THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023 AND THE RIGHT TO PRIVACY: A CRITICAL ANALYSIS OF INDIA'S NEW DATA PROTECTION REGIME

by

Dr. Prashant Yadav,
Advocate

ABSTRACT

The Digital Personal Data Protection Act, 2023, read with the Digital Personal Data Protection Rules, 2025 notified on 13 November 2025, constitutes India's first comprehensive statutory framework for digital personal data. Anchored in the nine-judge Bench ruling in Justice K.S. Puttaswamy (Retd.) v. Union of India that elevated informational privacy to a fundamental right under Article 21, the Act translates constitutional guarantees into obligations on Data Fiduciaries and rights of Data Principals. This paper critically examines whether the DPDP framework realises the Puttaswamy standards of legality, necessity and proportionality. It scrutinises the consent-centric architecture and 'legitimate uses' under Sections 4 to 7, the rights under Sections 11 to 14, the institutional design of the Data Protection Board of India, the breadth of State exemptions under Sections 7 and 17, the amendment to Section 8(1)(j) of the Right to Information Act, 2005 via Section 44(3), and the phased enforcement timeline culminating in full compliance on 13 May 2027. Drawing on comparative insights from the GDPR and the constitutional challenges pending before the Supreme Court, the paper argues that while the Act marks a decisive legislative advance, structural features, particularly expansive executive exemptions, limited regulatory independence, and the dilution of public-interest overrides, risk subordinating the right to privacy to administrative convenience and State surveillance imperatives. Meaningful realisation of constitutional privacy therefore requires robust judicial scrutiny and targeted legislative refinement.

Keywords: Digital Personal Data Protection Act 2023; informational privacy; Puttaswamy; proportionality; Data Protection Board; Right to Information Act; GDPR comparative analysis

1. Introduction: From Constitutional Recognition to Statutory Architecture

The right to privacy in India travelled a long and contested path before receiving unambiguous constitutional recognition.[1] In August 2017, a nine-judge Bench of the Supreme Court held that privacy, including informational privacy, is intrinsic to the guarantee of life and personal liberty under Article 21 of the Constitution, and that any State incursion into that right must satisfy a three-fold test of legality, legitimate aim, and proportionality. For six years thereafter, India possessed a constitutional right to informational privacy but no comprehensive statute translating that right into enforceable obligations on those who process personal data. The Digital Personal Data Protection Act, 2023[2], and the Digital Personal Data Protection Rules, 2025, notified on 13 November 2025[3], close that vacuum. This paper argues that while the DPDP framework represents a decisive legislative advance, four structural features, namely broad executive exemptions, a Board that is not institutionally independent, the dilution of the Right to Information Act's public-interest override, and gaps in the rights architecture, together mean that the regime falls short of the standards Puttaswamy demands. The argument proceeds cumulatively across seven sections, culminating in a case for calibrated judicial reading-down and targeted legislative refinement before the regime attains full force on 13 May 2027.

1.1. The Puttaswamy Mandate and the Pre-2023 Vacuum

Puttaswamy did more than declare privacy a fundamental right; it supplied a working test. Restrictions on informational privacy must rest on law, pursue a legitimate State aim, and be proportionate and necessary, with the least intrusive means preferred.[4] Before 2023, the only statutory anchor was Section 43A of the Information Technology Act, 2000[5],

[1] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).
[2] Digital Personal Data Protection Act, No. 22 of 2023, INDIA CODE (2023) [hereinafter DPDP Act].
[3] Digital Personal Data Protection Rules, 2025, G.S.R. 846(E) (India) (notified Nov. 13, 2025) [hereinafter DPDP Rules].
[4] Puttaswamy, supra note 1, ¶¶ 310, 325-326 (Chandrachud, J.).
[5] Information Technology Act, No. 21 of 2000, § 43A, INDIA CODE (2000).

supplemented by the 2011 Sensitive Personal Data Rules[6], a compensation provision addressed to corporate bodies rather than a rights-based regime, and silent on State processing altogether.

1.2. Scope, Methodology and Structure of the Argument

The analysis is principally doctrinal, testing the statutory text of the Act and the 2025 Rules against the Puttaswamy standard, and secondarily comparative, using the European Union's General Data Protection Regulation[7] to sharpen the critique. The paper also situates its argument within three writ petitions currently pending before the Supreme Court, which raise overlapping constitutional objections and have already been referred to a larger Bench.[8] Each subsequent section supplies one link in a cumulative chain: description of the statutory architecture, doctrinal testing of the consent and legitimate-use bases, evaluation of the rights and institutional design, scrutiny of State exemptions and the RTI amendment, and comparative confirmation, before the conclusion draws the threads together.

