Shodhbodhalaya: An International Peer reviewed
Multidisciplinary Journal
Volume 4 | Issue 2 | ISSN: 2584-1807 | (https://shodhbodh.com/)

From initial draft to Legislation: Tracing the evolution of Digital Personal Data Protection Act, 2023

Ms. Chesta

Assistant Professor, Department of Commerce

Chaudhary Ranbir Singh University, Jind, Haryana

Email id- chestabansal86@gmail.com

Abstract

The timeline of the evolution of the Indian privacy and personal data protection regime includes several constitutional, philosophical and legislative developments culminating in the passing of the Digital Personal Data Protection Act (DPDP Act), 2023 and the Digital Personal Data Protection Rules (DPDP Rules), 2025. The article traces the evolution of the privacy jurisprudence in India from the philosophical concepts of dignity, autonomy and informational self-determination to the ultimate recognition of privacy as a fundamental right in Justice K.S. Puttaswamy v. Union of India, the recommendations of the Srikrishna Committee, the controversial provisions of the 2019 Personal Data Protection Bill, the scrutiny by the Joint Parliamentary Committee and its subsequent withdrawal, and the transition to the simplified compliance-based structure under the DPDP Act, 2023. The paper analyses the fiduciary model of the Act, legal and transparent data processing, simplified rights of the Data Principal, cross-border data transfer, enforcement mechanisms before the Data Protection Board, and how these impact the regulation of consent, data breach notifications, and child data protection under the DPDP Rules, 2025. Furthermore, it traces India's journey of balancing personal privacy, economic innovation, and state interests to establish itself as a leading global player in digital governance and data regulation.

Keywords; Digital Personal Data Protection Act, Data Privacy, Puttaswamy Judgment, Data Fiduciary, Data Protection Board, Cross-border Data Transfer, Data Processing.

1. Introduction

Over the past decade, India's digital economy has transformed. Technology has become a part of the daily lives of over a billion people. The exponential proliferation of digital public infrastructure, Digital commerce, Digital governance, and innumerable other uses of technology required the establishment of a strong legal framework that could deliver technology-based innovation while safeguarding the fundamental rights of individuals. India's data protection framework has not only witnessed legislative actions but also evolved philosophically, constitutionally, and economically as part of a justifiable cost-benefit analysis. This journey culminated with the enactment of the Digital Personal Data Protection (DPDP) Act of 2023 and the coming into effect of its detailed Rules in November 2025. The legal regime seeks to strike the right balance between state security, commercial interests, and individual privacy rights in the context of a rapidly digitising environment (Ministry of Electronics and Information Technology, 2025a).

The legislative text in its current form in 2023 is a descendant of the philosophical inquiries into the self, the landmark judicial pronouncements that held the right to privacy to be a part of an individual's intrinsic rights and the lengthy debates that were held in the Parliament fine-tuning the architecture of an institution for regulating the data (National e-Governance Division, 2026a). The report traces the history of the right to privacy from its philosophical construct as a constitutional concept, to the interpretation of the Supreme Court, the first drafts of the Bill by the Srikrishna Committee, debates on the Bill in 2019, the recommitment towards a new journey culminating in the DPDP Act, 2023 and the DPDP Rules, 2025.

2. The Philosophical and Historical Foundations of Privacy

The philosophical roots of the right to privacy later made it possible to conceptualise data privacy as a legal right. Many scholars have described the right to privacy as a moral instinct as old as human civilization itself, with its roots in the human belief that each person has an inviolable and sacred inner world which others cannot breach without consent (NeGD, 2026a). While the word 'privacy' was not used in constitutional law, its essence was embraced in custom, for example ancient temples had a sacred area, common law protected a home as a person's castle and active communication through letters was protected

as it was widely understood that reading a private letter was an infringement of personal integrity (NeGD, 2026b).

2.1 The Western Philosophical Tradition

Modern privacy laws can be traced philosophically to Western political theory such as the natural law of John Locke, particularly his concept of "property in the person", creating a vocabulary for specifying what exactly is violated when the self is violated by a second party (NeGD, 2026a). The equal dignity of all human life was further reinforced by Immanuel Kant's moral philosophy, particularly his categorical imperative: each person must be treated as an end in themselves and never as a means to an end. Spying on a person's private life, extracting their data, or exposing their intimacies without their consent violates the Kantian imperative and fails to treat them as a person with equal moral worth. Rather, it treats them as mere data points for commercial exploitation (NeGD, 2026a).

2.2 Dignity, Autonomy, and Informational Control

Contemporary privacy jurisprudence is largely derived from three different 19th and 20th century philosophical foundations. The first, dignity, can be understood as self-worth. Continuing the argument made by Samuel Warren and Louis Brandeis in their 1890 Harvard Law Review article "The Right to Privacy" that the common law has always recognised a general right "to be let alone", philosopher Edward Bloustein argued in 1964 that all privacy invasions, including physical intrusions, violate human dignity (NeGD, 2026a) by treating the body, image or information as a public object, irrespective of any effect on reputation or emotion.

The second pillar is Autonomy. John Stuart Mill argued that privacy is strictly essential to protect an individual to conduct "experiments in living" and to make non-conformist and even socially unacceptable choices free from the crushing pressure of a watching society (NeGD, 2026a). In the context of the internet, theorists like Julie Cohen and Jennifer Nedelsky have adapted the schema, arguing that privacy exists to protect the dynamic subjectivity and relational autonomy of individuals from commercial and state attempts to bring human action to full transparency (NeGD, 2026a).

The third principle is Informational Control. Ferdinand Schoeman argued that the control of personal information is constitutive of selfhood and trust. Alex Pentland and Daniel Solove said that, in the digital age, data aggregation poses a danger: separately, a person's daily travels, health web searches or purchase history do not seem that interesting, but a highly private, detailed and dangerous profile can be constructed about that person without their knowledge or consent (NeGD, 2026a). This philosophical understanding of informational control later informed the concepts of data minimization and purpose limitation adopted into Indian law.

