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

BALANCING PRIVACY RIGHTS AND STATE INTEREST UNDER INDIA'S DIGITAL PERSONAL DATA PROTECTION REGIME

~Rudra Vinod Ramchandani

I. ABSTRACT

India's Digital Personal Data Protection Act, 2023 marks the country's first full attempt at managing personal data in the digital space. It specifies what people can expect when it comes to their data and what's expected from organizations that use it. But there's a catch, the law also gives the government a lot of wiggle room, letting state agencies dodge these rules or limit people's rights with a simple government order. This paper delves into that uneasy middle ground. The Supreme Court has recognized privacy as a fundamental right in K.S. Puttaswamy v. Union of India while this same new law hands the State broad powers to sideline that right. A close look at the law itself and comparing it to Europe's General Data Protection Regulation and Singapore's Personal Data Protection Act, the paper tests whether the Indian Act really meets the Constitution's demands for legality, necessity, and proportionality. The takeaway? Some of these wide-ranging exemptions don't hold up, especially when you stack them against both constitutional principles and international expectations. The paper concludes by suggesting a few ways to strike a better balance helping the government do its job, while making sure privacy doesn't get quietly written off.

Keywords: Digital Personal Data Protection Act 2023, Right to Privacy, Puttaswamy, State Exemptions, Proportionality, Surveillance.

II. INTRODUCTION

India's digital world has exploded. Nowadays, people use online banking, shop on e-commerce sites, check government portals, and scroll through social media like it's a usual human activity.

Every tap or click while navigating through such activites, they leave a trail of personal data searches, transactions, forms, messages all piling up and ready to be collected, analyzed, or shared. Sure, the upsides are clear. Daily tasks get easier, life gets more connected. But the dangers? They're not as easy to spot. Without strong rules, private companies, foreign interests, or even government authorities holding too much power can misuse this data.

The right to privacy was not recognised until recently in Indian constitutional law. Decades after independence, the Supreme Court was reluctant to treat privacy as a separate constitutional right. The position changed in 2017 when a nine-judge bench held in *K.S. Puttaswamy v. Union of India* that privacy is a fundamental right protected under Article 21 of the Constitution.[1] The judgment followed with a series of legislative efforts that eventually resulted in the enactment of the Digital Personal Data Protection Act, 2023, six years later.[2]

The Digital Personal Data Protection Act, 2023 showed up in the middle of all this. You'd think the law would settle things. Instead, it kicked off even more debate. People started questioning what section 17 actually covers and why government agencies got broad exemptions. Some worried about the Data Protection Board, does it really stand apart from the government, or is it just another extension of it? Arguments over surveillance and the fact that there's no special category for sensitive data, are still hanging in the air. Pull all these threads together, and a bigger question emerges: does this law actually defend privacy, or does it just hand more control to the state at the expense of people's rights?[3] A statute that advocates rights with one hand and withdraws them by executive notification with the other does not genuinely protect privacy. It only simulates protection.

This paper questions whether the Act is constitutionally faithful to the Puttaswamy guarantee. This paper follows through a literature review, a methodological statement, and a structured analysis of the Act's most contested features, before offering comparative observations and reform proposals.

III. LITERATURE REVIEW

[1] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (India).
[2] Digital Personal Data Protection Act, 2023, No. 22 of 2023 (India) [hereinafter DPDPA].
[3] Internet Freedom Foundation, *Analysis of the Digital Personal Data Protection Act, 2023* (2023); Usha Ramanathan, *The Data Protection Act Is a Surveillance Enabler*, THE WIRE (Aug. 14, 2023).

A. CONSTITUTIONAL SCHOLARSHIP ON PRIVACY

The conversation around privacy didn't just begin with the Puttaswamy case. Long before that landmark judgment, thinkers like Pratap Bhanu Mehta and Suhrith Parthasarathy were already raising questions about the perspectives taken in *M.P. Sharma v. Satish Chandra* and *Kharak Singh v. State of Uttar Pradesh.* They argued that the limited interpretation of privacy in those rulings was difficult to defend, both in terms of the text and the underlying philosophy.[4] The Puttaswamy judgment delved deeply into this very literature, pulling insights from comparative constitutional law in countries like Germany, South Africa, Canada, and the United States to anchor the right in universal principles of human dignity.

Since the Puttaswamy decision, academic direction has shifted to how this right can be effectively implemented. Chinmayi Arun's research on platform governance and Rishab Bailey's examination of data localization have pin pointed the significant structural issues that any new legislation will need to tackle.[5] Both scholars predicted the difficulty of building a rights-protective framework while accommodating India's significant digital economy and security interests.

