



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.

WHO WATCHES THE WATCHER? WHY THE GOVERNMENT IS BOTH REGULATOR AND BIGGEST DATA COLLECTOR UNDER THE DPDP ACT

~ Archi Ojha

I. INTRODUCTION

Data protection law is usually imagined as a contest between an individual and a company. The Digital Personal Data Protection Act, 2023 (DPDP Act)¹ does not fit that picture well, because the largest holder of personal data in India is the government. Aadhaar, welfare beneficiary lists, tax filings, land records and city camera networks all sit with the State. The same State drafted the Act, will appoint the body that enforces it, and kept for itself some of the widest exemptions in the statute.

Scholars noticed this early. Graham Greenleaf described the Act as business and government friendly and consumer hostile, and thought its treatment of State bodies reads like a blueprint for surveillance that is not clearly unlawful.² Vrinda Bhandari and Renuka Sane had made the deeper point about the 2018 Bill: where the State is also the regulator, it holds considerable power over the very entities that are supposed to restrain it.³ This article picks up that thread. It asks how the State's different roles under the Act reinforce one another, states the Government's answers fairly before assessing them, and examines the constitutional challenges now pending in the Supreme Court. My view is that some of the Government's answers are respectable, but most rest on safeguards the Act does not contain.

¹ Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India) [hereinafter DPDP Act].

² Graham Greenleaf, *India's 2023 Data Privacy Act: Business/Government Friendly, Consumer Hostile*, 185 Privacy L. & Bus. Int'l Rep. 1, 3–12 (2023).

³ Vrinda Bhandari & Renuka Sane, *Protecting Citizens from the State Post Puttaswamy: Analysing the Privacy Implications of the Justice Srikrishna Committee Report and the Data Protection Bill, 2018*, 14(2) Socio-Legal Rev. 143 (2018).

A note on timing. The provisions creating the Board and the amendment to the Right to Information Act came into force on 13 November 2025, while most substantive obligations, including those binding the State, apply from 13 May 2027.⁴

II. THE STATE AS DATA FIDUCIARY: PROCESSING WITHOUT CONSENT

Consent is the default ground for processing, but section 7 lists “legitimate uses” that need none. Some are ordinary, like medical emergencies. Others belong to the State alone. Section 7(b) lets the State and its instrumentalities process data to give a subsidy, benefit, service, licence, certificate or permit, where the person consented earlier or the data already sits in a State database notified by the Central Government.⁵ Section 7(c) covers any function under any law, or the interest of sovereignty, integrity or security, and section 7(d) covers disclosures the State can demand under other laws.⁶

The catch lies in sections 11 and 12. The rights to a summary of one’s data and to its correction are tied to data processed on consent, including the voluntary-provision ground in section 7(a). Where the State relies on the other limbs of section 7, a person has, on a plain reading, no clear statutory right to see what is held or to fix it.⁷ That is odd, because the people who most need to inspect a government database are the ones whose data went into it without being asked.

The Rules partly answer this. Rule 5 requires processing under section 7(b) to follow the Second Schedule, which broadly tracks lawfulness, purpose limitation, minimisation, accuracy, security and accountability.⁸ These are welcome standards, but they are framed as duties the State owes, not rights an individual can enforce, and Rule 5 binds only from May 2027.

III. EXEMPTIONS: WHERE THE ACT SWITCHES OFF

Section 17(1) removes most core duties, and the rights of the Data Principal, for processing connected with the prevention, detection, investigation or prosecution of offences, among other purposes.⁹ Most data protection laws carry a similar carve-out. The harder provision is section 17(2)(a). The Central Government may notify any instrumentality of the State, after which the Act does not apply to its processing at all, so long as the processing is in the interests of

⁴ Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), Gazette of India, pt. II, § 3(i), r. 1 (Nov. 13, 2025) (India) [hereinafter DPDP Rules]; *see also* Ministry of Electronics & Info. Tech., Notification G.S.R. 843(E) (Nov. 13, 2025) (India) (commencing the DPDP Act in phases).

⁵ DPDP Act, *supra* note 1, § 7(b).

⁶ *Id.* § 7(c)–(d).

⁷ *Id.* §§ 11(1), 12(1).

⁸ DPDP Rules, *supra* note 4, r. 5 & sched. II.