3. Constitutional Maturation: The Evolution of Indian Jurisprudence

While the generally accepted philosophical underpinnings of privacy are firmly established in global legal systems, the question of its jurisprudence in India has followed a convoluted path from its absolute denial as a fundamental right to its unanimous affirmation as a constitutionally guaranteed right in India.

3.1 Early Judicial Interpretations

The judiciary was reluctant to read the right to privacy into the Constitution for the first two decades of the Republic. In the landmark case of M.P. Sharma v. Satish Chandra (1954), an eight-member Supreme Court bench held that the Constitution of India did not guarantee the right to privacy as guaranteed by the Fourth Amendment of the Constitution of the United States (NeGD, 2026a). This narrow view was reiterated almost a decade later in Kharak Singh v. State of Uttar Pradesh (1963), where it was held by a six-judge bench of the Supreme Court that privacy was not guaranteed as a fundamental right, though Justice Subba Rao dissented on the view, seeing privacy as part of personal liberty (NeGD, 2026a).

The tide was beginning to turn by the 1970s. In Gobind v. State of M.P. (1975), the Supreme Court stated that the right to privacy must cover the personal intimacies of the home, the family, marriage, motherhood, and child-rearing, and that the right to privacy was represented in the concept of "ordered liberty" (NeGD, 2026a). A series of Supreme Court judgements throughout the 1990s first extended the protection of Article 21 (right to life and personal liberty) and Article 19 (freedom of speech and expression) to include privacy, before the issue was brought to a constitutional showdown (NeGD, 2026a).

3.2 The Puttaswamy Landmark and the Triple Test

However, a major event in the history of data privacy in India occurred in 2017 when the Supreme Court of India delivered its judgment in the case of Justice K.S. Puttaswamy (Retd.) v. Union of India (Lok Sabha Secretariat, 2024). The petition was a public interest litigation that constituted a constitutional challenge to the Aadhaar program of the Government of India, a biometric identification system that collects fingerprints and iris scans and issues a unique twelve-digit number for distribution of government subsidies. The main issue before the Court was thus whether the Indian Constitution guaranteed a right to privacy, and whether compulsory Aadhaar infringed on that right (NeGD, 2026a).

A nine-judge constitutional bench unanimously held the right to be extended as natural and inalienable to all humans, stating, Privacy is a fundamental right intrinsic to life and personal liberty protected by Article 21 and the other provisions of Part III of the Constitution (NeGD, 2026a). Further, it held that there are three broad aspects of the right to privacy: spatial privacy, or the right to create private spaces, decisional privacy, or the right to make intimate personal decisions, and informational privacy, or the right to control the dissemination of personal information. (NeGD, 2026a).

Equally important for future digital law, the Court established the "Triple Test" (or proportionality test) which applies whenever the State violates an individual's right to privacy; three strict criteria must be met for the violation to be constitutional:

1. Legality: The action must be authorised by an existing law.

2. Legitimacy: The law must pursue a legitimate state aim (e.g. national security, prevention or detection of crime or distribution of social welfare).

3. Proportionality: The restriction on privacy must be proportionate, meaning the state must achieve its aim through the least intrusive mechanism possible (NeGD, 2026a).

Applying the above test to the Aadhaar architecture, the Court upheld the core of Aadhaar Act, 2016 that provides for delivery of state subsidies and benefits using the Aadhaar authentication, as it furthered legitimate state interests. At the same time, the Court struck down Section 57 of Aadhaar Act, which permitted private corporate entities to authenticate individuals using the Aadhaar number. The Court also

recognised the structural threat to privacy posed by profiling, whose authentication metadata can construct a highly intrusive profile of a person's habits, preferences, and affiliations (NeGD, 2026a). Most importantly, the Puttaswamy judgment imposed on the State a positive, categorical duty to create a "viable legal regime" protecting informational privacy, setting in train the executive and legislative machinery that would eventually produce the DPDP Act (NeGD, 2026b).

4. The Genesis of the Framework: The Srikrishna Committee (2017-2018)

The Ministry of Electronics and Information Technology (MeitY) has promptly responded to the constitutional vision articulated by the Supreme Court by conceptualising a thorough legislative framework. The MeitY, in 2017, constituted a high-level Committee of Experts under the chairmanship of Mr. B. N. Srikrishna, former Supreme Court Judge (MeitY, 2018a). The committee's terms of reference included study of privacy regimes around the world, review of India's socio-economic and digital ecosystem, and drafting of a data protection law which can balance the right to privacy and the development of a free digital economy (MeitY, 2018a).

4.1 The Conceptual Architecture: The Fiduciary Shift

On 27 July 2018, the Srikrishna Committee submitted its final report "A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians" along with the Draft Personal Data Protection Bill, 2018 (MeitY, 2018a) which acted as a basis for setting up the data protection regime in India as an alternative to the Western data regulatory models.

In the EU General Data Protection Regulation (GDPR), the relationship is that of the "Data Controller" (the organization that determines the purposes and means of processing data) and the "Data Subject" (the person) (NeGD, 2026b). The Srikrishna Committee has pointed out that the language in the GDPR is passive and does not highlight the imbalance of power in digital markets. Rather than adopting these, the committee introduced the Indian legal terms Data Fiduciary and Data Principal (NeGD, 2026b).

This was a masterstroke in legal terminology. The fiduciary relationship in Indian law carries the full weight of the meaning including supreme trust, strict accountability, and the highest duty of care (NeGD, 2026b). By using the term "Fiduciaries" for technology companies and governments, the report recognises that

these parties do not own the data, they are merely holding it in trust for the individual who remains the "Principal" (i.e., owner of the data) (Accountant General West Bengal, n.d.). One of the main objectives of the legislation is to provide a formal recognition of this "trust-based relationship" (NeGD, 2026b).

