Page 2636 - 2643 **DOI:** *https://doi.org/10.63108/IJLMH.12740*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 4

2026

The Constitutional Enigma of India's Digital Personal Data Protection Act, 2023: Structural Exigency, State Exemptions, and the Dilution of Transparency

MUKESH KUMAR MISHRA*

ABSTRACT

The enactment of the Digital Personal Data Protection (DPDP) Act, 2023, marks a paradigm shift in India's evolving digital jurisprudence, ostensibly codifying the fundamental right to informational privacy recognized in Justice K.S. Puttaswamy v. Union of India. However, beneath its streamlined, twenty-six-section framework lies a complex matrix of constitutional and structural contradictions. This article provides a comprehensive evaluation of the DPDP Act, focusing on three systemic regulatory vulnerabilities. First, it critiques the "skeletal" architecture of the statute, which relies on excessive executive delegation that leaves critical compliance, localization, and operational parameters to future, unchecked rule-making. Second, it scrutinizes the extensive state exemptions under Section 17(2), evaluating their compliance with the constitutional standards of necessity and proportionality. Third, it examines the structural dependence of the Data Protection Board of India (DPBI) on executive oversight, which compromises its efficacy as an impartial regulator. Finally, the article analyzes the amendment to Section 8(1)(j) of the Right to Information (RTI) Act, 2005, arguing that the absolute restriction on personal data access threatens democratic accountability. By comparing these provisions with the European Union's General Data Protection Regulation (GDPR), this paper demonstrates how the DPDP Act prioritizes state convenience over individual rights, transforming the right to privacy into an executive concession.

Keywords: *DPDP Act, GDPR, Data Privacy, Excessive Delegation, State Exemptions*

I. INTRODUCTION: THE POST-PUTTASWAMY JURIDICAL IMPERATIVE

The legal landscape surrounding digital privacy in India changed fundamentally when the Supreme Court handed down its ruling in Justice K.S. Puttaswamy v. Union of India.[1] Before this nine-judge bench firmly anchored informational privacy within the constitutional guarantees of Article 21, data regulation in the country was an afterthought. For more than two

* Author is an Advocate in independent practice at the Delhi High Court, New Delhi, India.

[1] Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1 (India).

 [ISSN 2581-5369]

decades, a massive, hyper-connected digital economy was forced to rely on the skeletal provisions of Section 43A of the Information Technology Act, 2000,[2] and the rudimentary structural guidelines of the 2011 SPDI Rules.[3] It was a framework completely unequipped to handle the aggressive, algorithmic realities of modern data harvesting.

Getting to the final text of the Digital Personal Data Protection Act, 2023,[4] was a chaotic, politically fraught process. The legislative timeline is marked by sharp philosophical shifts. We saw the rights-heavy approach of the Justice B.N. Srikrishna Committee Draft in 2018[5] completely watered down by the state-centric, security-focused revisions of the Joint Parliamentary Committee's 2019 Bill.[6] Then came the abrupt withdrawal of the 2021 draft altogether.

What emerged in 2023 is a piece of legislative minimalism. With just twenty-six sections, the DPDP Act is presented by policymakers as a lean, business-friendly alternative to the European Union's General Data Protection Regulation (GDPR).[7] But this brevity is an illusion. The reality is far messier. By choosing a stripped-down statutory design, the legislature has effectively passed the buck to the executive branch. This structural choice shifts core policy decisions to future administrative rules, compromising the Act's constitutional purpose and creating a system where citizen privacy frequently takes a back seat to bureaucratic discretion.

