The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

Data Protection Laws in India: A Critical Analysis of the Digital Personal Data Protection Act, 2023

Mahipal Yagati

Abstract

For over ten years, India debated whether it required a data protection law. So, after this debate, the Digital Personal Data Protection Act 2023 was enacted, well, you know, it followed from there. It seems to take some inspiration from the Supreme Court's big 2017 ruling in K.S. Puttaswamy v. Union of India, which in turn, essentially, leaned into the idea that privacy counts as a fundamental right. That is because the Court recognised privacy under Article 21 of the Indian Constitution, in a way that mattered a lot. The DPDP Act establishes a legal framework for processing personal data, requiring consent or lawful grounds. It also grants individuals four rights over their data: access, rectification, erasure and restriction. It also sets up a Data Protection Board to deal with complaints about possible infringements of privacy rights and to make sure compliance with the DPDP Act is actually followed. In fact, people are comparing this kind of rule with the GDPR in the EU and the California Consumer Privacy Act (CCPA), kind of right away, as if it is a near match.

Key terms

Digital Personal Data Protection Act 2023, CCPA, GDPR, the Puttaswamy case, the Data Protection Board of India, SPDI, automated decision-making and comparative data protection law.

I. INTRODUCTION

The phrase "data is the new oil" has likely been familiar to most people at some point.[1] The phrase has become so overused that its original meaning has almost been forgotten. But stripped of the hype, the point is worth taking seriously. Oil created enormous concentrations of wealth and power in the twentieth century, and personal data is doing something similar today. It is behind every targeted advertisement, every credit score, every app recommendation, every profiling decision. And India — with over 900 million internet users[2] — is generating this data at a scale that is difficult to fully grasp.

Here is a simple way to think about what the legal gap meant before 2023. Every time someone in India downloads an app and clicks "I agree" without reading the privacy policy. Which, let us be honest, is every single person in India. They are basically giving away their personal data with almost no legal protection for the person.

Every single UPI transaction that people in India make every hospital booking that people in India do every Google search that people, in India perform is giving information to these databases that companies can use for their own purposes share with other people or even sell to someone else in ways that the person whose data it is has no real ability to challenge or even understand what is happening with their personal data. The IT Act had some provisions. The SPDI Rules helped a little. But there was no complete framework, no dedicated regulator, no individual rights. People had to take care of themselves for the part.

The Digital Personal Data Protection Act 2023 became a law on 11 August 2023.

India finally got approval from the President after talking about it for over ten years, making reports and trying with a bill that did not work.

The Digital Personal Data Protection Act 2023 is a deal because it is based on what the court said in 2017 when nine judges made a decision in the case of K.S. Puttaswamy, versus the Union of India, and it is a law that India needed to protect the Digital Personal Data of people. This overturned older precedent and established privacy – including the right to control your own

[1] *See World Economic Forum, The Global Risks Report 2023* 7 (18th ed. 2023); the phrase "data is the new oil" is attributed to Clive Humby at the ANA Senior Marketer Summit (2006).

[2] IAMAI & Kantar, *India Internet Report 2023* 12 (2023); Telecom Regulatory Authority of India, *Telecom Subscription Data as of Mar. 31, 2023* (TRAI 2023) (recording over 850 million broadband subscribers).

information – as a fundamental right under Article 21. The DPDP Act is, in large part, Parliament's response to that judgment.

This paper is an attempt to read the Act carefully and say something useful about it.

II. The Right to Privacy: A Fundamental Constitutional Right

To grasp the significance of the DPDP Act, we must consider a fundamental question: Did people in India possess a right to privacy before 2017?

The answer was not clear.

Two court cases, M.P. Sharma v. Satish Chandra (1954) and Kharak Singh v. State of U.P. (1963), suggested that perhaps people didn't have this right. This made it hard to argue for data protection based on the Constitution. The 2017 Puttaswamy judgement changed this.

A group of nine judges agreed that privacy is a right under Article 21. This judgment talked about data protection. Introduced the idea of keeping personal information private.

The Constitution says that people have the right to control their information. This right is protected by the Constitution. The 2017 Puttaswamy ruling was a deal. It had an impact on the Data Protection Bill that Parliament passed in December of last year.