4.2 The 2018 Draft Bill and localization of the AIAM

The Draft Personal Data Protection Bill, 2018, drafted by the Srikrishna Committee, outlined a detailed rights-based data protection framework, identifying several foundational Data Principal rights based on the European Union model. This included the Right to Data Portability and Right to be Forgotten (Rajya Sabha Secretariat, 2022a). The committee delineated the Right to be Forgotten by stating that given the limitations of human memory in an otherwise permanent and limitless digital sphere, individuals have the right to correct or delete misleading or embarrassing historical data (Rajya Sabha Secretariat, 2022b).

Data localization provisions were also controversial in the 2018 draft (Maheshwari & Co., 2026). The committee wanted to ensure that the data of those in India remains sovereign and that Indian law enforcement officials have immediate access to the data that can assist the country in maintaining national security. Hence, it was decided that some types of sensitive personal data must be stored on Indian servers. Many in the global tech industry opposed this harsh localization requirement, arguing that it would lead to data silos within countries, a fragmented global internet, increased cost of doing business, and contradict India's ease of doing business (Carnegie Endowment, 2023).

5. The Legislative Crucible: The Personal Data Protection Bill, 2019

Following the draft prepared by the Srikrishna Committee and the modifications made by the Government of India, the PDP Bill 2019 was presented in the Lok Sabha by the Government of India on 11 December 2019 (Lok Sabha Secretariat, 2019a). The introduction of the PDP Bill 2019 in the Lok Sabha moved the data protection debate from the expert committee rooms to the political arena of the national legislature (Lok Sabha Secretariat, 2019b).

5.1 Architectural Ambitions of the 2019 Bill

The 2019 Bill, on the other hand, sought to create a thorough regulatory framework, retaining the Fiduciary/Principal nomenclature and principles. It also introduced strong citizen rights, with explicit

provisions for the Right to Data Portability and the Right to be Forgotten, which were understood as essential to ensuring that citizens had complete ownership and control over their data in the digital environment (Lok Sabha Secretariat, 2022a).

To enforce the law, the Bill provided for an independent Data Protection Authority (DPA) that could seek criminal prosecution and jail time for company officers who wilfully de-identified or otherwise incorrectly handled personal data. The government argued that such severe penalties were necessary to induce compliance from transnational companies for whom corporate fines would otherwise be merely seen as the cost of doing business.

5.2 Controversial Provisions: Section 35 and Non-Personal Data

Despite including added privacy protections, the 2019 Bill was criticised by civil society and legal scholars as well as the technology industry for some structural changes made to the Srikrishna Committee draft.

Outside the provisions on exemptions, Section 35 of the Act was the most controversial provision. The section allowed the Central Government to unconditionally exempt any government agency from the provisions of the Act, if the exemption was required on grounds of the sovereignty and integrity of India, the defence of India, relations of India with foreign states, or public order, as nominated in the section (Lok Sabha Secretariat, 2019c). A number of parliamentarians in the opposition and privacy activists argued that section 35 created a fatal structural imbalance: the Bill granted an unconditional exemption to the state, which would have rendered the proportionality test featured in the Puttaswamy judgment irrelevant, allowing for unlimited state surveillance and infringement of the privacy right.

In addition to the privacy protection, the 2019 Bill also empowers the government to mandate private companies to furnish de-identified data that is not of personal nature for the purpose of targeted policymaking and delivery of services to the public (Lok Sabha Secretariat, 2019d). Some commentators and lawyers have opposed the inclusion of non-personal data rules in the regulation as a matter of competition and intellectual property, completely tangentially related to the core objective of personal data privacy. They stated the bundling of personal and non-personal data rules into a single legislative act created confusion in the regulation (Carnegie Endowment, 2023).

6. Rigorous Scrutiny: The JPC Review (2019-2021): Final Report

Considering the law's complexity and the heated national discourse regarding its provisions, the Parliament accordingly referred the 2019 Bill to a Joint Parliamentary Committee (JPC), a committee of members from both the houses of Parliament, the Lok Sabha and the Rajya Sabha. Meenakashi Lekhi, helped by P.P. Chaudhary, then sat as chairman of the JPC (Lok Sabha Secretariat, 2019e).

The JPC conducted what is said to be one of the most wide-ranging consultative exercises ever carried out by a parliamentary committee in Indian history. Over the course of two years, the JPC held multiple sittings, and received and recorded written and oral deposition from hundreds of people, including tech bigwigs, Indian start-ups, civil rights organizations, legal experts and GoI ministries. To do this, the committee analysed the economic costs of data localization, the national security implications of cross-border data flows, and the technical implication of consent management.

On 16 December 2021, the Committee submitted its final report to the 17th Lok Sabha (JPC, 2021a). The report not only outlined several structural concerns with the 2019 draft Bill, but also made 81 suggestions for amendments to the Bill to illustrate the gravity of the recommended revisions (IndiaAI, 2022).

The JPC recommended that the law should also be applicable to non-personal data under the same Data Protection Authority. The JPC suggested that there should be a single data regulator for the whole country. The committee also recommended that social media should be regulated (JPC, 2021b). The JPC recommended that platforms like those Google, Twitter, and Facebook which are not mere intermediaries but which objectively curate content should be considered to be "publishers", and should therefore be stripped of the immunity provided by the safe harbor principle under Section 79 of the Information Technology Act, 2000. (Lok Sabha Secretariat, 2019f)

Moreover, the JPC reiterated the need for data localization, given the need for India's data sovereignty in light of rising geopolitical tensions, and growing cyberwarfare capabilities of adversaries. The number and depth of the 81 amendments so altered the 2019 Bill, that the JPC stated the original text was overloaded. It was thus an attempt to reconcile conflicting governmental objectives such as respect for individual privacy, national security, sovereign control over the information, and competition in digital markets within one statute.

7. Strategic Realignment: Withdrawal and the 2022 Conceptual Reset

After the submission of the JPC report, MEITY had to revisit the legislative approach, given that the 2019 Bill, even if passed with the 81 amendments recommended by the JPC, would be unimplementable and would place severe compliance burdens on India's startup ecosystem and disrupt the entire global digital economy working in India.

