SUPREMO AMICUS

INDIA'S FIRST AI INTEGRATED LAW JOURNAL

Peer Reviewed, Refereed and Open access Journal

- Available in 331+ International Libraries
- Indexed at 32 Databases

ISSN NO. 2456-9704
Volume 10 Issue 2
www.supremoamicus.org

DISCLAIMER

The information presented in this article is intended for general informational and educational purposes only. While every effort has been made to ensure that the content is accurate, up-to-date, and reliable at the time of publication, the editorial board and publisher make no representations or warranties of any kind, express or implied, regarding the completeness, accuracy, reliability, suitability, or availability of the information contained herein.

The views and opinions expressed in this article are those of the author and are based on personal research, experience, and interpretation. They do not necessarily reflect the official policy, position, or opinions of any affiliated organization, institution, or entity.

This article is not intended to serve as professional advice of any kind. The editorial board and publisher shall not be held liable for any errors or omissions in the content, nor for any losses, injuries, or damages arising from the use of or reliance on this information.

ABOUT THE JOURNAL

Supremo Amicus is an online, peer-reviewed international journal devoted to the interdisciplinary fields of law and science. In an era marked by rapid technological progress and evolving legal frameworks, the journal seeks to bridge the gap between these two dynamic domains by offering comprehensive and critical insights into their various aspects. The journal places a strong emphasis on contemporary advancements, emerging trends, and the complex challenges faced by both the legal community.

The primary objective of the journal is to encourage and promote original, high-quality research. It is committed to publishing well-researched, analytically sound, and thought-provoking articles that adhere to rigorous academic standards. Each submission undergoes a thorough peer-review process to ensure authenticity, relevance, and scholarly integrity. In doing so, the journal maintains its commitment to excellence and credibility.

In addition to fostering research, the journal aims to make complex ideas accessible and engaging for a diverse readership. It strives to present content that is not only intellectually enriching but also clearly written and reader friendly.

Furthermore, the journal is committed to promoting interdisciplinary collaboration and global engagement. It welcomes diverse perspectives from contributors across different regions and backgrounds, thereby enriching the quality and scope of discussions presented within its pages.

With this vision we proudly present Supremo Amicus to our readers.

-Editorial Team
Supremo Amicus

PRIVACY ON PAPER: LEGISLATIVE GAPS IN INDIA'S DIGITAL PERSONAL DATA PROTECTION ACT 2023 AND RULES 2025

By *Shaily Navadia*
From *National Law Institute University, Bhopal.*

Abstract

When a constitutional court declares privacy a fundamental right and mandates legislative action to enforce it, the statute that follows carries the weight of that obligation made visible. The Digital Personal Data Protection Act 2023 and its 2025 Rules represent India's answer to that mandate. This paper asks, with doctrinal precision, whether the answer is constitutionally adequate.

Drawing on the proportionality framework of Justice KS Puttaswamy v Union of India (2017), this paper maps eight structural gaps in the legislative architecture: the Act's collision with the Right to Information framework through Section 44(3); overbroad state exemptions under Section 17 unanchored from necessity review; a publicly available data loophole that enables open-source intelligence-driven surveillance; an unimplemented cross-border transfer regime under Section 16; a Data Protection Board compromised in its institutional independence; an under-specified children's consent architecture; near-complete silence on automated decision-making and algorithmic accountability; and a fiduciary gap within the Consent Manager framework. Each gap, considered individually, reflects a discrete weakness in the statutory framework. Taken together, they illuminate a central question running through the Act's design: whether the legislation addresses the risks posed by state data processing with the same degree of institutional and legal scrutiny that it applies to private actors.

1. Introduction

India finally has a data protection law. It only took twenty-six years, four committee reports, three draft bills, and one landmark Supreme Court judgment to get there.[1] The Digital Personal Data Protection Act, 2023 (hereinafter "DPDPA") arrived trailing considerable fanfare – a "modern," "principles-based" framework fit for a digitally ascendant nation. The 2025 Rules, long delayed and finally notified, were supposed to complete the architecture.[2]

They don't.

What the DPDPA actually constructs is a structurally asymmetric regime: elaborate consent machinery trained almost entirely on private actors, while the entity that *Puttaswamy* identified as the primary threat to informational autonomy, i.e., the state, walks through a series of carefully drafted exits. The proportionality discipline that nine judges unanimously demanded in 2017 is nowhere operationalised in 2023.

While it stands true that the DPDPA's implementation remains incomplete, it must be noted that the deadline for mandatory compliance with core obligations extends to May 2027 and accordingly requires some caution in the assessment of the Act's practical operation. While the passage of time may clarify the operation of the regime, it cannot remedy the structural asymmetries and constitutional omissions already evident on the face of the legislation.

This paper makes two moves that have not been made together. First, it engages the live constitutional litigation testing the DPDPA's validity by reading the pending challenges not normatively, modelling what the Court *should* hold and why.[3] Second, it offers a unified structural critique: mapping eight distinct legislative gaps and tracing each to a single underlying

[1] *Justice K S Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1.
[2] Digital Personal Data Protection Rules 2025.
[3] Writ Petition (Civil) No 468 of 2023 and connected matters (Supreme Court of India, pending).

design pathology – state-centric carve-outs compounded by institutional capture risk. This purposeful coherent architecture and recognising them as such is the first precondition for fixing them.

2. Legislative Genealogy

Pre-Puttaswamy Privacy Doctrine

For most of its post-independence history, the Indian constitutional order treated privacy as a guest rather than a resident. The Supreme Court in *Kharak Singh v State of Uttar Pradesh*[4] acknowledged the existence of a "right to be let alone" only to deny that privacy enjoyed independent constitutional protection, holding that "the right to privacy is not a guaranteed right under our constitution", even as it invalidated domiciliary night visits on narrower Article 21 grounds. In *Gobind v State of Madhya Pradesh*[5] the court hesitantly resuscitated the concept, by deriving it from the Right to Liberty guaranteed in Article 21, but confined its protection to matters touching "the intimate relations of the person" such as family, marriage and sexuality. This was heavily drawn from the penumbral reasoning in *Griswold v Connecticut,* borrowed from American doctrine the idea that the constitutional guarantees cast shadows wide enough to shelter enumerated rights – a foreign framework that would eventually be given domestic constitutional grounding.[6] Privacy, according to the judicial register, in short, was something that the State might occasionally spare, rather than a right. However, R Rajagopal[7] brought some refinement by recognising a right against unauthorised publication of personal information, but was strictly limited to private harm and did not extended to State surveillance. The pre-2017 position therefore reflected doctrinal uncertainty; privacy interests were acknowledged in principle but protected only sporadically with their capacity to restrain state power significantly underdeveloped.

Puttaswamy I (2017): The Measuring Stick

The nine-judge bench in *Justice KS Puttaswamy (Retd) v Union of India*[8] (hereinafter *Puttaswamy I*) did more than reverse the mischief of *Kharak Singh*. It installed privacy as a fundamental right under Article 21 and, crucially, J Chandrachud in his 4 limbed proportionality standard provided constitutional law with the analytical vocabulary to assess subsequent legislative intervention on personal data.

(i) Legitimate Aim

Any legislative interference with informational privacy must pursue a constitutionally permissible objective. In the data protection context, this means that each statutory purpose for which the State may collect, process, or retain personal data must be traceable to a specific, enumerated public interest that is not, in itself, constitutionally impermissible. A statutory purpose as vague as "public order" or "sovereignty and integrity of India" is not automatically illegitimate but the aim must be stated in the legislation with sufficient precision that a reviewing court can assess its scope. Legitimate aim is the least demanding of the four limbs necessitating the precision with which legislative objectives are measured, an important safeguard against overbroad exercises of state authority.

(ii) Rational Nexus

The means chosen must bear a rational connection to the stated aim. In data protection terms, this requires asking whether a given processing activity such as the collection of biometric identifiers, the retention of transaction records, the transfer of health data to government agencies – is capable, in principle, of advancing the claimed objective.