Before July 2017, people did not think that the Indian Constitution would fully protect individuals. So, data protection laws were based on Article 21 of the Constitution.

The Puttaswamy ruling changed everything. Now people can use Article 21 to support data protection laws.

The Puttaswamy ruling will change how India handles data protection from now on. The Data Protection Bill and the Puttaswamy ruling are connected to data protection in India. Data protection is important. The Puttaswamy ruling will have a big impact on it. This decision particularly focused on data protection and introduced the idea of informational privacy. It recognised a constitutionally protected interest in controlling personal information.

THE PRE-DPDP LEGAL LANDSCAPE IN INDIA

Before August 2023, data protection in India was patchy at best. The main legal instrument was the IT Act, 2000. Section 43A created civil liability for body corporates that mishandled "sensitive personal data or information" (SPDI). Section 72A penalised disclosure of personal

information in breach of a contract.[3] Both provisions had obvious limitations: they applied only to body corporates, not government entities; they gave citizens no direct rights to enforce; and there was no dedicated regulatory body anywhere in the structure.

The SPDI Rules, 2011,[4] were an attempt to patch some of these gaps. They defined what counted as sensitive personal data — passwords, bank details, health records, biometric data — and required body corporates to get consent and publish a privacy policy. Frankly, these rules were largely disregarded. There was no enforcement, and most rule breakers weren't punished.

People had been asking for data protection laws for a time.

The Srikrishna Committee made a plan in 2018 to protect people's data. This plan caused a lot of talk and discussion. Then Parliament made a bill to protect people's data in 2019. A committee looked at the bill. Changed some things. The bill came back in 2021 with many changes.

In August 2022, the whole idea was dropped. The government's stated reasons included complaints from the technology sector about data localisation requirements and a general view that the bill had become too complicated. Starting over seemed like the easier option.

The DPDP Act 2023 emerged from that fresh start. It's shorter, simpler, and more business-friendly than the 2019 bill. Some of what was lost in the simplification process was probably unnecessary complexity. But some of it was substantive protection. This paper takes the position that the second category matters more than the government has been willing to acknowledge.

IV. Key Provisions of the Digital Personal Data Protection Act 2023

A.The scope and applicability of the law are crucial.

The Act covers digital personal data processed in India, regardless of whether it was originally collected online or converted from a physical format.[5] It also applies to foreign companies that offer goods or services to people in India or profile them, even if those companies have no office in the country. This extraterritorial reach is directly modelled on how the GDPR works, and it is

[3]The Information Technology Act, 2000, §§ 43A, 72A (India).

[4]Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, r. 3 (India) [hereinafter SPDI Rules].

[5]Digital Personal Data Protection Act, 2023, § 3(a)–(b) (India) [hereinafter DPDP Act].

a sensible approach. A data protection law that only covered Indian companies would have been easy to circumvent.

B. Key Definitions

The Act identifies three main roles. The Data Principal is the person the data is about. The Data Fiduciary is whoever decides why and how to process that data. The Data Processor is whoever actually does the processing on the Fiduciary's behalf. These map roughly onto the GDPR's data subject, controller, and processor categories.

The concept that is actually new here is the Consent Manager — a registered intermediary through which a Data Principal can give, manage, and withdraw consent across multiple platforms from a single interface. Nothing quite like this exists in GDPR or CCPA. It is a clever idea. Whether it will work in practice depends on subordinate Rules that have not yet been released, so it is hard to evaluate properly at this stage.

C. Grounds for Lawful Processing

Personal data can only be processed on one of two bases: the Data Principal's consent, or one of the "legitimate uses" listed in Section 7.[6] Legitimate uses include State welfare processing, legal compliance, medical emergencies, and employment purposes. Missing from this list is anything like GDPR's "legitimate interests" ground — Article 6(1)(f) — which lets a controller process data where its interests outweigh the individual's, after a genuine balancing exercise. The DPDP Act does not permit that kind of balancing. Whether this is more protective of individuals or just more restrictive for everyone depends on how it is enforced in practice, which remains to be seen.

