INTERNATIONAL JOURNAL OF JURIDICAL SCIENCE AND POLICY (IJJSP)

VOL. 1 · ISSUE 1 · 2026

EDITOR IN CHIEF

Mr. Ashish Kaushik

CENTRE FOR JURIDICAL SCIENCE AND POLICY RESEARCH

VOL. 1 — ISSUE 1

THE DPDP MOMENT: RETHINKING DATA PRIVACY LAWS IN INDIA

Vidhushi Bhati, Research Scholar (Ph.D.), Noida International University, Noida, Uttar Pradesh.,India.[1]
Dushyant Chaudhary, Research Scholar (Ph.D.), Noida International University, Noida, Uttar Pradesh,India.[2]

ABSTRACT

India's data privacy laws have changed a lot over the ten years. Now we have the Digital Personal Data Protection Act of 2023 and the Digital Personal Data Protection Rules of 2025. These laws have created a system that is based on principles. This research looks at how things have changed from an policy point of view. It also considers the case of Justice K.S. Puttaswamy versus the Union of India which said that people have a right to privacy according to the Constitution. It looks at the bodies that now oversee the processing of personal data, such as the Data Protection Board of India, the Consent Manager ecosystem and the new obligations imposed on Significant Data Fiduciaries. It also talks about the differences between the Indian framework and the General Data Protection Regulation. It says that the General Data Protection Regulation is risk based, whereas the Indian framework is consent and notification based. Emerging and trend-setting issues are examined in detail such as how to govern AI and algorithmic decision-making, the conflict between data localisation and India's plans for a Digital Public Infrastructure, dark patterns in platforms that users interact with and the three-stage enforcement timeline that ends in May 2027. The report finds that non-personal and non-digital data, independence of the regulatory Board and the impact of compliance on start-ups and micro, small and medium-sized businesses are still areas where there are gaps. India has a comprehensive set of laws to protect data privacy, but their effectiveness will depend on the strictness of enforcement, the attention they receive from the courts, and the degree of stakeholder involvement during the implementation period.

Keywords: *Data Privacy; Digital Personal Data Protection Act, 2023; Right to Privacy; Data Protection Board of India; Algorithmic Accountability*

[1] Research Scholar (Ph.D.), Noida International University, Noida, Uttar Pradesh.
[2] Research Scholar (Ph.D.), Noida International University, Noida, Uttar Pradesh.

INTRODUCTION

Within a single generation, the right to informational privacy has risen from the outskirts of Indian constitutional debate to the forefront of the country's digital governance agenda. India now has one of the world's largest collections of digitised personal data, thanks to the Aadhaar biometric identity system, the Unified Payments Interface, e-governance portals, and a growing number of mobile applications and social media platforms. This level of digitisation has resulted in a corresponding level of vulnerability: data breaches affecting government databases, health records, and financial platforms have become commonplace in the news cycle, while citizen profiling via algorithmic systems raises concerns that extend far beyond the traditional vocabulary of Indian privacy law.

Throughout its post-independence history, India lacked a legislated data protection act. Privacy safeguards were spread over contract law, tort principles, and the minimal provisions of the Information Technology Act of 2000, which were enhanced by the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules of 2011. With the advent of data-driven business models, cloud computing and cross-border data flows, this fragmented approach became less effective as the Indian economy underwent change. The Supreme Court's nine judgment bench decision, upholding privacy as a fundamental right, which is intrinsic to the right to life and personal liberty guaranteed under Article 21 of the Constitution, compelled the state to come up with a detailed legislative response.

This paper studies that reaction, as it exists in 2026, in the form of a statutory regime established under the Digital Personal Data Protection Act of 2023 and implementing statutory rules (DPDPR Rules) notified in November 2025, and which is now under a three-stage phased implementation plan that will end in May 2027.[3] The paper is organised to first trace the historical and constitutional evolution of privacy protection in India, then examine the current regime's substantive and institutional architecture, before concluding with a comparative analysis of international frameworks and a discussion of the trend-defining issues that will shape the next phase of India's data governance journey.

