Impact Factor (QJIF): 8.47 E-ISSN: 2583-1615, P-ISSN: 3049-3498

International Journal of Research in Academic World

Received: 06/April/2026 **IJRAW:** 2026; 5(6):88-91 **Accepted:** 09/May/2026

Digital Personal Data Protection Act, 2023: A Balancing Act between Digital Sovereignty and Individual Rights in India's Data Governance

[*1]Unnati Pandey and [2]Dr. Babita Verma

[*1]Research Scholar, Lakshmibai College, University of Delhi, Delhi, India.

[2]Associate Professor, Lakshmibai College, University of Delhi, Delhi, India.

Abstract

The 'Digital Personal Data Protection' (DPDP) Act, 2023 is India's first comprehensive 'Digital privacy law' that establishes a framework for processing digital personal data, safeguarding individual's rights to privacy as a fundamental right under article 21 (Right to life and personal liberty) while enabling lawful use of their data. The act applies to digital data within India and data processed outside India for goods and services provided to Indian residents. This article evaluates the DPDP Act against the constitutional standard established in Puttaswamy that is the triple test of legality, necessity, proportionality and combines this doctrinal analysis with original survey data from 87 respondents in Delhi-NCR to check the balance between the digital sovereignty and individual rights.

The analysis finds that the act passes the legality requirement and partially meets the necessity requirement for provisions governing private data fiduciaries, the broad executive exemption under Section 17(2) for state instrumentalities fails to satisfy the proportionality test. The empirical findings reveal a significant gap between citizens stated privacy concerns (93% consider data privacy "extremely important") and their actual understanding of the law (only 7% report a strong understanding), alongside low public trust in the government as a data custodian (12.3%) relative to demand for symmetric accountability standards (87.8% favor equal standards for state and private entities).

This article concludes that the DPDP Act is not balanced. It acts as shield against the Private entities and sieve against the state and also suggest some policy recommendations that are judicial oversight and independence of board, narrowing the exemption under section 12 and improve public digital literacy as a constitutional obligation.

Keywords: Digital Personal Data Protection, Data Sovereignty, Data security, Proportionality Test, Individual Rights, Right to privacy.

Introduction

Digitalization in India has been unprecedented from past decade in both speed and scale this happened with the combination of different sectors. Data has increasingly been recognized as a critical economic resource, often described as the "new oil" but unlike oil it's not just an economic resource it's deeply personal to Individuals.

Platforms operating at national scale including UPI-based payment systems, Aadhaar-linked services, and digital health records to process 'sensitive personal data' of hundreds of millions of citizens on a daily basis. However, this expansion has not occurred without consequence. The growth of the data economy has been accompanied by a significant rise in data breaches, identity theft, UPI fraud, phishing attacks, and unauthorized surveillance. The absence of a comprehensive legal framework for data protection prior to 2023 left citizens largely without recourse, and businesses without clear obligations regarding data handling, storage, and accountability. The DPDP 2023 emerged not merely as a regulatory response to existing harms, but as a foundational instrument for governing India's digital future.

The Evolution: From Sectoral Laws to Comprehensive Legislation

- **The Pre-2017 Era**

Prior to 2017, India's data protection framework consisted of sectoral and largely inadequate provisions under the Information Technology Act, 2000, its 2008 amendment, and the 2011 Sensitive Personal Data or Information Rules. The main focus of these act were on sectoral approach focusing on e-commerce and digital communication but lack to protect individual rights.

- **Turning Point - Justice K S Puttaswamy 2017**

'K.S Puttaswamy VS Union of India' is widely recognized as watershed moment for DPDP act as this judgement shifted legal status of privacy in India from a vague concept to enforceable constitutional right. Right to privacy is declared as a fundamental right under article 21(Right to life and personal liberty) and introduced Triple Test-Legality, Legitimacy, Proportionality. Focus on Informational self-determination where individual have control over their data and personal information.

***Corresponding Author:** Unnati Pandey

Before this data is often viewed as property or commodity but after this data is viewed as an extension of human dignity and autonomy.

- **The struggle - Trial and Error**

Following the watershed Puttaswamy judgment, the 'Ministry of Electronics and Information Technology' (MeitY) constituted a 10-member committee of experts headed by Justice B.N. Srikrishna (a retired Supreme Court judge) in July 2017. Their mission was to build the blueprint for India's first dedicated data protection law.
Draft Bill DPDP, 2019 this was introduced but in 2022 it is withdrawn by government after criticism.