[4] *Kharak Singh v State of Uttar Pradesh* AIR 1963 SC 1295.
[5] *Gobind v State of Madhya Pradesh* (1975) 2 SCC 148.
[6] *Griswold v Connecticut* 381 US 479 (1965).
[7] *R Rajagopal v State of Tamil Nadu* (1994) 6 SCC 632.
[8] *Puttaswamy (n 1).*

(iii) Necessity / Least Restrictive Means

The third limb is where proportionality does its hardest, most politically consequential work. The State must demonstrate not merely that the chosen means can achieve the aim, but that no less privacy-invasive alternative exists that would achieve it equally well.[9] Applied to data protection, necessity demands data minimisation: if aggregate anonymised data can serve the purpose, individual-level records may not be retained; if a pseudonymous identifier suffices, a biometric one cannot be mandated. The necessity limb has an important doctrinal cousin in EU data protection law, operationalised in GDPR's purpose limitation and data minimisation principles under Articles 5(1)(b) and (c) and is also the limb that the DPDPA 2023 most visibly neglects.[10]

(iv) Procedural Safeguards and Oversight

The fourth limb is, in some ways, the most under-theorised, but for the purposes of this paper it is the most important. Chandrachud J's articulation requires not merely that substantive standards be met, but that the architecture of enforcement i.e., the institutions through which the right is vindicated should be designed to provide genuine and independent oversight. This limb performs a structural constitutional function – it prevents the creations of enforcement bodies that are regulatory, on paper, but effectively subordinate to the very executive they are meant to oversee. Largely, in the history of the DPDPA, this limb has been substantially diluted.

These four limbs, taken together, constitute this paper's analytical measuring stick. Every legislative gap identified will be evaluated against one or more of them. The structure is deliberate: it is not enough to say that Indian data protection law is "weak" but that it is weak in *specific, assessable ways* that a proportionality-compliant legislature could, and should, have addressed. As Frederick Schauer has noted, the translation of judicial proportionality standards into statutory text is notoriously difficult;[11] but difficulty absolve the legislator of the obligation to give meaningful effect to the same requirements, an obligation only partially fulfilled by the legislative trajectory from 2013 to 2019.

The Srikrishna Committee Report (2018)

The Report of the Committee of Experts[12] chaired by Justice BN Srikrishna, delivered in July 2018, grounded in the *Puttaswamy* proportionality framework, remains the most intellectually serious document in the Indian data protection canon. It proposed a Data Protection Authority with a degree of structural independence from the executive, grappled with the problem of State surveillance as a threat to the right it was designed to protect. The Committee understood something that the subsequent legislative process appeared to forget: a data protection statute that exempts the very State actors most likely to violate privacy is not a data protection statute. It is merely a privacy-shaped object.

The Personal Data Protection Bill 2019

The Personal Data Protection Bill, 2019 preserved the core Srikrishna architecture containing 3 features worth foregrounding, because they are features subsequently deleted.

First, the Bill contained a judicial oversight mechanism for government exemptions.[13] Under cl 86 (a mechanism that survived all drafts until 2022), the

[9] Paul de Hert and Serge Gutwirth, 'Privacy, Data Protection and Law Enforcement' in Erik Claes, Anthony Duff and Serge Gutwirth (eds), *Privacy and the Criminal Law* (Intersentia 2006) 71.

[10] Orla Lynskey, *The Foundations of EU Data Protection Law* (Oxford University Press 2015) 167–171.

[11] Frederick Schauer, 'The Tyranny of Choice and the Rulification of Standards' (2005) 14 *William & Mary Bill of Rights Journal* 803, 809.

[12] Committee of Experts under the Chairmanship of Justice BN Srikrishna, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (Ministry of Electronics and Information Technology 2018) <https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf> accessed 12 May 2026.

[13] Personal Data Protection Bill, 2019, cl. 86.

Supreme Court was empowered to designate a High Court bench as the Appellate Tribunal for Data Protection Authority orders, in effect. This was not a merely procedural nicety: it ensured that government processing decisions would be subject to the judicial proportionality review, by passing it through an ordinary constitutional courts structure, exempt to mere executive second-guessing.

Second, the 2019 Bill guaranteed the Data Protection Authority's independence through its appointment and removal provisions.[14] Members were removable only on specified grounds by a committee that included the Chief Justice of India. This was far from perfect considering the lingering suspicion of controversy of judge's roles in appointments but it was a meaningful structural constraint on the temptation to staff a regulator with sympathetic nominees.

Third, and perhaps most significantly, cl 22[15] of the 2019 Bill conferred a right to object to and seek human review of purely automated decisions with significant effects on the individual. This was the Indian analogue of GDPR Article 22, and its existence demonstrated that the drafters of the 2019 Bill had thought seriously about the future of algorithmic governance. It did not survive.

The 2021 PDPB and the JPC Report

The 2019 Bill was referred to a Joint Parliamentary Committee, whose Report in December 2021 reshaped several of the institutional safeguards contained in the original framework.[16] The JPC recommended deleting the judicial oversight mechanism on the ground that existing appellate structures were "adequate". This conclusion was reached without examining whether those structures had ever been used to discipline executive data processing, which they manifestly had not. The recommendation was accepted, effectively severing the limb that would have given the proportionality framework its constitutional bite.

The DPDP Bill 2022 and DPDPA 2023

What arrived in Parliament in 2022 and was enacted in 2023 differed in several important aspects from the framework proposed by the Srikrishna Committee and Personal Data Protection Bill 2019. The DPDPA[17] establishes a Data Protection Board as the enforcement body but the Board's members are appointed and removable by the Central Government, with no independent committee oversight.[18] The government exemption clause in s 17, permits the Central Government to exempt itself and any instrumentality of the State from the Act's obligations on the grounds of "public order" and "sovereignty," without any necessity qualifier, sunset clause, or requirement of judicial pre-authorisation. The breadth of exemption has prompted constitutional concerns under each element of the proportionality framework, though the most significant concerns relate to the fourth limb, namely, procedural safeguards and independent oversight against abuse.

The Aadhaar Ecosystem: Puttaswamy II and the Consent Paradox

Any account of India's privacy legislative framework would be incomplete without confronting the Aadhaar ecosystem – challenged for constitutional validity *before* a data protection statute existed to govern it. The five-judge bench in *Justice KS Puttaswamy (Retd) v Union of India* (Puttaswamy II, the Aadhaar case), delivered in 2018, upholds the constitutional validity of the Aadhaar Act 2016 where Chandrachud J issued a powerful dissent that continued to exert considerable influence on contemporary debates circling privacy scholarship and the constitution.[19]

[14] Personal Data Protection Bill, 2019, cl. 41.
[15] Personal Data Protection Bill, 2019, cl. 22.
[16] Joint Parliamentary Committee on the Personal Data Protection Bill 2019, *Report* (Lok Sabha Secretariat, December 2021) ch 5.
[17] Digital Personal Data Protection Act, 2023.
[18] Graham Greenleaf, 'India's 2023 Data Privacy Act: Business/Government Friendly, Consumer Hostile' (2023) 185 *Privacy Laws & Business International Report* 1, 3–12.
[19] *Justice KS Puttaswamy (Retd) v Union of India (Aadhaar)* (2019) 1 SCC 1.

The central tension, and one unresolved by DPDPA 2023, is the relationship between mandatory biometric enrolment and meaningful consent. The Aadhaar system, as Usha Ramanathan observed well before the constitutional litigation began, converted consent into a precondition for welfare access, transforming a voluntary exercise into a practical compulsion.[20] By 2017, Aadhaar linkage was effectively mandated across seventeen central welfare schemes;[21] and the voluntariness of enrolment had become increasingly contested once access to essential welfare benefits became linked to Aadhaar authentication.

