ShodhSamajik: Journal of Social Studies
July-September 2026 3(2)
https://shodhsamajik.com/

Original Article

RIGHT TO PRIVACY AND DATA PROTECTION IN THE DIGITAL AGE: A CRITICAL LEGAL ANALYSIS OF INDIA'S DIGITAL PERSONAL DATA PROTECTION ACT, 2023

Dr. Rakhi Pande [1*]
[1] Assistant Professor, Oriental University, Indore, India

ABSTRACT

The right to privacy in India acquired constitutional status through the Supreme Court's landmark ruling in Justice K.S. Puttaswamy v. Union of India, which held informational privacy to be an intrinsic facet of the right to life and personal liberty. Six years later, Parliament enacted the Digital Personal Data Protection Act to give statutory shape to this right in the context of digital data processing. This paper undertakes a doctrinal legal analysis of the Act, examining its constitutional foundation, its core architecture of consent, data principal rights and data fiduciary obligations, and the institutional design of the Data Protection Board. The study adopts a qualitative, library-based method, drawing upon primary legal sources, government notifications and secondary academic and professional commentary, and situates the Indian framework within a brief comparative reading of the European Union's General Data Protection Regulation. The analysis finds that while the Act represents a significant legislative advance, it exhibits notable gaps, including broad governmental exemptions, the absence of a differentiated category of sensitive personal data, limited independence of the regulatory Board, and a phased and delayed implementation timeline. The paper concludes that the effectiveness of India's data protection regime will depend substantially on the manner in which subordinate rules are framed and enforced, and it offers recommendations for strengthening institutional independence and rights enforcement.

Keywords: Right to Privacy, Data Protection, Digital Personal Data Protection Act, 2023, Information Technology Law, Data Fiduciary, India

INTRODUCTION

The proliferation of digital technologies, e-governance platforms and data-driven commercial services has transformed personal data into one of the most valuable and vulnerable assets of the twenty-first century. In India, this transformation has occurred against the backdrop of one of the largest digital identity programmes in the world, the Aadhaar scheme, which alone processes the biometric and demographic data of over a billion residents. For much of the last two decades, India's data protection regime rested on the thin foundation of Section 43A of the Information Technology Act, 2000 and the Reasonable Security Practices Rules, 2011, neither of which was designed to address the scale or complexity of contemporary data processing AZB and Partners. (2023).

The constitutional turning point came in 2017, when a nine-judge bench of the Supreme Court, in Justice K.S. Puttaswamy (Retd.) v. Union of India, unanimously held that the right to privacy, including informational privacy, is protected as an intrinsic part of the right to life and personal liberty under Article 21 of the Constitution Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017). The Court, however, left the specific contours of informational privacy and its statutory protection to be worked out by the legislature

*Corresponding Author:
Email address: Dr. Rakhi Pande (rakhi.pande3838@gmail.com)

Received: 28 June 2026; **Accepted:** 23 July 2026; **Published:** 21 August 2026
DOI: 10.29121/ShodhSamajik.v3.i2.2026.141
Page Number: 82-85
Journal Title: ShodhSamajik: Journal of Social Studies
Journal Abbreviation: ShodhSamajik J. Soc. Stud.
Online ISSN: 3049-2319, **Print ISSN:** 3108-2009
Publisher: Granthaalayah Publications and Printers, India
Conflict of Interests: The authors declare that they have no competing interests.
Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.
Authors' Contributions: Each author made an equal contribution to the conception and design of the study. All authors have reviewed and approved the final version of the manuscript for publication.
Transparency: The authors affirm that this manuscript presents an honest, accurate, and transparent account of the study. All essential aspects have been included, and any deviations from the original study plan have been clearly explained. The writing process strictly adhered to established ethical standards.

Burman (2023). What followed was a prolonged legislative journey spanning the 2018 Srikrishna Committee draft, the Personal Data Protection Bill of 2019, and the 2022 draft Digital Personal Data Protection Bill, before Parliament finally enacted the Digital Personal Data Protection Act, 2023 (hereinafter 'the DPDP Act' or 'the Act') on 11 August 2023 (Digital Personal Data Protection Act, 2023).

The DPDP Act is India's first standalone, cross-sectoral data protection legislation. It seeks to balance the individual's right to protect personal data against the legitimate need of the State and private entities to process such data for lawful purposes. This paper critically examines the legal architecture of the DPDP Act, evaluates its adequacy in operationalising the constitutional right recognised in Puttaswamy, and compares its salient features with the European Union's General Data Protection Regulation (GDPR), which remains the global benchmark for data protection law. The paper further identifies structural gaps in the Indian framework and proposes measures for strengthening its rights-protective character.

