Page 834 - 846 **DOI:** *https://doi.org/10.63108/IJLMH.13264*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 6

2026

© 2026 *International Journal of Law Management & Humanities*

Follow this and additional works at: https://www.ijlmh.com/
Under the aegis of VidhiAagaz (https://www.vidhiaagaz.com/)

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of **any suggestions or complaints**, kindly contact **support@vidhiaagaz.com**.

To submit your Manuscript for Publication in the **International Journal of Law Management & Humanities**, kindly email your Manuscript to **submission@ijlmh.com.**

Proportionality and the Surveillance State: Testing the State Exemptions in the Digital Personal Data Protection Act, 2023 Against the Puttaswamy Standard

DEVYANI DIXIT* AND MANISH KUMAR SAHU**

ABSTRACT

The Digital Personal Data Protection Act, 2023 is India's first comprehensive statute on the processing of digital personal data, enacted in response to the Supreme Court's recognition of privacy as a fundamental right in 2017. This paper examines whether the provisions of the Act that favour the State, namely its exemption for notified instrumentalities, its non-consensual "legitimate use" ground, its power to call for information, and the accompanying amendment to the Right to Information Act, 2005, satisfy the proportionality standard that the Court laid down for restrictions on privacy. The study is doctrinal and comparative. It reconstructs the constitutional standard from the Court's privacy and Aadhaar decisions, applies its components of legality, legitimate aim, necessity and procedural safeguards to the statutory text, and draws on European and American authority to test its conclusions. The paper argues that the aims pursued are constitutionally acceptable, but that the Act fails the tests of necessity and procedural safeguards. It disapplies the entire statute by executive notification, retains no baseline security or accountability duties for exempted bodies, provides no independent prior authorisation or post-facto notice, and entrusts oversight to a Board whose members are appointed by the executive. The paper concludes that these defects are architectural rather than incidental, and proposes statutory reforms, including tailored exemptions, an express necessity standard, independent authorisation, transparency reporting and a restored public-interest override, together with an interpretive route open to the courts.

Keywords: *Informational Privacy, Proportionality, Digital Personal Data Protection Act, State Exemptions, Article 21, Surveillance*

I. INTRODUCTION

On 24 August 2017, a nine-judge Bench of the Supreme Court of India held that the right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21

* Author is an Assistant Professor at Shri Rawatpura Sarkar University, Raipur, Chhattisgarh, India. ORCID: https://orcid.org/0009-0003-4447-3862

** Author is an Assistant Professor at Shri Rawatpura Sarkar University, Raipur, Chhattisgarh, India.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

of the Constitution and as part of the freedoms guaranteed by Part III.[1] The Court did not stop at declaration. It recognised informational privacy as a distinct facet of the right, accepted that threats to it arise from State and non-State actors alike, and invited the Union to frame a data protection regime.[2] After a committee report, a Bill withdrawn in 2022 and several years of debate, Parliament enacted the Digital Personal Data Protection Act, 2023 (the DPDP Act).[3] The Digital Personal Data Protection Rules, 2025 were notified on 13 November 2025, and the substantive obligations are being brought into force in phases, with most provisions to commence in May 2027.[4]

The Act is oddly lopsided. For private data fiduciaries it builds a detailed regime of notice, consent, purpose limitation, security safeguards, breach notification and enforceable rights. For the State, it builds something close to the opposite: broad permissions and wide exemptions. The State may process personal data without consent for any function under any law; it may be exempted from the whole Act by a notification; it may require any fiduciary to hand over information; and the Act amends the Right to Information Act, 2005 in a way that narrows public access to information about individuals, including officials. This sits uneasily with *Puttaswamy I*, which was, at bottom, a judgment about limits on State power. This paper asks whether the State-facing provisions can be squared with the standard that the judgment set for any law that restricts privacy.

The answer offered here is that, for the most part, they cannot. The aims behind the exemptions, such as national security and public order, are legitimate, and nothing in this paper suggests otherwise. The trouble lies in how the exemptions are built. They disapply the Act wholesale instead of restricting it with care; they depend on executive notification and not on any standard of necessity; and they come with no independent authorisation, no notice to the individual and no real oversight. What makes this harder to defend is that the Act itself shows a narrower design was available, which undercuts any claim that the broad one is the least restrictive means.