The Sikri J majority in *Puttaswamy II* upheld mandatory Aadhaar seeding of bank accounts and mobile numbers while reading down certain provisions relating to the private sector and metadata aggregation. Chandrachud J's dissent characterised the entire edifice as a "surveillance architecture" that could not be reconciled with the proportionality standard the same judge had articulated in *Puttaswamy I*.[22] As Bhandari and Rahman have noted, the tension was structural: the Court was being asked to evaluate a biometric identity architecture against the fourth *Puttaswamy* limb's requirement of procedural safeguards, but the very data protection statute that would have provided those safeguards did not yet exist.[23]

When the State can condition access to food, housing, or healthcare on the processing of biometric data, the distinction between voluntary consent and practical compulsion becomes increasingly blurred.

3. The RTI–DPDPA Constitutional Collision

Section 44(3) of the DPDPA represents one of the most consequential modifications to the Right to Information since its enactment effectively dismantling a key pillar of the right to information in India.[24] Without any express repeal or formal announcement, Parliament quietly altered the scope of Section 8(1)(j) of the RTI Act by excising the proviso requiring disclosure raising significant concerns regarding democratic accountability.[25]

The proviso was of constitutional consequence, reflecting the Supreme Court's insistence, predating even *Puttaswamy I*, that the right to information is closely connected to freedom of governance and democratic self-governance.[26] Without it, a public servant's salary, a politician's undeclared assets, or a bureaucrat's conflict of interest may now be withheld on grounds of privacy – rendering the statutory mechanism through which public interest considerations could prevail over privacy claims in appropriate cases, ineffective. The Objects and Reasons of the DPDP Bill 2023 do not mention the RTI Act despite speaking in length the need to create a 'trust based' data economy with the amendment being buried in a schedule of consequential amendments.[27]

The constitutional challenge to Section 44(3) proceeds, on three grounds, each reinforced by the others.

The first ground is proportionality. The nine-judge bench in *Puttaswamy I* unanimously established Privacy, as fundamental right under Article 21, is not absolute, and that restrictions on privacy must satisfy legality, legitimate aim, proportionality, and procedural guarantees. The corollary applies symmetrically: restrictions on transparency – itself protected under Article 19(1)(a) – must be the least

[20] Usha Ramanathan, 'A Unique Identity Bill' (2010) 45(35) *Economic & Political Weekly* 10, 12–13.
[21] Anupam Saraph, 'Aadhaar: A Unique Identifier or a Unique Surveillance Architecture?' (2018) 53(24) *Economic & Political Weekly* 13, 16.
[22] *Puttaswamy* (n 1).
[23] Vrinda Bhandari and Faiza Rahman, 'The Aadhaar Judgment and the Right to Privacy' (2019) 54(14–15) *Economic & Political Weekly* 32, 35–36.
[24] Digital Personal Data Protection Act 2023 (n 17), s 44(3).
[25] Right to Information Act 2005, s 8(1)(j).
[26] Gautam Bhatia, *The Transformative Constitution: A Radical Biography in Nine Acts* (HarperCollins 2019) 214–221.
[27] The Digital Personal Data Protection Bill 2023, Statement of Objects and Reasons.

restrictive means of achieving a legitimate aim.[28] The removal of the proviso is a eliminates the principal statutory mechanism for reconciling privacy and transparency interests, leaving the justification unstated.[29]

The second ground is structural, and is an emergent rather than settled argument. The petition argues that the amendment violates the basic structure of the Constitution – specifically an essential democratic component, which requires an informed citizenry capable of holding power to account.[30] The PUCL called it the 'foundation of participatory democracy' [31] – a value that court has located within the basic structure doctrine[32] The conventional position dictates the basic structure doctrine operates as a constrain on constitutional amendments under article 368, not on ordinary legislation. However, academic and judicial commentary suggest that the Court's power of judicial review – in itself a basic structure doctrine – may be engaged to restore the constitutional values that the doctrine seeks to preserve.[33] This argument does not claim settled authority as no Supreme Court decision has applied basic structure doctrine to ordinary legislation – rather is advanced as a doctrinal extension that the Court may choose to accept or reject.

The third ground is the DPDPA's lack of journalistic exemption. Unlike the GDPR, the Act has no carve-out for journalism, academic research, or public interest investigation.[34] Read with the amended Section 8(1)(j), this creates a double foreclosure: the RTI Act can no longer compel disclosure in the public interest, and the DPDPA's obligations on data fiduciaries could be used against investigative reporters.[35] While the RTI governs disclosure by public authorities and DPDPA obligations bind data fiduciaries – investigative journalists who also data fiduciaries can face DPDPA compliance obligations, independent of their RTI rights. Against this background, describing this as arbitrary under article 14 is not implausible.[36] A legislature enacting data protection without a press freedom carve-out and removing public interest override from transparency law, risks transforming privacy from a shield for individual autonomy into a justification for reduced public scrutiny.

It is tempting to declare that privacy and transparency must be harmoniously construed. Tempting, but insufficient. Chandrachud J in *Puttaswamy I* emphasised that privacy 'is not an island unto itself' and must be evaluated against other constitutional values.[37] The Srikrishna Committee had recommended a robust public interest override for journalism, research, and statutory functions including under the RTI Act.[38]

DPDPA imposes extensive obligations on private data fiduciaries while exempting itself from many, and simultaneously shrinks the space in which citizens can hold the state's data practices to account. The citizen's data is doubly vulnerable: to private exploitation without adequate protection, and to state surveillance without the sword of transparency. The question is not whether privacy should be protected, but whose

[28] *Shreya Singhal v Union of India* (2015) 5 SCC 1.

[29] Gautam Bhatia, 'The DPDP Act and the Death of the Public Interest Override' (25 November 2023) 58(47) *Economic and Political Weekly* (online).

[30] *S.R. Bommai v Union of India* (1994) 3 SCC 1, 265.

[31] *PUCL v Union of India* (2003) 4 SCC 399.

[32] *Kesavananda Bharati v State of Kerala* (1973) 4 SCC 225.

[33] Rishad Chowdhury, 'Through a Glass Darkly: Judicial Independence and the Basic Structure Doctrine' (2012) 5(1) *NUJS Law Review* 1, 22.

[34] Digital Personal Data Protection Act 2023 (n 17), ss 17, 36.

[35] ibid.

[36] *Maneka Gandhi v Union of India* (1978) 1 SCC 248.

[37] *Puttaswamy* (n 1).

[38] Srikrishna Committee (n 12) ch 3.

interests the present architecture of privacy protection ultimately serves.[39]

4. Section 17 – Scope of State Exemptions

Section 17 is among the most consequential provisions in the DPDPA, not because of the obligations in creates, but because of the obligations it permits the State to avoid. In one legislative sweep, the provision exempts 'the State' and 'any instrumentality of the State' from virtually the entire architecture of data protection obligations wherever processing is deemed necessary in the interests of 'sovereignty and integrity of India,' 'security of the State,' 'friendly relations with foreign States,' 'public order,' or 'prevention of, detection, investigation or prosecution of any offence or contravention of any law.' The list is not exhaustive it merely requires the Central Government to be 'satisfied' that such processing is 'necessary.' These grounds effectively operate on the Central Government's satisfaction that such processing is necessary.

The risks posed by Section 17 are not merely theoretical. Existing surveillance programmes such as the Delhi Safe City Project, CCTNS, and facial-recognition deployments illustates the types of state processing that may fall within its broad exemptions. The Delhi Safe City Project (₹7,214 crore, ~1.5 lakh cameras) was framed as a women's safety initiative but operates as general-purpose biometric surveillance with no proportionality analysis, no judicial authorisation, and no independent oversight.[40][41] *Puttaswamy II* recognised purpose limitation as constitutionally embedded in the right to privacy. The project's scope creeping from gender-safety to criminal databases and protest monitoring is constitutionally unsanctioned mission drift.