[3] S. Rajagopal & Anirudh Burman, *India's Data Protection Journey: An Institutional Perspective* (Carnegie India, Working Paper No. 4, 2023).

THE EVOLUTION OF DATA PRIVACY LAW IN INDIA

1. The Pre-Statutory Era

Before 2023, Indian data protection law was mainly governed by Section 43A of the Information Technology Act, 2000, which imposed civil liability on a body corporate for failure to implement reasonable security practices while handling sensitive personal data, and Section 72A which penalised the unauthorised disclosure of personal information obtained under a lawful contract.[4] The 2011 Rules under Section 43A defined sensitive personal data and required consent and disclosure but were limited in scope, had weak enforcement mechanisms and mainly applied to corporate entities, not government agencies, which hold some of the biggest collections of citizen data in the country.[5]

2. The Puttaswamy Moment

The constitutional foundation for an all-encompassing privacy law was laid in 2017 when a nine-judge bench of the Supreme Court unanimously held that the right to privacy is a fundamental right under Part III of the Constitution, emanating from the guarantees of life and personal liberty under Article 21, and the freedoms enumerated under Article 19.[6] The judgment was significant not only for its constitutional holding but also for its precise articulation of informational privacy as a unique aspect of the right, and for its explicit invocation of the state to establish a robust data protection regime. This ruling moved data protection from a matter of policy discretion to that of constitutional obligation and set in motion the legislative process that would end six years later in the DPDP Act.

3. From the Srikrishna Committee to the DPDP Act, 2023

Following the Puttaswamy judgment, the Government of India set up a committee of experts, headed by Justice B.N. Srikrishna, to suggest a data protection framework.[7] In its 2018 report and draft law, the committee introduced principles that would echo throughout the

[4] The Information Technology Act, No. 21 of 2000, §§ 43A, 72A.
[5] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, G.S.R. 313(E) (India).
[6] *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1 (India).
[7] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* 1-30 (Ministry of Electronics and Information Technology, Government of India, 2018).

legislative road to follow, including the designation of data fiduciaries and data principals, purpose limitation and a dedicated regulatory authority.[8] Subsequent versions of the bill – one introduced in Parliament in 2019, and a revised draft released for public consultation in 2022 – gradually scaled back the regulatory architecture, moving away from the more prescriptive, GDPR-inspired approach of the original draft in favour of a more streamlined, consent-and-notice-based framework. The change was praised and criticised by commentators[9] alike. The culmination of this process was the enactment of the Digital Personal Data Protection Act, 2023, which was given Presidential assent in August 2023 and for the first time, established a single statutory system to oversee the processing of digital personal data in India.[10]

4. Operationalisation: The DPDP Rules, 2025

The DPDP Act was designed purposely as a principle-based law, with a lot of the practical complexity to be set out in delegated legislation. This vacuum was bridged after two years when the Ministry of Electronics and Information Technology notified the Digital Personal Data Protection Rules, 2025 after a public consultation process that attracted several thousand submissions from stakeholders.[11] The Rules were notified on 13 November 2025 and published in the official Gazette on 14 November 2025. The Rules lay down the procedural mechanics of consent, breach notification, the registration of Consent Managers and the specific requirements that apply to Significant Data Fiduciaries.[12] The Rules, read together with a separate Enforcement Notification issued the same day, create a phased three-stage compliance timeline that is staggered to give businesses, especially start-ups and micro, small and medium enterprises, sufficient time to adapt their systems before the regime becomes fully binding.

[8] Ministry of Electronics and Information Technology, Gov't of India, Personal Data Protection Bill, 2018 (Draft Bill accompanying the Srikrishna Committee Report) (2018).
[9] Vrinda Bhandari & Renuka Sane, *A Critique of the Personal Data Protection Bill, 2019*, 4 *IND.. J.L. & Tech.* 88, 91-95 (2019).
[10] The Digital Personal Data Protection Act, 2023 (India).
[11] Digital Personal Data Protection Rules, 2025, G.S.R. 700(E), Gaz. India (Nov. 14, 2025) (India) [hereinafter *DPDP Rules*].
[12] Press Release, Ministry of Elecs. & Info. Tech., Gov't of India, *DPDP Rules, 2025: A Citizen-Centric Framework for Privacy Protection and Responsible Data Use* (Nov. 14, 2025).