The approach is doctrinal, with some comparative support. Part II sets out the constitutional standard and Part III maps the State-facing provisions of the Act. Part IV tests those provisions

---

[1] *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1 (India) [hereinafter *Puttaswamy I*]. The Court overruled *M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300 (India), and *Kharak Singh v. State of U.P.*, AIR 1963 SC 1295 (India), to the extent that those decisions denied the existence of the right.

[2] *See generally Puttaswamy I*, *supra* note 1 (opinions of Chandrachud and Kaul JJ.).

[3] The Digital Personal Data Protection Act, No. 22 of 2023, INDIA CODE (2023) [hereinafter DPDP Act]. For the antecedent committee report, see COMM. OF EXPERTS UNDER THE CHAIRMANSHIP OF JUSTICE B.N. SRIKRISHNA, A FREE AND FAIR DIGITAL ECONOMY: PROTECTING PRIVACY, EMPOWERING INDIANS (2018) [hereinafter SRIKRISHNA REPORT].

[4] The Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), GAZETTE OF INDIA, pt. II sec. 3(i) (Nov. 13, 2025), r. 1(2)–(4) [hereinafter DPDP Rules].

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

against the standard and weighs the strongest defence open to the Union. Part V looks to European and American experience, Part VI proposes reforms, and Part VII concludes. Two caveats are worth stating early. The paper reads statutory text rather than enforcement practice, since most operative provisions are not yet in force. And challenges to aspects of the Act are pending before the Supreme Court,[5] so nothing here is meant to anticipate what the Court will decide.

II. THE CONSTITUTIONAL STANDARD: PRIVACY AND PROPORTIONALITY

A. From denial to recognition

Indian constitutional law reached the recognition of privacy by a long and uneven route. In *M.P. Sharma*, a bench of eight judges declined to read into the Constitution a protection analogous to the American Fourth Amendment against search and seizure.[6] In *Kharak Singh*, the Court held that a regime of domiciliary night visits violated personal liberty under Article 21, although the majority did not recognise privacy as a fundamental right.[7] The doctrinal opening came with a change in how Article 21 was read. After *Maneka Gandhi v. Union of India*, a law depriving a person of life or personal liberty must prescribe a procedure that is fair, just and reasonable, and Article 21 must be read together with Articles 14 and 19.[8] Building on that foundation, *Gobind v. State of M.P.* accepted that privacy could be a facet of personal liberty, subject to compelling State interest.[9]

The same period produced the first judicial template for regulating State surveillance. In *People's Union for Civil Liberties v. Union of India*, the Court, confronted with unregulated telephone tapping, laid down procedural guidelines requiring, among other things, that interception orders be issued only at a senior level of the executive and be reviewed by a committee.[10] The guidelines matter for two reasons. They show that the Court has long treated procedural safeguards as part of what makes an intrusion constitutional. They also show the limits of the model, in which both authorisation and review stayed within the executive.

---

[5] *See Venkatesh Nayak v. Union of India*, W.P. (C) No. 177 of 2026 (India) (notice issued Feb. 16, 2026); *Nat'l Campaign for People's Right to Info. v. Union of India*, W.P. (C) No. 212 of 2026 (India); *Reporters' Collective Tr. v. Union of India*, W.P. (C) No. 211 of 2026 (India); *'Some Creases To Be Ironed Out,' Supreme Court Refers Pleas Challenging DPDP Act Amendment to RTI Act to Larger Bench*, LIVELAW (Feb. 16, 2026), https://www.livelaw.in/amp/top-stories/supreme-court-refers-pleas-challenging-dpdp-act-amendment-to-rti-act-to-larger-bench-523266.

[6] *M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300 (India) (declining to import a fundamental right to privacy into the guarantee against self-incrimination).

[7] *Kharak Singh v. State of U.P.*, AIR 1963 SC 1295 (India).

[8] *Maneka Gandhi v. Union of India*, (1978) 1 SCC 248, ¶ 48 (India).

[9] *Gobind v. State of M.P.*, (1975) 2 SCC 148 (India).

[10] *PUCL v. Union of India*, (1997) 1 SCC 301, ¶ 35 (India).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

Puttaswamy I closed the period of doubt by overruling the contrary dicta of *M.P. Sharma* and *Kharak Singh* and by locating privacy in dignity, autonomy and liberty.