CCTNS, launched in 2009 and integrated across all State police forces by 2021, holds biometric data on persons merely accused, not convicted. It contains no erasure mandate: an acquitted person has no statutory right to removal.[42] Section 17 exempts this indefinite retention from DPDPA obligations, including the right to erasure under Section 12(3).

State-level FRT programmes are arguably more concerning: decentralised normalisation of biometric tracking with even less legal structure.[43] Tamil Nadu's deployment during protests –including the anti-NEET protests and Sterlite Thoothukudi invokes the Tamil Nadu City Police Act 1888, a colonial statute innocent of proportionality doctrine by invoking it as the basis for real-time facial recognition of political protesters is not statutory interpretation. The Supreme Court held that restrictions on fundamental rights must be proportionate and the least intrusive means available, which should not ideally include real-time biometric identifiers.[44]

In *Roman Zakharov* and *Big Brother Watch*, the ECtHR Grand Chamber held that surveillance frameworks lacking independent authorisation, necessity requirements, and end-to-end lifecycle safeguards violate Article 8 ECHR, treating structural incompatibility as independently Convention-violating.[45] The EU AI Act 2024, Article 5(1)(d), legislatively enacted a presumptive prohibition on real-time remote biometric identification in public

[39] Arghya Sengupta and Alok Prasanna Kumar, 'The Right to Information Act and Its Discontents' (2015) 50(22) *Economic and Political Weekly* 17, 19.

[40] Ministry of Home Affairs, 'Safe City Projects under Nirbhaya Fund' (PIB, 23 February 2021); Internet Freedom Foundation, 'Project Panoptic' <https://panoptic.in> accessed 3 March 2025.

[41] Astha Savyasachi, 'As AI Took Over Policing in Delhi, Who Bore the Brunt?' *The Wire* (2 July 2025) <https://thewire.in/government/delhi-police-ai-facial-recognition> accessed 22 May 2026.

[42] Srinivas Kodali, 'CCTNS and the Surveillance State' (Centre for Internet and Society 2022).

[43] Internet Freedom Foundation, 'Facial Recognition Technology and the Law in India' (2023) <https://internetfreedom.in> accessed 20 May 2026.

[44] *Anuradha Bhasin v Union of India* (2020) 3 SCC 637.

[45] *Roman Zakharov v Russia* App No 47143/06 (ECtHR Grand Chamber, 4 December 2015); *Big Brother Watch and Others v United Kingdom* App Nos 58170/13, 62322/14 and 24960/15 (ECtHR Grand Chamber, 25 May 2021).

spaces, with narrow exceptions requiring statutory authority, prior judicial approval, and geographic and temporal limits.[46] India has taken the precisely inverse approach. Where the EU treats city-wide FRT as the paradigm case of AI-mediated rights violation requiring categorical prohibition, Section 17 treats it as requiring no safeguards at all.

Whether Section 17 could survive a direct Article 21 challenge does not admit a confident answer – Indian constitutional litigation has a way of surprising optimists. It appears constitutionally vulnerable, as the proportionality test laid down in Modern Dental College and Research Centre v State of Madhya Pradesh requires the State to show a legitimate aim, necessity, and a fair balance between rights and State interests.[47]

5. The Data Protection Board of India

The DPDPA creates the Data Protection Board of India (hereinafter "DPBI") as the principle institution charged with translating the *Puttaswamy* judgment into an enforceable reality. This section examines whether the Bord's design is capable of performing that tile by advancing two arguments: first, that the Board's institutional design raises significant concerns regarding regulatory independence; second, that even a structurally sound Board may faces arithmetic that exceeds the Board's foreseebale administrative capacity, raising questions about the practical realisation of data protection rights.

A. The Independence Deficit

Section 27 vests appointment, removal, and procedural rulemaking exclusively in the Central Government,[48] and the Board's budget is funded by the Central Government.[49] No judicial member sits on it; procedural rules remain unpublished. In *Centre for PIL v Union of India*, the Supreme Court articulated a tripartite test for independence: security of tenure, financial autonomy, and procedural transparency.[5051] The DPBI fails all three simultaneously. The contrast with established regulators is, difficult to justify: the CCI, SEBI, and TRAI all contain statutory protections against arbitrary removal and guarantee independent budgets.[52] The Board regulating data – the defining resource of the twenty-first century DPDPA enjoys radically structurally weaker independence guarantees than even non- statutory government bodies, a disparity difficult to reconcile with its constitutional significance.

PUCL v Union of India made the constitutional logic explicit: a regulator whose budget is controlled by the executive it supervises cannot effectively hold that executive accountable.[53] This is what R. Sunstein and Adrian Vermeule call structural capture: not episodic corruption of individual decisions, but the systemic orientation of the institution toward regulated-entity preferences by design.[54] Unpublished procedures compound the problem. Under *Shayara Bano*, procedures affecting citizens' rights must be promulgated in advance.[55] A data principal who wishes to complain post-2027 cannot currently know what procedure governs that complaint. The absence of publicly available procedures substantially impairs the practical exercise of statutory rights. Given that the government is also a major data fiduciary, processing personal data through Aadhaar, DigiLocker, and CoWIN rendering concerns regarding institutional independence particularly acute.

[46] Regulation (EU) 2024/1689 [2024] OJ L1689, art 5(1)(d).
[47] *Modern Dental College and Research Centre v State of Madhya Pradesh* (2016) 7 SCC 353, para 76.
[48] Digital Personal Data Protection Act 2023 (n 17), s 27.
[49] ibid s 40.
[50] *Centre for PIL v Union of India* (2011) 4 SCC 1.
[51] ibid paras 45–48.
[52] Competition Act 2002, ss 8, 10; Securities and Exchange Board of India Act 1992, ss 4–5; Telecom Regulatory Authority of India Act 1997, ss 3, 5.
[53] *PUCL* (n 31).
[54] Cass R Sunstein and Adrian Vermeule, 'Libertarian Administrative Law' (2015) 82 *University of Chicago Law Review* 393, 431–434.
[55] *Shayara Bano v Union of India* (2017) 9 SCC 1, para 50.

B. Arithmetic of Enforcement

The Irish Data Protection Commission is the paradigm case. As lead supervisory authority under the GDPR's one-stop-shop mechanism, with 85 staff and a budget of €15.2 million for 4.9 million people,[56] the DPC took six years to issue its first major cross-border decision in the Meta/Facebook determination of December 2022 (the delay in part caused by GDPR's one-stop-shop mechanism – a structural feature absent in India's framework).[57] The UK's ICO issued 1,423 guidance documents against 47 enforcement notices in its first five post-GDPR years[58] – a ratio explained by institutional formation: newly established regulators systematically prioritise norm articulation over enforcement.[59]

The DPBI in contrast will, post-May 2027, face 1.4 billion data subjects across every sector of the Indian economy[60] without any published rules, precedents, and investigative protocols. Ayres and Braithwaite's 'enforcement pyramid' predicts the outcome: resource-constrained regulators tend to remain concentrated at the lower tiers of regulation such as advisories, consultations, and guidance documents and rarely ascend to punitive action – because serious investigations and penalties are expensive and time consuming.[61] Early India regulator experience broadly reflects this pattern. In its formative years, the Competition Commission of India relied heavily on advocacy, compliance-building and market studies before developing penalty-based enforcement practices, reflecting constraints faced by established regulators.[62] Black's work adds the sectoral dimension: under-resourced regulators selectively enforce in high-visibility sectors like fintech, health tech, social media and effectively ignore the rest.[63] Braithwaite identifies the resulting irony – exemplary enforcement against prominent actors substitutes deterrence theatre for deterrence reality.[64] On present projections, the DPBI creates substantial of selective and symbolic enforcement, particularly in its formative years, as resource constraints ay necessitate prioritisation among sectors and complaints.