Highlights of the DPDP Act

Key Definitions and Scope

The DPDP Act applies to the processing of digital personal data in India and also applies extraterritorially to the processing of personal data outside India, if such processing is in relation to the offering of goods or services to the individuals in India. The statute's key features are the responsibilities of the Data Principal (the person the personal data is about) and the Data Fiduciary (the body that determines the purpose and means of processing).[13] Data Fiduciaries will have enhanced obligations, and those who process large amounts of sensitive data will be called Significant Data Fiduciaries. It is noteworthy that the Act diverges from comparative models such as the GDPR, which do not establish a separate category of sensitive personal data, but rather apply a largely uniform set of obligations across categories of personal data, with the data of children, defined uniformly as all individuals below the age of eighteen, being afforded enhanced protection.

The Data Protection Board of India

The Act established the Data Protection Board of India as the apex adjudicatory and enforcement authority with powers to investigate breaches of the Act, impose penalties and issue directions to Data Fiduciaries.[14] The Board's initial and administrative provisions took effect immediately on notification of the Rules in November 2025, with the full force of its adjudicatory powers (excluding functions relating to Consent Managers) coming into force in the third and final phase of implementation under the staged implementation timeline.[15] The composition and appointment process of the Board, including the establishment of a search-cum-selection committee for its members, has generated scholarly interest, and in particular questions of institutional independence from the executive, a concern that recurs in comparative data protection literature wherever a regulator is appointed by, and answerable to, the same government whose own data practices it may have to scrutinise.[16]

[13] Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023, §§ 2(j), 2(v) (India).
[14] DPDP Act, 2023, § 33 (India).
[15] Min. Of Elecs. & Info. Tech., Notification on Establishment and Composition of the Data Protection Board of India (Nov. 13, 2025) (India).
[16] Anirudh Burman, *Understanding India's New Data Protection Law*, Carnegie India 2–3 (2023).

Consent Managers

The Indian system has a unique element in the shape of the Consent Manager, an interoperable platform that enables Data Principals to give, withdraw, evaluate and manage consent for numerous Data Fiduciaries through a single interface, which is not directly comparable to the GDPR. The DPDP Rules specify detailed eligibility criteria for entities to get registered as Consent Managers, including minimum net worth, incorporation as an Indian company, certified technical interoperability standards and conflict-of-interest safeguards to ensure that Consent Managers are not unduly influenced by the Data Fiduciaries whose consent flows they manage. [17]This institutional innovation is inspired by the broader Digital Public Infrastructure ideology of India as exhibited in the Account Aggregator architecture in the financial industry and is a distinctly Indian method to operationalising consent at a population size.[18]

Obligations of Data Fiduciaries and Significant Data Fiduciaries

All Data Fiduciaries will be expected to give explicit and itemised notice to the Data Principals before processing their personal data, take adequate security safeguards and report personal data breaches. Unlike many similar jurisdictions, the Rules currently do not set any materiality threshold for breach reporting, so that, on a literal interpretation, almost any breach must be informed to the Board and affected people, with a comprehensive report expected within seventy-two hours. Significant Data Fiduciaries have additional responsibilities including appointment of a Data Protection Officer based in India, conducting periodic Data Protection Impact Assessments and independent audits, and a duty of algorithmic due diligence to ensure that automated processing systems, including algorithmic software, do not pose risks to the rights of Data Principals.[19] The Rules also leave the possibility open of data localisation for certain categories of personal data to be disclosed by the Central Government, on the proposal of a committee named in the Rules, however the exact limits of this requirement remain, as yet, undefined.

COMPARATIVE PERSPECTIVES: THE DPDP ACT AND THE GDPR

[17] DPDP Rules, r. 4, sch. 1.
[18] DPDP Rules, r. 4, sch. 1.
[19] Digital Personal Data Protection Rules, 2025, r. 6, sch. 2 (India).

