(JOINT JURIST)

e-ISSN -3139-6186

[NATIONAL-LEVEL | PEER-REVIEWED | OPEN-ACCESS LEGAL JOURNAL]

/ VOLUME 1 / ISSUE 3 / (AUGUST - SEPTEMBER 2026)

ABOUT THE JOURNAL

"Joint Jurist" is an online legal platform and a national publication which is aimed at spreading online legal education, bridging the gap between academic research and litigation expertise among the legal audience. It was introduced in early 2026. It is an independent project, started by its founder and does not receive any funding from any person or organisation or body or government as the case maybe.

It is a ***'Dream Project'*** of ***Mr. Suraj Shandil*** *(Advocate) (Founder-CEO-Editor-in-Chief & Owner)*. We operate on a Double-Blind Peer-Review model, ensuring that every published work meets the highest standards of original scholarship, zero plagiarism, and academic integrity. Our platform is dedicated to providing an open-access environment for legal professionals, scholars, and students to contribute to the evolving legal discourse.

EDITORIAL & ADVISORY BOARD

The Joint Jurist Journal is guided by a distinguished panel of legal luminaries and academicians committed to fostering excellence in legal scholarship.

- **Advocate Suraj Shandil**
- **(Dr.) Seema Gupta**
- **(Dr.) Mohd Rafiq**
- **(Dr.) Harshita Thalwal**
- **Ms. Sabrina Bath**
- **Ms. Soumya Sharma**
- **Mrs. Shivani Kumari**
- **(Dr.) Vanita Sharma**

© 2026 Joint Jurist (All Rights Reserved) e-ISSN -3139-6186

No part of this publication may be reproduced without prior written permission, except for educational purposes.

- **Mr. Vineet Kumar**
- **Ms. Sunayana**

NAME	DESIGNATION	INSTITUTION/AFFILIATION
Advocate Suraj Shandil	Founder, CEO & Editor-in-Chief	**High Court of Himachal Pradesh**
Prof. (Dr.) Seema Gupta	Editorial Board Member	**Associate Professor / Chandigarh University (CU)**
Prof. (Dr.) Mohd. Rafiq Dar	Editorial Board Member	**Associate Professor/Lovely Professional University (LPU)**
(Dr.) Harshita Thalwal	Editorial Board Member	**Associate Professor & HOD, Chandigarh University(CU)**
Asst. Prof. Ms. Somya Sharma	Editorial Board Member	**Professor of law & Ph.D. Scholar/ Shoolini University**
Asst. Prof. Ms. Sabrina Bath	Editorial Board Member	**Assistant Professor & Ph.D. Scholar/Chandigarh University (CU)**
Asst. Prof. Mrs. Shivani Kumari	Editorial Board Member	**Assistant Professor & Ph.D. Scholar/ DDM Sai Law College Himachal Pradesh**
Prof. (Dr.) Vanita Sharma	Editorial Board Member	**Associate Professor / Chandigarh University (CU)**

© 2026 Joint Jurist (All Rights Reserved) e-ISSN -3139-6186

No part of this publication may be reproduced without prior written permission, except for educational purposes.

Asst. Prof. Mr. Vineet Kumar	Editorial Board Member	**Professor of law / Shoolini University**
Asst. Prof. Ms. Sunayana	Editorial Board Member	**Assistant Professor & Ph.D. Scholar/ Himachal Pradesh National Law University Shimla**

© 2026 Joint Jurist (All Rights Reserved) e-ISSN -3139-6186

No part of this publication may be reproduced without prior written permission, except for educational purposes.

e-ISSN -3139-6186

"CONSENT WITHOUT POWER: STRUCTURAL FAULT LINES IN INDIA'S DIGITAL PERSONAL DATA PROTECTION ACT, 2023 "

(RESEARCH PAPER)

AUTHOR:

Shivansh Verma

Advocate

Abstract

Six years after *Puttaswamy* made privacy a fundamental right, Parliament gave India its first data protection statute. Three years after that, the Digital Personal Data Protection Act, 2023 remains more promise than regime. This paper argues the gap is structural, not transitional. The Act's consent architecture demands what no real business can deliver — notices in twenty-two languages, verifiable parental consent, withdrawal chased down entire data pipelines — and will produce ritual compliance instead of autonomy. Its regulator, the Data Protection Board of India, exists in the statute book but has no chairperson, no members, and no orders to its name. Its exemptions let the state step outside the Act by notification, on grounds as elastic as "public order", with no reasons recorded, no time limit, and no review — a design that sits uneasily with *Puttaswamy*'s own proportionality test. Tested against recent case law, including the Supreme Court's July 2026 intervention in *Abhishek Baxi*, and against the GDPR's very different institutional choices, the paper proposes six repairs: constitute the Board and free it from the executive, give victims compensation, discipline Section 17, add a legitimate-interests ground, harmonise the breach-reporting clocks, and get Consent Managers running before the substantive duties bite around May 2027. Consent without power, the paper concludes, protects data on paper while leaving power untouched.

Keywords: Data protection; DPDP Act 2023; right to privacy; consent; Data Protection Board; state surveillance; GDPR.

I. Introduction

Privacy became a fundamental right in this country on 24 August 2017 — nine judges, one conclusion: privacy flows from Article 21 and Article 19, and any state intrusion must clear three hurdles called legality, legitimate aim, and proportionality.[1] I was still in school when it was decided. I met the judgment properly in law school, studying it the way my generation of students studied everything that mattered — and it made data protection feel like the future of constitutional law.

The future took its time getting here.

© 2026 Joint Jurist (All Rights Reserved) e-ISSN -3139-6186

No part of this publication may be reproduced without prior written permission, except for educational purposes.