B. DPDPA'S LEGISLATIVE AND POLICY COMMENTARY

The Justice B.N. Srikrishna Committee Report of 2018 is one starting point for the DPDPA which suggested a comprehensive data protection framework for India. The report included inspiration from international developments, particularly the GDPR, and recommended stronger safeguards for privacy than those found in the final version of the Act.[6] The Personal Data Protection Bill, 2019 incorporated many of the Committee's recommendations. At the same time, it introduced a broad governmental exemption under clause 35, which quickly became one of the most debated provisions of the Bill.

The legislative process had just begun, while the Joint Parliamentary Committee submitted its report in 2021, the government withdrew the Bill and began drafting a new framework. The Digital Personal Data Protection Act, 2023 which resulted from this process is noticeably

---

[4] *M.P. Sharma v. Satish Chandra*, A.I.R. 1954 S.C. 300 (India); *Kharak Singh v. State of U.P.*, A.I.R. 1963 S.C. 1295 (India).

[5] Chinmayi Arun, *On Weaponising Platform Governance*, 31 Yale J.L. & Tech. 74 (2019); Rishab Bailey & Nehaa Chaudhari, *Data Localisation in India: Questioning the Means and the Ends*, 9 Asian J.L. & Soc'y 171 (2022).

[6] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (2018) [hereinafter Srikrishna Report].

shorter and simpler than the earlier drafts. Some commentators, including Usha Ramanathan, have argued that this simplification came in exchange of a stronger privacy safeguards, particularly in relation to state power and government exemptions.[7]

C. COMPARATIVE LITERATURE

GDPR literature is huge in volume. Paul de Hert and Vagelis Papakonstantinou have written extensively on the GDPR's approach to state derogations, arguing that Article 23's requirement of legislative specificity is essential to prevent executive overreach.[8] Their analysis is directly relevant to section 17 of the Indian Act. Graham Greenleaf's global survey of data protection laws provides a useful framework for situating the DPDPA within the broader international landscape and identifying where India diverges from emerging global norms.[9]

Together, the existing literature establishes three things clearly. First, the constitutional foundation for strong data protection law exists in India and is judicially mandated. Second, the DPDPA as enacted falls short of what the Srikrishna Committee and most academic commentators had recommended. Third, comparative models, particularly the GDPR, offer workable templates for addressing the gaps.

IV. METHODOLOGY

This paper incorporates both doctrinal and comparative legal research, the primary focus is on doctrinal analysis. Aiming at studying the provisions of the Digital Personal Data Protection Act, 2023 and examining them against the constitutional principles laid down by the Hon’ble Supreme Court in *K.S. Puttaswamy v. Union of India* and subsequent privacy-related decisions. The analysis stems from the text of the Act and, where necessary, considers its legislative background and broader constitutional context.

A crucial part of the discussion is the proportionality principle established by the Supreme Court; the paper examines whether restrictions on privacy under the Act have a legal basis, pursue a legitimate objective, and remain proportionate to that objective. It also considers

[7] Usha Ramanathan, India's Data Protection Law Falls Short, THE WIRE (Aug. 11, 2023).
[8] Paul De Hert & Vagelis Papakonstantinou, The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?, 32 Comput. L. & Sec. Rev. 179 (2016).
[9] Graham Greenleaf, Global Data Privacy Laws 2023: 162 National Laws and Rising, 181 Privacy Laws & Bus. Int'l Rep. 3 (2023).

whether powers given to the executive are accompanied by adequate safeguards and whether the exemptions provided under the Act are sufficiently limited.

The paper also draws on comparative examples from the European Union and Singapore. These jurisdictions have been selected because both have established data protection frameworks and offer useful points of comparison. The aim is not to argue that India should copy either model. Instead, the comparison aims in helping place the Indian framework in a broader context and highlights alternative approaches to balancing privacy rights along with state interests.

This research does not engage in surveys, interviews, or statistical analysis. The Act is still relatively new, and limited enforcement material is available. The focus of this paper is on the legal framework itself, as a result the paper evaluates whether the design of the Act is consistent with constitutional principles, while recognising that its practical impact may become clearer as time goes on.

V. MAIN ANALYSIS

A. CONSTITUTIONAL FRAMEWORK: THE PUTTASWAMY TESTS

Any analysis of the DPDPA must begin with the constitutional standard. In *Puttaswamy*, the Supreme Court recognised three spectrums of privacy: informational privacy, bodily privacy and decisional autonomy. To simplify meaning control over personal data; rights related to ones own body; and autonomy in decision making of personal matters.[10] All are protected under Article 21 and are engaged by the DPDPA.

The Court held that the state may restrict privacy rights, consciously setting high standards, only if these following three requirements are met: the given restriction must have a legal basis, it must pursue a legitimate aim, and it must be proportionate. Meaning that the act must be grounded in specific laws, serving a genuine public interest rather than arbitrary state convenience, the means chosen must be the least restrictive available and the harm to privacy must not be disproportionate to the benefit achieved.