- **The Final Milestone**

The final version, the 'Digital Personal Data Protection Bill, 2023', was introduced, passed by both houses of Parliament, and received the President's assent on August 11, 2023, officially becoming the DPDP Act, 2023.

Structural Overview – The Three Pillars

- **The Data Principal**

The Data Principal is the one whose personal data is being collected or process by any Data fiduciary. They are granted a defined set of rights including the right to access information about how their data is processed, the right to correction and erasure, the right to grievance redressal, and the right to nominate another individual to exercise these rights in the case of death or incapacity.

- **The Data Fiduciaries**

The term "Data Fiduciary" in the 'DPDP Act' refers to any entity that determine the purpose and means a processing the data. It refers to the one that is collecting, processing, storing the data. Choice of term 'fiduciary' is also important because it means acting in another best interest. So, this entity not only own the data but they also hold the trust.
They are the one who decides on the purposes and means of the processing of personal data and who carries the primary compliance duties under the Act (e.g., the duty to acquire consent, implement reasonable security safeguards and inform both the DPBI and Data Principals affected, in case of a personal data breach).

- **The Data Protection Board — The Referee**

'Data Protection Board' is the institutional body between the 'Data Principle' and 'Data Fiduciary' that will act as a referee in case of grievances and penalties. But the independence of this board is often questioned because the appointment is done by the central government.

The Consent Framework and Its Limits

Section 6 states that processing of personal data by a Data Fiduciary shall be based on consent. The consent shall be free, specific, informed, unconditional and unambiguous, with a clear affirmative action. At first glance, this Section appears to bring the DPDP Act in line with the consent-driven models. However, Section 7 goes on to provide a significant exception where the Data Fiduciary is allowed to process personal data without consent for a variety of 'legitimate uses' this allows the government to use the personal data without any consent to provide any subsidy, benefit and services.
This matters because a huge amount of personal data in India is collected and used through government programs like Aadhaar, the Public Distribution System (PDS), Direct Benefit Transfers (DBTs), and various digital governance platforms. As a result, much of the data processing that affects citizens does not actually depend on consent.
Section 7 appears to exempt a significant proportion of the personal data processed in India from the concept of consent it laid down in Section 6. This seems to bring about a situation of 'consent asymmetry'. While private companies usually need a person's consent before using their data, government agencies can often rely on the "legitimate use" exception instead. In practice, this means that consent acts as a strong safeguard against private-sector data processing but a much weaker safeguard against government data processing, even though the government handles some of the largest volumes of personal data in the country.

Section 17(2) and the Proportionality Problem

The most important constitutional provision in the Act is Section 17(2). This section allows the Central Government to exempt any State agency from the provisions of the Act, including consent requirements, the rights of Data Principals, and the obligations of Data Fiduciaries. Such exemptions can be granted when the Government believes they are necessary in the interests of India's sovereignty and integrity, security of the State, friendly relations with foreign States, maintenance of public order, or prevention of offences related to these matters.
When the threefold test laid down in Puttaswamy is applied to this provision, the following observations can be made. First, the requirement of legality is satisfied because the power is contained in a validly enacted law. Therefore, there is a clear legal basis for the exemption. Second, the requirement of necessity is only partly satisfied. The objectives mentioned in the provision, such as national security, public order, and sovereignty, are undoubtedly legitimate State interests. However, the provision does not require the Government to show in each case that granting an exemption is actually necessary to achieve those objectives. Exemptions can be issued through a notification without explaining why a less restrictive measure would not be sufficient.
The most significant concern arises with regard to proportionality. The Supreme Court in Puttaswamy held that any restriction on the right to privacy must use the least restrictive means available and must include safeguards against arbitrary action by the State. Section 17(2), however, does not provide such safeguards. It does not set any time limit on exemptions, nor does it require periodic review. It also does not require prior or subsequent judicial approval. As a result, decisions regarding the necessity and scope of exemptions remain entirely within the discretion of the executive. Further, the provision does not require exemptions to be narrowly limited to a specific function or category of data processing. Instead, an exemption may apply to all or any provisions of the Act for any State instrumentality.
As a result, Section 17(2) gives the executive broad power to exclude State agencies from the data protection framework without any independent mechanism to verify whether such exemptions are proportionate to their stated purpose. This appears inconsistent with the Puttaswamy judgment, which emphasized that procedural safeguards are an essential part of a proportionate restriction on privacy rights. Therefore, this analysis concludes that while the Act satisfies the requirement of legality and substantially meets the requirement of necessity, it does not clearly satisfy the proportionality requirement of the Puttaswamy test.