B. The elements of proportionality

Puttaswamy I also stated the test that a law must pass if it encroaches on privacy. The opinion of Chandrachud J. required that the restriction satisfy legality, in the sense that there must be a law; a legitimate State aim; and proportionality, in the sense of a rational nexus between the means adopted and the object sought.[11] That formulation was elaborated in the Aadhaar decision, where the majority applied a structured proportionality analysis drawn from the Court's earlier decision in *Modern Dental College* and from comparative scholarship. The analysis asks whether the measure pursues a legitimate goal; whether it is a suitable means of furthering that goal; whether there is no less restrictive alternative that would achieve the goal equally well (necessity); and whether the measure has a disproportionate impact on the right-holder (balancing).[12] The Court has since applied the same structure to restrictions on expression, insisting that restrictive orders be reasoned, published and open to review.[13]

For the purposes of this paper, the standard reduces to four questions. Does the restriction rest on a clear, non-arbitrary law (legality)? Is its object legitimate (legitimate aim)? Is it suitable, the least restrictive effective means, and a fair balance (necessity and balance)? And does the law guard against abuse (procedural safeguards)? The fourth question is not really separate from the others. The Court treats safeguards as part of both legality and proportionality, because a power that cannot be reviewed cannot be shown to be necessary.

C. Informational privacy and the duty to legislate

Informational privacy is the aspect of privacy most exposed by digitisation. Its modern articulation begins with the claim of Warren and Brandeis to a right "to be let alone," and is developed by Westin as the claim of individuals to determine for themselves when, how and to what extent information about them is communicated to others.[14] The concern is not only with disclosure but also with aggregation, secondary use and the exercise of power over a person who does not know what is held about her.

---

[11] *Puttaswamy I*, (2017) 10 SCC at ¶ 310 (Chandrachud J.).

[12] *K.S. Puttaswamy v. Union of India*, (2019) 1 SCC 1, ¶¶ 157–158 (Sikri J.) (India) [hereinafter *Puttaswamy II*]; *Modern Dental Coll. & Rsch. Ctr. v. State of M.P.*, (2016) 7 SCC 353, ¶ 60 (India); AHARON BARAK, PROPORTIONALITY: CONSTITUTIONAL RIGHTS AND THEIR LIMITATIONS (2012).

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

[14] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890); ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967). For a modern typology of privacy harms, see Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2006).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

Two features of the Court's approach matter here. First, *Puttaswamy I* treated the State as a principal, though not the only, threat to informational privacy, and its call for legislation was a call for rules that bind the State as well as private actors. Second, the Aadhaar decision demonstrated what that means in practice. The Court struck down a provision of the Aadhaar Act that permitted disclosure of identity information in the interest of national security on the direction of an officer of the executive, reasoning in substance that such a power lacked adequate safeguards.[15] The invocation of national security was therefore treated as the beginning of the constitutional inquiry rather than its end. That holding is the closest judicial analogue to the questions raised by the DPDP Act.

III. The State in the DPDP Act

A. Legitimate uses without consent

The Act's architecture is consent-based. A data fiduciary may process personal data only for a lawful purpose, after notice, and with the consent of the data principal, subject to specified exceptions described as "legitimate uses."[16] Several of those exceptions benefit the State. A State instrumentality may process data without consent in order to provide a subsidy, benefit, service, certificate, licence or permit where the individual has previously consented to receive another such benefit from the State or where the data is already held in a database or record of the State that the Central Government has notified.[17] More broadly, the State and its instrumentalities may process data without consent for the performance of any function under any law in force, or in the interest of the sovereignty and integrity of India or the security of the State.[18]

Of these, section 7(c) matters most. The phrase "any function under any law" is not limited by gravity, urgency or the sensitivity of the data. It follows that consent, the organising principle of the Act, is displaced whenever the State can point to a statutory function, however routine. The provision leaves the question of proportionality to the law that confers the function; but the DPDP Act, which is the general data protection law, supplies no independent standard against which the use of data under that other law is to be tested.

[15] *See Puttaswamy II*, *supra* note 12 (striking down § 33(2) of The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, No. 18 of 2016, INDIA CODE (2016)).
[16] DPDP Act, §§ 4–7.
[17] DPDP Act, § 7(b).
[18] *Id.* § 7(c).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

B. The exemptions

Section 17 is the heart of the State-facing regime. Sub-section (1) lists cases in which Chapter II (other than the general duty to comply with the Act and the duty to maintain reasonable security safeguards), Chapter III on the rights of data principals, and section 16 on cross-border transfers do not apply. These include processing for the prevention, detection, investigation or prosecution of an offence.[19] It is significant that this sub-section preserves the fiduciary's overarching responsibility to comply with the Act and its duty to protect data with reasonable security safeguards.[20] It shows that the legislature understood how to draft an exemption that relaxes consent and rights while leaving intact baseline duties that guard against misuse and breach.