In 2022, the Government of India withdrew the Personal Data Protection Bill, 2019 on 8 August during the Monsoon Session of Parliament (Press Information Bureau, 2022a). Minister of Communications and IT Ashwini Vaishnaw justified that the Government of India had to withdraw the Bill because the JPC had made too many amendments requiring the Government to bring a new and thorough law incorporating personal data protection, regulation of telecommunications networks and systems, and other aspects of information technology (PIB, 2022b).

The reset was immediate: the draft Digital Personal Data Protection Bill, 2022 (MeitY, 2022a) was released by the government on 18 November 2022. This legislation is redefining the Indian regulatory landscape with its focus on simplicity, easier compliance and strict adherence to principles of privacy.

Changes were made in the 2022 draft to address earlier criticisms.

- Decoupling Non-Personal Data: The Bill's scope was limited to the safeguarding of digital personal data, entirely removing the controversial provisions on mandating the sharing of non-personal data. This brought the focus back to the protection of individual privacy (Carnegie Endowment, 2023).

- Relaxed Data Localization: The 2022 draft relaxed data localization given the internet's global nature and the absence of a direct correlation between physical location and effective data protection (MeitY, 2022b). Data could still be transferred across borders if made available to Indian authorities and when appropriate security safeguards were in place.

- Decriminalisation: In order to ease the process of doing business and remove any disincentives for innovation that criminal provisions put in place, the draft omitted all references to criminal provisions and imprisonment, replacing them with a strict regime of massive, deterrent financial penalties (Carnegie Endowment, 2023).

To prepare the 2022 draft, the Ministry put the Bill out for public consultation and received more than 22,600 comments from industry representatives, civil society, academics, and international bodies to ensure the Bill is evidence-based and practical (PIB, 2023a).

8. The Architecture of the Digital Personal Data Protection Act, 2023

The government introduced the rights-based Digital Personal Data Protection Bill, 2023 in Parliament after synthesising the feedback received on the draft 2022 consultations. The Bill was debated and passed in the Parliament and received the Presidential assent on 11 August 2023 (Gazette of India, 2023a). The DPDP Act, 2023 (Act No. 22 of 2023), provides for the protection of the personal data of digital citizens, balancing the fundamental right of individuals to protect their privacy, with the need of organizations to use data for creating innovative products and services that ease lawful economic growth (Gazette of India, 2023b).

8.1 The Seven Foundational Principles

The architecture of the DPDP Act, 2023 is based on seven globally accepted immutable principles of data protection (PIB, 2023b) :

1. Lawful, Fair and Transparent Use: Personal data should only be processed with the consent or for a legitimate purpose envisaged under the DPA, in a manner that is transparent to the Data Principal.

2. Purpose Limitation: Personal data should be used only for the purpose for which it was collected, unless new consent is obtained.

3. Data Minimization: Fiduciaries may only collect the minimum amount of personal data necessary for the performance of the declared purpose.

4. Data Accuracy: A Data Fiduciary has an affirmative duty to ensure that the personal data is accurate, complete, and kept up to date.

5. Storage Limitation: Personal data must not be held for longer than necessary: personal data relating to a data subject must be deleted once the specific purpose has been achieved.

6. Reasonable Security Safeguards: Fiduciaries must implement state-of-the-art technical and organisational measures to protect the data from unauthorised access and leaks.

7. Accountability: The Act provides for proceedings to be brought in respect of breaches of the Act and imposes very substantial financial penalties for non-compliance.

8.2. Obligations of Data Fiduciaries.

Chapter II of the Act imposes several obligations on the Data Fiduciaries. Section 4 of the Act imposes strict conditions for processing of personal data. Personal data can only be processed where there is a valid reason together with explicit consent, or there are "legitimate uses" (medical emergencies or provision of state benefits) (MeitY, 2023a).

Beyond these general principles, the Act also seeks to provide more granular requirements related to consent. Specifically, Section 5 requires that each request for consent must be presented with a clear, itemised notice of the specific data sought and the exact purpose of processing (MeitY, 2023a). Consent under Section 6 is stricter and must be "free, specific, informed, unconditional and unambiguous with clear affirmative action". The Act also states that where consent is needed, the burden of proving consent and notice lies with the Data Fiduciary (MeitY, 2023a). The Central Government may specify persons as "Significant Data Fiduciaries" (SDFs) based on the volume and sensitivity of data. As a result of these additional responsibilities, these SDFs are required to appoint a resident Data Protection Officer, conduct independent data audits, and complete periodic Data Protection Impact Assessments (PIB, 2023c).

8.3 Rights and Duties of Data Principals

Chapter III essentially empowers the Indian citizen, who is now termed as a Data Principal in law, with rights that are easily accessible in practice.

- Right to Access: The Data Principals have the right to obtain a summary of the personal information processed by the Data Fiduciary and the identity of third-party Data Fiduciaries or Processors to whom such information is shared (MeitY, 2023a).

- Right to Correct and Delete: The Fiduciaries may be directed by the Principal to correct inaccurate data, complete incomplete data, update outdated data, or delete data no longer required for the stated purpose (MeitY, 2023a).

- Right to Nominate: A world-first, Section 14 enables an individual to designate another person as an agent to exercise personal data rights in the case of the data principal's death or physical/mental incapacity, thus ensuring the continuity of the data principal's digital rights despite physical/mental incapacitation (MeitY, 2025b).

Crucially, the Act also puts in place some specific obligations on the Data Principal. So as to ensure the integrity of the ecosystem, and to avoid frivolous litigation, principals are barred from registering false or frivolous complaints, impersonating others and from providing untruthful information in the right to correction (MeitY, 2024a).