Synthesis of Findings: Identifying the 'Balancing' Failure
The survey has 87 respondents in Delhi-NCR 54% aged 18–25 which reflects youngster dominated the survey. While the sample is concentrated among urban, digitally engaged respondents. The data collected throughout the survey have four core findings.

Finding I: The Awareness-Protection Gap
Despite 93% of respondents considering data privacy 'extremely important' in today's digital world and despite 61.4% being aware that the DPDP Act exists, only 7% claimed a 'Very Good' understanding of its provisions. A further 61.4% of respondents believed that Indians are aware of their data rights under the new law only 'to some extent,' while 36.8% felt they were 'not at all' aware. These two data points 'high awareness' of privacy as a value but having 'low awareness' of the law that is supposed to protect it define the Awareness-Protection Gap.

Finding II: The Sovereignty-Surveillance Paradox
The survey reveals a public that simultaneously supports digital sovereignty (77.2% favor data localization) and fears the consequences of unchecked state power (75.4% believe the Act grants the government too much power through national interest exemptions). This is not confusion it is the recognition of a genuine tension. Respondents support state control as a check on foreign corporations and they also resist state control as a tool of domestic surveillance. The' DPDP Act', by granting broad government exemptions without independent oversight. It has satisfied the sovereignty demand while ignoring the surveillance concern.

Finding III: The Consent Illusion
The legal architecture of the' DPDP Act' is premised on informed consent. This survey finds that 70.2% of respondents either find consent processes confusing, have never noticed them, or believe they are deliberately designed to confuse. When layered against the finding that only 7% have a 'Very Good' understanding of the Act, the picture is clear consent under the current framework is often procedural rather than substantive. The checkbox is ticked but the autonomy is not exercised.

Finding IV: The Asymmetric Accountability Demand
Perhaps the most legally decisive finding of this survey is the public near-unanimous demand for symmetric accountability. A combined 87.8% of respondents believe that private companies and the government should face either equal or comparably strict data protection standards. The DPDP Act, as analyzed creates a fundamentally asymmetric framework — private fiduciaries are subject to detailed compliance requirements and significant penalties, while the government can exempt itself from these obligations by invoking 'national interest.' The citizens surveyed here did not ask for this asymmetry. They did not endorse it. The Act, in this respect, reflects the preferences of the state rather than the preferences of those the state is meant to govern.

The Institutional Question: Board Independence
A further structural concern relates to the composition and accountability of the Data Protection Board of India. Under the Act, the appointment, tenure, and removal of Board members are determined by the Central Government and the board have to work against them in some cases under Section 7 and Section 17 exemption disputes. This raises a structural question of independence. The conduct of any individual Board member as an adjudicatory body whose composition is wholly determined by one category of regulated entity faces an inherent appearance of bias problem, regardless of the actual independence exercised by its members in practice. Comparative scholars have noted that the European Union's GDPR framework, by contrast, vests supervisory authority in bodies with statutorily entrenched independence from executive direction (Sonkar, 2025) as structural feature the DPDP Act does not replicate.

The Compliance Asymmetry and the Domestic Enterprise
An additional point of concern separate from the rights-based perspective above but related to the policy consistency of the Act, is the varied effect it would have on different sized entities regulated. The requirements laid out by the act for security measures, notification procedures and complaint redressal systems and data protection impact assessments for a "significant data fiduciary" are not substantially different whether the entity in question is a multinational technology giant or a small startup company, international entity who has likely established similar systems in response to the GDPR is well-equipped to meet the compliance costs whereas smaller domestic entities will have the weight of a similar regime on the proportions of their business (Kumar, 2024). If a goal of a strong digital sovereign posture is to nurture Indian digital companies over their foreign counterparts, then compliance requirements with disparate relative costs might prove counterproductive.

Policy Recommendation
The findings of this research point clearly toward a set of specific reforms.

Recommendation 1: Judicial Oversight and Board Independence
The most urgent reform is the restructuring of data protection board as of now, it is appointed by the executive and accountable to the executed. This must change.
The appointment should not be done entirely by the central government. The board appointment process should involve a collegium system comprising representative from different background for example judiciary, civil society and technology sector. In addition, the Board Member term should be fixed and non-renewable to eliminate corruption and biased decision making.