II. The Skeletal Law Problematic and the Doctrine of Excessive Delegation

The core structural flaw of the DPDP Act is its skeletal nature. By deliberately leaving major regulatory mechanisms to be built later through executive rule-making, Parliament has run straight into the constitutional boundaries of the Doctrine of Excessive Delegation. It is a foundational principle of Indian constitutional law that while Parliament can delegate routine administrative details, it cannot delegate its essential legislative function.[8] The parent statute

[2] The Information Technology Act, 2000, § 43A, No. 21, Acts of Parliament, 2000 (India).
[3] The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Gazette of India, pt. II sec. 3(i) (Apr. 11, 2011).
[4] The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).
[5] Committee of Experts on a Data Protection Framework for India, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians, Ministry of Electronics and Information Technology (2018).
[6] Report of the Joint Committee on the Personal Data Protection Bill, 2019, Seventeenth Lok Sabha, Parliament of India (2021).
[7] Council Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 (EU).
[8] In re Delhi Laws Act, 1912, AIR 1951 SC 332 (India).

 [ISSN 2581-5369]

must lay down an intelligible principle, a clear policy guide, or a definitive fence to contain executive discretion.[9]

A quick reading of the DPDP Act shows that variations of the phrase "as may be prescribed" appear over twenty-five times in twenty-six sections. This is not minor administrative delegation; it is an open-ended surrender of statutory authority. Parliament has left crucial components of data infrastructure entirely to the executive's rule-making powers under Section 40. Look at how much ground is left completely open:

- Notice Requirements (Sec 5): The actual manner and depth of details a company must present to users are left to future executive mood.
- Parental Consent (Sec 9): The technology and verification rules for identifying children's data are unwritten.
- Breach Notifications (Sec 15): Critical timelines and reporting routes for systemic data leaks remain blank.
- Cross-Border Data Flows (Sec 16): The specific criteria for blacklisting or whitelisting foreign countries are unmapped.
- Penalty Adjudication (Sec 33): The procedural pathways for how the DPBI calculates and imposes fines are left entirely to executive choice.

This approach creates severe legal uncertainty for businesses and individuals alike. Take Section 9's mandate for "verifiable parental consent." The Act demands this verification but fails to define the underlying technological architecture. Will it require deep biometric scans, or central government identity verification? Leaving this to subsequent rules risks creating highly intrusive digital identification systems that could easily destroy the very privacy rights the Act claims to protect.

The same problem plagues cross-border transfers under Section 16. The Act shifts from the strict "local storage" rules of earlier drafts to a loose blacklisting model where data flows anywhere unless the Central Government explicitly bans it. Because the law lacks explicit economic, diplomatic, or human rights criteria to guide these bans, data sovereignty becomes a matter of political expediency. The Act ceases to operate as a firm legislative code. It functions instead as an enabling framework, giving the executive broad authority to shape digital commerce without active parliamentary oversight.

[9] Vasanlal Maganbhai Sanjanwala v. State of Bombay, AIR 1961 SC 4 (India).

 [ISSN 2581-5369]

III. The State Exemption Matrix and the Triple-Test Validity

A data protection law can only be constitutionally legitimate if it holds the state and private corporations to the same standard of accountability. Section 17(2)(a) of the DPDP Act shatters this parity. It grants the Central Government absolute authority to exempt any instrument, agency, or organ of the State from the entire application of the Act.[10] The grounds for doing so are broad and subjective: sovereign security, public order, or the maintenance of foreign relations.

To see if Section 17(2)(a) can withstand constitutional scrutiny, we have to look at the three-part proportionality test laid down in Puttaswamy.[11] Any state-sponsored invasion of a citizen's privacy must clear three concurrent hurdles:

- Legality: The action must be backed by an explicit, unambiguous statutory law.
- Legitimate Objective: The restriction must map directly onto the state goals recognized under Article 19(2).
- Proportionality and Necessity: The state must use the least restrictive means available to achieve its purpose.

Section 17(2)(a) fails this third prong. By letting state agencies completely off the hook, the Act strips citizens of their rights to demand data accuracy (Section 8(3)), enforce data erasure (Section 12), or receive notifications when their data is breached (Section 8(6)). This creates an asymmetric regulatory environment.

Compare this with Article 23 of the GDPR.[12] European member states can restrict data protection obligations only when it is a strictly necessary and proportionate measure in a democratic society to safeguard national security or public safety. Crucially, the GDPR requires the law to specify the exact categories of data, the scope of the restriction, and the precise safeguards against abuse.