What followed was a legislative saga. The Srikrishna Committee report in July 2018.[2] The Personal Data Protection Bill, 2019, sent to a Joint Parliamentary Committee. Then — to everyone's surprise — a complete withdrawal in August 2022 and a redraft from scratch.[3] When the Digital Personal Data Protection Act finally received assent on 11 August 2023, the relief in privacy circles was genuine.[4]

I wish the relief had been justified.

Three years on, the Act is in force only in stages. The institutional shell stands; the duties that actually protect people do not bite yet, and will not

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

2Committee of Experts under Justice B.N. Srikrishna, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (July 2018).

3The Personal Data Protection Bill, 2019 was withdrawn in August 2022; the Digital Personal Data Protection Bill, 2022 was released for consultation in November 2022.

4The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023), assented to 11 August 2023.

until around May 2027.[5] The regulator the Act creates — the Data Protection Board of India — has no chairperson, no members, and has not passed a single order.[6] And in July 2026, the Supreme Court had to do the Board's job for it. In *Abhishek Baxi*, the Court examined APAAR — the twelve-digit lifelong student ID seeded from Aadhaar and DigiLocker — and directed that parental consent forms across the country must actually offer an opt-out.[7]

Read that again. Three years into a consent-based privacy law, the Supreme Court had to order that a consent form include a way to say no.

These are not teething troubles. They are three cracks running through the design itself.

The first crack is consent. The Act demands notices in twenty-two languages, verifiable parental consent for anyone under eighteen, and withdrawal signals propagated down entire data pipelines. No real business can deliver all of that. So businesses will perform compliance instead — box-ticking where autonomy was promised.

The second crack is enforcement. The Board is appointed by the executive it is meant to regulate, and the executive has not even bothered to constitute it. A right whose forum does not exist is a right in cold storage.

5The DPDP Rules, 2025 were notified on 13 November 2025 (G.S.R. 843(E)), with corrigendum in December 2025; institutional and definitional provisions commenced first, with substantive fiduciary obligations and data-principal rights widely expected to apply from around May 2027, eighteen months later. See MediaNama, "India notifies DPDP Rules 2025" (14 Nov 2025).

6See Part V below.

7*Abhishek Baxi v. Union of India*, W.P.(C) 832/2026, order dated 20 July 2026, 2026 SCC OnLine SC 1391.

© 2026 Joint Jurist (All Rights Reserved) e-ISSN -3139-6186

No part of this publication may be reproduced without prior written permission, except for educational purposes.

The third crack is the state itself. Section 17 lets the government exempt any of its instrumentalities from the entire Act by notification — no reasons, no time limit, no review. It is hard to square that with the proportionality test *Puttaswamy* laid down. The judgment that made this law necessary may be the judgment that undoes its broadest exemption.

What follows maps the Act as it stands, takes each crack in turn, measures the design against the GDPR, and proposes repairs. My claim is simple: a privacy law that cannot be enforced, whose consent is fictional, and from which the state is largely exempt, protects data on paper while leaving power exactly where it was. *Puttaswamy* promised more than that.

II. From *Puttaswamy* to the Statute Book

The backstory matters, because the delays were not accidental. They reveal what the state wanted this law to be — and what it did not.

Indian courts spent decades refusing to decide whether privacy was a fundamental right at all. *M.P. Sharma* (1954) and *Kharak Singh* (1962) both declined to recognise it, and the question festered for half a century. *Puttaswamy* ended the equivocation, but with a caveat that would matter enormously: privacy was not absolute. Every intrusion had to pass legality, legitimate aim, and proportionality — necessary, and the least restrictive means available.[8] Remember that third hurdle. It comes back.

The legislative response began fast and then stalled. The Srikrishna Committee's *A Free and Fair Digital Economy* arrived in July 2018.[9] The

8*Puttaswamy*, supra note 1, per Chandrachud J. (plurality): legality, legitimate aim, and proportionality (including necessity and least-restrictive-means).

9Srikrishna Committee Report, supra note 2.

2019 Bill went to a Joint Parliamentary Committee. And then, in August 2022, the government simply withdrew it.[10] No other major economy writes privacy law this way — scrapping years of committee work and starting over. The replacement, the Digital Personal Data Protection Bill, 2022, went up for consultation that November, and the final Act passed in August 2023.[11] Shorter, simpler, and — as this paper will argue — structurally weaker than what the committee had imagined.

Then came the waiting. Draft Rules on 3 January 2025. Final DPDP Rules notified on 13 November 2025.[12] Phased commencement after that: definitions and institutions first, substantive duties — notice, consent, safeguards, breach reporting, children's data, data-principal rights — only around May 2027, eighteen months after the Rules.[13] The 2011 SPDI Rules under the IT Act hold the fort meanwhile.[14]

So here is where things stand in late 2026: India has a data protection statute but not a data protection regime. Everything this paper says must be read against that fact — what the text promises, what has actually been built, and what the design makes unlikely to ever work.

III. How the Act Is Built

10PDP Bill, 2019, supra note 3.

11DPDP Act, 2023, supra note 4.

© 2026 Joint Jurist (All Rights Reserved) e-ISSN -3139-6186

No part of this publication may be reproduced without prior written permission, except for educational purposes.

12Draft DPDP Rules released 3 January 2025; final DPDP Rules, 2025 notified 13 November 2025.

13DPDP Rules, 2025, supra note 5.

14The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

Strip away the commentary and the Act is a short statute — forty-four sections, eight chapters, three characters. The Data Principal is the individual the data is about. The Data Fiduciary decides why and how it gets processed. The Data Processor just follows the fiduciary's instructions.[15] Note the word "fiduciary". It imports trust, loyalty, care — the vocabulary of doctors and trustees. The Act's great gamble is that consent, collected at scale through screens, can manufacture that kind of trust.

Here is how the machine is supposed to work.