D. Rights of Data Principals

Sections 11 to 14 give Data Principals four rights.[7] The right to know what data a Fiduciary holds about them (Section 11). The right to have that data corrected, completed, or erased (Section 12). The right to raise a grievance with the Fiduciary (Section 13). And the right to nominate someone to exercise these rights if they pass away or become incapacitated (Section 14). Four rights sounds like a lot until you compare it to GDPR's eight. The missing ones are not obscure: there is no portability right, no free-standing right to object to processing, and no

[6] *Id.* §§ 4, 7.
[7] *Id.* §§ 11–14.

protection against being subjected to purely automated decisions. Those are significant absences and this paper comes back to them in the critical analysis.

E. Children's Data

Section 9 is probably the strongest part of the entire Act. Any Data Fiduciary that wants to process a child's personal data — and "child" means anyone under eighteen[8] — has to get verifiable consent from a parent or guardian first. On top of that, targeted advertising aimed at children and behavioural monitoring of minors are flatly prohibited. This is serious protection. Other countries have moved in a similar direction — the UK's Children's Code, the US COPPA regime — and India's approach here is consistent with that trend. If someone asks what the DPDP Act got unambiguously right, this section is the answer.

F. Penalties

The Schedule to the Act sets financial penalties: up to Rs. 250 crore for children's data violations, and up to Rs. 200 crore for security failures leading to a breach.[9] On paper, those numbers look serious. However, their treatment under GDPR is quite different. The General Data Protection Regulation allows for fines of up to 4 per cent of a company's worldwide turnover or twenty million euros, whichever amount is bigger. The General Data Protection Regulation is really strict about this. The company has to pay the General Data Protection Regulation fine, which is either 4 per cent of the company's total worldwide turnover or twenty million euros. For Meta or Google, Rs. 250 crore is genuinely not a deterrent. For smaller Indian companies, it probably is. The penalty regime works for some actors and not others — which is a problem worth acknowledging.

V. CRITICAL ANALYSIS OF THE DPDP ACT, 2023

A. What the Act Gets Right

Before getting into the problems, it is fair to acknowledge what the Act actually achieves. India now has a comprehensive data protection statute for the first time. That is not nothing — it took long enough. The Act is also written in plain language, which is more than can be said for most Indian legislation. A person without legal training can read it and roughly understand their rights. Given that the whole point is to empower ordinary citizens, the drafting style matters.

[8] *Id.* § 9; § 2(g) (defining "child" as a person below eighteen years of age).
[9] Id. Schedule, Items 1–7.

The Consent Manager is the most original thing in the Act. In theory, instead of clicking through privacy settings on fifty different apps, a person could manage all their data consents in one place through a single registered intermediary. No other major data protection law has tried this. Whether the execution will match the concept is still unknown — but the concept itself is worth credit. The Act's extraterritorial scope and its straightforward prohibition on targeting children are also positive features.

B. Where It Falls Short

The single biggest gap is the absence of a right to data portability. Under GDPR Article 20,[10] you can demand that a platform give you all your data in a format you can use, and you can take that data to a competing service. This matters enormously in practice. Without portability, switching from one app to another means losing everything — your history, your preferences, your connections. Platforms use this to keep people locked in. A data protection law that does not address this is leaving one of the most commercially significant privacy problems completely unresolved.

Then there is Section 17.[11] Government processing done for national security, public order, sovereignty, or preventing cognisable offences is exempted from the consent requirements, Data Principal rights, and Data Fiduciary obligations. National security exemptions exist in every data protection regime, so that is not the objection. The objection is to "public order" — a phrase that Indian courts have interpreted broadly in other contexts — appearing here without any proportionality requirement. Under the standard laid down in *Puttaswamy*, any interference with privacy has to be necessary and proportionate. Section 17 does not require either. That is a constitutional problem, not just a policy one.

A third issue: large chunks of the Act will not actually function until the Central Government releases the Rules. The Consent Manager framework, the security standards Data Fiduciaries must maintain, the procedural details of the Data Protection Board — all of this lives in the Rules, not the statute. Until the Rules come out, these provisions are essentially aspirational. Citizens cannot enforce rights that exist only in theory.