METHOD

This study adopts a doctrinal, or black-letter, legal research method, which is the method most suited to the systematic analysis of statutory text, judicial precedent and subordinate legislation. The primary sources examined include the text of the Digital Personal Data Protection Act, 2023, the Digital Personal Data Protection Rules, 2025, the Information Technology Act, 2000, and the Supreme Court's judgment in Justice K.S. Puttaswamy v. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017). These primary materials are read alongside secondary sources, comprising peer-reviewed commentary, policy briefs from research institutions, and professional legal analyses published by law firms and international organisations, to situate the statutory provisions within their interpretive and policy context.

The doctrinal analysis is supplemented by a limited comparative method, in which selected provisions of the DPDP Act are read against corresponding provisions of the GDPR (Regulation (EU) 2016/679) to identify points of convergence and divergence. This comparative reading is not exhaustive but is confined to areas most relevant to the research questions, namely the definition of personal data, the consent architecture, the categorisation of sensitive data, and the independence of the regulatory authority. The paper does not involve empirical fieldwork or primary data collection; its findings are accordingly interpretive and normative rather than statistical.

RESULTS AND DISCUSSION

CONSTITUTIONAL FOUNDATION: FROM PUTTASWAMY TO STATUTE

The Puttaswamy judgment is the constitutional anchor of the DPDP Act. The nine-judge bench held that privacy is not an elitist construct but a right available to every individual, and that informational privacy, understood as control over the dissemination of personal information, is protected under Article 21 Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017). Importantly, the Court also laid down a three-fold test for any restriction on privacy, requiring the existence of law, a legitimate state aim, and proportionality between the means adopted and the object sought to be achieved. This proportionality standard continues to inform judicial review of data-related state action, as seen subsequently in Joseph Shine v. Union of India (2018), where privacy considerations again shaped the Court's reasoning on personal autonomy.

While the Puttaswamy bench did not prescribe a specific statutory model, it created an unmistakable constitutional obligation on the State to enact a data protection framework Burman (2023). The six-year gap between the judgment and the DPDP Act reflects both the technical complexity of the subject and successive shifts in legislative approach, from the rights-centric 2019 Bill to the more consent- and business-facilitation-oriented 2022 and 2023 drafts Nachiappan (2025).

ARCHITECTURE OF THE DPDP ACT, 2023

The Act applies to the processing of digital personal data within India, whether collected in digital form or collected offline and subsequently digitised, and extends extraterritorially to entities outside India that process personal data in connection with offering goods or services to individuals in India Digital Personal Data Protection Act, 2023. Personal data that has been voluntarily made public by the data principal, and data processed for narrowly defined domestic or research purposes, are excluded from its scope Linklaters. (2023).

At the core of the Act is a consent-based processing model. Processing is permitted only where the data principal gives free, specific, informed and unambiguous consent, signified through a clear affirmative act, or where processing falls within one of the enumerated 'legitimate uses,' such as voluntary sharing of data for a specified purpose, the State's provision of benefits, subsidies or services, and compliance with judgments or orders AZB and Partners. (2023). The Act further recognises a set of enforceable rights for data principals, including the right to access information about processing, the right to correction and erasure of personal data, the right to grievance redressal, and the right to nominate another individual to exercise these rights in the event of death or incapacity Digital Personal Data Protection Act, 2023.

Corresponding obligations are placed on data fiduciaries, the entities that determine the purpose and means of processing. These include obligations to ensure the accuracy and completeness of data, to implement reasonable security safeguards, to notify the Data

Protection Board of India and affected data principals in the event of a personal data breach, and to erase personal data once the purpose of processing is fulfilled and retention is no longer necessary Future of Privacy Forum. (2023). The Act creates a distinct, more stringent set of obligations for 'Significant Data Fiduciaries,' a category to be notified by the Central Government based on factors such as the volume and sensitivity of data processed and the risk to electoral democracy or state security.

Enforcement is vested in the Data Protection Board of India, a body corporate established under the Act with the power to inquire into complaints, impose penalties and direct remedial measures. Financial penalties for non-compliance are substantial, extending up to two hundred and fifty crore rupees for a single instance of breach involving inadequate security safeguards Digital Personal Data Protection Act, 2023. The Digital Personal Data Protection Rules, 2025, notified on 13 November 2025, operationalise the Act's provisions in a phased manner, with full compliance obligations to take effect by 13 May 2027 Ministry of Electronics and Information Technology. (2025).

COMPARATIVE READING WITH THE GDPR

A comparison with the European Union's GDPR highlights both structural parallels and significant departures. Like the GDPR, the DPDP Act adopts an extraterritorial scope and a consent-centred processing model, and both frameworks impose breach-notification obligations on data controllers or fiduciaries. However, unlike the GDPR, which distinguishes 'special categories' of sensitive personal data, such as health, biometric and genetic information, and subjects them to heightened protection, the DPDP Act treats all personal data uniformly, without a separate, more protective regime for sensitive data Lexology. (2025). This is a notable divergence, given that Indian jurisprudence in Puttaswamy itself recognised bodily and health-related privacy as deserving of heightened constitutional protection.