⁹ DPDP Act, *supra* note 1, § 17(1).

sovereignty and integrity, security of the State, friendly relations with foreign States, public order, or preventing incitement to related offences.¹⁰

The Act does not define “instrumentality” for this purpose, and nothing requires the notification to be reasoned, time-bound, laid before Parliament or reviewed by anyone outside the executive. A notified body is not bound even by the duty to protect the data it holds from breach. Section 17(4) gives every State body, notified or not, a quieter privilege: it need not erase data once the purpose is served, and is spared the erasure right and, where no decision about the individual is involved, the correction right.¹¹ A private company must delete what it no longer needs. The State may keep it. Section 17(5) adds a power, available for five years after commencement, to exempt any fiduciary or class from any provision by notification.¹²

All of this sits beside an interception framework the DPDP Act leaves alone: section 69 of the Information Technology Act, 2000 and the 2009 interception rules.¹³ Chinmayi Arun has argued that the safeguards in that framework are thin because orders are approved and reviewed within the executive itself.¹⁴ A data protection law that steps aside for the same bodies inherits the same weakness.

IV. WHO APPOINTS THE BOARD? THE INDEPENDENCE PROBLEM

A regulator can check the State only if it is independent of the State. The Board is established under section 18 and its Chairperson and Members are appointed by the Central Government.¹⁵ Under Rule 17, names come from search-cum-selection committees. The Chairperson’s committee is chaired by the Cabinet Secretary and includes the Secretaries for Legal Affairs and for Electronics and Information Technology, plus two experts; the Members’ committee is chaired by the Electronics and IT Secretary.¹⁶ The officials are serving members of the executive, and their ministries are themselves large data fiduciaries. The Government then appoints after “considering the suitability” of those recommended, so it is not bound by the

¹⁰ *Id.* § 17(2)(a).

¹¹ *Id.* § 17(4).

¹² *Id.* § 17(5).

¹³ Information Technology Act, 2000, No. 21, Acts of Parliament, 2000, § 69 (India); Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, G.S.R. 780(E) (Oct. 27, 2009) (India).

¹⁴ Chinmayi Arun, *Paper-Thin Safeguards and Mass Surveillance in India*, 26 Nat’l L. Sch. India Rev. 105 (2014).

¹⁵ DPDP Act, *supra* note 1, §§ 18–19.

¹⁶ DPDP Rules, *supra* note 4, r. 17(1)–(2).

list.¹⁷ Terms are two years with eligibility for reappointment, which PRS Legislative Research flagged as a threat to independence, and pay and conditions are set by executive rule.¹⁸

The Supreme Court has been more demanding elsewhere. In *Anoop Baranwal v. Union of India*, it found that appointments to the Election Commission made only on the executive's advice were not adequately insulated, and directed a broader selection committee until Parliament legislated.¹⁹ The Data Protection Board will decide disputes in which the Government is a likely respondent.

Other features deepen the concern. Section 36 lets the Central Government require the Board itself, as well as any fiduciary or intermediary, to furnish information, and Rule 23 with the Seventh Schedule allows the Government to direct that a request not be disclosed where disclosure could harm sovereignty or security.²⁰ The regulator is answerable to the entity it oversees. Section 35 shields the Government, the Board and its members from suits for acts done in good faith, and section 39 bars civil courts from matters within the Board's jurisdiction.²¹ Commentary from mid-2026 also observed that, although the Board exists in law, its Chairperson and Members had yet to be appointed.²² Even so, the State can in principle be penalised, since "person" includes the State and penalties reach ₹250 crore for failing to secure data.²³

V. THE RTI AMENDMENT: REMOVING THE CITIZEN'S TORCH

Transparency is the other classic check on the watcher. Section 44(3) of the DPDP Act substituted section 8(1)(j) of the Right to Information Act, 2005. Before, personal information was exempt only if it had no relationship to any public activity or interest, or would invade privacy without justification, and even then it was to be disclosed if the larger public interest required.²⁴ Now the clause simply exempts "information which relates to personal information".²⁵

¹⁷ *Id.* r. 17(3).

¹⁸ PRS Legis. Rsch., *The Digital Personal Data Protection Bill, 2023*, <https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023> (last visited Sept. 28, 2026); DPDP Rules, *supra* note 4, r. 18 & sched. V.

¹⁹ *Anoop Baranwal v. Union of India*, (2023) 6 S.C.C. 161 (India).

