The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

FROM CONTRACT TO CONSTITUTION: MAPPING THE EVOLUTION OF DATA PROTECTION LAW IN INDIA

~ Gurnika Dhillon

ABSTRACT

For most of its digital history, India protected personal data almost by accident. The earliest safeguards came from a single compensation clause in the Information Technology Act, 2000 and from whatever a company chose to promise in its privacy policy. This paper traces how that contract-based model gave way to a rights-based one. It follows two connected tracks. The first is constitutional: the slow recognition of privacy by the Supreme Court, which ended in the nine-judge bench decision in Justice K.S. Puttaswamy v. Union of India*. The second is legislative: the SPDI Rules of 2011, the Srikrishna Committee Report, the Personal Data Protection Bill of 2019 and its withdrawal in 2022, followed by the Digital Personal Data Protection Act, 2023 and the Rules notified in November 2025. With this history in place, the paper looks closely at two features of the new framework that are still at an early stage. These are the working of notice and consent for a very diverse body of users and the independence and capacity of the Data Protection Board of India. The paper closes with a set of practical reforms. It argues that the phased roll-out running until May 2027 gives the framework a real chance to live up to the constitutional promise made in* Puttaswamy.

Keywords: *Data Protection; DPDP Act, 2023; Right to Privacy; Puttaswamy; Data Protection Board; India*

I. INTRODUCTION

Few countries have digitised the daily life of their citizens as quickly as India. Aadhaar-based identification, the Unified Payments Interface, direct benefit transfers and a fast-growing e-commerce market now reach almost every household. By the end of March 2026, India had

more than 1,092 million internet subscribers.[1] Each of these systems runs on personal data. Yet for close to two decades that data was collected without any law written for its protection. A person whose information was misused had to fall back on a mix of contract, tort and constitutional remedies, none of which had been designed with this problem in mind.

In the early model, the relationship between a user and a company was treated as a private bargain. The company published its terms, the user clicked "I agree" and the law asked few further questions. The Delhi High Court reflected this approach in 2016 when it declined to strike down WhatsApp's revised privacy policy, treating the terms of service as an arrangement that users were free to accept or reject.[2] The later model begins from a different premise. Informational privacy is now part of the fundamental right to life and personal liberty under Article 21 of the Constitution of India. The State must protect it and may restrict it only on settled grounds. The Digital Personal Data Protection Act, 2023 ("DPDP Act") and the Digital Personal Data Protection Rules, 2025 ("DPDP Rules") are the statutory outcome of that change in thinking.

II. DOCTRINAL AND LEGISLATIVE FOUNDATIONS

A. CONSTITUTIONAL BASIS: TRACING THE RIGHT TO PRIVACY

For a long time it was unclear whether the Constitution protected privacy at all. In *M.P. Sharma v. Satish Chandra*, an eight-judge bench upheld search powers under the Code of Criminal Procedure, 1898 (since replaced by the Bharatiya Nagarik Suraksha Sanhita, 2023). The Court reasoned that the framers had not written anything like the Fourth Amendment of the United States Constitution into the Indian text and that such a right could not be imported by interpretation.[3] A similar caution marked *Kharak Singh v. State of U.P.* There, a six-judge bench struck down the police regulation permitting nightly domiciliary visits to the homes of persons under surveillance, holding them to be an invasion of personal liberty under Article 21. The majority nonetheless refused to accept privacy as a guaranteed right. Justice Subba Rao took a wider view in his dissent. In his opinion, personal liberty included freedom from

[1] Press Release No. 76/2026, Telecom Regul. Auth. of India, The Indian Telecom Services Performance Indicator Report for the Quarter January-March, 2026 (June 22, 2026), https://www.trai.gov.in/sites/default/files/2026-06/PR_No.76of2026.pdf.
[2] *Karmanya Singh Sareen v. Union of India*, 2016 SCC OnLine Del 5334 (India).
[3] *M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300 (India).

intrusion into one's private life, whether by physical entry or by watching a person's movements.[4] That dissent would be vindicated more than fifty years later.