Notice first. Before or while seeking consent, the fiduciary must give a standalone, itemised notice — what data, for what purpose, what rights you hold, how to withdraw, whom to complain to.[16] Then comes Section 5(3), which I consider the Act's most well-meaning unworkable provision: the notice must be available in English and, at the principal's option, in any of the twenty-two Eighth Schedule languages.[17] Twenty-two. Consent itself must be free, specific, informed, unconditional and unambiguous, through clear affirmative action — given, managed and withdrawn, if you like, through a registered Consent Manager.[18] And Section 6(4): withdraw consent, and the fiduciary must stop processing and make its processors

15DPDP Act, 2023, s. 2 (definitions of Data Fiduciary, Data Principal, and Data Processor).
16DPDP Act, 2023, s. 5 (notice); s. 5(3) (twenty-two languages).

17DPDP Act, 2023, s. 5, supra note 16.

18DPDP Act, 2023, s. 6 (consent); s. 6(4) (effect of withdrawal); s. 6(7) (Consent Managers).

stop "within a reasonable time".[19] A simple sentence. A brutal engineering problem. I will come back to it.

No consent? Section 7 permits processing only on nine specified grounds — "certain legitimate uses": state functions, legal compliance, medical emergencies, disasters, employment, publicly available data, and a few more.[20] Closed list. And what is missing from it? Any general "legitimate interests" ground like Article 6(1)(f) of the GDPR.[21] So in practice the Act has two lawful bases: consent, and the state's exceptions to consent. Everything else lives in a grey zone.

Section 8 heaps duties on the fiduciary: reasonable security safeguards, and breach notification with real teeth — inform the Board "without delay" on learning of a breach, file a detailed report within seventy-two hours, tell every affected principal. No de-minimis threshold. No risk filter.[22] Children's data — under-eighteens — needs verifiable parental consent, and tracking, behavioural monitoring and targeted advertising directed at children are banned outright.[23] The government may designate Significant Data Fiduciaries, who must then appoint an India-based Data Protection

19DPDP Act, 2023, s. 6, supra note 18.

© 2026 Joint Jurist (All Rights Reserved) e-ISSN -3139-6186

No part of this publication may be reproduced without prior written permission, except for educational purposes.

20DPDP Act, 2023, s. 7 (certain legitimate uses, a closed list of nine grounds). Contrast Regulation (EU) 2016/679 (GDPR), Art. 6(1)(f) (legitimate interests).

21DPDP Act, 2023, s. 7, supra note 20.

22DPDP Act, 2023, s. 8(5) (reasonable security safeguards); s. 8(6) (breach notification: intimation to the Board "without delay," detailed report within seventy-two hours, and notification to affected principals; no de-minimis threshold).

23DPDP Act, 2023, s. 9 (children's data; child defined as under eighteen; verifiable parental consent; bar on tracking, behavioural monitoring, and targeted advertising); DPDP Rules, 2025, rr. 10–12.

Officer, hire an independent auditor, and file yearly impact assessments and audits with the Board.[24]

Data principals get rights: a summary of their processing, correction, erasure, grievance redressal, nomination.[25] And — this still surprises me — duties. Section 15 imposes duties on the individual, breach of which can draw a Rs. 10,000 penalty.[26] A privacy law that fines the person it exists to protect. I have read that provision several times and it doesn't get less strange.

Cross-border transfers are free unless the government blacklists the destination. No country has been blacklisted. The Act states no criteria for blacklisting one.[27] Draw your own conclusions.

Enforcement sits with the Data Protection Board of India: a body corporate, a chairperson, four members, functioning digitally.[28] It inquires into breaches and fines per a statutory Schedule — Rs. 250 crore for safeguard failures, Rs. 200 crore for breach-notification and children's-data violations, Rs. 150 crore for Significant Data Fiduciary defaults, Rs. 50 crore

24DPDP Act, 2023, s. 10 (Significant Data Fiduciaries); s. 10(2)(a) (Data Protection Officer, responsible to the fiduciary's governing body); DPDP Rules, 2025, r. 13 (annual impact assessments and audits). No designations had issued as of August 2026.

25DPDP Act, 2023, ss. 11–14 (rights of access, correction and erasure, grievance redressal, nomination); s. 15 (duties of Data Principals, including s. 15(b), punishable up to Rs. 10,000).

26DPDP Act, 2023, ss. 11–14, supra note 25.

27DPDP Act, 2023, s. 16 (cross-border transfers; blacklist approach). No country had been blacklisted as of 2026.

28DPDP Act, 2023, ss. 18–26 (Data Protection Board of India); DPDP Rules, 2025, rr. 17–21.

residually.[29] Formidable numbers. Where does the money go? The Consolidated Fund of India. The person whose data was breached gets nothing. No compensation. No private right of action.[30] Appeals lie to the Telecom Disputes Settlement and Appellate Tribunal.[31]

Finally, Section 17 — the state's carve-out, and the subject of Part VI. Section 17(1) exempts defined state purposes (security, public order, law enforcement, research, archiving) from the fiduciary-duty and rights chapters, keeping accountability and security duties alive.[32] Defensible. But Section 17(2)(a) lets the Central Government exempt any State instrumentality from the *entire*

© 2026 Joint Jurist (All Rights Reserved) e-ISSN -3139-6186

No part of this publication may be reproduced without prior written permission, except for educational purposes.

Act by notification — on sovereignty, security, public order — with no definition of the class, no reasons, no duration, no review.[33] Sections 17(4)–(5) permit indefinite state retention for research and statistics, erasure duties aside.[34] And Section 44(3) rewrites the RTI Act's personal-information exemption into something close to a categorical bar.[35]

29DPDP Act, 2023, ss. 27–33 and the Schedule (penalties: up to Rs. 250 crore for safeguard failures, Rs. 200 crore for breach-notification and children's-data contraventions, Rs. 150 crore for Significant Data Fiduciary defaults, Rs. 50 crore residually).

30DPDP Act, 2023, s. 34 (penalties credited to the Consolidated Fund of India); no compensation or private right of action. Contrast GDPR, Art. 82 (right to compensation).