2. Foundational Architecture of the DPDP Regime

The DPDP Act builds around five moving parts: a binary basis for lawful processing, notice obligations, a defined set of Data Principal rights, graduated obligations on Data Fiduciaries, and an adjudicatory body, the Data Protection Board of India.[9] The Rules, in force in phases beginning 14 November 2025, with Consent Manager registration from 13 November 2026 and the remaining substantive obligations from 13 May 2027, operationalise this architecture.[10] An accurate account of this design is a necessary precondition to testing its constitutional adequacy.

[6]Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, G.S.R. 313(E) (India).
[7]Regulation (EU) 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, 2016 O.J. (L 119) 1 [hereinafter GDPR].
[8]See infra Section 6.2.
[9]DPDP Act, supra note 2, §§ 4-14, 18-26.
[10]DPDP Rules, supra note 3, r. 1(2)-(3).

2.1. Consent, Notice and Legitimate Uses under Sections 4-7

Section 4 permits processing only on the basis of consent under Section 6 or one of the enumerated legitimate uses under Section 7.[11] Section 5 requires an itemised notice, in English or a Scheduled language, stating the purpose of processing and the manner of exercising the right to withdraw consent and lodge a grievance. Unlike the GDPR's six lawful bases, of which the open-ended 'legitimate interests' ground is among the most frequently invoked, the DPDP Act offers no general legitimate-interest ground; every non-consensual processing activity must instead fit within one of nine closed categories in Section 7, ranging from the voluntary provision of data to State functions and employment.

2.2. Rights of Data Principals and Institutional Framework

Sections 11 to 14 confer rights of access, correction and erasure, grievance redressal, and nomination on death or incapacity.[12] Sections 18 to 26 establish the Data Protection Board of India as the adjudicatory authority, with power to inquire into breaches and to impose penalties of up to two hundred and fifty crore rupees.[13] The Board's establishing provisions took immediate effect on notification of the Rules, while its full jurisdiction, along with the substantive Data Fiduciary obligations, activates only on 13 May 2027, leaving an extended interval in which the statutory right exists on paper before it becomes fully enforceable.

3. Testing the Consent Architecture against Puttaswamy Standards

Applying the necessity and proportionality limbs of Puttaswamy to the binary processing model exposes two related deficits. First, the consent mechanism, though textually robust, risks operating formalistically in practice. Second, the legitimate-use categories are not narrowly tailored to the ends they purport to serve, and their invocation is largely self-assessed rather than independently authorised.

3.1. The Narrowness of Valid Consent and the Risk of Formalism

[11]DPDP Act, supra note 2, §§ 4, 6-7.
[12]DPDP Act, supra note 2, §§ 11-14.
[13]DPDP Act, supra note 2, §§ 18, 27.

Section 6 requires that consent be free, specific, informed, unconditional and unambiguous, evidenced by a clear affirmative act, and capable of being withdrawn as easily as it was given.[14] In principle this tracks the Puttaswamy insistence on genuine, informed autonomy. In practice, the 2025 Rules permit consent notices to be presented through standardised, templated formats administered through registered Consent Managers, a design that risks reducing the exercise of consent to a single affirmative click made under conditions of information asymmetry and unequal bargaining power, particularly where realistic alternatives to a given digital service do not exist.[15] The formal architecture of consent is therefore necessary but not, without more, sufficient to satisfy the substantive proportionality inquiry Puttaswamy requires.

3.2. Legitimate Uses as a Parallel Track: Necessity and Proportionality Deficits

The nine legitimate-use categories in Section 7 include processing for the performance of State functions, compliance with law, medical emergencies, and employment purposes.[16] Two categories bear particularly heavily on the individual: State-function processing, which permits processing for the provision of any subsidy, benefit, service, certificate, licence or permit, and employment-related processing, which permits processing without consent for a broad range of employer purposes. Neither category is subject to independent prior authorisation, a data-minimisation threshold, or an external necessity review of the kind Puttaswamy contemplates; the Data Fiduciary itself determines whether processing falls within the exemption, subject only to after-the-fact Board scrutiny. This self-assessed necessity inverts the proportionality burden that Puttaswamy places on the State, and by extension on those exercising State-delegated functions.