The decades in between saw slow, case-by-case progress. In *Gobind v. State of M.P.*, the Court accepted with some hesitation that a limited right to privacy could be drawn from Articles 19 and 21 and that it would yield only to a compelling state interest.[5] *R. Rajagopal v. State of T.N.* recognised a "right to be let alone" against the unauthorised publication of a person's life story.[6] In *People's Union for Civil Liberties v. Union of India*, the Court held that telephone tapping without procedural safeguards violated Article 21.[7] *District Registrar and Collector v. Canara Bank* went a step further. It held that privacy attaches to the person and not to the place, so that bank records held by a third party still carried a privacy interest.[8] *Selvi v. State of Karnataka* later carried this reasoning into the mind itself, holding that involuntary narco-analysis and similar techniques intruded upon mental privacy.[9] Each of these rulings protected privacy in a particular setting. None of them settled whether privacy was a fundamental right in its own right.

The question finally reached a nine-judge bench through the Aadhaar litigation. The Union of India relied on *M.P. Sharma* and *Kharak Singh* to argue that citizens had no fundamental right to privacy. A three-judge bench, unable to reconcile those decisions with later case law, referred the question to a larger bench.[10] In *Justice K.S. Puttaswamy (Retd.) v. Union of India*, the nine judges unanimously held that privacy is an intrinsic part of the right to life and personal liberty under Article 21 and is also protected by the freedoms guaranteed under Articles 14 and 19. *M.P. Sharma* and *Kharak Singh* were overruled to the extent that they held otherwise.[11] The Court expressly recognised informational privacy as one aspect of the right. Justice Chandrachud also noted that threats to privacy in the information age come from private actors as much as from the State and called upon the Government to put a data protection regime in place.[12]

---

[4] *Kharak Singh v. State of U.P.*, AIR 1963 SC 1295 (India); *see id.* (Subba Rao, J., dissenting).
[5] *Gobind v. State of M.P.*, (1975) 2 SCC 148 (India).
[6] *R. Rajagopal v. State of T.N.*, (1994) 6 SCC 632 (India).
[7] *People's Union for C.L. v. Union of India*, (1997) 1 SCC 301 (India).
[8] *Dist. Registrar & Collector v. Canara Bank*, (2005) 1 SCC 496 (India).
[9] *Selvi v. State of Karnataka*, (2010) 7 SCC 263 (India).
[10] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2015) 8 SCC 735 (India) (order of reference).
[11] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).
[12] *Id.* (Chandrachud, J.).

Equally important was the test the Court laid down for judging restrictions on privacy. Building on its earlier decision in *Modern Dental College and Research Centre v. State of M.P.*,[13] the plurality opinion required that any intrusion must have a basis in law, must pursue a legitimate state aim and must be proportionate to that aim.[14] Justice Kaul added a fourth requirement of procedural guarantees against the abuse of such power.[15] This four-part standard was applied a year later in the Aadhaar judgment. The Court upheld the scheme in a modified form but struck down Section 57 of the Aadhaar Act, 2016, which had allowed private companies to demand Aadhaar-based authentication from their customers.[16]

Two points emerge from this history. First, the right to privacy in India is a creation of the courts. The constitutional text does not mention it. It took six decades of argument before the Supreme Court read it into Articles 14, 19 and 21.[17] Second, legislation followed the courts instead of leading them. Parliament did not act on data protection in any serious way until *Puttaswamy* left it with little choice. The legislative history that follows should be read against this background.

B. EVOLUTION OF THE LEGISLATIVE JOURNEY

Before 2008, Indian law had very little to say about personal data held by private businesses. Disputes were left to the Indian Contract Act, 1872 and to the equitable action for breach of confidence. In practice, a company owed its users only what its own terms of service promised. The Information Technology (Amendment) Act, 2008 introduced two provisions that would remain the core of the law for the next fifteen years. Section 43A made a body corporate liable to pay compensation if it was negligent in maintaining "reasonable security practices and procedures" while handling sensitive personal data and that negligence caused wrongful loss or gain to any person.[18] Section 72A made it an offence for a service provider who had obtained personal information under a lawful contract to disclose it without consent or in breach of that contract, with intent to cause wrongful loss or gain.[19] The second provision shows how closely the early model tied privacy to contract. The wrong lay in breaking the bargain. A person's interest in their own data was protected only to the extent that the bargain recognised it.

---

[13] *Modern Dental Coll. & Res. Ctr. v. State of M.P.*, (2016) 7 SCC 353 (India).
[14] *Puttaswamy*, (2017) 10 SCC 1, ¶ 325 (Chandrachud, J.).
[15] *Id.* ¶ 638 (Kaul, J., concurring).
[16] *Justice K.S. Puttaswamy (Retd.) v. Union of India (Aadhaar)*, (2019) 1 SCC 1 (India).
[17] INDIA CONST. arts. 14, 19, 21.
[18] The Information Technology Act, 2000, § 43A, No. 21, Acts of Parliament, 2000 (India) [hereinafter IT Act] (inserted by The Information Technology (Amendment) Act, 2008, No. 10, Acts of Parliament, 2009 (India)).
[19] IT Act § 72A.