A further point of departure lies in institutional design. The GDPR mandates that national supervisory authorities act with 'complete independence,' whereas the members of India's Data Protection Board are appointed by, and hold office at the pleasure of, the Central Government, which also frames the search-and-selection process Digital Personal Data Protection Act, 2023. This raises legitimate concerns about the functional independence of the Board, particularly in matters involving government data fiduciaries. Additionally, the DPDP Act grants the Central Government wide-ranging exemptions for its own instrumentalities on grounds of sovereignty, security of the State, public order and prevention of offences, exemptions that are considerably broader than those available to private data fiduciaries AZB and Partners. (2023).

GAPS AND CHALLENGES

Several structural concerns emerge from this analysis. First, the absence of a distinct category for sensitive personal data leaves health records, financial information and biometric data without the enhanced procedural safeguards that their intrinsic sensitivity would warrant. Second, the broad exemptions available to government agencies risk perpetuating precisely the kind of unregulated state surveillance that the Puttaswamy Court sought to guard against, since government processing for stated purposes of national security or crime prevention escapes many of the Act's core obligations Digital Personal Data Protection Act, 2023. Third, the composition and tenure of the Data Protection Board, being subject to executive control, may compromise its ability to adjudicate impartially against the government itself, an issue that assumes particular significance where the State is among the largest processors of citizen data in the country.

Fourth, the phased and considerably delayed implementation timeline, with certain provisions deferred until May 2027, nearly four years after the Act received Presidential assent, leaves data principals without effective statutory remedies in the interim Ministry of Electronics and Information Technology. (2025). Finally, the absence of a mandatory data protection impact assessment requirement for all but Significant Data Fiduciaries limits the Act's preventive, as opposed to remedial, character. Taken together, these gaps suggest that while the DPDP Act constitutes an important legislative milestone, it does not yet fully operationalise the expansive vision of informational privacy articulated in Puttaswamy.

CONCLUSION

The Digital Personal Data Protection Act, 2023 represents a watershed moment in India's legal history, translating the constitutional right to privacy recognised in Justice K.S. Puttaswamy v. Union of India into a dedicated statutory framework for the digital era. The Act establishes a workable, consent-based architecture for data processing, confers enforceable rights upon data principals, and creates a dedicated regulatory body with meaningful penalty powers. At the same time, this analysis has shown that the Act falls short of international best practice in several respects: it does not distinguish sensitive personal data for heightened protection, it grants government bodies unusually broad exemptions, and it structures the Data Protection Board in a manner that raises questions about its independence from executive influence.

For the DPDP Act to fully realise the constitutional promise of Puttaswamy, subsequent rule-making and institutional practice should move towards recognising a differentiated category of sensitive personal data, narrowing governmental exemptions to what is strictly necessary and proportionate, and insulating the composition and functioning of the Data Protection Board from executive

control. Future research may usefully examine the practical implementation of the Digital Personal Data Protection Rules, 2025 as compliance deadlines approach, and assess, through empirical study, the extent to which data principals are able to exercise their statutory rights in practice.

ACKNOWLEDGMENTS

None.

REFERENCES

AZB and Partners. (2023). Digital Personal Data Protection Act, 2023 – Key Highlights.

Burman, A. (2023). Understanding India's New Data Protection Law. Carnegie Endowment for International Peace.

Digital Personal Data Protection Act, 2023, No. 22 of 2023 (India).

Future of Privacy Forum. (2023). The Digital Personal Data Protection Act of India, Explained.

Information Technology Act, 2000, No. 21 of 2000 (India).

Joseph Shine v. Union of India, AIR 2018 SC 4898 (India).

Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, AIR 2017 SC 4161 (India).

Lexology. (2025). India's Digital Personal Data Protection Act 2023 Brought into force. https://www.lexology.com/library/detail.aspx?g=06a5c11c-6f5d-4aec-8d07-851cf89d992d

Linklaters. (2023). India – The Digital Personal Data Protection Act, 2023 Finally Arrives.

Ministry of Electronics and Information Technology. (2025). Digital Personal Data Protection Rules, 2025. Government of India.

Nachiappan, K. (2025). India's new Data Protection Regime (ISAS Brief No. 1198). Institute of South Asian Studies, National University of Singapore. https://www.isas.nus.edu.sg/wp-content/uploads/2025/01/ISAS-Brief-1198.pdf

Regulation (EU) 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 (General Data Protection Regulation). (2016). Official Journal of the European Union, L 119, 1–88.