[10]Regulation 2016/679 of the European Parliament and of the Council, art. 20, 2016 O.J. (L 119) 1 [hereinafter GDPR] (right to data portability).

[11]DPDP Act, *supra* note 5, § 17.

And finally — no criminal liability. Every penalty in the Act is civil and financial. For a large company that has deliberately misused personal data, paying a fine might simply be cheaper than changing its behaviour. Criminal sanctions for wilful or serious violations are how you signal that data protection is not just a compliance exercise. Their absence is a choice that will be difficult to defend if a major violation occurs and the Board can only respond with a monetary penalty.

VI. THE DATA PROTECTION BOARD OF INDIA: INSTITUTIONAL ANALYSIS

Sections 18 to 27 establish the Data Protection Board of India (DPBI), responsible for handling complaints and enforcement.[12] The Board operates entirely digitally with complaints filed online and hearings conducted virtually. For a country of India's size, this makes practical sense. People in smaller cities and rural areas should not have to travel to Delhi to assert a data protection right. The Board has real teeth on paper: it can investigate, issue binding directions, and impose the financial penalties listed in the Schedule.

The independence problem, though, is serious. Board members are appointed by the Central Government, on the recommendation of a committee that the Central Government itself sets up.[13] The government is also, simultaneously, one of the largest Data Fiduciaries in the country — it processes data in Aadhaar, in income tax, in health schemes, in practically every major public programme. A regulator whose leadership is chosen by the entity it is supposed to regulate cannot function as an independent check on that entity, regardless of the good intentions of the individuals involved. The GDPR requires supervisory authorities to act with "complete independence." By that standard, the DPBI as currently designed does not qualify.

An independent regulator's value lies in being willing to say uncomfortable things to powerful actors. If the DPBI is staffed by people who owe their positions to the executive, that willingness is structurally compromised from day one. Fixing this is not a second-order reform — it is foundational. Without genuine independence, the Board risks becoming a dispute resolution forum for private sector complaints while giving the government a free pass.

VII. SECTOR-SPECIFIC DATA PROTECTION REGIMES

[12] *Id.* §§ 18–27.

[13] PRS Legislative Research, *The Digital Personal Data Protection Act, 2023: Legislative Brief* 10 (Aug. 2023).

One gap that does not get enough attention is the Act's silence on its relationship to existing sectoral data frameworks. The RBI already requires payment system operators to store payment data locally within India.[14] SEBI has its own cybersecurity framework. IRDAI has data governance requirements for insurers. The National Health Authority runs its own Health Data Management Policy under the Ayushman Bharat Digital Mission. These are not minor overlapping rules — they cover billions of transactions and hundreds of millions of people.
The DPDP Act does not say anything about what happens when its requirements conflict with one of these frameworks. If the RBI says one thing about data storage and the DPBI says another, which does a payment company follow? If a hospital is required to handle health data in a particular way under the NHA policy and the DPDP Act says something different, what is the legal answer? Right now, there is none. This will eventually end up in litigation, and the courts will have to work it out case by case. That is an inefficient and unpredictable way to resolve what is, at its core, a drafting problem that could have been solved in the statute itself.

VIII. ARTIFICIAL INTELLIGENCE AND THE DPDP ACT

Perhaps the most glaring gap in the DPDP Act, given the moment we are living through, is its complete silence on AI and automated decision-making. AI systems are not peripheral to data protection — they are the most consequential way in which personal data is now being used. Automated systems are now processing personal data to influence decisions across various areas including credit scoring, hiring, insurance pricing bail recommendations and content moderation. These systems impact real people's lives and GDPR Article 22 addresses this.[15] EU citizens have the right to be exempt from decisions made solely by automated processing if those decisions significantly impact them. Furthermore, they must be able to request human review. Indian citizens have no equivalent right under the DPDP Act.
MeitY has said that AI regulation will come through a separate framework.[16] That may or may not be the right structural approach, but the result for now is a gap. As AI systems become more

[14]Reserve Bank of India, Storage of Payment System Data, RBI/2017-18/153 (Apr. 6, 2018).
[15]GDPR, *supra* note 10, art. 22 (right not to be subject to solely automated decision-making).
[16]Ministry of Electronics and Information Technology, *India's Approach to AI Governance: Discussion Paper* 8 (MeitY, 2023).

embedded in employment, credit, healthcare, and public services in India, the absence of any automated decision-making protection will become increasingly difficult to justify. A future amendment should address this directly, rather than leaving it to a regulatory framework that may or may not materialise.