6. Section 3(c)(ii) of the DPDPA 2023 — The 'Publicly Available' Loophole

The DPDPA arrived as India's answer to *Puttaswamy*. Section 3(c)(ii)[65] substantially narrows the statute's protective reach by exempting any data 'made available by the data principal' or 'publicly available' from the Act's entire protective apparatus – no consent, no purpose limitation, no minimisation, no rights of correction or erasure. Read literally: this means that a data fiduciary who compiles, aggregates, and deploys personal data drawn from public sources is entirely unregulated by the statute. The breadth of this exclusion sits uneasily with *Puttaswamy's* recognition that informational privacy concerns do not disappear merely because information has entered the public domain

[56] Data Protection Commission, 'Data Protection Commission Welcomes Significant Increased Funding of €3.5 Million in 2019 Budget' (Press Release, 9 October 2018) <https://dataprotection.ie/en/news-media/press-releases/data-protection-commission-welcomes-significant-increased-funding-eu35?|> accessed 17 May 2026.

[57] Data Protection Commission (Ireland), Decision pursuant to Section 111 of the Data Protection Act 2018 (Facebook/Meta) (December 2022).

[58] Information Commissioner's Office, *Annual Report 2019/20* (ICO 2020) 8–10.

[59] Cary Coglianese, 'Measuring Regulatory Performance' (OECD Expert Paper No 1, 2012) 12–14.

[60] Digital Personal Data Protection Act 2023 (n 17), s 44.

[61] Ian Ayres and John Braithwaite, *Responsive Regulation* (Oxford University Press 1992) 35–40.

[62] Competition Commission of India, *Competition Advocacy* (CCI 2022) <https://www.cci.gov.in/images/whatsnew/en/competition-advocacy1652513183.pdf> accessed 21 May 2026.

[63] Julia Black, 'Regulatory Conversations' (2002) 29 *Journal of Law and Society* 163, 179.

[64] John Braithwaite, 'The Essence of Responsive Regulation' (2011) 44 *University of British Columbia Law Review* 475, 481.

[65] Digital Personal Data Protection Act 2023 (n 17), s 3(c)(ii).

Consider the following individually unexceptionable data points: A name on a community forum, a political opinion at a town hall, a home district in a biography: each is 'publicly available,' none a privacy violation in isolation. Aggregate them through an OSINT framework and cross-reference with property records and voter rolls, and the output is a surveillance profile assembled without statutory constraint.[66] OSINT-as-surveillance is a documented and expanding routine – deployed by investigators, data brokers, and political operatives[67] – and automated aggregation has rendered Section 3(c)(ii)'s 'public vs private' binary classification of data positively dangerous. In *Rotaru v Romania*[68] the European Court held that public-source information engages the right to private life when systematically collected, tracking what Chandrachud J recognised in *Puttaswamy*.

Helen Nissenbaum's contextual integrity theory holds that disclosure in one context is not consent to use in another.[69] Information shared in one social context carries with it a set of implicit norms about how it should flow like who should receive it, for what purposes, and on what terms – for example, a medical disclosure to a physician flows appropriately to a specialist, but not to an employer. Section 3(c)(ii), treating 'publicly available' as a context-free category, largely disregarding the contextual limitations attached to personal ifnromation when it is disclosed.

A recent *Indian Law Review* article mounts a rigorous proportionality challenge, arguing the provision fails *Puttaswamy*'s necessity limb.[70] This article extends that framework: the provision's vice lies in enabling aggregation into surveillance architectures Chandrachud J identified as incompatible with privacy,[71] and the *ILR* stopped short of proposing a remedy. The California Consumer Privacy Act conditions its equivalent exemption on purpose compatibility;[72] the Indian legislature did not. The proposed rider:

'Section 3(c)(ii): Personal data made publicly available shall be excluded from this Act only to the extent processed for a purpose compatible with the context and purpose of its original disclosure. Processing involving aggregation, profiling, surveillance, or materially different purposes shall not fall within this exclusion.'

This preserves the exemption for journalism, research, and civic discourse (supporting Nissenbaum's framework) while closing the aggregation loophole. It is not a radical proposal but something that proportionality already requires.

7 The Digital Boundary and Governance Vacuum

The DPDPA applies only to *digital* personal data – data in digital form, or data collected non-digitally and subsequently digitised.[73] The moment data is printed or filed on paper, it escapes the Act entirely.

A data fiduciary facing onerous compliance obligations may avoid compliance obligations by designing workflows that keep sensitive records entirely outside digital systems, creating the possibility of lawful regulatory arbitrage.[74] The gap also has concrete human costs. The overwhelming majority of health centres in rural India operate on

[66] Paul Ohm, 'Broken Promises of Privacy' (2010) 57 *UCLA Law Review* 1701, 1716.
[67] Yannick Penders, 'OSINT and the Right to Privacy' (2021) 7 *European Data Protection Law Review* 214, 219–220.
[68] *Rotaru v Romania* App No 28341/95 (ECtHR, 4 May 2000), para 43.
[69] Helen Nissenbaum, 'Privacy as Contextual Integrity' (2004) 79 *Washington Law Review* 119; Helen Nissenbaum, *Privacy in Context* (Stanford University Press 2010) 140.
[70] [Author names redacted], 'Reevaluating Publicly Available Data under the DPDPA 2023' (2026) 10(1) *Indian Law Review* 31.
[71] Aharon Barak, *Proportionality* (Cambridge University Press 2012) 317–318.
[72] California Consumer Privacy Act 2018, Cal Civ Code, s 1798.140(ab).
[73] Digital Personal Data Protection Act 2023 (n 17), s 2(t).
[74] Ramanathan (n 20) 11.

paper. A patient in Jharkhand whose tuberculosis treatment history sits in a dog-eared register has no statutory right to access, correction, or erasure. The constitutional right to privacy declared fundamental in *Puttaswamy* does not discriminate between digits and paper. The DPDPA, regrettably, does.

The exclusion of analog records is compounded by the absence of a corresponding framework governing non-personal data ('NDP'). The Kris Gopalakrishnan Committee (2020, revised 2021) proposed community data trusts, revenue-sharing obligations, and a dedicated NPD Authority.[75] The Committee's recommendations are detailed, coherent, and entirely unimplemented.

The DPDPA simply does not address NPD. Everything but 'personal data' – such as anonymised data, aggregated datasets, community level information – is left entirely ungoverned. Using Couldry and Mejias's *data colonialism* framework as an analytical lens, this permits the appropriation of social activity as commercially valuable data without reciprocity.[76] When a platform aggregates Indian farmers' yield patterns or analyses district –level public health trends, it extracts value from communities who receive nothing. Shoshana Zuboff's 'behavioural surplus' captures the dynamic: extraction exceeds what the service requires, and the excess accumulates as capital.[77]

The IndiaAI Mission (2024, ₹10,372 crore) accelerates into this vacuum.[78] Its dataset initiatives operate without any NPD framework ensuring communities whose data fuels AI training receive any benefit or control. India cannot credibly assert data sovereignty internationally while declining to govern how community data is extracted domestically.

India has been active participant in the BRICS – wide debates on data sovereignty involving Brazil, Russia, China and South Africa where the widely accepted stance remains that the global data economy is structured to extract value from the Global South and accumulate it in the North Atlantic platform economy.[79] This extends domestic regulatory concern into a claim for international economic justice.

§8 Verifiable Consent without Verifiable Standards

The DPDPA announces that no Data Fiduciary shall process a child's personal data without *verifiable* parental consent.[80] The problem is that 'verifiable' carries enormous weight without being given tools to lift it. The Draft Digital Personal Data Protection Rules 2025 gesture toward verification mechanisms but leave the standard entirely to Data Fiduciary discretion.[81]

The most plausible verification candidate is DigiLocker-based parental authentication, which allows parents to authenticate their identity using Aadhar-linked credentials and thereby provide 'verifiable' consent on behalf of their child, but a substantial proportion of rural and low-income parents lack Aadhaar-linked accounts.[82] Children whose parents have the required digital literacy receive protection. Those whose parents lack it face either systematic exclusion from digital services or processing on legally questionable unverified consent – neither consistent with Article 14 or 15(2) which

[75] Kris Gopalakrishnan Committee, *Report on Non-Personal Data Governance Framework* (MeitY 2020, revised 2021) 23–27.