8.4 Resolution of Cross-Border Data Flows (Section 16)

Section 16 of DPDP Act 2023 now assuages the data localization concerns that earlier iterations of the DPDP Act had encountered. DPDP Act 2023 has moved away from the prescriptive, economically prohibitive physical localization mandates of the DPDP 2019 to a realistically guided "negative list" approach (DPDPA.com, 2023).

The Central Government may also, by official gazette notification, prescribe a country or a jurisdiction outside India to which the transfer of personal data may be restricted or prohibited under this section. Thus, unless a country or jurisdiction is blacklisted, cross-border data transfer is allowed by default (DPDPA.com, 2023). In the implementation of the Act, Indian tech start-ups and multinational corporations (MNCs) could take advantage of economies-of-scale from global cloud infrastructure and global data supply chains. A savings clause in the DPDP Act states that if India has other sectoral laws like the data localization mandates laid down by the Reserve Bank of India, or if the sectoral law safeguards are more stringent than those in the DPDP Act (DataGuidance, 2023), the DPDP Act will not apply. While this mechanism takes into account the needs of global economic integration, it also respects national security and financial autonomy (DPO India, 2023).

8.5 Pragmatic Exemptions (Section 17)

As a response to concerns that the legislation could lead to regulatory freeze or state paralysis, Section 17 provides for limited exceptions that are clearly specified in law (Gazette of India, 2023c).

• Innovation Ecosystem : The Central Government may exempt any notified startups, being fragile entities at an early stage of development, from any requirements prescribed under the rules in relation to the mode or manner of furnishing information or return, maximum retention period of records, and the minimum period for providing access to information (Gazette of India, 2023d).

• State Instrumentalities: Section 35 of the 2019 Bill was criticised for its blanket grounds for exemption. The exemptions in the 2023 Act are much narrower in scope. The conditions on deletion of data and the ability to rectify/update their data do not apply in situations where processing takes place in the absolute interest of the sovereignty and integrity of India, national security or the maintenance of public order (MeitY, 2024b). This provision prevents critical intelligence and security operations from being completely prevented by a single individual request to have their data deleted.

8.6 Enforcement

In a clear departure from the criminal liability regimes envisaged by previous drafts, the DPDP Act adopts the 'deterrent' or 'strict' liability regime. DPDP shall be exercised by the Data Protection Board (DPB) of India, an independent adjudicatory authority, digital by default. The DPB will consist of a chairperson and members with expertise in data, technology, and law (Gazette of India, 2023e).

The DPB is a civil court that adjudicates data breaches and orders mitigation measures against such cases. It has the authority to impose important penalties (MeitY, 2024c). The law expressly intends to levy stringent penalties on companies that fail to meet reasonable security standards. In the event that data breaches occur due to non-compliance with reasonable security measures, or if children's personal data is severely impacted, the fine can reach up to ₹200 crore per breach (PIB, 2025a). General breaches of fiduciary duties are liable for a fine of up to ₹50 crore (PIB, 2025a). Aggrieved parties of a DPB direction also have the option to appeal before the Telecom Disputes Settlement and Appellate Tribunal (TDSAT) for a review of any decision taken by the DPB (PIB, 2025b).

Table 1: The Data Protection Board and Deterrent Penalties

Feature	Srikrishna Draft (2018) / PDP Bill (2019)	DPDP Act (2023) & Rules (2025)
Philosophical Base	Trust-based fiduciary model; expansive, discretionary state exemptions (Sec 35).	Fiduciary model maintained; strictly defined, targeted exemptions (Sec 17).
Data Localization	Strict physical localization mandates; sensitive data must be stored on servers within India.	"Negative list" approach; seamless cross-border flow permitted unless explicitly restricted by government notification (Sec 16).
Data Principal Rights	Highly complex, included the Right to Data Portability and a subjective Right to be Forgotten.	Streamlined and pragmatic: Right to Access, Correct, Erase, and structurally novel Right to Nominate.
Scope of Data	Ambiguous boundaries; actively explored mechanisms for mandatory non-personal data sharing.	Scope strictly and exclusively limited to digital personal data.
Enforcement Model	Relied heavily on criminal penalties, threatening corporate officers with potential imprisonment.	Completely decriminalized; leverages an economic deterrence model with massive monetary fines (up to ₹200 crore).

9. Operational Execution: The DPDP Rules, 2025

Though the DPDP Act, 2023 provided the main statutory skeleton, the Digital Personal Data Protection Rules, 2025 were expected to flesh out the necessary musculature for procedures. MeitY released the draft rules for a public consultation in early 2025 and extended the deadline for processing the 6915 detailed responses received from industry stakeholders and civil society (MeitY, 2025c). The Government of India notified the DPDP Rules, 2025 on 14 November 2025 to fully operationalize the provisions of the Act (PIB, 2025c).

9.1 Phased Compliance and Stringent Notice Framework

Given the enormity of the changes, the Rules sensibly provide for an 18-month transition period for the global technology industry to comply with the new law (PIB, 2025d).

Rule 3 has a strong influence on the manner of consents being obtained on electronic platforms. Any consent notice provided by a Data Fiduciary must be presented separately from other complex terms and conditions and privacy policies. It must also be written in simple and plain language and must provide an itemised list of all personal data that would be processed and an itemised list of goods or services that are being enabled by such processing (MeitY, 2025d). This notice must explicitly provide a specific, highly visible communication link allowing the Data Principal to withdraw their consent with the exact same level of technological ease with which it was initially granted, effectively banning the use of manipulative "dark patterns" designed to trap user consent (MeitY, 2025d).

9.2 Institutionalising the Consent Manager Ecosystem

The stellar innovation of the Indian architecture is the statutory provisioning of the "Consent Manager" ecosystem. In the Rules, Consent Manager is a specialised entity that operates an accessible, transparent, and technically interoperable platform that allows citizens to centrally give, manage, review, and withdraw consent across hundreds of different Data Fiduciaries from a single digital dashboard (MeitY, 2025d).