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("SPDI Rules") gave Section 43A some content. They identified categories of sensitive data such as passwords, financial information, health records, sexual orientation and biometric information. They also required a published privacy policy and consent in writing before such data was collected. Compliance with the IS/ISO/IEC 27001 standard was treated as one way of meeting the security requirement.[20] The limits of the framework were nevertheless clear. It applied only to a "body corporate" and so left government departments outside its scope. It created no regulator, gave individuals no general right to access or erase their data and offered compensation as the only remedy. Comparative scholarship has pointed to how rarely these rules were enforced in practice.[21]

Pressure for a complete statute built up while *Puttaswamy* was still pending. In July 2017, the Ministry of Electronics and Information Technology constituted a Committee of Experts under the chairmanship of Justice B.N. Srikrishna. The Committee submitted its report, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians*, in July 2018 along with a draft bill. It recommended an independent Data Protection Authority, a separate class of sensitive personal data and a requirement that at least one serving copy of personal data be stored in India.[22]

These recommendations formed the basis of the Personal Data Protection Bill, 2019, which was introduced in the Lok Sabha in December 2019 and referred to a Joint Parliamentary Committee. The Bill departed from the Committee's draft in one important respect. Clause 35 allowed the Central Government, by a simple executive order, to exempt any of its agencies from the whole of the law on grounds such as sovereignty, security of the State and public order. Commentators warned that this power could be used to shield state surveillance from scrutiny.[23] The Joint Parliamentary Committee reported in December 2021. It proposed eighty-one amendments and twelve further recommendations, including bringing non-personal data

---

[20] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, rr. 3-5, 8, G.S.R. 313(E), Gazette of India, pt. II sec. 3(i) (Apr. 11, 2011) (India) [hereinafter SPDI Rules].

[21] *See generally* GRAHAM GREENLEAF, ASIAN DATA PRIVACY LAWS: TRADE AND HUMAN RIGHTS PERSPECTIVES (2014).

[22] COMM. OF EXPERTS UNDER THE CHAIRMANSHIP OF JUSTICE B.N. SRIKRISHNA, A FREE AND FAIR DIGITAL ECONOMY: PROTECTING PRIVACY, EMPOWERING INDIANS (2018).

[23] The Personal Data Protection Bill, 2019, Bill No. 373 of 2019, cl. 35 (India); *see* Anirudh Burman, *Will India's Proposed Data Protection Law Protect Privacy and Promote Growth?* (Carnegie India, Working Paper, Mar. 2020), https://carnegieendowment.org/research/2020/03/will-indias-proposed-data-protection-law-protect-privacy-and-promote-growth.

within the scope of the law.[24] This wider scope made an already complex bill harder to pass. In August 2022, the Government withdrew the Bill and announced that a "comprehensive legal framework" would be brought in its place.[25]

The DPDP Act received Presidential assent on 11 August 2023. It is far shorter and simpler than the bills that came before it. Three changes stand out. First, the strict localisation proposals were dropped. Personal data may now be transferred to any country unless the Central Government restricts transfers to it by notification.[26] Second, the separate category of sensitive personal data was abandoned, so that all personal data is now treated alike. Third, the Act gives the State wide room to process data without consent. Section 7 lists "certain legitimate uses" that include the provision of subsidies, benefits and services by the State. Section 17 allows the Central Government to exempt any of its instrumentalities from the Act in the interests of sovereignty, security of the State, public order and friendly relations with foreign States.[27]

At its centre, the Act relies on consent. Section 6 requires consent to be "free, specific, informed, unconditional and unambiguous with a clear affirmative action". Such consent must be preceded by a notice under Section 5 describing the personal data to be collected and the purpose of collection.[28] The Act also formally closes the contract era. Once the relevant provisions are brought into force, Section 44(2) omits Section 43A of the IT Act. The legal foundation of the SPDI Rules falls away with it.[29]

The DPDP Rules were notified on 13 November 2025.[30] They are being brought into force in three stages. The rules relating to the Data Protection Board took effect at once. The rules on the registration of Consent Managers take effect after one year, in November 2026. The remaining duties of data fiduciaries, including notice, security safeguards, breach intimation and the rights of data principals, take effect after eighteen months, in May 2027.[31] In early