31Appeals lie to the Telecom Disputes Settlement and Appellate Tribunal.

32DPDP Act, 2023, s. 17(1) (chapter-limited exemptions); s. 17(2)(a) (notification-based exemption of any State instrumentality from the entire Act); ss. 17(4)–(5) (indefinite retention for research/archiving/statistical purposes).

33DPDP Act, 2023, s. 17, supra note 32.

34DPDP Act, 2023, s. 17, supra note 32.

35DPDP Act, 2023, s. 44(3), amending s. 8(1)(j) of the Right to Information Act, 2005.

That is the machine as designed. Now — can it run?

IV. The Consent Problem

Ask any data protection lawyer the one question her field must answer — when may someone process my data? — and the GDPR gives her six answers. The DPDP Act gives one. Consent. Plus a closed list of exceptions that mostly serve the state.[36]

That makes consent load-bearing. If it fails in practice, nothing holds the building up.

It is failing. Let me count the ways.

The notice nobody will write. Section 5(3) wants every privacy notice in English plus any of twenty-two scheduled languages the principal chooses.[37] I admire the ambition. Now picture who must implement it: a health-tech startup in Jaipur, a D2C seller in Kochi. Every notice, in Dogri and Maithili and the rest, revised with each material change in processing. I don't believe twenty-two careful translations will ever exist. What will exist is machine-translated boilerplate — unread by principals, unmaintained by fiduciaries. A right that cannot be operationalised is decoration.

The withdrawal nobody can execute. Section 6(4): consent withdrawn, processing stops, processors stop, "within a reasonable time".[38] Now picture where personal data actually lives. Not in one database — replicated across

36DPDP Act, 2023, s. 7, supra note 20.

37DPDP Act, 2023, s. 5, supra note 16.

38DPDP Act, 2023, s. 6, supra note 18.

© 2026 Joint Jurist (All Rights Reserved) e-ISSN -3139-6186

No part of this publication may be reproduced without prior written permission, except for educational purposes.

backups, streamed to analytics vendors, baked into training sets, written into immutable audit logs. Propagating a withdrawal through that chain means finding every downstream copy and certifying deletion. Most Indian companies, large or small, aren't built for that.[39] The law demands the button. It never reckoned with the pipeline behind it.

The manager that does not exist. The Act's answer to consent fatigue is the Consent Manager — one registered intermediary through which you give, review and revoke consent.[40] Rule 4 sets the entry ticket: Indian company, Rs. 2 crore net worth, architecture blind to the data itself.[41] As of late 2026, zero Consent Managers are registered. How could it be otherwise? The registry needs a functioning Board. There is no Board.[42] So the citizen-facing layer of the consent economy is a dead letter — while Indians keep tapping "I agree" dozens of times a day, and nothing in this design reduces that number.

The children nobody can verify. Under-eighteens need *verifiable* parental consent.[43] The threshold sits above the GDPR's sixteen, and "verifiable" in practice means age-gating the Indian internet against identity documents. Two outcomes are possible: mass non-compliance, or compliance through

39See, e.g., the analysis of s. 6(4)'s propagation problem across processor chains (LinkedIn, 2025–26 commentary on DPDP consent withdrawal).

40DPDP Act, 2023, s. 6, supra note 18.

41DPDP Rules, 2025, r. 4 (Consent Manager registration: India incorporation, Rs. 2 crore minimum net worth, data-blind architecture, seven-year record retention).

42No Consent Manager was registered as of September 2026; registration depends on a functioning Board.

43DPDP Act, 2023, s. 9, supra note 23.

verification infrastructure that collects more personal data than it protects. When obeying a privacy law requires building more surveillance, something has gone wrong in the drafting. I don't know how else to put it.

The courts have noticed. In *Abhishek Baxi* (July 2026), the Supreme Court took up APAAR — the twelve-digit lifelong student ID seeded from Aadhaar and DigiLocker — and held the DPDP Act applies even though APAAR is an administrative programme, not a statute.[44] The Court ordered genuine opt-outs in parental consent forms nationwide and barred third party sharing of student data without explicit statutory backing.[45] Strip away the formality and the message is blunt: three years in, the highest court had to teach the government how consent works. If consent needs judicial rescue in a school-ID scheme, what are its chances in the ad-tech supply chain?

I am not arguing against consent. I am arguing against consent as the *only* value. Without a legitimate-interests ground, every benign, low-risk activity — fraud prevention, network security, product improvement — must squeeze through a consent funnel that is already overflowing.[46] The GDPR's balancing test is imperfect. But it at least admits that not all processing without explicit consent is predatory. Our Act's binary — consent, or the state's exceptions — leaves honest companies performing

© 2026 Joint Jurist (All Rights Reserved) e-ISSN -3139-6186

No part of this publication may be reproduced without prior written permission, except for educational purposes.

44*Abhishek Baxi*, supra note 7. The Court applied the DPDP Act to APAAR, the twelve-digit lifelong student ID, directed pan-India adoption of an opt-out parental consent model, and barred third-party sharing of student data absent explicit statutory authorisation.

45*Abhishek Baxi*, supra note 44.

46GDPR, Art. 6(1)(f).

theatre and citizens exhausted by forms. Theatre is not autonomy. I keep returning to that sentence because I cannot improve on it.

V. The Regulator That Isn't There

A rights statute is only as strong as its enforcer. On paper, ours is formidable: the Data Protection Board of India — body corporate, chairperson plus four members, inquiries, directions, fines up to Rs. 250 crore.[47] The constituting Rules have been in force since November 2025.[48]

In reality: no chairperson. No members. No inquiries. No directions. No penalties. LiveLaw found the exact phrase — "established in law, absent in fact".[49] I have nothing to add to it.