Suitability, necessity, balancing, and strict proportionality the standard of a four-stage test developed further from *Puttaswamy,* in *Modern Dental College v. State of Madhya Pradesh*

[10] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1, ¶ 127 (India) (Chandrachud, J.).

by The Hon'ble Supreme Court.[11] Applying the same to data protection, meaning asking whether a given restriction actually advances the stated state interest, whether a less intrusive alternative exists, whether the privacy cost is justified by the benefit, and whether the restriction is strictly proportionate in its effect on individual rights.

B. SECTION 17 AND THE STATE EXEMPTION PROBLEM

The exemption granted by executive notification, parliament need not approve each exemption, and there is no requirement of judicial oversight. In the interest of sovereignty and integrity of India, security of the state, friendly relations with foreign states, maintenance of public order, or preventing incitement to any cognisable offence relating to these, section 17(1) of the Act grants power to the Central Government to exempt any instrumentality of the state from all or any provisions of the Act.[12]

In *Puttaswamy*, the Supreme Court emphasised that restrictions on privacy must have a clear legal basis, whether this provision satisfies the legality requirement is open to serious doubt. Section 17 allows the Central Government to exempt state agencies through executive notification on grounds that are framed in broad terms, including public order and security of the State. This raises concerns about whether the scope of the exemption is defined with sufficient precision and whether Parliament has provided adequate guidance regarding the limits of such power.

A comparison with Article 23 of the GDPR is essential. The GDPR permits restrictions on certain data subject rights, but those restrictions must be grounded in legislative measures and along with clearly defined purposes and safeguards, the contrast highlights the extent of discretion available under section 17 and raises questions about its compatibility with the constitutional standards articulated in *Puttaswamy*.[13] The Court of Justice of the European Union has read these requirements strictly. In *La Quadrature du Net*, it struck down national

[11] Modern Dental Coll. & Research Ctr. v. State of Madhya Pradesh, (2016) 7 S.C.C. 353 (India).
[12] DPDPA, supra note 2, § 17(1).
[13] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 Apr. 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, 2016 O.J. (L 119) 1 [hereinafter GDPR].

laws authorising bulk data retention because they were not targeted and did not contain adequate safeguards.[14] India's section 17 would not pass this standard.

The grounds listed in section 17(1) are not new. Similar expressions appear in Articles 19(2) and 19(3) of the Constitution, where they are used to justify restrictions on rights such as free speech and assembly. Their use in a data protection law is more difficult to assess. Terms like "public order" and "security of the State" are very broad and can cover a wide range of situations. The Act does not explain how these grounds should be applied when exempting government agencies from privacy obligations.

This creates uncertainty. It is not always clear when an exemption would be justified or what limits exist on the exercise of this power. The provision leaves considerable discretion in the hands of the executive while offering relatively little guidance on how that discretion should be used. In practice, this may weaken the protections that the Act is otherwise intended to provide.

C. THE RIGHT TO INFORMATION AMENDMENT

Section 44(3) of the Act amends section 8(1)(j) of the Right to Information Act, 2005. The amendment requires that personal information be withheld unless the public interest in disclosure clearly outweighs the harm to privacy.[15] The principle is sound, but the implementation is concerning.

The Supreme Court in *Central Board of Secondary Education v. Aditya Bandopadhyay* held that the RTI Act must be read broadly and exemptions narrowly.[16] The amendment appears to shift the balance more strongly towards privacy. In practice, information may now be withheld unless the public interest in disclosure is considered sufficiently compelling. How this standard will be applied remains unclear. Much will depend on the approach taken by public information officers and appellate authorities when balancing privacy concerns against the public's right to know.

This concern is not entirely speculative as access to information plays an important role in accountability journalism, public-interest investigations, and democratic oversight more

[14] Joined Cases C-511/18, C-512/18 & C-520/18, La Quadrature du Net v. Premier Ministre, ECLI:EU:C:2020:791 (2020).
[15] DPDPA, supra note 2, § 44(3) (amending Right to Information Act, No. 22 of 2005, § 8(1)(j) (India)).
[16] Ctr. Bd. of Secondary Educ. v. Aditya Bandopadhyay, (2011) 8 S.C.C. 497 (India).

generally. A privacy exemption framed broadly may make disclosure more difficult in some cases, particularly where the information relates to public officials. At the same time, not all personal information deserves the same level of protection. Medical records of a public servant, for example, raise very different privacy concerns from information relating to the financial interests or public responsibilities of elected representatives. The amendment does not expressly distinguish between these situations, leaving much to future interpretation.

D. CONSENT, LEGITIMATE USE, AND GOVERNMENT PROCESSING

The Act builds its primary framework around consent as the lawful basis for processing. But section 7 recognises several "legitimate uses" that do not require consent, including processing necessary for performing state functions, providing subsidies and benefits, issuing licences, and maintaining national security.[17] These categories are broad enough to cover most government data processing.

