INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed



www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

Copyright © International Journal for Legal Research & Analysis. All rights reserved.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

FROM CONSTITUTIONAL PRIVACY TO STATUTORY DATA PROTECTION: A CRITICAL ANALYSIS OF INDIA'S DIGITAL PERSONAL DATA PROTECTION ACT, 2023 AND THE RULES, 2025

AUTHORED BY - DASARI DIVYA
LLM (Cyber and Technology Law), School of Law, Aurora University

Abstract.

India moved from a constitutional principle of privacy to a data protection statute in a little over six years. The Supreme Court recognised privacy as a fundamental right in 2017, Parliament passed the Digital Personal Data Protection Act in 2023, and the Central Government notified the implementing Rules in November 2025. This paper asks how far the resulting framework carries the constitutional right into practice. It sets out the structure of the Act and Rules, including their staggered commencement, and then tests five features against the standard laid down in *Puttaswamy*: the quality of consent, the breadth of the State's exemptions, the amendment to the Right to Information Act, the independence of the Data Protection Board, and the remedies open to an individual whose data is misused. The paper argues that the framework gives individuals workable procedural rights against private organisations but weaker protection against the State, and that its remedies are thinner than those of the regime it replaces. The study is doctrinal and relies on statutory text, judicial decisions and official notifications. The law is stated as on 5 November 2026.

Keywords: Right to privacy; data protection; Digital Personal Data Protection Act 2023; Data Protection Board; consent; Puttaswamy; India

1. Introduction

Digital services collect personal data as a by-product of ordinary use. A banking app records where and when a person pays, a map service records where they go, and a social media account gathers years of opinions, contacts and photographs. Taken together, this information can describe a person more completely than anything they have chosen to disclose. The legal question is therefore wider than whether a particular fact was shared. It is how much control

ISSN: 2582-6433

an individual should keep over information about themselves, and what duties fall on the organisations that collect and use it.

India reached its answer in two stages, and in an unusual order. The constitutional right came first. In *Justice KS Puttaswamy (Retd) v Union of India*, a nine-judge Bench of the Supreme Court held in 2017 that privacy is a fundamental right.[1] The statute came later. Parliament enacted the Digital Personal Data Protection Act, 2023 (DPDP Act), which received assent on 11 August 2023,[2] and the Central Government notified the Digital Personal Data Protection Rules, 2025 (DPDP Rules) on 13 November 2025.[3] Until then, the main statutory protection for personal data was section 43A of the Information Technology Act, 2000, which allowed compensation where a company was negligent in protecting sensitive personal data.[4]

This paper asks how far the new framework carries the constitutional right into practice. Its argument is that the DPDP Act gives individuals workable procedural rights against private organisations, gives them much less against the State, and offers remedies that are thinner than the regime it replaces. The paper is doctrinal. It relies on the text of the Act and Rules, on decisions of the Supreme Court and on official notifications, and it states the law as on 5 November 2026. Sector-specific regulation, such as the directions issued by the Reserve Bank of India, is outside its scope.

Part 2 recalls the constitutional foundation. Part 3 describes the structure of the Act and Rules. Part 4 deals with their staggered commencement and their overlap with the Information Technology Act. Part 5 examines five points on which the framework is open to criticism, and Part 6 makes suggestions.

2. The constitutional foundation

For much of the twentieth century the Supreme Court's position on privacy was uncertain. *MP Sharma v Satish Chandra* and *Kharak Singh v State of UP* were long read as denying that the Constitution contains a general right of privacy.[5] Smaller benches later recognised aspects of privacy in particular settings, but the two decisions were not formally displaced until the question reached nine judges.

In *Puttaswamy* the Court unanimously held that privacy is protected under article 21, read with the other rights in Part III of the Constitution, and overruled the earlier decisions to the extent they held otherwise.[6] Control over personal information was treated as part of the right. The plurality opinion of Chandrachud J also set out what the State must show before it interferes

ISSN: 2582-6433

with privacy: a law that authorises the interference, a legitimate aim, proportionality between the aim and the means chosen, and procedural safeguards against abuse.[7] The Court applied a proportionality standard again in the Aadhaar judgment of 2019.[8] These four requirements are the yardstick used in Part 5 to assess the State-facing provisions of the DPDP Act.