This is not a paperwork jam. Search-cum-selection committees were constituted — chaired, tellingly, by the Cabinet Secretary for the chairperson's post and the MeitY Secretary for members. Nominations were invited from ministries and states in May and June 2026. In September 2026 came word the Cabinet "may clear" the five posts.[50] Whether it did, no official notification confirms. The enforcement record, meanwhile, is confirmed.

Zero.

47DPDP Act, 2023, ss. 18–26, supra note 28.

48Draft DPDP Rules (Jan 2025), supra note 12.

49LiveLaw, "Data Protection Board of India: Established in Law, Absent in Fact" (1 Aug 2026).

50Search-cum-selection committees chaired by the Cabinet Secretary (Chairperson) and the MeitY Secretary (Members); nominations invited May–June 2026; September 2026 reporting that the Cabinet "may clear" the five posts — unconfirmed against any official notification.

The absurdity has reached the courts. In *Parth Sharma*, the Madhya Pradesh High Court directed a petitioner to the Board as an "efficacious alternate remedy".[51] An efficacious remedy that cannot receive a complaint, staff an inquiry, or pass an order. A right whose forum does not exist is a right in cold storage — and the clock is unforgiving, because the substantive duties switch on around May 2027, making breaches actionable before a body that has never functioned.[52]

But I want to be clear: delay is the smaller scandal. Design is the larger one.

The Board is appointed by the executive it must regulate. Its selection committees are chaired by the country's top bureaucrats. Members serve short tenures at modest rank-equivalence. The statute builds in none of the insulation the GDPR demands of supervisory authorities — independent establishment, independent members, freedom from external influence.[53] Ask yourself the obvious question: can an adjudicator that owes its selection and tenure to the government credibly investigate the government's data practices? And remember Part VI — given the state's sweeping

© 2026 Joint Jurist (All Rights Reserved) e-ISSN -3139-6186

No part of this publication may be reproduced without prior written permission, except for educational purposes.

exemptions, the Board's most politically sensitive docket would concern the very executive that appointed it.

It gets worse. The Data Protection Officer that Significant Data Fiduciaries must appoint answers to the fiduciary's own governing body,

51*Parth Sharma v. Union of India* (Madhya Pradesh High Court, 2026). 52DPDP Rules, 2025, supra note 5.

53Contrast GDPR, Arts. 51–58 (independent supervisory authorities) and Art. 38 (independence of the Data Protection Officer).

with no statutory shield — compare Article 38 of the GDPR, which protects a DPO from dismissal for doing her job.[54] Penalties flow to the Consolidated Fund, so the breach victim sees none of it. No compensation. No private right of action — compare Article 82 of the GDPR.[55] So enforcement is concentrated in a single forum that is empty, producing penalties the victim never touches. If you designed a system to look severe while changing nothing, it would look like this.

Meanwhile the breach-notification clock is already ticking elsewhere. CERT-In's 2022 Directions demand cyber-incident reports within six hours and are enforced independently. The DPDP Act will add "without delay" plus a seventy-two-hour detailed report — no risk threshold, no filter.[56] Companies face parallel clocks: CERT-In's, the Board's, sectoral regulators' like the RBI's. And the Board cannot yet receive the reports the Act requires it to receive. IBM's 2026 Cost of a Data Breach Report puts the average Indian breach at a record Rs. 25.5 crore.[57] The threat is real. The reporting machinery is fragmented. The adjudicator is missing.

A regulator that does not exist cannot deter. A regulator designed as the executive's appointee cannot check the executive. Fix the first urgently; fix the second structurally. Until both happen, Rs. 250 crore is a paper tiger, and the Act's rights are petitions addressed to an empty chair.

54GDPR, Arts. 51–58, supra note 53.

55DPDP Act, 2023, s. 34, supra note 30.

56CERT-In Directions under s. 70B of the Information Technology Act, 2000 (28 April 2022) (six-hour cyber-incident reporting); DPDP Act, s. 8(6).

57IBM, Cost of a Data Breach Report 2026 (released 3 Aug 2026): average breach cost in India Rs. 25.5 crore.

VI. The State's Blank Cheque

Puttaswamy gave privacy with one hand and fenced it with the other. Any intrusion needs a valid law, a legitimate aim, and proportionality — necessary, and the least restrictive means available.[58] Section 17 is where that test comes to be applied to the Act itself.

It doesn't survive the encounter. Let me show you.

Section 17(1) is fine. It lifts the fiduciary-duty and rights chapters for defined state purposes — security, public order, law enforcement, research, archiving — while keeping accountability and security duties alive.[59] Narrow, chapter-limited, safeguards intact. That is what proportionality looks like.

© 2026 Joint Jurist (All Rights Reserved) e-ISSN -3139-6186

No part of this publication may be reproduced without prior written permission, except for educational purposes.

Section 17(2)(a) is a different animal. It empowers the Central Government to exempt *any* instrumentality of the State from the *entire* Act, by notification, on grounds like "sovereignty and integrity of India", "security of the State", "public order".[60] No definition of the class. No categories of processing. No reasons to be recorded. No duration. No review. The Board gets no say. And Sections 17(4)–(5) let the state retain personal data indefinitely for research and statistics, erasure duties aside.[61]

Call it what it is: a blank cheque.

58*Puttaswamy*, supra note 8.

59DPDP Act, 2023, s. 17, supra note 32.

60DPDP Act, 2023, s. 17, supra note 32.

61DPDP Act, 2023, s. 17, supra note 32.

Run it through *Puttaswamy*'s three limbs. Legality — yes, validly enacted. Legitimate aim — national security qualifies if anything does. Proportionality, necessity stage — here it collapses. Because the Act itself proves a narrower alternative exists: Section 17(1), sitting two sub-sections above, suspends rights while preserving security safeguards. Section 17(2) (a) suspends even duties that have nothing to do with the security objective — including the duty to keep the data secure.[62] A measure that discards less-restrictive alternatives found in its own statute can't be the least intrusive means. The argument almost makes itself.