[76] Nick Couldry and Ulises A Mejias, 'Data Colonialism' (2019) 20(4) *Television & New Media* 336, 337–343.

[77] Shoshana Zuboff, 'Big Other: Surveillance Capitalism and the Prospects of an Information Civilization' (2015) 30(1) *Journal of Information Technology* 75, 81.

[78] MeitY, 'IndiaAI Mission' (Government of India 2024).

[79] Arjun Jayadev and others, 'Data and Development: A Political Economy Perspective' (2021) 56(22) *Economic and Political Weekly* 30, 34.

[80] Digital Personal Data Protection Act 2023 (n 17), s 9.

[81] Draft Digital Personal Data Protection Rules 2025, r 10.

[82] Kanchi Kohli and Maju Varghese, 'Digital Access and Exclusion' (2024) 8 *Indian Journal of Law and Technology* 45, 49–52.

requires the state to ensure equal access to statutory benefits.

Comparative law is instructive. The UK's Age Appropriate Design Code requires services accessible to children to apply privacy-protective defaults – minimal data collection, geolocation off – before consent is considered.[83] Article 8 of the General Data Protection Regulation sets the default age of digital consent at 16 while permitting Member States to lower it to thirteen, provided appropriate safeguards are maintained.[84] US COPPA specifies FTC-approved verification mechanisms, providing a measurable floor.[85] The DPDPA provides none.

The children's framework provided by DPDPA, when compared to other global frameworks, rests predominantly on parental consent despite significant disparities in parental capacity, digital literacy, and access raising concerns regarding an equivalent level of protection to all children in practise.

9. Cross-Border Data Transfers and the Adequacy Problem

Section 16 of the DPDPA contemplates a controlled framework for cross-border transfers of personal data. It solemnly permits cross-border transfers of personal data unless restricted by the Central Government, which may notify a whitelist of permissible jurisdictions.[86] As of May 2026, no whitelist has been notified.

In the absence of a notified transfer framework, the practical governance of cross-border transfers remains heavily dependent on private contractual arrangements between Data Fiduciaries and foreign recipients The result is a statutory regime whose central operations safeguard has yet to be implemented.[87] Commentators call it a ghost framework: present on paper, absent in practice.[88] Given *Puttaswamy's* recognition of privacy as a fundamental right, the postponement of a key transfer safeguard through executive notification creates an important statutory gap between the statutory framework contemplates by the Act and its practical operation.

Section 16's vacancy threatens India's adequacy prospects under GDPR Article 45[89] particularly India's ability to secure an adequacy decision from the European Commission, which for practical purposes, is the passport that allows personal data to flow freely from a European Union to a third party – granted only when the third country's data protection offers a satisfactory standard of protection 'essentially equivalent' to that guaranteed within the union.[90] The Commission assesses supervisory independence, effective remedies, exemption scope, and transfer control rigour, each of which, the DPDPA's current posture is uncomfortable with.[91] The whitelist leaves no operative framework to assess. When we take account of overbroadd exemptions under Section 17 include state instrumentalities and certain processing activities in ways that may preclude meaning

[83] Information Commissioner's Office, *Age Appropriate Design Code* (ICO 2021), Standards 2, 4, 7.

[84] Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L119/1, art 8.

[85] Children's Online Privacy Protection Act 1998, 15 USC s 6501; FTC, 'Complying with COPPA: FAQs' (2020) pt 5.

[86] Digital Personal Data Protection Act 2023 (n 17), s 16(1).

[87] U Varottil and VK Khanna, 'Regulating Cross-Border Data Flows: India's Quiet Crisis' (2024) 16 *Indian Journal of Law and Technology* 45, 52.

[88] A Sharma, 'The Ghost Framework: Cross-Border Data Transfer Under the DPDPA 2023' (2024) 5 *National Law School of India Review* (Online) 1, 7.

[89] Regulation (EU) 2016/679 (n 84), art 45.

[90] European Commission, 'Adequacy Decisions: How the EU Determines if a Non-EU Country Has an Equivalent Level of Data Protection' (2024) <https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en> accessed 1 May 2026.

[91] R Bailey and S Parsheera, 'Data Localisation in India: Questioning the Means and Ends' (2018) 14 *Indian Journal of Law and Technology* 183, 201.

oversight – the picture is further eroded.[92] The structural dependence of the DPBI on the Central Government, makes equivalency finding difficult.[93] The Schrems II enforcement requirement further compound the problem.[94] EU-India export flows underpin approximately USD 28 billion in annual IT exports.[95] In the absence of such adequacy, compliance costs associated with alternative transfer mechanisms – such as standard contractual clauses and additional due diligence obligations – fall disproportionately on smaller and mid-sized vendors, which often lack the financial and administrative capacity to absorb them.[9697]

A. The LLM Regulatory Vacuum

Consider the factual context. Indian users interact daily with LLMs hosted and operated outside India such as OpenAI's ChatGPT, Anthropic's Claude, Google's Gemini, and a growing constellation of others. These systems process vast quantities of personal data: names, email addresses, queries that may reveal medical conditions, financial circumstances, or political views. This data is transmitted to and processed on servers outside India, in data centres operated by foreign entities under foreign law. The processing is continuous, diffuse, and from the perspective of the individual Data Principal – entirely invisible.

Section 16 was designed for bilateral B2B transfers while LLM processing is categorically different. The DPDPA has no equivalent of GDPR Article 3(2),[98] extending regulation to foreign controllers offering services to in-jurisdiction residents; a foreign LLM operator may fall outside DPDPA scope entirely even when its Data Principals are Indian.[99] This is the defining failure mode of legacy frameworks applied to foundation models: the controller-processor chain assumes discrete transactions, but LLMs produce probabilistic inferences over aggregated data, where personal data may be extractable from model parameters rather than any conventional database.[100101] Section 16 exposes not merely a gap but the conceptual limits of a statute designed for an economy superseded by a model economy.

Section 26 of Singapore's PDPA addresses cross-border transfers through a contractual obligations regime functioning immediately, without awaiting government notification; with the suggestion being India should adopt a similar mandatory interim regime.[102] In the context of large language models (LLMs) and other AI systems, a territorial scope provision modelled on GDPR Article 3(2) may further strengthen the effectiveness of cross-border data governance. Ultimately, the effectiveness of any international transfer regime depends upon the robustness of the domestic data protection framework on which it rests.

[92] Digital Personal Data Protection Act 2023 (n 17), s 17(2)(b).
[93] V Bhandari, 'The Many Faces of the Data Protection Board: Executive Capture and the Illusion of Independence' (2024) 10 *Indian Law Review* 215, 230.
[94] *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems (Schrems II)* Case C-311/18 EU:C:2020:559, paras 186–202.
[95] NASSCOM, *India IT-BPM Industry Report 2024* (NASSCOM 2024) 12.
[96] Commission Implementing Decision (EU) 2021/914 on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries [2021] OJ L199/31.
[97] Greenleaf (n 18) 105827.
[98] Regulation (EU) 2016/679 (n 84), art 3(2).
[99] D Joshi, 'Personal Data Flows in the Age of Foundation Models: A Regulatory Gap Analysis' (2024) 3 *Journal of International Data Privacy Law* 189, 204.
[100] M MacCarthy, 'Making Sense of Privacy Law's Inadequacy for AI Governance' (2023) 108 *Cornell Law Review Online* 130, 151; A Solow-Niederman, 'Administering Artificial Intelligence' (2020) 93 *Southern California Law Review* 633, 671.
[101] Nicholas Carlini and others, 'Extracting Training Data from Large Language Models' (31st USENIX Security Symposium 2022) 2633.
[102] Personal Data Protection Act 2012 (Singapore), s 26.