To ensure complete local accountability and to prevent foreign interference in this vital digital public infrastructure, the Rules specify that every Consent Manager must be a registered company present in India (PIB, 2025d). The Data Protection Board also has sweeping authority over these companies, permitting

them to suspend or permanently cancel the registration of any Consent Manager that fails their technical and fiduciary duties under the rules (MeitY, 2025e).

9.3 Breach Notification Protocols and Security Safeguards

Rule 7 provides for a clear and user-friendly procedure for notifying about and reporting a personal data breach. Upon becoming aware of a personal data breach, the Data Fiduciary must notify the Data Protection Board and Data Principals "without delay" (MeitY, 2025e). The notification sent to the citizen shall not be confusing to the citizen and shall clearly state the nature and extent of the security incident, the breach's likely real-world impact, the remedial action taken or proposed to be taken by the business, and the steps the citizen can take to protect themselves in the immediate term (PIB, 2025e).

The Bill provides for several security measures in Rule 6. It mandates fiduciaries to implement strict controls to provide access to all computer resources, carry out thorough monitoring, and back up all data so that availability of personal data is never compromised (MeitY, 2025e). All system logs and records of access must be maintained for at least one year to assist any forensic investigations by the DPB concerning unauthorised access (MeitY, 2025e).

9.4 Tailored Data Retention and Protections for the Vulnerable

Rules have prescribed differential retention periods, based on the Data Fiduciary's size and its classification. For e-commerce platforms with more than 20 million registered users in India, Rule 8 mandates that the personal data shall be permanently deleted from the system after three years of the Data Principal's last interaction with the platform. This algorithmically enforces data minimization (MeitY, 2025e).

Additionally, the rules impose absolute legal prohibitions on the ability of a controller to process the data of vulnerable data subjects. For children's data, processing is only permitted with the prior verifiable consent of a parent or other legal guardian (PIB, 2025f). Direct deliverance of emergency healthcare, education and live physical safety interventions is an exception (PIB, 2025g), but only in genuinely outstanding circumstances. The protection does not extend to people with disabilities who do not have capacity to make a decision and who cannot be exploited by predatory commercial targeting (PIB, 2025f).

9.5 Harmonisation with the Right to Information (RTI) Act

A statutory confrontation occurred while drafting both the DPDP Act and the Right to Information (RTI) Act, 2005. Balancing the state's accountability to its citizens and the unconditional nature of the explicit right to privacy granted under the Puttaswamy judgment, the DPDP Act amended Section 8(1)(j) of the RTI Act (Lok Sabha Secretariat, 2025). This amendment prevents the disclosure of details of the private life of a citizen by state departments in the name of openness and transparency, but at the same time, the amendment does not create an absolute barrier. It does not issue an absolute prohibition on access to information. It only attaches importance to the principle and practice of utmost caution in the provision of personal information. Even after the RTI Amendment Act, Section 8(2) of the Act is still in force, stating that personal information can be shared if the public authority feels that larger public interest in disclosure outweighs the harm to the privacy of the individual. This would leave room for balancing between public interest and privacy (PIB, 2025g).

10. Theoretical and Economic Implications: Second and Third-Order Insights

The intervening-eight years between the Srikrishna Committee's first draft of India's potential constitution and the promulgation of DPDP Rules 2025 alone have seen multiple fundamental structural shifts in India's regulatory landscape, with deep second and third order effects for the evolution of the global digital economy.

The most drastic departure from existing law is around the issue of data transfer across borders, with both the 2018 and the 2019 drafts being substantially tilted towards the idea of strict physical data localization (Maheshwari & Co., 2026). This was based on an old model whereby sovereign control over data was fundamentally conflated with the geographic location of the server farms hosting the data, ensuring that domestic data was not vulnerable to foreign state surveillance, while allowing its access to Indian law enforcement as per local law (Carnegie Endowment, 2023). Notably, the 2023 Act's adoption of the "negative list" approach in Section 16 reflects a highly matured, technologically advanced mindset in the economics of the digital world (DPDPA.com, 2023). By allowing cross-border data flows by default, Indian policymakers had recognised that the modern data economy, with its distributed cloud computing, global AI training models, and transnational value chains, could not be incubated behind geographic walls. As such, the law creates a different form of "data sovereignty", one that is not dependent on the server and

other infrastructure, but rather one where the moment an organization holds data on Indian citizens, no matter the geographical location, the DPDP Act would have enforcement and jurisdictional purview over them, with associated audit provisions and severe financial penalties for non-compliance.

The Act explicitly enshrines the "Data Fiduciary" and "Data Principal" terminology, dispelling the "Controller/Subject" dichotomy of the EU GDPR (NeGD, 2026b). The difference between a Data Fiduciary and a Data Principal is not merely semantic, but goes to the legal burden and corporate liability of the entities. The law of subjects confers subject status: it gives statutory rights against the controller. The law of principals is different because it gives the principal the final word and ownership. The fiduciary's mandate is only conditional: the fiduciary can only exercise their power and discretion for the sole benefit of the principal. So, the Data Fiduciary has responsibilities beyond mere legal compliance and must act in the interest of the data principals. When the Data Protection Board adjudicates, the imbalance of power is not just reversed but is deliberately such that it is multi billion-dollar tech corporation which must prove to the Board that its algorithms used the information safely and that consent was not gamed via dark patterns.

At a third-order level, the overreliance on so-called "Consent Managers" mandated by the DPDP Rules 2025 is a well-intentioned attempt at resolving the global issue of "consent fatigue", where users accept incomprehensible privacy policies with a click of the "Accept" button (MeitY, 2025e). By aggregating consent management in one dashboard, the government is creating an entirely new class of digital intermediaries, similar to the Account Aggregator model of financial services. In effect, this creates a second massive layer of institutional reliance: the entire DPDP structure becomes dependent upon the technological interoperability, uptime, and absolute cybersecurity of these specialised Consent Managers. If a central database of a Consent Manager were ever compromised, the consent preferences of millions of citizens could be altered or wiped out in one fell swoop. By only permitting Consent Managers to be Indian entities (PIB, 2025d), the government has preemptively ensured that this highly critical node of the digital public infrastructure remains within absolute domestic jurisdiction and under the immediate regulatory oversight of the DPB.