And there is precedent for what courts do with uncanalised executive power. In *PUCL v. Union of India* (1997), on telephone tapping, the Supreme Court read procedural safeguards into surveillance — defined authority, inter-ministerial review — because unchecked executive access to private communications offended Article 21.[63] Section 17(2)(a) offers none of that. No defined authority. No review. No oversight. Compare Article 23 of the GDPR: restrictions on rights only through *legislative measures* respecting the essence of fundamental rights, necessary and proportionate in a democratic society.[64] Our version permits restriction by notification. No legislative measure at all.

62Economic Laws Practice, *Government Exemptions and the Balance between Privacy and State Interests* (July 2026) (proportionality analysis of s. 17).

63*People's Union for Civil Liberties v. Union of India*, (1997) 1 SCC 301; Yash Verma, critique of s. 17(2)(a), *Indian Journal of Law and Legal Research*.

64GDPR, Art. 23 (restrictions only by legislative measures respecting the essence of rights, necessary and proportionate).

Now read Section 17 with Section 44(3), and watch the asymmetry lock into place. That provision amends the RTI Act, replacing a calibrated personal-information exemption — which yielded to a larger-public interest override — with something close to a categorical bar.[65] On 16 February 2026, a three-judge bench led by the Chief Justice of India referred the challenge to a five-judge Constitution Bench, calling it "constitutionally sensitive" — but declined a stay, so the amended clause operates today.[66] The Internet Freedom Foundation's label for the whole structure is precise: the "legitimate uses paradox". Section 7 lets the state process your data without consent. Section

© 2026 Joint Jurist (All Rights Reserved) e-ISSN -3139-6186

No part of this publication may be reproduced without prior written permission, except for educational purposes.

17 exempts the state from the Act's duties. Section 44(3) stops you from using transparency law to find out what it did.[67] The state knows more. The citizen may ask less.

An honest caveat: no court has struck down Section 17, and I won't prejudge constitutional adjudication. The Supreme Court may yet read safeguards into it, as it did in *PUCL*.[68] But a privacy statute that needs future judicial rescue for its most basic proportionality compliance has the design backwards. *Puttaswamy* demanded that intrusions be justified. Section 17(2)(a) proceeds as if they need not be. That, I think, is the Act's

65DPDP Act, 2023, s. 44(3), supra note 35.

66Petitions by Venkatesh Nayak, The Reporters Collective Trust, and the National Campaign for People's Right to Information; referred to a five-judge Constitution Bench on 16 February 2026, interim stay declined; see LiveLaw, "When the State Knows Everything" (2026).

67Nayak RTI petitions, supra note 66.

68No Supreme Court ruling on the constitutionality of s. 17 has been reliably reported as of October 2026.

deepest flaw — deeper than the empty Board, deeper than the fictional consent. Because it is a choice, not an accident.

VII. What Europe Gets Right

I should say at the outset: comparison is not worship. The GDPR has its own pathologies. Europeans suffer consent fatigue too, and some of its fines have looked arbitrary. But on this paper's three questions, the European design has answers and ours does not.

Who may process, and on what basis? Six lawful bases, including legitimate interests under a balancing test.[69] We have two: consent, and a closed list of exceptions that mostly serve the state.

Who enforces? Every member state must maintain independent supervisory authorities — independent members, adequate resources, freedom from external influence — wielding everything from warnings to processing bans.[70] We have an executive-appointed Board that is currently unstaffed and mostly adjudicatory. A court for data breaches, not a regulator of data processing.

What does the victim get? Article 82 of the GDPR: anyone suffering damage gets compensation from the controller or processor, enforceable in national courts.[71] Our penalties go to the Consolidated Fund. The individual gets an order she cannot spend, through a grievance portal that leads to an empty Board.

69GDPR, Art. 6(1)(f), supra note 46.

70GDPR, Arts. 51–58, supra note 53.

71DPDP Act, 2023, s. 34, supra note 30.

The lesson is not "copy Brussels". It is that rights without an independent enforcer, remedies without compensation, and consent without alternatives produce a distinctive species of law — severe on paper, weightless in practice. Rs. 250 crore concentrates the mind wonderfully. It deters nobody if nobody is there to impose it.

© 2026 Joint Jurist (All Rights Reserved) e-ISSN -3139-6186

No part of this publication may be reproduced without prior written permission, except for educational purposes.

VIII. Six Repairs

Diagnosis without prescription is complaint. The good news: most of this can be fixed before the substantive duties switch on around May 2027, and none of it requires tearing the architecture down.

Staff the Board — then set it free. Staffing is the emergency; independence is the cure. Move appointments from executive-chaired search committees to a bipartisan selection process with statutory eligibility, fixed non-renewable tenures, and removal protections matching other independent regulators. Give at least one member judicial or quasi judicial experience. And grant own-motion inquiry powers — a regulator's toolkit, not merely an adjudicator's.[72]

Give the victim something. Penalties to the Consolidated Fund punish without compensating. Create a private right of action — or, more modestly, a compensation fund fed by a share of penalties — so the person whose data was breached has a reason to invoke the law. A right nobody is paid to enforce is a right nobody enforces. I said that in Part V; it bears repeating because it is the cheapest fix on this list.

72Cf. the pending Supreme Court challenges to the breadth of s. 36 regulation-making powers and Board independence.

Discipline Section 17. Define which instrumentalities can be exempted. Require recorded reasons. Put sunset clauses with periodic review on every exemption. Import *PUCL*-style safeguards — defined authorising authority, inter-ministerial oversight — into surveillance-adjacent processing.[73] The Constitution Bench reference on Section 44(3) may force some of this; Parliament should not wait to be ordered.[74]

Relieve the consent bottleneck. A bounded legitimate-interests ground — statutory balancing test, Board-issued guidance, on the Article 6(1)(f) model — would let low-risk, obviously benign processing proceed without manufacturing fictional consent.[75] If that is politically impossible, expand Section 7's closed list with care, rather than leaving every non-consensual private processing in a grey zone.