10. The AI Governance and the Limits of the DPDPA

Automated decision-making presents a distinctive challenge for data protection such as a system that collects your data, feeds it to a machine, and delivers a life-altering verdict – a loan rejected, a job screened out, a benefit denied – with no explanation and no avenue for challenge. This section identifies three consequential absences in the DPDPA's treatment of automated decision-making, charts the contrast of the IndiaAI Mission with the EU framework, and examines the extent to which existing policy initiatives address those gaps.

A. No Algorithmic Transparency

The DPDPA allows data fiduciaries to deploy automated systems to make decisions affecting creditworthiness, employment, and benefits entitlement without any obligation to explain the decision logic to the person affected.[103] Knowing that your credit score used your transaction history tells you nothing about why the model weighted old late payments more heavily than current income, or whether your postal code served as a proxy for caste. The Supreme Court in *Puttaswamy* held that privacy encompasses the right to control the 'narrative of one's own life' and this right is hollow if a machine can silently alter that narrative without even affording the data principal the right to request the information used against them. Soumyajit Mazumder's comparative study observes that transparency obligations perform a dual function: enabling individual contestation and creating systemic incentives for fiduciaries to audit their models.[104] Without either mechanism, the DPDPA removes the regulatory pressure that would cause fiduciaries to care whether their models work fairly at all.

B. No Right to Contest Automated Decisions

GDPR Article 22 grants every data subject the right not to be subject to a decision based solely on automated processing where it produces legal or similarly significant effects, including rights to human intervention and to contest the outcome.[105] Edwards and Veale fairly argue that even Article 22 is a weaker protection than it appears, given the doctrinal ambiguity around what constitutes a decision 'based solely' on automated processing.[106] But even a compromised right to contest is categorically superior to the DPDPA's alternative, which is no right at all. The DPDPA's remedial architecture is grievance-centric rather than rights-centric: a data principal may complain about breaches of the Act's provisions, but since the Act imposes no obligation of explanation or contestability, there is nothing to breach and therefore nothing to complain about. The result is a remedial framework that provides avenues for complaint only where the Act first creates a substantive obligation.[107] The technical literature has developed robust methodologies – counterfactual explanations, SHAP values, LIME – that enable meaningful human-readable accounts of individual automated decisions without disclosing proprietary model architectures.[108] The objection that explainability requirements would compromise commercial confidentiality is an argument about the form of implementation, not an argument against the right.

C. No Liability for Algorithmic Discrimination

If a model trained on historically biased data produces outputs that replicate or amplify discrimination, the

[103] Digital Personal Data Protection Act 2023 (n 17), ss 6, 11–13, 16–26.

[104] Soumyajit Mazumder, 'Algorithmic Accountability in the Age of Artificial Intelligence' (2023) 15 *NUJS Law Review* 44, 57–59.

[105] Regulation (EU) 2016/679 (n 84), art 22.

[106] Lilian Edwards and Michael Veale, 'Slave to the Algorithm? Why a Right to an Explanation Is Probably Not the Remedy You Are Looking For' (2017) 16 *Duke Law & Technology Review* 18, 67–76.

[107] Shyam Divan and Arghya Sengupta, 'Data Protection in India: A Policy Critique' (2023) 58 *Economic & Political Weekly* 34, 39.

[108] Sandra Wachter, Brent Mittelstadt and Chris Russell, 'Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GDPR' (2017) 31 *Harvard Journal of Law & Technology* 841, 872–873.

DPDPA offers the affected individual no remedy.[109] A fiduciary can comply fully with every DPDPA obligation and still deploy a model that systematically disadvantages women in credit underwriting or applicants from scheduled castes in employment screening. Articles 14 and 15 of the Constitution prohibit discrimination on specified grounds; a statute that by its silence blesses discriminatory algorithmic output is constitutionally uncomfortable territory, and even that argument can currently only be made only before a constitutional court but not before the DPBI.

D. The EU Contrast and IndiaAI Mission

The EU AI Act classifies credit scoring and employment screening as high-risk applications, requiring risk management systems, transparency, human oversight, and pre-deployment conformity assessments.[110] The regulatory arbitrage this produces is stark: an Indian bank deploying an AI credit model for Indian customers faces none of these obligations; the same model for European customers must satisfy all of them. The model does not change, while obligations to different populations differ. The IndiaAI Mission's safety framework, released by MeitY in 2024, is aspirational and voluntary – its own documentation describes it as a 'living document' to be updated as best practices evolve, which is not the language of legally enforceable obligation. Voluntary commitments are revocable at will, and generate no private cause of action, precisely the inverse of what a privacy-protective framework demands.[111]

The three absences – no algorithmic transparency, no right to contest, no liability for discrimination – collectively reveal the limited extent to which the DPDPA engages with the challenges posed by automated decision-making. If India's privacy framework is to be constitutionally adequate, these absences must be addressed by statute, with obligations owed directly to data principals and enforced by a body with jurisdiction to provide them a remedy.

11. Legislative Reform Proposals

The deficiencies documented in the preceding sections admit of concrete remedies. Each proposal below is keyed to a specific doctrinal failure, organised around the constitutional proportionality framework articulated in *Puttaswamy I*. Proposals 11.1-11.3 address the fourth limb – procedural safeguards against abuse. Proposals 11.4 and 11.6 tackle the third limb requiring necessity or proportionality. While proposals 11.5, 11.7, and 11.8 seek to operationalise self-determination.

11.1 Prior Judicial Authorisation

Section 17(1)(b) and (c) permit State processing on grounds of national security and public order on the Central Government's own satisfaction – essentially creating a self-referential standard satisfying none of the four *Puttaswamy* limbs. A new sub-section should require that any processing under these heads be preceded by authorisation from an independent judicial commissioner, modelled on the UK Investigatory Powers Act 2016.[112] The commissioner's mandate should encompass necessity and proportionality review, time-limited authorisation not exceeding six months, and an annual transparency report tabled in Parliament.[113] The European Court of Human Rights in *Roman Zakharov v Russia* held that prior independent authorisation is the minimum Article 8 – compatible standard for secret surveillance – a floor that Section 17 currently undercuts entirely.[114]

[109] Arjun Rajagopalan and Bhargavi Zaveri, 'Algorithmic Credit Scoring in India' (2023) 9 *NLSIU Law Review* 112, 119–125.
[110] Regulation (EU) 2024/1689 (n 46), arts 6, 9, 13, 14 and Annex III.
[111] Madhav Khosla and Ananth Padmanabhan, 'The Constitutional Architecture of Data Protection' (2024) 10 *Indian Law Review* 1, 18.
[112] Investigatory Powers Act 2016 (UK), s 23A; Investigatory Powers Tribunal Rules 2018 (SI 2018/1334).
[113] David Anderson QC, *A Question of Trust: Report of the Investigatory Powers Review* (HMSO 2015) 20–22.
[114] *Roman Zakharov v Russia* (n 45), paras 258–261.