Two points follow for the statute. First, a fundamental right binds the State. It does little by itself against a private company that mines its customers' data, and that gap is what a data protection law exists to fill. Second, because the right was declared in broad terms, the detailed rules fell to the legislature. A government-appointed expert committee under Justice BN Srikrishna had already proposed a model in 2018, framed around the idea that an entity holding personal data owes duties to the person it relates to.[9]

3. The structure of the DPDP Act and Rules

3.1 Scope and vocabulary

The Act applies to digital personal data, meaning personal data collected in digital form or digitised after collection.[10] The person to whom the data relates is the Data Principal, and whoever decides the purpose and means of processing is the Data Fiduciary.[11] The terminology reflects the fiduciary idea that the Srikrishna Committee had proposed.[12] The Act also reaches processing outside India where it is connected with offering goods or services to Data Principals in India, so a foreign platform with Indian users falls within it.[13]

3.2 Grounds for processing

Personal data may be processed only for a lawful purpose, and only with the Data Principal's consent or for a "certain legitimate use".[14] Before asking for consent, the Data Fiduciary must give a notice that tells the person what data is sought and why, how rights may be exercised and how to complain to the Board.[15] Under section 6, consent must be free, specific, informed, unconditional and unambiguous, given by a clear affirmative action, and limited to the data necessary for the stated purpose.[16] It can be withdrawn at any time, and withdrawal must be as easy as giving consent.[17]

Section 7 lists the legitimate uses for which consent is not needed. They include voluntary provision of data for a specified purpose, the provision of subsidies, benefits and services by the State, the performance of State functions under law, compliance with legal obligations and court orders, medical emergencies and employment.[18]

ISSN: 2582-6433

3.3 Duties and rights

A Data Fiduciary must maintain reasonable security safeguards, report personal data breaches to the Board and to affected persons, and erase personal data once its purpose is spent, unless the law requires retention.[19] Processing the data of a child requires verifiable consent from a parent or lawful guardian, and tracking, behavioural monitoring and targeted advertising directed at children are barred, subject to exemptions the Rules may allow.[20] Significant Data Fiduciaries, which the Government notifies on factors such as the volume and sensitivity of the data they handle, carry further duties, including an India-based Data Protection Officer, an independent data auditor and periodic impact assessments.[21]

Data Principals have the right to obtain information about their data, to seek correction and erasure, to have grievances redressed and to nominate another person to act for them in the event of death or incapacity.[22] They also owe duties, which include not impersonating another person and not filing false or frivolous grievances.[23]

3.4 The Board and penalties

Enforcement rests with the Data Protection Board of India, which the Government established by notification GSR 844(E) on 13 November 2025.[24] A second notification of the same date, GSR 845(E), fixed its strength at a Chairperson and four Members.[25] The Board receives complaints and breach intimations, conducts inquiries, and can impose monetary penalties after giving the person concerned a hearing. Appeals lie to the Telecom Disputes Settlement and Appellate Tribunal.[26] The Schedule sets maximum penalties: ₹250 crore for failing to take reasonable security safeguards where a breach results, ₹200 crore for failing to notify a breach or for breaching the provisions on children's data, and lower sums for other contraventions.[27]

4. Commencement and the overlap with the Information Technology Act

The Act did not take effect all at once. Notification GSR 843(E) of 13 November 2025 brought it into force in three phases, and rule 1 of the DPDP Rules follows the same pattern.[28] Table 1 summarises the position.

Table 1: Phased commencement of the DPDP Act and Rules

Phase	Date	Provisions of the Act	Provisions of the Rules
1	13 November 2025	ss 1(2), 2, 18 to 26, 35, 38 to	rr 1, 2 and 17 to 21

ISSN: 2582-6433

		43, 44(1) and 44(3)	
2	13 November 2026	ss 6(9) and 27(1)(d)	r 4
3	13 May 2027	Remaining provisions, including s 44(2) and s 33	rr 3, 5 to 16, 22 and 23

Source: Notification GSR 843(E) and rule 1 of the DPDP Rules.

Two consequences deserve attention. First, the Board has existed in law since November 2025, but the penalty provision, section 33, does not commence until 13 May 2027. For the time being the Board has no power to impose penalties. Second, section 43A of the Information Technology Act remains in force until section 44(2)(a) of the DPDP Act omits it on 13 May 2027.[29] For about eighteen months after the Rules were notified, the older compensation regime and the new framework therefore run side by side. Consent Managers fall in the middle phase: rule 4 comes into force on 13 November 2026, six months before the consent provisions bind Data Fiduciaries.[30]

The text of the Act has also been adjusted once already. In October 2026 the Government used its power to remove difficulties to correct the wording of sections 9(1) and 10(2)(c)(ii). The order changed two phrases and left the commencement dates as they were.[31]

5. Critical analysis

5.1 Consent

The Act leans heavily on consent, and section 6 is carefully drafted. The difficulty lies elsewhere. Most people meet consent as a screen they must accept to use a service, and the requirement that consent be "unconditional" does not by itself stop a service from making access depend on data it truly needs. A person who wants a ride-hailing app has no practical choice about sharing location. The Act narrows the problem by limiting consent to the data necessary for the stated purpose, but "necessary" is first answered by the Data Fiduciary and reaches the Board only if someone complains.