The Indian law contains no such guardrails. The moment a state agency is exempted under Section 17(2)(a), its operations vanish into a regulatory black hole. The Data Protection Board of India (DPBI) losing all supervision over them means citizens have zero independent remedy against mass state surveillance, bulk data retention, or algorithmic profiling. This creates a system of administrative exceptionalism where the state operates entirely outside the law, raising serious constitutional questions under the equality guarantees of Article 14.

---

[10] The Digital Personal Data Protection Act, 2023, § 17(2)(a), No. 22, Acts of Parliament, 2023 (India).
[11] Puttaswamy, (2017) 10 SCC 1 at ¶ 310.
[12] GDPR, *supra* note 7, at art. 23.

 [ISSN 2581-5369]

IV. The Data Protection Board of India: An Institutional Critique

Even the strongest rights in a statute are useless without an independent enforcement mechanism. The Supreme Court has repeatedly affirmed—most clearly in Modern Dental College & Research Centre v. State of Madhya Pradesh—that specialized regulatory bodies must remain structurally independent from the executive branch if they are to carry out their oversight duties effectively.[13] Yet, looking at the institutional design of the DPBI under Sections IV and V of the Act, its operational autonomy appears compromised from the start.

The institutional vulnerabilities are built directly into the structure:

- Appointment Mechanism (Section 19): The selection process is entirely controlled by the Central Government, completely bypassing independent judicial or parliamentary oversight panels.
- Tenure and Service Terms (Section 20): There is no fixed statutory security of tenure. The length of service and compensation terms are left to the executive to write via rules.
- Operational Funding (Section 21): The Board is fully dependent on central budgetary allocations, destroying financial autonomy.

This setup stands in contrast to other specialized regulatory bodies in India. The Competition Commission of India (CCI)[14] and the Securities and Exchange Board of India (SEBI)[15] have selection panels that explicitly include judicial figures or independent experts to buffer them from political interference.

By keeping the DPBI on an administrative leash, the Act creates an institutional conflict of interest. The state is, by definition, the largest data collector and processor in the country. The DPBI is therefore expected to act as an impartial referee in disputes where its own employer—the executive—is the defendant. A board that relies on the government for its appointments, salary updates, and operational survival will face severe structural pressures when trying to hold a government department accountable for a massive data leak. It risks acting as a bureaucratic rubber stamp rather than an independent defender of privacy.

[13] Modern Dental College & Research Centre v. State of Madhya Pradesh, (2016) 7 SCC 353 (India).
[14] The Competition Act, 2002, § 8, No. 12, Acts of Parliament, 2003 (India).
[15] The Securities and Exchange Board of India Act, 1992, § 4, No. 15, Acts of Parliament, 1992 (India).

 [ISSN 2581-5369]

V. The Dilution of the Right to Information: The Amendment to Section 8(1)(j)

The structural choices of the DPDP Act create a clear legal conflict with democratic transparency, primarily through its quiet amendment to Section 8(1)(j) of the Right to Information (RTI) Act, 2005.[16] Before this amendment, the RTI Act had a carefully constructed balance. It exempted personal information from public disclosure only if that information had no connection to public activity or if it caused an unwarranted invasion of individual privacy. Most importantly, it contained a vital democratic proviso: "Provided that the information, which cannot be denied to the Parliament or a State Legislature shall not be denied to any person."[17]

The DPDP Act completely strikes down this balancing framework, substituting an absolute prohibition on the disclosure of personal information.[18] This change removes the requirement to evaluate whether the public interest in transparency outweighs the privacy interest of an individual.

This amendment fundamentally weakens democratic accountability. Public officials can now use the incredibly broad definition of "personal data" under Section 2(t) of the DPDP Act as an all-encompassing shield to reject legitimate RTI requests. We are already seeing this used to block public access to crucial accountability records:

- The asset and liability declarations of public servants.
- Verified beneficiary lists under major government welfare schemes.
- The disciplinary records and corruption histories of bureaucrats.
- Educational credentials submitted during public recruitment drives.