The decision to drop criminal penalties between the 2019 Bill and the 2023 Act reflects a shift towards an economic deterrence model (Carnegie Endowment, 2023). Imposing criminal penalties for corporate data breaches before the 2023 Act was passed would have created decades of litigation in conventional courts

of law with a high burden of proof ("beyond a reasonable doubt") preventing responsive regulatory enforcement and deterring foreign direct investment. By replacing jail time with ₹200 crore (approx $30 million) fines to be tried in fast-track digital courts, the state has perfectly aligned punishment with the precise nature of the crime (PIB, 2025a). Data privacy violations are fundamentally corporate, economic crimes driven by the pursuit of algorithmic profit. It could be concluded that the threat of decapitalization on an unprecedented scale, now, pervasively, would achieve compliance far more effectively and more quickly than prospect of a corporate manslaughter or corporate criminal negligence charge against a corporate officer.

11. Conclusion

The Digital Personal Data Protection Act, 2023 has a history from the wide philosophical principles of the Supreme Court landmark judgment in Puttaswamy to the medically precise yet highly controversial cauldrons of the Srikrishna Committee and the Joint Parliamentary Committee, and has been carefully calibrated to India's sovereign role in a digital world. (Lok Sabha Secretariat, 2024) The transformation from the earlier 2019 Bill, which was restrictive, state-centric, and localization-oriented to the more flexible, economised, citizen-centric 2023 Act, is an example of evolutionary democracy at work with the inputs from thousands of stakeholders (PIB, 2023a). With the notification of the DPDP Rules in November 2025, India will move from the abstract, academic debate on privacy to implementation of privacy rights (PIB, 2025c). By combining a strong, rights-based fiduciary relationship with realistic cross-border data flows, but without the draconian criminal penalties some have sought, the Indian privacy law in effect achieves an ideal balance. It further fortifies a hard constitutional right to the sanctum of the individual's digital self, while enabling the data-driven engines of the global digital economy to power up and engage innovation with gusto. The epoch making character of this regime, at the end of the 18-month phase-in period for compliance, will be judged by both the institutional maturity of the Data Protection Board, and the technological maturity of the ecosystem of the Consent Manager that will develop under it (PIB, 2025b).

References

1. Accountant General West Bengal. (n.d.). *iCISAs Study Paper and Presentation*.(https://agwb.cag.gov.in/files/agae/circular_order/iCISAs_Study_Paper_and_Presentation.pdf)

2. Carnegie Endowment for International Peace. (2023). *Understanding India's New Data Protection Law*. https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law
3. DataGuidance. (2023). *Guidance on Cross-Border Data Transfers for Indian Organizations*. https://www.dataguidance.com/sites/default/files/dcsi_privacy_across_borders-_guidance_on_cross-border_data_transfers_for_indian_organizations.pdf
4. DPDPA.com. (2023). *Section 16: Transfer of Personal Data Outside India*. https://www.dpdpa.com/dpdpa2023/chapter-4/section16.html
5. DPO India. (2023). *Impact of DPDPA on Cross Border Data Transfer*.(https://www.dpo-india.com/Blogs/impact-dpdpa-cross-border/)
6. Gazette of India. (2023a). *The Digital Personal Data Protection Act, 2023 - Short title and commencement*.(https://egazette.gov.in/WriteReadData/2023/247847.pdf)
7. Gazette of India. (2023b). *The Digital Personal Data Protection Act, 2023 - Section 1*.(https://egazette.gov.in/WriteReadData/2023/247847.pdf)
8. Gazette of India. (2023c). *The Digital Personal Data Protection Act, 2023 - Exemptions Section*.(https://egazette.gov.in/WriteReadData/2023/247847.pdf)
9. Gazette of India. (2023d). *The Digital Personal Data Protection Act, 2023 - Part II*.(https://egazette.gov.in/WriteReadData/2023/247847.pdf)
10. Gazette of India. (2023e). *The Digital Personal Data Protection Act, 2023 - Composition of Board*.(https://egazette.gov.in/WriteReadData/2023/247847.pdf)
11. IndiaAI. (2022). *MeitY releases draft of Digital Personal Data Protection Bill, 2022*. https://indiaai.gov.in/news/meity-releases-draft-of-digital-personal-data-protection-bill-2022
12. Joint Parliamentary Committee [JPC]. (2021a). *Report of the Joint Committee on The Personal Data Protection Bill, 2019*. https://eparlib.sansad.in/handle/123456789/835465
13. Joint Parliamentary Committee [JPC]. (2021b). *JPC Reports Browse*.(https://eparlib.sansad.in/handle/123456789/13/browse?type=committeename&order=ASC&rpp=20&value=JPC+Reports)
14. Lok Sabha Secretariat. (2019a). *Lok Sabha Questions Annex AU2641*. https://sansad.in/getFile/loksabhaquestions/annex/176/AU2641.pdf