IX. COMPARATIVE ANALYSIS: INDIA, THE EUROPEAN UNION, AND THE UNITED STATES

Looking at the DPDP Act alongside GDPR and CCPA is useful — not to hold India to an unrealistic standard, but to understand concretely what the differences mean for the people these laws are supposed to protect.

GDPR is the world's most ambitious data protection framework. It grants EU citizens eight rights, including data portability and protection against automated decision-making. Furthermore, companies exceeding a certain risk threshold must appoint a Data Protection Officer and conduct impact assessments before initiating new data processing activities. Penalties can reach 4% of global annual revenue. Supervisory authorities are constitutionally required to be independent. It is not perfect — enforcement has been uneven across member states — but the architecture is serious. Countries from Brazil to Japan have used GDPR as the template for their own laws.

The CCPA is a narrower instrument. California residents can find out what data companies have collected about them, opt out of their sale, and ask for it to be deleted. It does not apply to government entities. It imposes no obligation on companies to justify their processing, and there is no portability right. It is better understood as a transparency and opt-out regime than as a rights-based framework in the European sense.

India's DPDP Act is stronger than CCPA but weaker than GDPR. It gives citizens real rights, has a national regulator, applies to foreign companies, and protects children meaningfully. Where it lags is in the depth of those rights — no portability, no automated decision-making protection, a less independent regulator, and weaker penalties for large actors. For India to achieve what is called "adequacy" under GDPR — a status that would allow data to flow freely between Indian and EU entities — these gaps would need to be filled. That has commercial and diplomatic implications beyond data law itself.

X. CONCLUSION AND RECOMMENDATIONS

The DPDP Act, 2023, is a real achievement. After ten years of waiting, India has a data protection law that ordinary people can read and understand, that gives them rights they can actually invoke, and that applies to foreign platforms as well as domestic ones. The children's data provisions are strong. The Consent Manager is genuinely original. We are moving from a lot of rules before 2023 to one big law that covers everything. This is a deal. If we are going to write a paper about this Act, we also have to talk about what the Act cannot do. No portability right. Government exemptions that are too broad by the standards the Supreme Court itself set. No criminal liability even for deliberate violations. Key Rules are still unpublished. A regulator whose independence is undermined by its appointment structure. Silence on AI at a moment when AI-driven decisions are affecting more and more people. These are not quibbles. They are the difference between a law that fulfils the promise of
Puttaswamy and one that only partially does.
Six specific reforms would substantially improve the Act:

1. Introduce a right to data portability so that citizens can take their data to competing services and platforms cannot use data lock-in as a competitive tool.
2. Amend Section 17 to require that all government processing under the exemptions satisfy the Puttaswamy proportionality test — a legal basis, a legitimate aim, and necessity.
3. Publish the Rules without further delay. Rights that depend on unpublished subordinate legislation are not enforceable in any meaningful sense.
4. Reform the DPBI appointment process so that Board members are selected through a mechanism that is genuinely insulated from the executive, with security of tenure.
5. We need to put in place checks to prevent automated decision-making from going wrong. This means citizens should know when AI is being used to make decisions that affect them. They should also have the right to ask a human to review the decision if they're not happy with it.

6. People who deliberately break data protection rules should face consequences. This includes making sure that serious breaches do not just result in fines but lead to criminal charges.

India’s data protection law is unlikely to remain static. The DPDP Act has just started a discussion instead of ending an old one. As AI systems get better and we use public infrastructure more our lives are going to be online even more. This will put a lot of pressure on the DPDP Act framework. The DPDP Act will have to deal with this. For those of us studying law right now, this is one of the fields where the work of the coming decades will actually be done. The statute that exists today is good enough to build on. The question is whether the political will to keep building exists.