²⁰ DPDP Act, *supra* note 1, § 36; DPDP Rules, *supra* note 4, r. 23 & sched. VII.

²¹ DPDP Act, *supra* note 1, §§ 35, 39.

²² Raghvendra Kumar Chaudhary, *India's Data Protection Board: Established in Law, Absent in Fact*, LiveLaw, <https://www.livelaw.in/articles/india-data-protection-board-established-law-543751> (last visited Sept. 28, 2026).

²³ DPDP Act, *supra* note 1, §§ 2(s), 33 & sched.

²⁴ Right to Information Act, 2005, No. 22, Acts of Parliament, 2005, § 8(1)(j) (India) (as originally enacted).

²⁵ DPDP Act, *supra* note 1, § 44(3).

Attendance registers, beneficiary lists, muster rolls and the credentials of public servants all relate to individuals, and social audits of ration or pension leakage depend on exactly these records. In *Central Public Information Officer, Supreme Court of India v. Subhash Chandra Agarwal*, the Court treated the rights to information and privacy as parts of one scheme to be balanced case by case.²⁶ A flat exemption removes that balance, and it does so for information in every form, although the DPDP Act itself governs only digital data.

VI. READING THE PROVISIONS TOGETHER

Taken one at a time, each provision has an explanation. Taken together, they produce three conflicts of interest. The first is a conflict of enforcement: the body most likely to breach the Act appoints, and can question, the body that would penalise it. The second is a conflict of knowledge. Every remedy under the Act begins with a complaint, and a complaint needs awareness. Yet sections 11 and 12 deny access rights against most State processing, Rule 23(2) allows secret information requests, and section 17(2)(a) can remove the Act altogether. The remedial system works best where the State is least involved. The third is a conflict of scrutiny. The other routes by which outsiders check the State, namely RTI and civil suits, have been narrowed by sections 44(3) and 39. What remains is the Board and the writ courts, and the Board's independence is the very point in doubt.

For this reason I think the common framing, that the Act merely “exempts” the State, understates the problem. An exemption is a gap. What the Act builds is closer to a closed circuit, in which the State collects the data, controls who may ask for it, appoints the enforcer and, through the exemptions, decides how far it is accountable. The capacity concern raised by Bhandari and Sane applies as well.²⁷ A young Board with two-year members, no power to make regulations and a largely digital docket must face ministries with far more institutional weight.

VII. THE GOVERNMENT'S CASE

The Government has real answers, and an article on this topic should state them properly. The first concerns national security. Almost every data protection regime exempts security and policing in some form, and *Puttaswamy* itself accepts security as a legitimate aim. Anirudh Burman notes that exemptions for State functions have appeared in every version of the law since the 2018 draft.²⁸ Notice, consent and access make little sense for an intelligence agency,

²⁶ Cent. Pub. Info. Officer, Sup. Ct. of India v. Subhash Chandra Agarwal, (2020) 5 S.C.C. 481 (India).

²⁷ See Bhandari & Sane, *supra* note 3.

²⁸ Anirudh Burman, *Understanding India's New Data Protection Law*, Carnegie India (Oct. 3, 2023), <https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law>.

and telling a suspect about a breach would defeat the purpose. The Solicitor General has also told the Court that the law remains subject to judicial review.²⁹

That argument justifies exemption from notice, consent and access. It does not obviously justify exemption from everything, including basic security safeguards, and judicial review is of little use to someone who never learns that her data was taken, which is exactly what Rule 23(2) allows.

On the Board, the Government points out that section 28(1) declares it an independent body, that each selection committee includes outside experts, and that appeals go to a specialist tribunal.³⁰ Burman adds that the Board is an adjudicator rather than a rule-making regulator, with no power to frame regulations or call for information, so the room for executive influence is smaller than critics assume.³¹ Executive-led selection committees are also common in Indian tribunals. But a statutory declaration of independence is not independence, officials outnumber experts on the committees, and the narrow mandate cuts the other way: because section 39 makes the Board the only forum, the quality of its adjudication is the whole of the citizen's remedy.

On consent-free processing, the Government can say that asking a person to consent before receiving a ration or a pension is hollow, since refusal means losing the benefit. Statutory standards are more honest than consent theatre. That is fair, and I accept it. But it is an argument for stronger safeguards after collection, such as access, correction and purpose limitation, and those are the very protections sections 11, 12 and 17(4) withhold.