15. Lok Sabha Secretariat. (2019b). *Lok Sabha Bulletin Part I - December 2019*. https://eparlib.sansad.in/bitstream/123456789/799396/1/lsb_17_02.pdf
16. Lok Sabha Secretariat. (2019c). *Bills Texts: As Introduced - 341 of 2019*.(https://sansad.in/getFile/BillsTexts/LSBillTexts/Asintroduced/341%20of%202019As%20Int....pdf)
17. Lok Sabha Secretariat. (2019d). *Lok Sabha Questions Annex AU2637*. https://sansad.in/getFile/annex/253/AU2637.pdf
18. Lok Sabha Secretariat. (2019e). *Joint Committee on the Personal Data Protection Bill, 2019 Composition*. https://sansad.in/ls/committee/other-committees/73-joint%20committee%20on%20the%20personal%20data%20protection%20bill,%202019
19. Lok Sabha Secretariat. (2019f). *Lok Sabha Questions Annex AU1514*. https://sansad.in/getFile/loksabhaquestions/annex/175/AU1514.pdf
20. Lok Sabha Secretariat. (2022a). *Bills Texts: RS Bill Texts As Introduced*.(https://sansad.in/getFile/BillsTexts/RSBillTexts/Asintroduced/22e214202550212PM.pdf)
21. Lok Sabha Secretariat. (2024). *Standing Committee on Communications and Information Technology - Report 55*.(https://sansad.in/getFile/lsscommittee/Communications%20and%20Information%20Technology/17_Communications_and_Information_Technology_55.pdf)
22. Lok Sabha Secretariat. (2025). *Lok Sabha Debates - August 2025*. https://eparlib.sansad.in/bitstream/123456789/2992951/1/lsd_18_V_20-08-2025.pdf
23. Maheshwari & Co. (2026). *The Digital Personal Data Protection Act, 2023: Comprehensive Framework*. https://www.legal500.com/developments/thought-leadership/the-digital-personal-data-protection-act-2023-comprehensive-framework-latest-developments-and-compliance-roadmap/
24. Ministry of Electronics and Information Technology. (2018a). *Data Protection Committee Report*.(https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf)
25. Ministry of Electronics and Information Technology. (2022a). *Digital Personal Data Protection Bill, 2022*. https://www.meity.gov.in/content/digital-personal-data-protection-bill-2022

26. Ministry of Electronics and Information Technology. (2022b). *CEG Archievenews*. https://ceg.meity.gov.in/archievenews.jsp
27. Ministry of Electronics and Information Technology. (2023a). *Digital Personal Data Protection Act, 2023*. https://www.meity.gov.in/content/digital-personal-data-protection-act-2023
28. Ministry of Electronics and Information Technology. (2024a). *DPDP Act Uploads - Duties*. https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf
29. Ministry of Electronics and Information Technology. (2024b). *DPDP Act Uploads - Exemptions*. https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf
30. Ministry of Electronics and Information Technology. (2024c). *DPDP Act Uploads - Board*. https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf
31. Ministry of Electronics and Information Technology. (2025a). *Draft Digital Personal Data Protection Rules, 2025*. https://www.meity.gov.in/static/uploads/2025/02/f8a8e97a91091543fe19139cac7514a1.pdf
32. Ministry of Electronics and Information Technology. (2025b). *PIB Specific Docs 2025*.(https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/nov/doc20251117695301.pdf)
33. Ministry of Electronics and Information Technology. (2025c). *DPDP Rules Feedback Extension*. https://www.meity.gov.in/static/uploads/2025/02/0da2ec7e6bbf7d4803d256b9be0fadfb.pdf
34. Ministry of Electronics and Information Technology. (2025d). *Draft Rules Notification*. https://www.meity.gov.in/static/uploads/2025/02/f8a8e97a91091543fe19139cac7514a1.pdf
35. Ministry of Electronics and Information Technology. (2025e). *Draft Rules Details*. https://www.meity.gov.in/static/uploads/2025/02/f8a8e97a91091543fe19139cac7514a1.pdf
36. National e-Governance Division. (2026a). *The Right to Privacy: History, Philosophy, and Law*. https://negd.gov.in/blog/the-right-to-privacy-history-philosophy-and-law/
37. National e-Governance Division. (2026b). *The Right to Privacy: History, Philosophy, and Law - Part 2*. https://negd.gov.in/blog/the-right-to-privacy-history-philosophy-and-law/
38. Press Information Bureau. (2022a). *Monsoon Session 2022 Parliament Adjourned*.(https://www.pib.gov.in/PressReleaseDetail.aspx?PRID=1849999)
39. Press Information Bureau. (2022b). *Monsoon Session 2022 Parliament Adjourned Detail*.(https://www.pib.gov.in/PressReleaseDetail.aspx?PRID=1849999)

40. Press Information Bureau. (2023a). *Press Release PRID 2158506*.(https://www.pib.gov.in/PressReleseDetailm.aspx?PRID=2158506)
41. Press Information Bureau. (2023b). *Salient Features of the Digital Personal Data Protection Bill, 2023*.(https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=1947264)
42. Press Information Bureau. (2023c). *Press Release PRID 1947264*.(https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=1947264)
43. Press Information Bureau. (2025a). *Press Release PRID 2190655*.(https://www.pib.gov.in/PressReleasePage.aspx?PRID=2190655)
44. Press Information Bureau. (2025b). *Key Highlights of DPDP Rules 2025*.(https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/nov/doc20251117695301.pdf)
45. Press Information Bureau. (2025c). *Press Note Details - DPDP Rules 2025*.(https://www.pib.gov.in/PressNoteDetails.aspx?NoteId=156054&ModuleId=3)
46. Press Information Bureau. (2025d). *Press Release PRID 2190014*.(https://www.pib.gov.in/PressReleasePage.aspx?PRID=2190014)
47. Press Information Bureau. (2025e). *Key Highlights of DPDP Rules 2025 - Part 2*.(https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/nov/doc20251117695301.pdf)
48. Press Information Bureau. (2025f). *Press Release PRID 2190014 - Part 2*.(https://www.pib.gov.in/PressReleasePage.aspx?PRID=2190014)
49. Press Information Bureau. (2025g). *Specific Docs November 2025*.(https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/nov/doc20251117695301.pdf)
50. Rajya Sabha Secretariat. (2022a). *Bills Texts: As Introduced - 22e*.(https://sansad.in/getFile/BillsTexts/RSBillTexts/Asintroduced/22e214202550212PM.pdf)
51. Rajya Sabha Secretariat. (2022b). *Bills Texts: As Introduced - Exemptions*.(https://sansad.in/getFile/BillsTexts/RSBillTexts/Asintroduced/22e214202550212PM.pdf)