4. Rights Architecture and Institutional Design: Effective Remedies?

A rights regime is only as strong as the body that enforces it and the completeness of the entitlements it confers. This section evaluates both, and engages the counter-argument that

[14]DPDP Act, supra note 2, § 6.
[15]DPDP Rules, supra note 3, r. 3-4, sched. 1.
[16]DPDP Act, supra note 2, § 7.

steep pecuniary penalties and a digitally accessible Board provide sufficient deterrence regardless of institutional design.

4.1. Completeness of Data Principal Rights and Missing Safeguards

The DPDP Act omits three protections common to mature data-protection regimes: a standalone right to data portability, a general right to object to processing, and specific safeguards against solely automated decision-making.[17] The 2025 Rules require Data Fiduciaries to respond to access and correction requests, but permit response timelines running up to ninety days in specified circumstances.[18] A ninety-day window sits uneasily with the urgency ordinarily associated with a fundamental right, particularly for data subjects seeking to correct inaccurate information used in credit, employment or welfare decisions.

4.2. Independence and Composition of the Data Protection Board

The Board's Chairperson and Members are appointed by the Central Government on the recommendation of a Selection Committee dominated by government nominees, for a tenure of two years, renewable, with no requirement of a sitting or retired judicial member.[19] The Central Government additionally retains a power to issue directions to the Board on questions of policy. The Supreme Court's tribunal jurisprudence treats security of tenure, an independent and non-executive-dominated selection process, and the presence of judicial members as constitutionally necessary safeguards for adjudicatory bodies exercising functions that would otherwise fall to courts.[20] Measured against that jurisprudence, a two-year, executive-appointed, non-judicial Board adjudicating claims arising from a fundamental right presents a structural independence deficit that the availability of statutory appeal does not fully cure, since appellate correction after the fact is not a substitute for first-instance independence.

[17] DPDP Act, supra note 2, §§ 11-14 (omitting equivalents to GDPR arts. 20-22, supra note 7).
[18] DPDP Rules, supra note 3, sched. 2.
[19] DPDP Act, supra note 2, §§ 19-20.
[20] Union of India v. R. Gandhi, President, Madras Bar Ass'n, (2010) 11 S.C.C. 1 (India); Rojer Mathew v. South Indian Bank Ltd., (2020) 6 S.C.C. 1 (India).

5. State Exemptions, Surveillance Risks and the RTI Dilution

It is in the exemptions under Sections 7 and 17, and in the RTI amendment carried through Section 44(3), that the proportionality deficit identified above becomes most acute, converting privacy from a guaranteed entitlement into a contingent one.

5.1. Breadth of Exemptions under Sections 7 and 17 and Absence of Judicial Oversight

Section 17 empowers the Central Government, by notification, to exempt any instrumentality of the State from the Act's obligations, including notice, purpose-limitation and data-retention obligations, in the interests of sovereignty, security of the State, public order, or the prevention, investigation or prosecution of offences.[21] The exemption is triggered by executive notification rather than case-specific judicial or quasi-judicial authorisation, and the Act prescribes no sunset clause, proportionality threshold, or independent oversight mechanism comparable to what Puttaswamy demanded of surveillance and interception regimes.[22] Read together with Section 36, which grants the Central Government power to call for information from Data Fiduciaries and intermediaries, the exemption architecture concentrates a wide surveillance-adjacent capability in the executive with limited external checks.[23]

5.2. Section 44(3) and the Recalibration of the RTI-Privacy Balance

Section 44(3) substitutes Section 8(1)(j) of the Right to Information Act, 2005, removing the public-interest override that previously required a public authority to disclose personal information where the public interest in disclosure outweighed the harm to privacy.[24] The Supreme Court had construed that override in Central Public Information Officer, Supreme Court of India v. Subhash Chandra Agarwal to require a case-by-case weighing of privacy against public interest, including in matters touching judicial appointments and asset

[21]DPDP Act, supra note 2, § 17.
[22]Puttaswamy, supra note 1, ¶¶ 638-641 (Kaul, J.).
[23]DPDP Act, supra note 2, § 36; DPDP Rules, supra note 3, r. 23.
[24]DPDP Act, supra note 2, § 44(3) (amending Right to Information Act, No. 22 of 2005, § 8(1)(j), INDIA CODE (2005)).

disclosures.[25] The amended provision permits withholding of any information that qualifies as personal information without that balancing exercise, a change RTI activists and journalists argue removes precisely the tool investigative reporting relies upon to expose maladministration. The counter-argument, that Section 8(2) of the RTI Act still permits disclosure where public interest outweighs exempted harm, does not fully answer the objection: Section 8(2) has traditionally operated as a residual override for the exemptions in Section 8(1) generally, and its scope once the specific personal-information override in Section 8(1)(j) has itself been narrowed remains contested and is presently before the Supreme Court.