On the RTI amendment, the Minister has said it will not restrict disclosure and aims to strengthen privacy and stop misuse of the law,³² and the IT Secretary has said section 8(2) of the RTI Act still lets a public authority release information where the public interest outweighs the harm.³³ The reply is that section 8(2) is permissive ("may allow") and is framed around harm to protected interests, whereas the deleted proviso obliged the authority to disclose where the larger public interest justified it. A discretion is not the same as a duty.

²⁹ Namrata Banerjee, *Challenge to DPDP Act | Day 2: Law May Impede Investigative Journalism, Petitioners Argue*, Sup. Ct. Observer (Aug. 7, 2026), <https://www.scobserver.in/reports/challenge-to-dpdp-act-day-2-law-may-impede-investigative-journalism-petitioners-argue/>.

³⁰ DPDP Act, *supra* note 1, §§ 28(1), 29.

³¹ Burman, *supra* note 28.

³² Provision of DPDP Act Weakens RTI: Opposition Members of Parliament, Bus. Standard (Apr. 10, 2025), https://www.business-standard.com/amp/politics/india-bloc-mps-urge-centre-to-repeal-a-amendment-in-dpdp-act-weakening-rti-125041001100_1.html.

³³ DPDP Act Leaves RTI Intact, VARINDIA (Aug. 2025), <https://www.varindia.com/news/dpdp-act-leaves-rti-intact>.

VIII. THE PENDING CONSTITUTIONAL CHALLENGES

Three writ petitions were filed in February 2026: *Venkatesh Nayak v. Union of India* (W.P.(C) 177/2026), *Reporters Collective Trust v. Union of India* (W.P.(C) 211/2026) and one by the National Campaign for People's Right to Information (W.P.(C) 212/2026), later joined by a petition from journalist Geeta Seshu and the Software Freedom Law Centre.³⁴ On 16 February 2026 a bench headed by Chief Justice Surya Kant issued notice, declined an interim stay and referred the matter to a larger bench.³⁵

The challenge is wider than the RTI amendment. Nayak attacks sections 17(1)(c), 17(2), 33(1), 36 and 44(3), and Rules 17 and 23(2). He argues that the exemptions create a surveillance regime with no safeguards, that section 36 gives the Union power to demand information without statutory guidance, that Rule 23(2) allows secret requests, and that executive dominance of the selection committee offends the separation of powers.³⁶ The Seshu petition adds sections 7, 17(2)(a), 19(3) and 24.³⁷ Almost every structural point discussed above is therefore before the Court.

At the hearing on 7 August 2026, however, the reported exchanges centred on section 44(3). Justice Bagchi observed that the RTI Act operates in a much larger domain than the DPDP Act, and said the Court would examine whether distinguishing digital personal data from other information rests on an intelligible differentia and whether a blanket prohibition or a proportionate approach is required. The Chief Justice remarked that the balance has to be worked out with privacy. The Solicitor General promised a reply and, according to one report, said no case is as bad as the petitioners portray.³⁸

Two observations follow. First, if the Court reads down section 44(3), perhaps by restoring a public interest test, the sections on exemption and the Board could still survive untouched, because they have drawn less attention. The Government may also argue that section 17(2)(a) is

³⁴ *Venkatesh Nayak v. Union of India*, W.P.(C) No. 177/2026 (India); *Reporters Collective Trust v. Union of India*, W.P.(C) No. 211/2026 (India); *Nat'l Campaign for People's Right to Info. v. Union of India*, W.P.(C) No. 212/2026 (India); *Constitutionality of the Digital Personal Data Protection Act, 2023*, Sup. Ct. Observer, <https://www.scobserver.in/cases/constitutionality-of-the-digital-personal-data-protection-act-2023/> (last visited Sept. 28, 2026).

³⁵ *Challenge to DPDP Act | Bench Refuses to Stay Amendment, Issues Notice*, Sup. Ct. Observer (Feb. 16, 2026), <https://www.scobserver.in/reports/challenge-to-dpdp-amendment-of-rti-bench-refuses-to-stay-amendment-issues-notice/>.

³⁶ *Constitutionality of the Digital Personal Data Protection Act, 2023*, *supra* note 34.