11.2 DPBI Independence: Security of Tenure and Non-Lapsable Budget

Sections 27 and 40 vest appointment, removal, and budget control exclusively in the Central Government.[115] The DPDPA should be amended to provide: (i) that DPBI members are removable only on specified grounds by a process equivalent to removal of a High Court judge under Article 217 of the Constitution; and (ii) that the Board's budget is a non-lapsable charged appropriation on the Consolidated Fund, not subject to annual executive discretion similar to structural protections enjoyed by CCI, SEBI, TRAI.[116] Without them, the *Centre for PIL* tripartite test for regulatory independence cannot be satisfied.[117] The Law Commission has endorsed a ring-fenced budget is the baseline independence guarantee for statutory adjudicatory bodies.[118]

11.3 Restoring the RTI Public Interest Proviso

Section 44(3) excised the proportionality proviso from Section 8(1)(j) of the RTI Act without analysis, argument, or acknowledgment.[119] The legislature should restore the proviso in full, or at minimum introduce by amendment a proportionality requirement: disclosure shall be ordered where, weighing public interest in accountability against individual privacy, the former demonstrably prevails.[120] Far from radical; this proposal is the *Puttaswamy I* standard applied symmetrically to restrictions on transparency.[121]

11.4 Inclusion of Non-Personal Data

Parliament should enact a standalone Non-Personal Data Governance Framework incorporating the Gopalakrishnan Committee's recommendations on community data trusts, mandatory revenue-sharing for commercially valuable community datasets, and a dedicated NPD regulatory authority.[122] The absence of which means that the mobility data of Indian communities remain legally unowned and commercially appropriable without reciprocity.

11.5 Right to Contest Automated Decisions

A new provision should confer on Data Principals the right to contest any automated decision significantly affecting them, and to receive a reasoned explanation of the logic applied.[123] This is the Indian analogue of GDPR Article 22, while avoiding the doctrinal ambiguities that have limited its operation in Europe. An Indian analogue previously existed in clause 22 of the Personal Data Protection Bill 2019 before deletion by the Joint Parliamentary Committee. Edwards and Veale have established that an explanation obligation is the minimum accountability standard consistent with rule-of-law values in algorithmic governance.[124]

11.6 Whitelist Criteria and Adequacy Baseline

Section 16's cross-border transfer framework is, in operational terms, a ghost: no whitelist has been published since enactment.[125] The Central Government should publish whitelist criteria, adopting GDPR Article 45 as the baseline standard of *essentially equivalent* protection. For LLM and foundation-model processing by foreign operators serving Indian Data Principals, a new territorial scope provision modelled on GDPR Article 3(2) should extend DPDPA jurisdiction to foreign controllers offering services in India. Without adequacy, smaller

[115] Digital Personal Data Protection Act 2023 (n 17), ss 27, 40.
[116] Competition Act 2002 (n 52), ss 8, 10; Securities and Exchange Board of India Act 1992 (n 52), ss 4–5; Telecom Regulatory Authority of India Act 1997 (n 52), s 5.
[117] *Centre for PIL* (n 50), paras 45–48.
[118] Law Commission of India, Report No 272, *Assessment of Statutory Frameworks of Tribunals in India* (Law Commission of India 2017), paras 5.6–5.9.
[119] Right to Information Act 2005, s 8(1)(j) (n 25), as amended by Digital Personal Data Protection Act 2023, s 44(3) (n 24).
[120] *Puttaswamy (n 1), paras 180–185; Shreya Singhal (n 28), para 88.*
[121] Bhatia (n 29); *PUCL* (n 31).
[122] Gopalakrishnan Committee (n 75) ch 4.
[123] Personal Data Protection Bill 2019, cl 22 (n 15); Regulation (EU) 2016/679 (n 84), art 22.
[124] Edwards and Veale (n 106) 44–46.
[125] Digital Personal Data Protection Act 2023 (n 17), s 16(1); Regulation (EU) 2016/679 (n 84), art 45.

players the IT-BPM sector face disproportionate compliance costs on standard contractual clauses.

11.7 Children's Consent

Section 9 mandates verifiable parental consent without defining verification; the Draft Rules 2025 leave the standard entirely to Data Fiduciary discretion.[126] The amended Rules should: (i) mandate a government-approved technical verification mechanism within 12 months, with the FTC's COPPA-compliant approved-mechanism model as comparative baseline; (ii) require offline-accessible alternatives to DigiLocker-based verification for parents without Aadhaar-linked accounts; and (iii) adopt privacy-by-default standards for services accessible to children, as required by the UK Age Appropriate Design Code.[127] A consent architecture resting exclusively on digital infrastructure that a substantial proportion of rural and low-income parents cannot access creates a constitutionally suspect equity gap under Article 15.[128]

11.8 Consent Manager Fiduciary Duty and Prohibition on Metadata Exploitation

The Consent Manager institution is constructed without a duty of loyalty to the Data Principal: a structural vulnerability with no equivalent omission in the RBI's Account Aggregator framework, from which the DPDPA drew its inspiration.[129] The DPDPA Rules should import three already-operative AA obligations: (i) a prohibition on commercial use of consent metadata beyond the consent-management function; (ii) an explicit fiduciary duty of loyalty enforceable by the DPBI with personal liability for senior management; and (iii) mandatory independent audits filed with the Board.[130] A Consent Manager consolidating consent signals across dozens of fiduciaries builds – from patterns of consent and refusal alone — a granular behavioural map whose commercial value may exceed that of the underlying personal data. Without fiduciary constraint, the institution designed to operationalise informational self-determination under *Puttaswamy* becomes a vehicle for its commercial erosion.[131]

Taken together, these eight reforms would not transform the DPDPA into the GDPR. They would, more modestly, bring the statute into constitutional compliance with the proportionality framework that the nine-judge bench in *Puttaswamy I* made binding. That is the minimum the constitutional order requires and, on the evidence of the legislative arc between 2019 and 2023, the minimum that the legislature has so far declined to deliver.

12. Conclusion

The eight gaps documented in this paper are not random oversights. They share a common pathology that the legislative history makes visible. Between the 2019 Bill and the enacted DPDPA, Parliament systematically removed oversight mechanisms - judicial pre-authorisation for state exemptions, independent appointment for the regulatory board, human review of automated decisions - while simultaneously expanding the state's exemptive footprint. The Srikrishna Committee understood that a statute exempting the actors most likely to violate privacy is not a data protection statute. The DPDPA has proved the Committee right.

The DPDPA's consent architecture for private-sector processing is elaborate and sincere, within its limits. The same statute's public-sector architecture is a constitutional placeholder: Section 17 exempts the State on grounds of its own satisfaction, the DPBI is

[126] Digital Personal Data Protection Act 2023 (n 17), s 9; Draft Digital Personal Data Protection Rules 2025, r 10 (n 81).
[127] ICO, *Age Appropriate Design Code* (n 83); Regulation (EU) 2016/679 (n 84), art 8; Children's Online Privacy Protection Act 1998 (n 85), 15 USC s 6501.
[128] Kohli and Varghese (n 82) 49–52.
[129] Tamar Frankel, *Fiduciary Law* (Oxford University Press 2011) 1–5.
[130] Reserve Bank of India, Master Direction — Account Aggregator (Reserve Bank) Directions 2016, cl 8.
[131] Regulation (EU) 2016/679 (n 84), art 7(4); *Puttaswamy* (n 1).

appointed and removed by the executive it is meant to check, and Section 44(3) withdrew the citizen's most effective tool for democratic accountability. The fourth *Puttaswamy* limb regarding procedural safeguards and independent oversight is structurally precluded.

The enforcement realism verdict is correspondingly bleak. Even the private-sector protections the DPDPA affords will be honoured in the breach for the foreseeable future. The Board's capacity constraints and structural dependence are design features requiring legislative correction. Comparative experience with the Irish DPC's six-year delay and the ICO's guidance-to-enforcement ratio confirms that newly established, resource-constrained regulators default to norm articulation over punitive action. The DPBI, facing 1.4 billion data subjects without published rules or precedents, will not be an exception.

Two gaps constitute genuine scholarly white space: the RTI collision and the Consent Manager fiduciary gap warrant sustained doctrinal treatment beyond what is possible here. The AI liability gap and the non-personal data vacuum require separate analysis as India's AI governance framework matures; they are the next research agenda.

The DPDPA's architects cited *Puttaswamy* and structured the Act around consent and data-principal rights in a language that echoes the judgment but a privacy law that cannot answer the question 'who watches the watchers?' is not a privacy law for people, but for the government.

*****