Harmonise the breach clocks. CERT-In's six hours, the DPDP Act's "without delay" plus seventy-two, sectoral windows like the RBI's — running in parallel, no de-minimis filter under the Act.[76] A single-window or deemed-compliance mechanism would turn triple jeopardy into coherent supervision.

Get Consent Managers running before May 2027. Open the registration framework, with net-worth and technical thresholds set to admit

73*PUCL*, supra note 63.

74Nayak RTI petitions, supra note 66.

75GDPR, Art. 6(1)(f), supra note 46.

76CERT-In Directions (2022), supra note 56.

competition rather than entrench incumbents — so the consent layer actually exists when the duties do.[77]

© 2026 Joint Jurist (All Rights Reserved) e-ISSN -3139-6186

No part of this publication may be reproduced without prior written permission, except for educational purposes.

None of this asks Parliament to abandon the Act's architecture. It asks Parliament to take the Act's promises seriously. There is a difference.

IX. Conclusion

I began with a law-school memory: *Puttaswamy*, nine judges, privacy declared a fundamental right. Three years after the statute that judgment demanded, here is where we are. A consent machinery that asks more than the ecosystem can give. A regulator that exists in the statute book and nowhere else. State exemptions that sit uneasily with the proportionality standard that created the right being protected. And a Supreme Court that, in *Abhishek Baxi*, had to insist in 2026 that a consent form must offer refusal — less reassurance, I think, than warning. The judiciary won't wait for the machinery to start.[78]

None of which makes the Act a failure. I mean that. A phased, imperfect statute that Parliament is willing to repair is worth more than a perfect Bill that never passes. But the repairs must come before May 2027, when the substantive duties switch on and the paper tiger is expected to roar. Constitute the Board. Free it from the executive. Compensate victims. Discipline the state's exemptions. And admit, finally, that consent alone cannot carry a nation's data protection on its back.

Puttaswamy promised privacy as a fundamental right. Fundamental rights are not protected by notifications. Not by penalties payable to the 77DPDP Rules, 2025, r. 4, supra note 41.

78*Abhishek Baxi*, supra note 44.

Consolidated Fund. Not by consent forms nobody reads. They are protected by institutions with the independence to say no — including, when it matters most, no to the state.

The DPDP Act still has time to build those institutions.

Time, though, is the one thing a phased commencement does not pause. **Notes**

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

2. Committee of Experts under Justice B.N. Srikrishna, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (July 2018).

3. The Personal Data Protection Bill, 2019 was withdrawn in August 2022; the Digital Personal Data Protection Bill, 2022 was released for consultation in November 2022.

4. The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023), assented to 11 August 2023.

5. The DPDP Rules, 2025 were notified on 13 November 2025 (G.S.R. 843(E)), with corrigendum in December 2025; institutional and definitional provisions commenced first, with substantive fiduciary obligations and data-principal rights widely expected to apply from around May 2027, eighteen months later. See MediaNama, "India notifies DPDP Rules 2025" (14 Nov 2025).

6. See Part V below.

7. *Abhishek Baxi v. Union of India*, W.P.(C) 832/2026, order dated 20 July 2026, 2026 SCC OnLine SC 1391.

© 2026 Joint Jurist (All Rights Reserved) e-ISSN -3139-6186

No part of this publication may be reproduced without prior written permission, except for educational purposes.

8. *Puttaswamy*, supra note 1, per Chandrachud J. (plurality): legality, legitimate aim, and proportionality (including necessity and least-restrictive-means).

9. Srikrishna Committee Report, supra note 2.

10. PDP Bill, 2019, supra note 3.

11. DPDP Act, 2023, supra note 4.

12. Draft DPDP Rules released 3 January 2025; final DPDP Rules, 2025 notified 13 November 2025.

13. DPDP Rules, 2025, supra note 5.

14. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

15. DPDP Act, 2023, s. 2 (definitions of Data Fiduciary, Data Principal, and Data Processor).

16. DPDP Act, 2023, s. 5 (notice); s. 5(3) (twenty-two languages).

17. DPDP Act, 2023, s. 5, supra note 16.

18. DPDP Act, 2023, s. 6 (consent); s. 6(4) (effect of withdrawal); s. 6(7) (Consent Managers). **19.** DPDP Act, 2023, s. 6, supra note 18.

20. DPDP Act, 2023, s. 7 (certain legitimate uses, a closed list of nine grounds). Contrast Regulation (EU) 2016/679 (GDPR), Art. 6(1)(f) (legitimate interests).

21. DPDP Act, 2023, s. 7, supra note 20.

22. DPDP Act, 2023, s. 8(5) (reasonable security safeguards); s. 8(6) (breach notification: intimation to the Board "without delay," detailed report within seventy-two hours, and notification to affected principals; no de-minimis threshold).

23. DPDP Act, 2023, s. 9 (children's data; child defined as under eighteen; verifiable parental consent; bar on tracking, behavioural monitoring, and targeted advertising); DPDP Rules, 2025, rr. 10–12.

24. DPDP Act, 2023, s. 10 (Significant Data Fiduciaries); s. 10(2)(a) (Data Protection Officer, responsible to the fiduciary's governing body); DPDP Rules, 2025, r. 13 (annual impact assessments and audits). No designations had issued as of August 2026.

25. DPDP Act, 2023, ss. 11–14 (rights of access, correction and erasure, grievance redressal, nomination); s. 15 (duties of Data Principals, including s. 15(b), punishable up to Rs. 10,000).