[24] LOK SABHA SECRETARIAT, REPORT OF THE JOINT COMMITTEE ON THE PERSONAL DATA PROTECTION BILL, 2019 (Dec. 2021) (India).
[25] *Govt Withdraws Data Protection Bill from Lok Sabha, To Bring New One with Digital Privacy Provisions*, (Aug. 3, 2022).
[26] The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India) [hereinafter DPDP Act], § 16.
[27] *Id.* §§ 7, 17.
[28] *Id.* §§ 5, 6(1).
[29] *Id.* § 44(2)(a).
[30] The Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), Gazette of India, pt. II sec. 3(i) (Nov. 13, 2025) (India) [hereinafter DPDP Rules].
[31] *Id.* r. 1(2)-(4).

2026, the Ministry consulted industry on a proposal to shorten the eighteen-month period to twelve months. No amendment to this effect had been notified at the time of writing.[32]

Read in sequence, each version of the law moved further away from the Srikrishna Committee's model of strong regulation and data localisation. Each moved closer to a lighter model that leaves a good deal to executive discretion.

III. AREAS FOR CONTINUED DEVELOPMENT

A. NOTICE-AND-CONSENT IN PRACTICE

The DPDP Act relies on consent far more heavily than the European Union's General Data Protection Regulation ("GDPR"). The GDPR recognises six lawful bases for processing that stand on an equal footing, including contract, legal obligation and legitimate interests.[33] Under the Indian Act, a private data fiduciary must usually either obtain consent or bring its processing within the short list of legitimate uses in Section 7. This choice reflects respect for individual autonomy. It also assumes that the person giving consent will read the notice, understand it and make a real decision.

That assumption is open to doubt even in wealthy markets. One well-known American study estimated that reading every privacy policy a person encounters would take around two hundred hours a year.[34] Daniel Solove has argued that people cannot realistically manage their privacy one consent at a time, since they face too many decisions and lack the information needed to make them well.[35] Europe's experience with cookie banners, where users routinely click "accept" simply to reach the content, points in the same direction. In India the problem is sharper. Many users have come online only recently, often on low-cost smartphones and in languages other than English. Terms such as "data fiduciary" or "specified purpose" mean little to them. The law does take a sensible first step here. A data principal may ask for the notice in English or in any language listed in the Eighth Schedule to the Constitution. The Rules also require the notice to be understandable on its own without reference to other documents.[36]

---

[32] *MeitY Plans to Cut Short DPDP Compliance Timeline and Notify Cross Border Restrictions for SDFs*, S.S. RANA & CO. (Feb. 13, 2026), https://ssrana.in/articles/meity-plans-to-cut-short-dpdp-compliance-timeline-and-notify-cross-border-restrictions-for-sdfs/.

[33] Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), art. 6(1), 2016 O.J. (L 119) 1 [hereinafter GDPR].

[34] Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J.L. & POL'Y FOR INFO. SOC'Y 543 (2008).

[35] Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880 (2013).

[36] DPDP Act § 5(3); DPDP Rules r. 3.

The Act's main answer to consent fatigue is the Consent Manager. This is a registered intermediary through which a data principal can give, review and withdraw consent across many data fiduciaries from a single platform.[37] The idea borrows from the Account Aggregator system that the Reserve Bank of India created for financial data.[38] Whether it works will depend on choices that are still being made. Much turns on how simple the interfaces are, whether they function in regional languages and whether people trust them enough to use them. The Account Aggregator experience shows that such systems need time and steady adjustment by the regulator before they gain wide acceptance. A consent dashboard cannot by itself make consent meaningful if the notices behind it remain long and opaque.

B. BUILDING THE DATA PROTECTION BOARD'S CAPACITY

The Data Protection Board of India is the body on which enforcement of the Act depends. It is meant to receive complaints, inquire into personal data breaches, direct urgent remedial measures and impose penalties. These penalties can go up to two hundred and fifty crore rupees for a failure to take reasonable security safeguards.[39] Section 28 declares that the Board shall function as an independent body.[40] Its design, however, gives the executive a large role. The Chairperson and Members are appointed by the Central Government[41] on the recommendation of a search-cum-selection committee chaired by the Cabinet Secretary.[42] They hold office for only two years and are eligible for re-appointment.[43] A short renewable term offers weak protection, because members may hesitate to take decisions that displease the authority deciding whether to reappoint them. The GDPR, by contrast, requires every supervisory authority to act with "complete independence".[44] Measured against the procedural safeguards limb of the *Puttaswamy* test, the Indian arrangement needs strengthening. This matters all the more because the State is itself one of the largest processors of personal data that the Board will oversee.