Recommendation 2: Narrowing the Section 12 Exemptions
Section 12 gives the government very broad and unclear powers to ignore the law. This is the biggest problem in the Act. Replace the general phase like 'national security' and 'public order' with a defined list of specific circumstances. Proportionate exemptions should be limited to contexts such as emergency medical response, genuine and specific national security threats that are subject to prior or immediate judicial review. The DPB should give the authority to check this exemption applied appropriately. Without any limitations on exemption this becomes the tool for state surveillance.

Recommendation 3: Public Digital Literacy as a Constitutional Obligation
The survey findings indicate that 47.4% of respondents became aware of the Act's enforcement body through media sources rather than through government efforts, while 17.5% reported having no understanding of the Act at all. A law

premised on informed consent cannot function if the state makes no serious effort to ensure citizens are informed. Government should increase public digital literacy.

Limitations

First, the survey sample of 87 respondents, while diverse and analytically useful, is not statistically representative of India's 1.4 billion people. The survey finding does reflect the indicative trend and qualitative inside about people knowledge.

Second, the DPDP Act is still in its early implementation phase. Many of the 2025 Draft Rules have not been finalized, and the Data Protection Board has not yet been formally constituted at the time of this writing.

Third, this study has focused primarily on the framework-level analysis of the Act and on urban educated citizens perceptions of it. The lived experience of data rights among India's most vulnerable populations the migrant workers who are using Aadhaar for welfare access, rural citizens navigating e-governance platforms, individuals whose data is processed by state systems without their knowledge are still left.

Fourth, the rapidly evolving nature of technology means that some of the Act's provisions will need to be assessed against a technological landscape that continues to shift significantly. The analysis offered here reflects conditions as of 2025 the trajectory of artificial intelligence, cloud computing, and data brokerage will require ongoing legal review.

Conclusion

The Digital Personal Data Protection Act, 2023 represents a significant legislative achievement: it establishes, for the first time, a comprehensive statutory framework for data protection in India, and it does so against the backdrop of a constitutional mandate established in Puttaswamy. Measured against that mandate's threefold test, however, the Act's record is mixed. It satisfies the legality requirement unambiguously. It substantially satisfies the necessity requirement, particularly with respect to the obligations it imposes on private Data Fiduciaries. It does not clearly satisfy the proportionality requirement with respect to the exemptions available to state instrumentalities under Section 17(2), which lack the temporal limitation, judicial oversight, and narrow tailoring that the proportionality standard contemplates.

The empirical findings presented above suggest that this doctrinal asymmetry is not merely a matter of legal abstraction but corresponds to a measurable public perception that the Act's accountability standards are not symmetrically applied, and to a measurable gap between the importance citizens attach to data privacy and their capacity to understand and exercise the rights the Act confers. Addressing this asymmetry through institutional reform of the Data Protection Board, narrower and more accountable exemption provisions, and sustained investment in digital literacy would move the DPDP Act closer to the constitutional standard it was enacted to fulfil, without requiring any compromise of the legitimate digital sovereignty objectives the Act was also designed to advance.

References

1. Article-14. How India's new data law enables a surveillance regime. 2024.
2. *Constitution of India*, Art. 21.
3. Digital Personal Data Protection Act, 2023, No. 40, Acts of Parliament (India).
4. Digital Personal Data Protection Rules, 2025 (Draft).
5. European Union. General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679). 2016.
6. Information Technology Act, 2000.
7. Information Technology (Amendment) Act, 2008.
8. *Justice K. S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
9. Kashyap R. Data security concerns in public-private partnerships. 2023.
10. Kaur H. Global standards and the citizen-centric approach in India's privacy regime. 2025.
11. Kumar A. Digital sovereignty and cross-border transfer restrictions. 2024.
12. Ministry of Electronics and Information Technology. A free and fair digital economy: Protecting privacy, empowering Indians (Justice B. N. Srikrishna Committee Report). 2018.
13. Pandey U. Data democracy in practice: An empirical study of public perception of the DPDP Act, 2023 [Unpublished bachelor's thesis]. University of Delhi; 2026.
14. Sharma V. Growth of India's digital economy and government exemptions. 2023.
15. Sonkar S. Comparative study: DPBI vs. EU GDPR independence. 2025.