26. DPDP Act, 2023, ss. 11–14, supra note 25.

27. DPDP Act, 2023, s. 16 (cross-border transfers; blacklist approach). No country had been blacklisted as of 2026.

28. DPDP Act, 2023, ss. 18–26 (Data Protection Board of India); DPDP Rules, 2025, rr. 17–21.

© 2026 Joint Jurist (All Rights Reserved) e-ISSN -3139-6186

No part of this publication may be reproduced without prior written permission, except for educational purposes.

29. DPDP Act, 2023, ss. 27–33 and the Schedule (penalties: up to Rs. 250 crore for safeguard failures, Rs. 200 crore for breach-notification and children's-data contraventions, Rs. 150 crore for Significant Data Fiduciary defaults, Rs. 50 crore residually).

30. DPDP Act, 2023, s. 34 (penalties credited to the Consolidated Fund of India); no compensation or private right of action. Contrast GDPR, Art. 82 (right to compensation).

31. Appeals lie to the Telecom Disputes Settlement and Appellate Tribunal.

32. DPDP Act, 2023, s. 17(1) (chapter-limited exemptions); s. 17(2)(a) (notification-based exemption of any State instrumentality from the entire Act); ss. 17(4)–(5) (indefinite retention for research/archiving/statistical purposes).

33. DPDP Act, 2023, s. 17, supra note 32.

34. DPDP Act, 2023, s. 17, supra note 32.

35. DPDP Act, 2023, s. 44(3), amending s. 8(1)(j) of the Right to Information Act, 2005. **36.** DPDP Act, 2023, s. 7, supra note 20.

37. DPDP Act, 2023, s. 5, supra note 16.

38. DPDP Act, 2023, s. 6, supra note 18.

39. See, e.g., the analysis of s. 6(4)'s propagation problem across processor chains (LinkedIn, 2025–26 commentary on DPDP consent withdrawal).

40. DPDP Act, 2023, s. 6, supra note 18.

41. DPDP Rules, 2025, r. 4 (Consent Manager registration: India incorporation, Rs. 2 crore minimum net worth, data-blind architecture, seven-year record retention).

42. No Consent Manager was registered as of September 2026; registration depends on a functioning Board.

43. DPDP Act, 2023, s. 9, supra note 23.

44. *Abhishek Baxi*, supra note 7. The Court applied the DPDP Act to APAAR, the twelve-digit lifelong student ID, directed pan-India adoption of an opt-out parental consent model, and barred third-party sharing of student data absent explicit statutory authorisation.

45. *Abhishek Baxi*, supra note 44.

46. GDPR, Art. 6(1)(f).

47. DPDP Act, 2023, ss. 18–26, supra note 28.

48. Draft DPDP Rules (Jan 2025), supra note 12.

49. LiveLaw, "Data Protection Board of India: Established in Law, Absent in Fact" (1 Aug 2026).

50. Search-cum-selection committees chaired by the Cabinet Secretary (Chairperson) and the MeitY Secretary (Members); nominations invited May–June 2026; September 2026 reporting that the Cabinet "may clear" the five posts — unconfirmed against any official notification.

© 2026 Joint Jurist (All Rights Reserved) e-ISSN -3139-6186

No part of this publication may be reproduced without prior written permission, except for educational purposes.

51. *Parth Sharma v. Union of India* (Madhya Pradesh High Court, 2026). **52.** DPDP Rules, 2025, supra note 5.

53. Contrast GDPR, Arts. 51–58 (independent supervisory authorities) and Art. 38 (independence of the Data Protection Officer).

54. GDPR, Arts. 51–58, supra note 53.

55. DPDP Act, 2023, s. 34, supra note 30.

56. CERT-In Directions under s. 70B of the Information Technology Act, 2000 (28 April 2022) (six-hour cyber-incident reporting); DPDP Act, s. 8(6).

57. IBM, Cost of a Data Breach Report 2026 (released 3 Aug 2026): average breach cost in India Rs. 25.5 crore.

58. *Puttaswamy*, supra note 8.

59. DPDP Act, 2023, s. 17, supra note 32.

60. DPDP Act, 2023, s. 17, supra note 32.

61. DPDP Act, 2023, s. 17, supra note 32.

62. Economic Laws Practice, *Government Exemptions and the Balance between Privacy and State Interests* (July 2026) (proportionality analysis of s. 17).

63. *People's Union for Civil Liberties v. Union of India*, (1997) 1 SCC 301; Yash Verma, critique of s. 17(2)(a), *Indian Journal of Law and Legal Research*.

64. GDPR, Art. 23 (restrictions only by legislative measures respecting the essence of rights, necessary and proportionate).

65. DPDP Act, 2023, s. 44(3), supra note 35.

66. Petitions by Venkatesh Nayak, The Reporters Collective Trust, and the National Campaign for People's Right to Information; referred to a five-judge Constitution Bench on 16 February 2026, interim stay declined; see LiveLaw, "When the State Knows Everything" (2026).

67. Nayak RTI petitions, supra note 66.

68. No Supreme Court ruling on the constitutionality of s. 17 has been reliably reported as of October 2026.

69. GDPR, Art. 6(1)(f), supra note 46.

70. GDPR, Arts. 51–58, supra note 53.

71. DPDP Act, 2023, s. 34, supra note 30.

72. Cf. the pending Supreme Court challenges to the breadth of s. 36 regulation-making powers and Board independence.

73. *PUCL*, supra note 63.

74. Nayak RTI petitions, supra note 66.

© 2026 Joint Jurist (All Rights Reserved) e-ISSN -3139-6186

No part of this publication may be reproduced without prior written permission, except for educational purposes.

75. GDPR, Art. 6(1)(f), supra note 46.

76. CERT-In Directions (2022), supra note 56.

77. DPDP Rules, 2025, r. 4, supra note 41.

78. *Abhishek Baxi*, supra note 44.

* * *

© 2026 Joint Jurist (All Rights Reserved) e-ISSN -3139-6186

No part of this publication may be reproduced without prior written permission, except for educational purposes.