The core idea is pretty straightforward: data collected for one reason shouldn't just be repurposed for another. Purpose limitation is one area where the Act seems a bit murky. For instance, if someone shares their personal information to get a driving license, they probably expect that info to stay tied to that specific purpose.

Unfortunately, the Act doesn't offer any clear guidance on this. Things get even trickier when the government is involved. Private data handlers typically have to clarify why they're collecting personal data and how it will be used. Problems arise when that same data can be linked to health, financial, or other government records. Without fresh consent or clear legal authorization, it's tough to figure out where the boundaries really are.

However, government processing often falls under the umbrella of legitimate uses, which means consent isn't always required. While people may have rights under the framework, exercising those rights becomes a challenge if they're not aware of what data is being collected, where it's headed, or who else might have access to it. This raises a pressing question: how much information will citizens actually get about how their data is being used? The Act doesn't really shed light on this either.

E. SURVEILLANCE AND JUDICIAL OVERSIGHT

[17] DPDPA, supra note 2, § 7.

In India, there isn't a dedicated surveillance law in place. The government is allowed to intercept communications under section 5(2) of the Indian Telegraph Act, 1885, and section 69 of the Information Technology Act, 2000. Both of these sections require executive authorization instead of judicial approval. Unfortunately, the DPDPA doesn't change this framework, meaning that government agencies can access personal data held by private data fiduciaries without needing to get a court's approval.

Indicating that mass surveillance without independent oversight could lead to significant constitutional concerns, the Supreme Court briefly discussed this issue in the Aadhaar judgment.[18] More recently, in the Pegasus spyware case, the Court set up a technical committee to investigate claims of unlawful surveillance and criticized the government for not being transparent about its surveillance programs.[19] The DPDPA could have addressed some of these concerns, but it leaves the existing position unchanged. Questions relating to government access to personal data and independent oversight remain unresolved.

Emergencies may justify exceptions, but such cases could still be reviewed afterwards within a fixed time period. Similar approaches can be found in other jurisdictions and are difficult to reconcile with the idea that privacy restrictions should be lawful, necessary, and proportionate. One possible safeguard would be to require judicial approval before government agencies access personal data held by private data fiduciaries.

F. THE DATA PROTECTION BOARD: INDEPENDENCE AND EFFECTIVENESS

The Data Protection Board is established under Chapter VI of the Act as the primary enforcement authority. Its members are appointed by the Central Government, which also determines their terms and conditions of service.[20] The Board operates as a digital office. While this has efficiency advantages, it also means that physical hearings and the adversarial processes that tend to generate clear precedent are not the default.

Independent regulatory authorities in India, such as the Election Commission and the Comptroller and Auditor General, derive their credibility from constitutional protection of their independence. An enforcement authority whose members are appointed and can effectively be removed by the very executive it is meant to hold accountable is structurally compromised.

[18] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2019) 1 SCC 1, para. 317 (Chandrachud, J., dissenting) (India).
[19] Manohar Lal Sharma v. Union of India, (2022) 8 S.C.C. 1 (India).
[20] DPDPA, supra note 2, §§ 18–27.

This is not a criticism of any individual who might serve on the Board. It is an observation about institutional design. The Data Protection Board has no comparable protection. Its effectiveness will depend on political will rather than structural guarantee.

VI. CONCLUSION

India now has a dedicated framework for personal data protection, something that was missing for many years. The Digital Personal Data Protection Act, 2023 is undoubtedly an important step. The Act recognises rights for data principals, places obligations on data fiduciaries, and creates a mechanism for enforcement. Those are significant developments.

Yet the picture is not entirely reassuring. Several of the Act's most debated provisions concern the State itself. Section 17 is perhaps the clearest example. While the Act creates rights, it also leaves room for those rights to be restricted through broad exemptions. Similar concerns arise in relation to the RTI amendment, the absence of clear limits on government use of personal data, and the lack of a dedicated surveillance framework. The Data Protection Board exists. Whether it will function with sufficient independence is a different question.

This tension runs through the Act. Privacy is recognised, but not always protected with equal force. Private entities are subject to detailed obligations. Government agencies, in some situations, are treated differently. Whether that distinction can be justified under the constitutional principles laid down in *Puttaswamy* remains open to debate.

None of this means the Act is without value. Far from it. The framework can still be strengthened. Narrower exemptions, greater institutional independence, clearer rules on government processing, and stronger safeguards for surveillance would go a long way towards addressing the concerns discussed in this paper. These are not dramatic changes. In many ways, they simply reflect the constitutional commitment to privacy that the Supreme Court has already recognised.

The DPDPA is an important beginning. Not the end of the conversation. The real test will be whether privacy remains meaningful when the State, and not just private companies, is the one handling personal data.