6. Comparative Insights from the GDPR and the Pending Constitutional Challenges

A brief comparative glance at the GDPR, and at the litigation already testing the DPDP regime in the Supreme Court, confirms that the design choices critiqued above are neither inevitable nor externally compelled.

6.1. Lawful Bases, Rights and Institutional Independence: GDPR Benchmarks

The GDPR recognises six lawful bases for processing, including an open legitimate-interests ground subject to a documented balancing test against the data subject's interests.[26] It confers rights to data portability and to object to processing, including profiling, that have no DPDP counterpart.[27] Supervisory authorities under the GDPR must act with complete independence, a guarantee reinforced by security of tenure and a prohibition on seeking or taking instructions from any government.[28] Restrictions on data-subject rights for reasons of State security or defence must be provided for by a legislative measure that is itself necessary and proportionate and that respects the essence of the

[25] Cent. Pub. Info. Officer, Sup. Ct. of India v. Subhash Chandra Agarwal, (2020) 5 S.C.C. 481 (India).
[26] GDPR, supra note 7, art. 6(1)(f).
[27] GDPR, supra note 7, arts. 20-21.
[28] GDPR, supra note 7, art. 52.

fundamental right.[29] Each of these features answers, in the European context, precisely the structural deficit this paper identifies in the Indian regime.

6.2. Pending Litigation as a Constitutional Safety-Valve

Three writ petitions, Venkatesh Nayak v. Union of India, The Reporters Collective Trust v. Union of India, and National Campaign for People's Right to Information v. Union of India, are pending before the Supreme Court, challenging the Section 44(3) RTI amendment, the breadth of Section 36 and Rule 23, and the independence of the Board.[30] On 16 February 2026, a three-judge Bench headed by the Chief Justice of India issued notice, referred the matters to a five-judge Constitution Bench, and declined to grant an interim stay.[31] These petitions supply the doctrinal safety-valve this paper's argument anticipates: a forum in which the necessity and proportionality deficits identified above can be tested and, if the Court agrees, cured through reading-down before the regime attains full force on 13 May 2027.

7. Conclusion: Earning Constitutional Fidelity through Judicial and Legislative Vigilance

The DPDP Act and the 2025 Rules are, on any fair reading, a decisive advance over the pre-2023 vacuum in which Section 43A of the Information Technology Act stood as the only statutory response to a constitutionally entrenched right. That advance does not, however, complete the constitutional project Puttaswamy set in motion. The cumulative analysis in the preceding sections, self-assessed necessity under the legitimate-use categories, an executive-dominated and non-judicial Board, unbounded State exemptions without independent authorisation, and the removal of the RTI public-interest override, reveals a pattern rather than an isolated defect: each provision resolves a tension between

[29]GDPR, supra note 7, art. 23.
[30]Venkatesh Nayak v. Union of India, W.P.(C) No. 177/2026 (India); The Reporters Collective Trust & Anr. v. Union of India & Ors., W.P.(C) No. 211/2026 (India); Nat'l Campaign for People's Right to Info. v. Union of India, W.P.(C) No. 212/2026 (India).
[31]See The Reporters Collective Trust & Anr. v. Union of India & Ors., W.P.(C) No. 211/2026 (order dated Feb. 16, 2026) (India).

privacy, State convenience and commercial interest in favour of the latter two, without the external checks Puttaswamy requires.

7.1. Summary of Structural Shortfalls

Four shortfalls recur across the analysis: closed but self-applied legitimate-use categories in place of a supervised necessity test; a Board that lacks tenure security and judicial composition; State exemptions triggered by executive notification rather than case-specific authorisation; and a rights architecture missing portability, objection and automated-decision safeguards found in comparable regimes.

7.2. Dual Pathway for Realisation of Informational Self-Determination

Two pathways can close this gap before or after 13 May 2027. Judicially, the pending Constitution Bench reference offers an opportunity to read down Sections 7, 17 and 44(3) to import a necessity and proportionality filter consistent with Puttaswamy, and to require reasoned, case-specific authorisation for State exemptions. Legislatively, Parliament could narrow the legitimate-use categories, insert a judicial member and a fixed, non-renewable tenure into the Board's composition, and restore a public-interest balancing test to Section 8(1)(j) of the RTI Act. Absent one or both correctives, the DPDP regime risks functioning less as an instrument for realising the fundamental right recognised in Puttaswamy than as a framework for administratively managing it.