Consent Managers are the Act's main answer. A Consent Manager is a registered entity through which a Data Principal can give, manage, review and withdraw consent across services.[32] The idea is promising, though it is untested at scale in this form, and its success will depend on whether people actually use such intermediaries rather than click through as before.

5.2 The State and the exemptions

The sharpest difference in the Act's treatment of private and public actors lies in sections 7 and

ISSN: 2582-6433

17. Under section 7 the State may process personal data without consent to provide subsidies, benefits and services and to perform functions under law.[33] Under section 17(2)(a), the Central Government may by notification exempt any instrumentality of the State from all or any provisions of the Act, in the interests of sovereignty and integrity, security of the State, friendly relations with foreign States, public order or preventing incitement to a cognisable offence.[34] Section 17(1)(c) separately switches off the notice, consent and rights provisions where data is processed to prevent, detect, investigate or prosecute offences.[35] Section 36 allows the Central Government to call for information from the Board, from any Data Fiduciary and from any intermediary.[36]

Measured against the four *Puttaswamy* requirements, these provisions meet the first two. Each rests on a statute and names a legitimate aim. The difficulty lies with the other two. Section 17(2)(a) permits the exemption of an entire instrumentality from the entire Act, which is hard to reconcile with a proportionality inquiry that looks at whether the means are no wider than the aim requires. The text also points to no independent review of such a notification and no duty to publish reasons for it.

The Supreme Court has been firm that executive action touching fundamental rights must be proportionate, supported by reasons and open to judicial review. In *Anuradha Bhasin v Union of India* it applied that standard to orders suspending internet services.[37] The same expectations ought to apply to a notification under section 17(2)(a), although the Act does not say so. Whether courts will read them in is the open question.

5.3 The amendment to the Right to Information Act

Section 44(3) of the DPDP Act rewrote section 8(1)(j) of the Right to Information Act, 2005, and it came into force on 13 November 2025.[38] Before the amendment, personal information could be withheld only where it had no relationship to any public activity or interest, or where its disclosure would be an unwarranted invasion of privacy, and even then it had to be disclosed if the larger public interest justified it.[39] The amended clause exempts "information which relates to personal information" without those qualifications.

This is the clearest point at which the privacy statute cuts into another right. The earlier clause already weighed privacy against the public interest, and it did so case by case. The amendment removes the weighing. Records of public work, such as beneficiary lists or the names of officials on a contested decision, can contain personal information, and a public authority now has a statutory reason to refuse them. *Puttaswamy* recognised privacy as a right, but it never

ISSN: 2582-6433

treated privacy as a trump over every competing interest, and the amendment sits uneasily with that approach.

5.4 The independence of the Board

A data protection law is only as strong as the body that enforces it. The Board consists of a Chairperson and Members whom the Central Government appoints, and the Act provides for a short term, which may be renewed.[40] A body that depends on the executive for appointment and re-appointment will find it harder to decide against the executive, and the State is likely to be a frequent respondent given the breadth of its own processing. The Board's dependence on the executive is therefore a structural concern, not a matter of personalities.

The Board is also not yet operational in practice. The Ministry of Electronics and Information Technology invited applications for the posts of Chairperson and Members in May 2026,[41] and appointments had not been reported when this paper was written. Until the Board sits and the penalty provision commences, the Act's enforcement machinery exists mainly on paper.

5.5 Remedies for the individual

Under section 43A, a person who suffers wrongful loss because a company was negligent with sensitive data can claim compensation.[42] The DPDP Act replaces that with a penalty paid to the State. Sums the Board recovers go to the Consolidated Fund of India, not to the person harmed,[43] and the Act gives the Data Principal no right to compensation. Section 39 meanwhile bars civil courts from entertaining suits on matters the Board is empowered to decide.[44]

The practical result is that a person whose data is leaked can complain to the Board, which can fine the company, but no provision of the Act lets the Board award that person a sum for the harm. When section 43A is omitted on 13 May 2027, the one statutory route to compensation will go with it. Whether general remedies in tort or contract survive the bar in section 39 has not been tested. Until it is, individuals have reason to be uncertain about what the Act gives them when their data is misused.