Comparative analysis of European Union General Data Protection Regulation brings out the ambience and individuality of the Indian approach. While the GDPR recognises six alternative lawful bases for processing personal data, including legitimate interest and contractual necessity, the DPDP Act adopts a narrower architecture in which consent operates as the primary lawful basis, supplemented by a closed list of 'certain legitimate uses' that permit processing without consent in specified circumstances, such as for the performance of state functions or in medical emergencies.[20] Under the GDPR, the requirement to notify a breach is risk based and only applies if the breach is likely to result in harm to individuals. This is contrasted with the DPDP Rules where the reporting responsibility appears to be unqualified. The penalty structures also differ sharply. While the GDPR allows for penalties up to four percent of an undertaking's global annual turnover, the DPDP Act limits penalties to a fixed rupee amount in hundred crores, which, while still significant, does not scale with the size of the offending enterprise in the same proportionate manner.

Simultaneously, the Indian system has significant structural similarities to its European parent, such as extraterritorial application, a specialised regulatory authority, and strengthened safeguarding for the personal data of children. The comparison indicates that India has deliberately opted for a lighter-touch, more implementation-friendly model, appropriate to its particular economic composition, where a large proportion of data-controllers are small and resource-constrained, rather than simply copying the compliance-heavy architecture of the European regulation wholesale.

EMERGING ISSUES of DPDT Act

Artificial Intelligence and Algorithmic Accountability

[20] GDPR: 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), 2016 O.J. (L 119) 1.

The growing deployment of generative and predictive artificial intelligence systems in Indian financial services, healthcare, and e-governance has pushed algorithmic responsibility to the forefront of the current privacy discussion.[21] The DPDP Rules' requirement that Significant Data Fiduciaries exercise due diligence over algorithmic software is an early, albeit modest, legislative acknowledgement of this concern, but it falls short of the more granular obligations found in emerging international instruments governing automated decision-making, explainability, and the right to contest algorithmic outcomes. As AI-powered credit scoring, insurance underwriting, and content moderation systems become more prevalent, Indian regulators will face increasing pressure to establish clearer rules for algorithmic transparency and redress.

Data Localisation and Digital Public Infrastructure

India's Digital Public Infrastructure projects – Aadhaar, Unified Payments Interface and the Account Aggregator ecosystem – have made it a prominent global example of state-led digital transformation. This achievement has also fanned the flames of controversy about data localisation, with sectoral authorities in banking and payments long requiring in-country storage of some classes of data. There is a tension between the comparatively liberal approach to cross-border data transfer under the DPDP Act, which allows such transfers except to jurisdictions restricted by government order, and the possibility under the Rules for the government to notify certain categories of personal data that Significant Data Fiduciaries shall not transfer outside India. The resolution of this dispute – whenever the required notification is released – would have major ramifications for cloud infrastructure investment and the operations of multi-national technology enterprises in India.

Dark Patterns and Consent Fatigue

An additional trend influencing Indian privacy discourse is the governmental response to deceptive design tactics, known as dark patterns, that digital platforms use to push users to share more data than they might otherwise wish to. Under consumer protection legislation, the Central

[21] Rahul Matthan, *Privacy 3.0: Unlocking Our Data-Driven Future* 45–62 (2018).

Consumer Protection Authority has already issued guidance on similar activities.[22] The DPDP Rules' emphasis on explicit, itemised and non-bundled permission letters might be interpreted as a parallel privacy-legal remedy to the same underlying problem. The real challenge ahead is to ensure that the giving of consent does not become a ritual that leads to fatigue, particularly considering that the DPDP Rules require notices to be made available in twenty-two scheduled Indian languages, a linguistically ambitious mandate that will test the design capacities of digital platforms at a national scale.