The Board also has to be built from the ground up. The provisions for its establishment have been in force since November 2025. Even so, the Ministry invited applications for the posts of

[37] DPDP Act §§ 2(g), 6(7)-(9); DPDP Rules r. 4, sch. I.
[38] Reserve Bank of India, Account Aggregator (Reserve Bank) Directions, 2016, Master Direction DNBR.PD.009/03.10.119/2016-17 (Sept. 2, 2016) (India).
[39] DPDP Act §§ 27, 33, sch.
[40] *Id.* § 28(1).
[41] *Id.* § 19(3).
[42] DPDP Rules r. 17.
[43] DPDP Act § 20(1).
[44] GDPR art. 52(1).

Chairperson and four Members only in May 2026.[45] Its powers to inquire and adjudicate will come into force along with the rest of the Act in May 2027.

The scale of the task is large. India now has more than a billion internet subscribers.[46] Every one of them becomes a potential complainant once the main duties take effect. The Act expects the Board to work, as far as practicable, as a digital office with complaints filed and heard online. That may help it cope with volume. Experience elsewhere is still a caution. Ireland's Data Protection Commission supervises many of the world's largest technology companies from a country of about five million people. It has faced repeated criticism for the slow pace of its cross-border decisions.[47] A careful study of the staff and technical expertise needed per million users would be a useful next step for Indian policy-makers. Appeals from the Board lie to the Telecom Disputes Settlement and Appellate Tribunal, a forum that already carries a heavy telecom docket.[48] Unless the Tribunal receives additional benches or members, appeals may well become the next bottleneck.

IV. CONSOLIDATING THE FRAMEWORK: CHALLENGES AND REFORMS

Placing India's data protection law on a statutory footing is a real achievement. The phased roll-out until 2027 offers an opportunity to correct the weaker parts of the framework before they harden into settled practice. Five concerns deserve attention.

The first concern is the breadth of the exemptions available to the State. Section 17(2)(a) allows the Central Government to exempt any instrumentality of the State by notification in the interests of sovereignty, security of the State, public order and similar grounds.[49] These grounds are not defined. The notification need not give reasons, is not subject to review and has no fixed life. Exemptions of this kind are common in data protection laws. Yet *Puttaswamy* requires every restriction on privacy to be necessary and proportionate and to be accompanied by safeguards against abuse. A blanket exemption granted by executive notification sits uneasily with that requirement. The *PUCL* judgment offers a familiar model, since it required

[45] Ministry of Elecs. & Info. Tech., F. No. 2(1)/2026-Pers.I, Inviting Applications for the Posts of Chairperson and Members of the Data Protection Board of India (May 6, 2026) (India), https://www.meity.gov.in/static/uploads/2026/05/cd481c027470b420b4cb85fb40a91c53.pdf.
[46] *See* Press Release No. 76/2026, *supra* note 1.
[47] *See* IRISH COUNCIL FOR CIVIL LIBERTIES, EUROPE'S ENFORCEMENT PARALYSIS: ICCL'S 2021 REPORT ON THE ENFORCEMENT CAPACITY OF DATA PROTECTION AUTHORITIES (2021).
[48] DPDP Act § 29; The Telecom Regulatory Authority of India Act, 1997, § 14, No. 24, Acts of Parliament, 1997 (India).
[49] DPDP Act § 17(2)(a).

interception orders to be made by a senior official in writing and to be examined by a review committee.[50]

A related question has already reached the Supreme Court. Section 44(3) of the DPDP Act substitutes Section 8(1)(j) of the Right to Information Act, 2005. The amended clause exempts all personal information from disclosure and removes the earlier public interest override.[51] Journalists and transparency groups have challenged this amendment along with other parts of the Act. In February 2026, the Court issued notice and referred the central questions to a larger bench. It declined, however, to stay the operation of the Act.[52] The outcome will shape how privacy and transparency are balanced under the new law.

The second concern is the independence of the Board, discussed above. A new regulator had to be set up quickly. Some executive involvement in its early design is therefore understandable. Its long-term credibility, however, depends on clearer insulation from the Government it will sometimes have to rule against.

