights such as data portability and the right to object to processing present in earlier drafts were dropped or diluted. The final Act recognizes rights like access, correction, and grievance redressal but does not empower individuals to challenge data processing as robustly as GDPR does.
- Reduced Regulatory Autonomy: The Data Protection Authority envisioned in the 2019 Bill was replaced with a Data Protection Board, whose composition, powers, and functioning are heavily controlled by the central government, reducing independence.

These legislative changes attracted criticism for undermining the constitutional safeguards established in *K.S. Puttaswamy v. Union of India (2017),* where the Supreme Court emphasized proportionality, necessity, and legality as preconditions for any restriction on the right to privacy.

- Role of Civil Society and Judicial Oversight

The importance of civil society activism and judicial review cannot be overstated. The Puttaswamy case itself was initiated by a group of concerned citizens, highlighting the role that strategic litigation plays in expanding constitutional protections. Moving forward, judicial

scrutiny of government actions under DPDPA will be critical. Terms like "public interest" and "legitimate use" are vague, and their interpretation by courts will shape how far the privacy protections of Indian citizens actually extend.

Several public interest litigations (PILs) challenging aspects of government surveillance and data handling practices are already being contemplated, which could lead to further refinement and judicial guidelines supplementing the DPDPA.

## V. CONCLUSION

The *Digital Personal Data Protection Act, 2023* represents an important milestone in India's journey toward a structured data protection regime. Rooted in the constitutional right to privacy articulated in *K.S. Puttaswamy v. Union of India (2017)*, the Act attempts to establish a legal framework for safeguarding personal information in a digital age. However, the Act's broad government exemptions, diluted consent framework, limited rights for Data Principals, and weak enforcement mechanisms reveal significant shortcomings. While the DPDPA modernizes India's approach to data protection, it compromises too heavily on state interests and corporate convenience at the expense of individual autonomy. Comparisons with global standards like GDPR and CCPA highlight the missed opportunity to create a genuinely citizen-centric and globally credible framework. Emerging technologies such as AI and facial recognition, coupled with low digital literacy rates, further challenge the effectiveness of the Act. The legislative amendments from earlier drafts reflect a retreat from earlier commitments to strong oversight and user empowerment. Ultimately, the success of the DPDPA will depend not only on its statutory text but also on vigilant judicial oversight, active civil society engagement, and continuous legal reforms to align India's privacy protection regime with constitutional values and evolving global norms

*****

 [ISSN 2581-5369]

## VI. REFERENCES


1. GDPR Text (2024) *Full GDPR Regulation*
2. GDPR.eu (2024) General Data Protection Regulation (GDPR) Overview
3. K.S. Puttaswamy v. Union of India (2017) 10 SCC 1
4. Ministry of Electronics and Information Technology (2023) Digital Personal Data Protection Act, 2023
5. *California Consumer Privacy Act (CCPA)* CCPA – *California Department of Justice*
6. Kaur, T. (2024). Right to Privacy in Digital Age: A Study with Indian Context
7. Thapa, J. (2024). Data Privacy Vis-A-Vis the Digital Personal Data Protection Act, 2023
8. Chaudhary, P., & Chaudhari, P. (2025). Critical Analysis of Initiatives Taken By Government for Digital Data Protection in India
9. Singh, N. (2024). Data Protection and Privacy as a Fundamental Right
10. Saha, S., & Mukhopadhyay, S. (2024). A New Age of Data Privacy Laws in India
11. Saurabh, S. (2024). The Digital Personal Data Protection Act of 2023: Strengthening Privacy
12. Dalal, P., & Richa. (2025). The Right to Privacy in India: Historical Evolution and Contemporary Challenges
13. Banerjee, S. (2024). "Digital Personal Data Protection Act" - A Strudel Served Raw
14. Sharma, N. (2024). Legislative Realm of Informational Privacy in India


*****