Sub-section (2)(a) is drafted differently. It provides that "the provisions of this Act" shall not apply to the processing of personal data by such instrumentality of the State as the Central Government may notify in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, the maintenance of public order, or preventing incitement to any cognisable offence relating to any of these.[21] The exemption is complete. A notified body is relieved not only of notice, consent and the data principal's rights but also of the duty to keep data secure, the duty to limit its use to a stated purpose, the duty to report breaches, and the supervisory jurisdiction of the Board. Further, sub-section (4) disapplies, for all processing by the State or any of its instrumentalities, whether or not notified, the duty to erase data once its purpose is served and the data principal's right to erasure; and, where the processing is for a purpose that does not include making a decision that affects the data principal, it also disapplies the duty to correct, complete and update her data on request.[22] Sub-section (5) adds a power, exercisable within five years of commencement, to declare by notification that any provision of the Act shall not apply to specified fiduciaries or classes of fiduciaries for a specified period.[23]

C. Calling for information and the amendment to the RTI Act

Section 36 authorises the Central Government, "for the purposes of this Act," to require the Board and any data fiduciary or intermediary to furnish such information as it may call for.[24] The provision is not confined to the interests listed in section 17(2)(a), contains no threshold of

[19] DPDP Act, § 17(1).
[20] DPDP Act, §§ 8(1), 8(5), 17(1).
[21] DPDP Act, § 17(2)(a).
[22] DPDP Act, § 17(4) (disapplying §§ 8(7) and 12(3) for all processing by the State or its instrumentalities, and § 12(2) where the processing is for a purpose that does not include making a decision that affects the Data Principal).
[23] DPDP Act, § 17(5).
[24] DPDP Act, § 36.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

suspicion or necessity, and does not require that the individual be told. Although the 2025 Rules supply procedural detail for such requests, they do not, on the reading adopted in this paper, introduce prior authorisation by an authority independent of the executive.[25]

Section 44(3) amends section 8(1)(j) of the Right to Information Act, 2005. As originally enacted, that clause exempted personal information whose disclosure had no relationship to any public activity or interest, or would cause an unwarranted invasion of privacy, but allowed disclosure where the competent authority was satisfied that the larger public interest justified it.[26] The amendment reduces the exemption to information that "relates to personal information," removing the balancing language.[27] The change is relevant to proportionality because it alters, in the State's favour, the balance between the constitutional values of privacy and transparency, a balance that the earlier text had struck through a public-interest test. It also bears on accountability: the information most likely to be withheld on this ground is information about individuals who exercise public functions.

D. The Data Protection Board

The Act establishes the Data Protection Board of India to determine non-compliance, impose penalties and direct remedial measures.[28] The Chairperson and Members are appointed by the Central Government for renewable two-year terms, and the Board's orders are appealable to the Telecom Disputes Settlement and Appellate Tribunal.[29] The Board thus has no jurisdiction over a notified instrumentality under section 17(2)(a), and elsewhere it is an executive-appointed body supervising a regime in which the executive is itself the largest processor of personal data. That design bears directly on the question of safeguards taken up in Part IV.

IV. TESTING THE EXEMPTIONS AGAINST PROPORTIONALITY

A. Legality

Legality requires a law, and the State-facing provisions are found in an Act of Parliament. In that formal sense the requirement is met. But the Court has treated legality as more than formal enactment. A law that restricts a fundamental right must be sufficiently clear for the individual

[25] *See* DPDP Rules, *supra* note 4, r. 23(1) & sch. 7 (information to be called for through the authorised person specified in the Seventh Schedule, being an officer designated by the Central Government or the head of the notified instrumentality, or a person authorised under the applicable law); *id.* r. 23(2) (power, where disclosure is likely to prejudicially affect the sovereignty and integrity of India or security of the State, to require the Data Fiduciary or intermediary not to disclose the furnishing of information to the affected Data Principal except with the written permission of the authorised person).

[26] The Right to Information Act, No. 22 of 2005, INDIA CODE (2005), § 8(1)(j).

[27] DPDP Act, § 44(3).

[28] DPDP Act, §§ 18, 27.