6. Conclusion and suggestions

The DPDP Act and Rules give India a working data protection framework, and in its dealings with private organisations the framework is fairly detailed. Data Principals receive notice, a standard of consent, rights of access and correction, and a grievance route. Data Fiduciaries face specific duties on security, breach notification and children's data. These are real gains over a regime that rested on a single compensation provision.

The weaker side of the framework is the one *Puttaswamy* was most concerned with, which is

ISSN: 2582-6433

the relationship between the individual and the State. Broad exemptions by notification, the narrowing of the Right to Information Act, a Board that depends on the executive and the absence of any compensation route all point the same way. Four changes would address most of this. First, notifications under section 17(2)(a) should be published with reasons and made expressly open to judicial review. Second, the public-interest test in section 8(1)(j) of the Right to Information Act should be restored by legislative amendment, since subordinate rules cannot undo a statutory text. Third, Board Members should have longer fixed terms without renewal and a selection process that is open to scrutiny. Fourth, the Act should give the Data Principal a right to compensation, or section 43A should stay in force until it does.

The first decisions of the Board, once penalties become enforceable in May 2027, will show which reading of these provisions prevails.

[1] *Justice KS Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1.

[2] Digital Personal Data Protection Act 2023 (Act 22 of 2023), assented to on 11 August 2023.

[3] Digital Personal Data Protection Rules 2025, GSR 846(E) (13 November 2025), as corrected by GSR 892(E) (10 December 2025).

[4] Information Technology Act 2000, s 43A, read with the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.

[5] *MP Sharma v Satish Chandra* AIR 1954 SC 300; *Kharak Singh v State of UP* AIR 1963 SC 1295.

[6] *Puttaswamy* (n 1).

[7] *Puttaswamy* (n 1) (Chandrachud J, plurality opinion).

[8] *Justice KS Puttaswamy (Retd) v Union of India* (2019) 1 SCC 1.

[9] Committee of Experts under the Chairmanship of Justice BN Srikrishna, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (Ministry of Electronics and Information Technology 2018).

[10] DPDP Act (n 2) s 3(a).

[11] DPDP Act (n 2) s 2.

[12] Srikrishna Committee report (n 9).

[13] DPDP Act (n 2) s 3(b).

[14] DPDP Act (n 2) s 4.

[15] DPDP Act (n 2) s 5; DPDP Rules (n 3) r 3.

[16] DPDP Act (n 2) s 6(1).

[17] DPDP Act (n 2) s 6(4).

[18] DPDP Act (n 2) s 7.

[19] DPDP Act (n 2) s 8(5)–(7).

[20] DPDP Act (n 2) s 9; DPDP Rules (n 3) rr 10–11.

[21] DPDP Act (n 2) s 10.

[22] DPDP Act (n 2) ss 11–14.

[23] DPDP Act (n 2) s 15.

[24] Notification GSR 844(E) (13 November 2025) establishing the Data Protection Board of India under DPDP Act

ISSN: 2582-6433

(n 2) s 18.

[25]Notification GSR 845(E) (13 November 2025), made under DPDP Act (n 2) s 19.

[26]DPDP Act (n 2) ss 27–29.

[27]DPDP Act (n 2) s 33 and Schedule.

[28]Notification GSR 843(E) (13 November 2025) under DPDP Act (n 2) s 1(2); DPDP Rules (n 3) r 1.

[29]DPDP Act (n 2) s 44(2)(a); GSR 843(E) (n 28).

[30]DPDP Rules (n 3) r 4.

[31]Digital Personal Data Protection (Removal of Difficulties) Order 2026, SO 5458(E) (5 October 2026).

[32]DPDP Act (n 2) s 6(7)–(9); DPDP Rules (n 3) r 4.

[33]DPDP Act (n 2) s 7.

[34]DPDP Act (n 2) s 17(2)(a).

[35]DPDP Act (n 2) s 17(1)(c).

[36]DPDP Act (n 2) s 36.

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

[38]DPDP Act (n 2) s 44(3); GSR 843(E) (n 28).

[39]Right to Information Act 2005, s 8(1)(j) (before amendment by DPDP Act (n 2) s 44(3)).

[40]DPDP Act (n 2) ss 19–20; DPDP Rules (n 3) r 17.

[41]Ministry of Electronics and Information Technology, F No 2(1)/2026-Pers.I (6 May 2026), inviting applications for the posts of Chairperson and Members of the Data Protection Board of India.

[42]Information Technology Act 2000 (n 4).

[43]DPDP Act (n 2) s 34.

[44]DPDP Act (n 2) s 39.