By removing the public interest exception, the Act breaks the complementary relationship between transparency and privacy, both of which are rooted in Articles 19(1)(a) and 21. Instead of building a sophisticated ecosystem where both rights enhance each other, the DPDP Act uses privacy as an excuse to limit transparency, shielding state operations from public view and weakening the RTI framework.

[16] The Right to Information Act, 2005, § 8(1)(j), No. 22, Acts of Parliament, 2005 (India).
[17] *Id.* at § 8(1)(j) proviso.
[18] The Digital Personal Data Protection Act, 2023, § 26, No. 22, Acts of Parliament, 2023 (India).

 [ISSN 2581-5369]

VI. Comparative Analysis: The DPDP Act vs. the European Union GDPR

A comparative analysis with the European Union's GDPR highlights the unique characteristics and limitations of the Indian regulatory model. While the DPDP Act adopts familiar terminology —using "Data Fiduciaries" for Controllers and "Data Principals" for Data Subjects—the underlying philosophies of the two regimes are completely different.

Consider the baseline lawful grounds for processing data. The GDPR sets out a balanced framework across multiple distinct bases, including contractual necessity, legal obligations, and legitimate interests. The DPDP Act, by contrast, relies almost entirely on consent, supplemented by a broad "Legitimate Uses" clause under Section 7. This section allows data processing without consent for any "specified purpose" where a user has voluntarily provided their information, a provision that lacks the strict, clear limitations found in European data protection law.

Furthermore, look at the actual rights granted to individuals. While the GDPR explicitly guarantees the Right to Data Portability (Article 20) and a comprehensive Right to Erasure (Article 17), the DPDP Act drops portability entirely and limits erasure to cases where a user actively withdraws consent.

The most revealing difference is Section 15 of the Indian Act, which introduces enforceable duties for Data Principals, backed by fines of up to ten thousand rupees if an individual files a "false or frivolous" complaint with the DPBI. Such punitive measures against data subjects are unusual in global privacy laws. By threatening citizens with penalties for bad complaints, the Act risks creating a chilling effect that discourages ordinary individuals from challenging powerful corporate or state entities. This structural choice prioritizes corporate and administrative efficiency over rights enforcement.

VII. Conclusion and Recommendations for Juridical Re-Alignment

The Digital Personal Data Protection Act, 2023, establishes a basic statutory framework for data protection in India, but its current architecture presents significant constitutional challenges. By relying on extensive executive delegation, broad state exemptions, and an enforcement body with limited institutional independence, the Act falls short of the robust, rights-protective standards envisioned in Justice K.S. Puttaswamy v. Union of India. To align the statute with constitutional requirements and international best practices, the following targeted amendments are recommended:

 [ISSN 2581-5369]

- Enact Statutory Limits on Executive Rules: Amend Section 40 to include clear guidelines for all delegated legislation, ensuring that key issues such as age verification mechanisms and cross-border data transfer parameters are subject to parliamentary review.
- Introduce Judicial Oversight for State Exemptions: Modify Section 17(2)(a) to require that any state exemption be reviewed and approved by an independent judicial authority, applying a strict proportionality test to prevent unauthorized surveillance.
- Reform the Selection Process for the DPBI: Revise Section 19 to establish an independent selection committee for the DPBI, led by judicial officials and independent technical experts, to secure its autonomy from the executive branch.
- Restore the Balancing Test in the RTI Act: Repeal the absolute barrier introduced to Section 8(1)(j) of the Right to Information Act, restoring the public-interest balancing test to maintain democratic transparency.

Without these structural corrections, the DPDP Act risks serving as a statutory tool for executive convenience rather than a protective shield for individual rights. The true test of India's data protection regime will be its willingness to address these foundational gaps, ensuring that the fundamental right to digital privacy is protected against both state overreach and commercial exploitation.

*****

 [ISSN 2581-5369]