The third concern is the loss of a separate category of sensitive personal data. The SPDI Rules recognised that health records, biometric data, financial details and sexual orientation call for greater care because their misuse causes graver harm.[53] The GDPR takes the same view.[54] The DPDP Act, in contrast, treats a person's shopping history and medical records in exactly the same way. The simplicity is welcome. It nonetheless removes a safeguard that Indian law had already tested.

The fourth concern relates to erasure. Section 12 gives data principals a right to have their data erased. Section 8(7) also requires data fiduciaries to erase data once consent is withdrawn or the purpose is served.[55] The right gives way, however, wherever retention is required by law. It also does not reach personal data that the data principal has made publicly available, because the Act does not apply to such data at all.[56] Courts have had to fill this gap through the "right to be forgotten". In *Jorawer Singh Mundy v. Union of India*, the Delhi High Court directed that a judgment acquitting the petitioner be blocked from search engine results while the case was

[50] *People's Union for C.L.*, (1997) 1 SCC 301.
[51] DPDP Act § 44(3); The Right to Information Act, 2005, § 8(1)(j), No. 22, Acts of Parliament, 2005 (India).
[52] *Reporters Collective Tr. v. Union of India*, W.P. (C) No. 211/2026 (Feb. 16, 2026) (India) (order issuing notice).
[53] SPDI Rules r. 3.
[54] GDPR art. 9.
[55] DPDP Act §§ 8(7), 12(3).
[56] *Id.* § 3(c)(ii).

pending, recognising the lasting harm that easily searchable records can cause.[57] A clearer statutory standard, informed by Article 17 of the GDPR and by the ruling of the Court of Justice of the European Union in *Google Spain*,[58] would give data principals more certainty and spare courts from deciding these questions one case at a time.

The fifth concern is capacity. The real test of the Board will come once the main duties apply and complaints begin to arrive in large numbers. The appellate route through the Tribunal adds a further point of pressure.

Each of these concerns can be met within the structure the Act already provides. Exemptions under Section 17(2)(a) could be granted only through a reasoned order for a fixed period, subject to periodic review by an independent committee. The grounds on which they rest could also be narrowed in line with the safeguards developed for interception after *PUCL*. The Board's independence could be secured through an appointments committee with judicial, executive and civil society members, a fixed tenure of at least five years, removal only for proven misconduct and an assured budget. The Supreme Court's insistence in *Anoop Baranwal v. Union of India* that appointments to the Election Commission should not rest with the executive alone shows how seriously Indian law already treats this concern for constitutional bodies.[59]

On the consent side, layered notices in regional languages, a plain-language readability standard and periodic independent audits of Consent Managers would reduce the gap between formal and real consent. Graded categories of sensitive personal data could be restored, with stricter breach notification thresholds for health, biometric and financial information. The right to erasure could be defined more fully, with clear exceptions for legal retention, journalism and archiving. It could then be phased in alongside the Consent Manager framework. Finally, a capacity plan tied to the November 2026 and May 2027 milestones should set minimum numbers of legal and technical staff for the Board. It could also provide for regional benches instead of a single centralised body. Taken together, these measures would build on what the DPDP Act has already achieved and would help the framework grow into a regime that honours the constitutional foundation laid in *Puttaswamy*.

---

[57] *Jorawer Singh Mundy v. Union of India*, 2021 SCC OnLine Del 2306 (India).
[58] GDPR art. 17; Case C-131/12, *Google Spain SL v. Agencia Española de Protección de Datos*, ECLI:EU:C:2014:317 (May 13, 2014).
[59] *Cf. Anoop Baranwal v. Union of India*, (2023) 6 SCC 161 (India).

V. CONCLUSION

India's data protection law has come a long way in a short time. What began as one compensation clause and a set of rules for corporate bodies has become a dedicated statute with its own regulator and detailed rules. The change in thinking matters as much as the change in form. Personal data is no longer protected only because a company promised to protect it. It is protected because the Constitution, as read in *Puttaswamy*, gives every person a right to control information about themselves. Measured against the vision of the Srikrishna Committee, the framework still has ground to cover. This is especially true of state exemptions and the independence of the Board. The four-part test in *Puttaswamy* offers a practical yardstick for that work.[60] The months until May 2027 are therefore an opportunity. If the reforms suggested here are taken up, the DPDP framework can mature into a regime that protects individuals while respecting the legitimate interests of the State, instead of remaining a compliance checklist aimed mainly at private industry.

[60] *Puttaswamy*, (2017) 10 SCC 1, ¶¶ 325, 638.