[29] DPDP Act, §§ 19, 20, 29.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

to foresee its application and must not confer unguided discretion, since a law that is manifestly arbitrary violates Article 14.[30]

Section 17(2)(a) is vulnerable on this footing in two respects. First, it leaves to the executive the selection of the bodies that will be exempted and supplies only a list of heads of interest. The list is borrowed from the grounds on which the freedom of speech may be restricted, but the Court has long distinguished between public order and the security of the State, treating them as concentric circles of differing gravity.[31] The provision does not require the executive to match the body to the interest, or to identify the processing for which exemption is needed. Second, the notion of an "instrumentality of the State" is not defined for this purpose, so that the class of bodies that may be exempted is open-ended. A statute that allows the executive to remove an entire class of State bodies from a fundamental-rights statute by notification is, in practical terms, a delegation of the legislative decision on the scope of the right. These features do not make the provision void for vagueness. They do mean that legality, understood as predictability and constraint on discretion, is only weakly satisfied.

B. Legitimate aim

The aims enumerated in section 17(2)(a) are national security, the integrity of the State, friendly relations with foreign States, public order and the prevention of incitement to cognisable offences. These are recognised grounds for restricting fundamental freedoms and are, in principle, legitimate aims. The same may be said of the aims that section 7(c) names expressly, namely sovereignty, integrity and security.

The position is less clear for the general limb of section 7(c) and for section 17(4). Performing "any function under any law" is not an aim at all but a description of State activity, and administrative convenience, without more, is not a justification for intrusion into a protected right. The relevant aim must therefore be sought in the law that confers the function, which is exactly where the DPDP Act, as the general data protection statute, withholds any scrutiny. The aim stage is thus passed for the security-related provisions and left open for the rest.

C. Suitability, necessity and balance

The suitability requirement asks whether the means adopted advance the aim. Exempting a security agency from consent and notice plausibly does so, since secrecy may be necessary to an investigation. It is much harder to explain how disapplying the duty to keep data secure, or

[30] *See Shayara Bano v. Union of India*, (2017) 9 SCC 1 (India) (holding that manifest arbitrariness is a ground for invalidating legislation); *Anuradha Bhasin*, *supra* note 13.
[31] *See Dr. Ram Manohar Lohia v. State of Bihar*, AIR 1966 SC 740 (India).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

the duty to limit its use to the purpose for which it was obtained, advances national security. These duties do not impede an investigation; they protect the data against leaks, misuse and breach, which are as much threats to security as to privacy. To that extent the exemption is not rationally connected to its object.

The necessity requirement asks whether a less restrictive alternative would have achieved the aim equally well. Here the Act supplies its own comparator. Section 17(1) shows that the legislature could relax consent, notice and rights while preserving the baseline duties of compliance and security. The same technique could have been used for the interests listed in section 17(2)(a), perhaps with a specific carve-out for operational secrecy. It was not. Where the statute itself demonstrates that a narrower design was available, the broader one is difficult to describe as the least restrictive means. The point applies with equal force to section 17(5), which permits the executive to extend exemptions to categories of fiduciaries without any statutory test of need, and to section 17(4), which dispenses with erasure for all State processing irrespective of the purpose, and with correction, completion and updating wherever the processing does not involve a decision affecting the data principal.

Balancing requires that the benefit to the State interest not be outweighed by the harm to the right. The amendment of the RTI Act illustrates the problem. The earlier clause balanced privacy and transparency through a public-interest test that permitted disclosure in appropriate cases. Its removal protects the privacy of individuals in the abstract, but it does so by eliminating the mechanism through which the competing public interest was weighed. A legislature may reasonably decide that a categorical rule is preferable to case-by-case balancing; but it must then justify the categorical rule, and the Act contains no such justification beyond the assertion of privacy.

D. Procedural safeguards

This is the weakest part of the State-facing regime. The Aadhaar decision and the PUCL guidelines both stand for the proposition that powers of intrusion must be accompanied by safeguards at the stage of authorisation, in the manner of use, and in review.[32] The DPDP Act has none of these for the State. There is no requirement of a written, reasoned order before a body is exempted or before information is demanded; no requirement of authorisation by an

[32] *See PUCL*, *supra* note 10, ¶ 35 (directions 1, 7, 8 and 9: interception orders to issue only from the Home Secretary (or, in an urgent case, a delegated officer not below the rank of Joint Secretary), use of intercepted material limited to the minimum necessary, copies destroyed once no longer necessary, and review by a Review Committee); *Puttaswamy II*, *supra* note 12 (Sikri J.) (striking down § 33(2) of the Aadhaar Act in its existing form and indicating that the power of disclosure in the interest of national security should rest with an officer above the rank of Joint Secretary, with a judicial officer associated).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

authority independent of the executive; no duty to notify the individual, even after the need for secrecy has passed; and no periodic review or sunset. The data principal's rights of access, correction and grievance redress, which are the ordinary means by which an individual would discover and contest misuse, are disapplied by the same provisions that confer the exemption. Judicial review under Articles 32 and 226 remains available in theory, but a petitioner who is not told that data has been collected cannot invoke it.