³⁷ *'Interesting Question Is What's Public Data & Personal Data?': Supreme Court on Challenge to DPDP Act*, LiveLaw, <https://www.livelaw.in/top-stories/whats-public-data-personal-data-supreme-court-on-challenge-to-dpdp-act-526194> (last visited Sept. 28, 2026).

³⁸ Banerjee, *supra* note 29; *SC Seeks Centre's Response on Pleas Challenging Data Protection Law*, ETV Bharat (Aug. 7, 2026), <https://www.etvbharat.com/en/bharat/supreme-court-seeks-centre-response-on-pleas-challenging-data-protection-law-enn26080702945>.

premature, since no instrumentality has yet been notified and the provision is not in force. Second, the pre-enforcement setting is a weakness for petitioners but also an opportunity: the Court can lay down guidance on necessity and review before a single notification is issued. I have not found a reported judgment as of the date of writing, and the position should be checked again before publication.

IX. THE CONSTITUTIONAL YARDSTICK AND A COMPARISON

Puttaswamy held privacy to be part of Article 21 and the freedoms in Part III, and said that State interference must satisfy legality, a legitimate aim and proportionality.³⁹ The Aadhaar decision applied proportionality to a State data programme, asking for a rational connection, the least intrusive suitable measure and safeguards against abuse.⁴⁰ *PUCL* had earlier insisted on procedure for telephone tapping, and *Anuradha Bhasin* required restrictions to be reasoned and reviewable.⁴¹

Section 17(2)(a) fits poorly with these cases. A notification can switch off the whole Act with no finding of necessity, no time limit and no independent review. The 2018 draft of the Srikrishna Committee tied the security exemption to a law made by Parliament that was necessary and proportionate, and paired it with an independent authority.⁴² The final Act kept the exemption and dropped the safeguards.

European law offers a contrast. The Charter of Fundamental Rights makes compliance with data protection rules subject to control by an independent authority, and *Orla Lynskey* reads that requirement as part of the right itself rather than an enforcement detail.⁴³ The Court of Justice has held that even the risk of political influence over a data authority breaches this independence.⁴⁴ Policing is regulated by a separate directive with its own principles and oversight.⁴⁵

X. THE WAY FORWARD

Reform need not weaken legitimate security functions. Notifications under section 17(2)(a) should record reasons, run for a fixed renewable period, and be reported annually to a

³⁹ Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).

⁴⁰ Justice K.S. Puttaswamy (Retd.) v. Union of India, (2019) 1 S.C.C. 1 (India).

⁴¹ *PUCL v. Union of India*, (1997) 1 S.C.C. 301 (India); *Anuradha Bhasin v. Union of India*, (2020) 3 S.C.C. 637 (India).

⁴² Comm. of Experts under the Chairmanship of Justice B.N. Srikrishna, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (2018); Personal Data Protection Bill, 2018, cl. 42 (India).

⁴³ Charter of Fundamental Rights of the European Union art. 8(3), 2012 O.J. (C 326) 391; see generally *Orla Lynskey, The Foundations of EU Data Protection Law* (2015).

⁴⁴ Case C-518/07, *Comm'n v. Germany*, ECLI:EU:C:2010:125 (Mar. 9, 2010).

⁴⁵ Directive 2016/680, 2016 O.J. (L 119) 89 (EU).

parliamentary committee. Exempted bodies should still owe basic duties such as security safeguards and breach reporting under section 8(5) and (6). Board appointments should involve the Leader of the Opposition or a judicial member, with a longer non-renewable term, following the logic of *Anoop Baranwal*.⁴⁶ Rule 23(2) directions should lapse after a stated period and be reviewable independently. Finally, the Court should read down section 44(3) so that a public interest test survives, and the Government should publish every notification under sections 7(b) and 17(2)(a). The five-year window in section 17(5) is a natural moment to revisit all of this.

XI. CONCLUSION

The DPDP Act is a serious attempt at a modern privacy law, and its demands on private companies are real. But a data protection regime is judged by how it treats the most powerful data holder in the country. The Act lets the State decide when it is bound, choose the body that enforces the rules against it, ask that body for information, and limit what the public can learn through RTI. Each choice has a defensible explanation, as Part VII shows. Together they leave the watcher largely watching itself. The pending cases give the Supreme Court a chance to supply through *Puttaswamy* the safeguards the statute omitted, and it should not confine itself to section 44(3).

⁴⁶ Anoop Baranwal, *supra* note 19.