The Phased Enforcement Trajectory

Perhaps the single most important procedural development is the phased, three-stage enforcement architecture itself. The first phase, which came into force in November 2025, initiated the administrative life of the Board. Phase two, in November 2026, will operationalise the Consent Manager registration scheme. The third and final phase, due in May 2027, will see the substantial core of the Act come into force, including notification requirements, breach reporting and the entire range of obligations for Significant Data Fiduciaries. The graduated approach is purposefully set up to avoid a sudden compliance shock for start-ups and smaller firms, and 2026 will be a key year of planning and testing for Indian companies and their global counterparts, even as the Act's major obligations only become fully enforceable the following year.

CHALLENGES

The DPDP Act & Rules is a step in the right direction, but there are a number of deficiencies that should be explored. First, the Act applies only to digital personal data, and non-digital and non-personal data are completely outside its scope. This limitation is becoming increasingly artificial as physical and digital records converge by means of scanning, digitisation drives and hybrid record-keeping practices across Indian government departments.

Secondly, there are worries over the independence of the Data Protection Board. The Board members are appointed through a search-cum-selection process formed by the government and

[22] Central Consumer Protection Authority, *Guidelines for Prevention and Regulation of Dark Patterns, 2023*, Gazette of India (Nov. 30, 2023).

its functioning, at least in its initial phase, is tightly related to the executive branch. In other jurisdictions, the credibility of a data protection regulator is seen to depend a lot on its perceived and actual insulation from the very government bodies that it is meant to oversee, particularly when public authorities in India including welfare and law-enforcement agencies are themselves major processors of personal data.

Thirdly, the absence of a clear threshold for breach notification, while in the abstract protective of Data Principals, has the potential to cause notification fatigue amongst regulators and the public alike, if the threshold is interpreted literally for every trivial security incident, diluting the significance of reports pertaining to truly serious breaches.

Fourth, the compliance burden of itemised, multilingual notices, breach response protocols and, for Significant Data Fiduciaries, annual audits and impact assessments, is a proportionately greater challenge for micro, small and medium enterprises than for large, well-resourced technology firms, raising questions about the practical accessibility of the regime for India's vast base of smaller digital businesses despite the extended implementation timeline.

Finally, the interaction of the DPDP framework with sector-specific regulations, including those issued by the Reserve Bank of India, the Insurance Regulatory and Development Authority and the Telecom Regulatory Authority of India, remains to be fully harmonised, which risks creating overlapping or inconsistent obligations for entities operating in multiple regulated sectors.

CONCLUSION

India's transition from a fragmented, sectoral approach to data protection to a comprehensive legislative regime rooted in the DPDP Act, 2023 and the DPDP Rules, 2025, represents both constitutional need and economic pragmatism. The staggered rollout of the

framework to May 2027 is a wise compromise between the immediacy of safeguarding a fast digitising populace of over a billion people and the practical realities of a business ecosystem dominated by small and medium companies. But a law wording, no matter how finely calibrated, cannot itself ensure real privacy protection. The ultimate test of India's new data protection regime will be the independence and rigour of the Data Protection Board, the government's willingness to put its own data practices under the same scrutiny as private actors, and the ability of ordinary citizens to exercise meaningful control over their personal data through the Consent Manager ecosystem and allied mechanisms. As artificial intelligence, cross-border data flows, and the Digital Public Infrastructure goal keep evolving, India's data privacy law will require continued legislative attention and judicial vigilance to remain responsive to the technologies and harms of the future decade.

In light of the preceding analysis, this paper makes the following recommendations. The Data Protection Board's appointment procedure should be changed to increase court and civil society participation, thereby improving its perceived and functional independence. The Central Government should make it clear as soon as possible how data localisation works for SDFs, as this will have significant consequences for infrastructure planning for affected enterprises. A threshold for notification of breaches should be adopted, based on risk, rather than whether the breach is serious enough to warrant notification, in order to ensure that breaches are reported only when they are serious. The sectoral regulators should be instructed to harmonize their existing Data Governance rules with DPDP rules to eliminate duplicative and contradictory compliance obligations. Lastly, sustained efforts in digital literacy and public awareness campaigns in multiple languages will be needed to make the Act's consent process into one that results in informed and real consent decisions, instead of being a formality for India's diverse citizenry.