The institutional position compounds the problem. The Board does not supervise notified instrumentalities, and its members are appointed by the Central Government, on terms and conditions of service that the Government prescribes. Interception regimes under the Information Technology Act, 2000 and the Telecommunications Act, 2023 do contain some procedural safeguards, but oversight under them is exercised by committees of executive officers, and they regulate interception of communications, not the holding, aggregation and onward use of personal data in State databases or data obtained from private fiduciaries under section 36.[33] The DPDP Act therefore leaves a gap in which data-centred State activity attracts neither the safeguards of the general data protection law nor those of the interception statutes.

E. The Union's strongest defence

The Union has four obvious lines of defence. First, national security is the paradigm area for judicial deference, and the executive is best placed to decide which bodies need relief from compliance. Second, operational secrecy is intrinsic to security work, so notice to the individual would defeat its purpose. Third, other laws, including the interception regimes and the statutes that constitute the notified bodies, already regulate State conduct, so the DPDP Act need not duplicate them. Fourth, the exemptions operate only upon future notification, so any abuse can be challenged when it occurs.

Each has some force, but none answers the objection at its core. Deference is not abdication, and the Aadhaar decision shows that the Court will examine national security claims for adequate safeguards. Secrecy may justify delaying notice; it does not justify never giving it, and it does not explain why security and accountability duties should fall away. The existence of other laws is a reason to tailor the exemption to the gaps they leave, not to exclude the Act entirely, and, as noted above, those laws do not reach the data-centred conduct at issue. Finally, a challenge after notification is a poor remedy when the notification comes without reasons and

[33] The Information Technology Act, No. 21 of 2000, INDIA CODE (2000), § 69; The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, G.S.R. 780(E), GAZETTE OF INDIA, pt. II sec. 3(i) (Oct. 27, 2009); The Telecommunications Act, No. 44 of 2023, INDIA CODE (2023), § 20.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

individuals have no way of learning that they are affected. The better view is that the defects lie in the architecture of the Act and not merely in its possible misapplication.

V. COMPARATIVE PERSPECTIVES

A. The European Union

The General Data Protection Regulation permits Member States to restrict the rights of data subjects and the obligations of controllers to safeguard national security, defence, public security and the prevention of crime, but only by a legislative measure that respects the essence of fundamental rights and is a necessary and proportionate measure in a democratic society.[34] The restricting measure must itself contain specific provisions on matters such as the purposes of processing, the categories of data, the scope of the restriction, the safeguards against abuse and the right of data subjects to be informed.[35] A restriction is thus defined in law, limited in scope and accompanied by safeguards; section 17(2)(a) has none of these features.

European courts have been exacting about safeguards even where national security is invoked. The Court of Justice of the European Union invalidated the Data Retention Directive for failing to confine retention to what is strictly necessary and to provide objective criteria and independent review of access, and it has since insisted on prior review by a court or an independent administrative body.[36] The European Court of Human Rights has likewise held that secret surveillance regimes must contain adequate and effective guarantees against arbitrariness, including supervision and remedies, and has found violations where bulk interception lacked independent authorisation.[37] The comparison must be handled with care, since the legal contexts differ and national security remains in large part a matter for Member States. Still, the shape of the analysis, which asks for a law, a defined scope, necessity and independent oversight, is very close to the one that *Puttaswamy I* prescribes.

B. The United States

American law is organised around a different constitutional text, but recent authority is instructive. In *Carpenter v. United States*, the Supreme Court declined to extend the third-party doctrine to historical cell-site location records held by a telecommunications carrier, and held

[34] Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 23(1), 2016 O.J. (L 119) 1.
[35] *Id.* art. 23(2).
[36] Joined Cases C-293/12 & C-594/12, *Digital Rights Ireland Ltd. v. Minister for Commc'ns*, ECLI:EU:C:2014:238 (Apr. 8, 2014); Joined Cases C-511/18, C-512/18 & C-520/18, *La Quadrature du Net v. Premier ministre*, ECLI:EU:C:2020:791 (Oct. 6, 2020).
[37] *Roman Zakharov v. Russia*, App. No. 47143/06 (Eur. Ct. H.R. Dec. 4, 2015); *Big Brother Watch v. United Kingdom*, App. Nos. 58170/13, 62322/14 & 24960/15 (Eur. Ct. H.R. May 25, 2021).

that the Government must generally obtain a warrant to acquire them.[38] The reasoning, which turns on the capacity of aggregated digital data to reveal the intimate details of a person's life, supports the proposition that data in the hands of an intermediary does not lose constitutional protection. That proposition is directly relevant to section 36 of the DPDP Act, which allows the Government to demand information from private fiduciaries without any requirement of independent authorisation.

VI. RECOMMENDATIONS

None of these defects is beyond repair, and fixing them need not compromise legitimate security interests. Six measures are proposed.

First, section 17(2)(a) should be replaced by tailored exemptions. Exempted bodies should be relieved of notice, consent and access rights to the extent that secrecy requires, while remaining bound at least by the duty of compliance and the duty to maintain reasonable security safeguards, as section 17(1) already contemplates, and preferably by purpose limitation and breach reporting as well. Second, the Act should state an express standard of necessity and proportionality for exemption, for non-consensual processing under section 7(c), and for calls for information under section 36, and should require that exemptions be granted by reasoned notification identifying the body, the purpose and the data concerned.

Third, intrusive access to data, including demands under section 36, should require prior authorisation by a judicial or otherwise independent authority, with post-facto notice to the individual once the need for secrecy has lapsed, in line with the direction of the comparative authorities and the logic of the Aadhaar decision. Fourth, the power in section 17(5) and the notifications under section 17(2)(a) should be subject to a sunset and periodic review, and the Government should lay before Parliament an annual report on exemptions granted and information demanded.

Fifth, the public-interest balancing in section 8(1)(j) of the Right to Information Act should be restored, or replaced with a defined test of serious harm to privacy, so that the balance between privacy and transparency is struck by a rule rather than by omission. Sixth, the independence of the Board should be strengthened through appointment by a committee that includes members from outside the executive, longer and secure tenures, and jurisdiction over the State, including exempted bodies, in respect of the baseline duties of security and breach reporting.[39]

---

[38] *Carpenter v. United States*, 138 S. Ct. 2206, 2217, 2221 (2018).

[39] For a discussion of regulatory independence in the earlier committee proposals, see generally SRIKRISHNA REPORT, *supra* note 3.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

Pending legislative reform, the courts have an interpretive route. Section 17(2)(a) can be read down to require that any notification be reasoned, be limited to the processing that the stated interest necessitates, and leave the baseline security duties in place, in the manner in which the Court has read safeguards into other provisions that confer wide discretionary power.[40] Such a reading would preserve the provision while aligning it with *Puttaswamy I*.

VII. Conclusion

The DPDP Act answers the Supreme Court's invitation to legislate for informational privacy, and for private actors it does so in considerable detail. The provisions that govern the State, however, depart from the standard the Court itself set. Their aims are legitimate; their form is not proportionate. They exempt wholesale where they could have exempted selectively, they rest on executive notification where the standard calls for a clear and constrained law, and they offer no independent authorisation, no notice and no effective oversight. The Act's own structure shows that the legislature knew how to draft more narrowly.

The right to privacy recognised in 2017 was a right against the State before it was a right against anyone else. A data protection law that is rigorous towards private fiduciaries and permissive towards the State turns that order of priority on its head. The reforms proposed here would restore it without weakening the protection of national security, and would bring the Act closer to both the Indian constitutional standard and the practice of comparable jurisdictions. Whether the correction comes from Parliament or from the Court, it is needed if the promise of *Puttaswamy I* is to be kept.

*****

[40] *See, e.g.*, *PUCL*, *supra* note 10, ¶¶ 34–35 (laying down procedural safeguards for the power of interception under § 5(2) of the Indian Telegraph Act, 1885, until rules were framed); *Anuradha Bhasin*, *supra* note 13, ¶¶ 86–87 (reading the requirement of a reasoned order under the Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017 to extend to orders passed by an authorised officer, so as to integrate the proportionality analysis within the Rules).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]