The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2025

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

DATA PROTECTION IN INDIA: ANALYSIS OF CURRENT LEGAL FRAMEWORK AND THE NEED FOR REFORM

Simran Mhade

ABSTRACT:

This paper critically examines the evolution of data protection laws in India, with a focus on the recently enacted Digital Personal Data Protection Act, 2023. Tracing the legal journey from the Information Technology Act and the Puttaswamy judgment to the present framework, it analyses how the DPDP Act addresses core privacy principles like consent, purpose limitation, and data minimisation. While the Act represents progress in codifying digital rights, it also raises concerns—particularly regarding its sweeping government exemptions, limited regulatory independence, and lack of provisions for sensitive data and algorithmic harms. By comparing India's framework with global models like the EU's GDPR and the U.S. sectoral approach, the paper highlights both alignment and divergence. It concludes with recommendations to strengthen the legal architecture through risk-based safeguards, institutional reforms, and protections against AI-era threats, emphasising the need for a more robust, rights-based, and future-ready data protection regime in India.

INTRODUCTION:

In today's digital landscape, the constant exchange of personal data across countless platforms presents a central challenge: protecting individual privacy. For India, where dependence on digital infrastructure permeates financial services, healthcare, education, and public administration, this reliance significantly heightens the dangers of data misuse, ubiquitous surveillance, and unauthorised profiling. The sheer scope of data collection, encompassing everything from biometric databases to granular mobile app permissions, has expanded dramatically, frequently outpacing the foundational legal frameworks designed to govern it.

Data protection can be defined as rules and processes that control how personal data is collected, stored, used and shared. Its main objective is to safeguard an individual's right to privacy, personal liberty and dignity. It helps prevent misuse of personal data and guarantees that people who handle such data comply with the law, behave transparently, and are held accountable.[1]

A compelling need for a coherent and enforceable data protection law gained constitutional urgency following the Supreme Court's pivotal decision in Justice K.S. Puttaswamy (Retd.) v. Union of India. There, a nine-judge bench unanimously declared the right to privacy a fundamental right under Article 21 of the Constitution.[2] The Court also stressed that informational privacy was inherently linked to personal liberty, mandating the state to govern the collection, processing, and sharing of personal data via a just, fair, and proportionate legal framework.[3]

Before this crucial Supreme Court decision, India's approach to data protection was notably insufficient. It largely relied on the rather narrow reach of Sections 43A and 72A of the Information Technology Act, 2000, along with the 2011 SPDI Rules. Significantly, these older rules only set specific requirements for certain sectors, and, quite simply, offered very weak ways to ensure compliance.[4] But, driven both by this new constitutional requirement and the rapidly growing global focus on privacy – seen in regulations like the EU's General Data Protection Regulation (GDPR) – India finally passed the Digital Personal Data Protection Act, 2023. This highly important law now paves the way for a truly comprehensive legal framework.

This research paper examines the evolution of India's data protection laws, analyses the current statutory framework under the 2023 Act, identifies critical gaps and emerging challenges, and compares India's model with international standards. It also proposes reforms to strengthen the legal regime and ensure that individual autonomy, transparency, and accountability are prioritised in India's digital transformation.

EVOLUTION OF DATA PROTECTION IN INDIA:

[1] *The Digital Personal Data Protection Act, 2023*, No. 22 of 2023, Acts of Parliament, 2023, https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf
[2] *Justice K.S. Puttaswamy (Retd.) v. Union of India,* AIR 2017 SC 4161, ¶ 180.
[3] *Id*. at ¶¶ 185–187.
[4] *The Information Technology Act, 2000* §§ 43A, 72A, No. 21 of 2000, Acts of Parliament, 2000, https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf

India's path toward creating an extensive data protection system has been anything but simple. Its development happened slowly, largely because of court judgments and changing international rules, rather than through planning. Essentially, personal data at first did not have its specific law; instead, its limited protections were scattered throughout existing laws, mainly found within the Information Technology Act, 2000 (known as the "IT Act").

The IT Act's 2008 Amendment marked the first truly significant legislative acknowledgement of data protection, notably by introducing Section 43A. This section rendered corporate entities liable in civil law for negligence when implementing adequate security protocols for 'sensitive personal data or information.[5] Furthermore, Section 72A laid down criminal sanctions for service providers; specifically, it covered situations where personal information was knowingly disclosed without authorisation or in violation of an existing contract.[6]

To put these provisions into practice, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules) were brought into force.[7] These Rules then attempted to define 'sensitive personal data' and introduced obligations concerning consent, disclosure protocols, and restrictions on data retention periods. However, their reach proved quite limited: they only applied to body corporates, lacked robust enforcement powers, and did not extend to cover state data collection or surveillance.

The limitations of India's data protection framework became starkly apparent as internet use, mobile applications, and Aadhaar-linked authentication systems expanded exponentially. Concurrently, public concern regarding privacy violations intensified considerably, fueled by the government's escalating utilisation of biometric and demographic data, a trend most visibly demonstrated under the Aadhaar project.

The absence of clear laws on data protection led courts to step in, examining the issue based on constitutional rights. In 2012, a series of petitions challenging the Aadhaar scheme ultimately resulted in the formation of a nine-judge constitutional bench for Justice K.S. Puttaswamy (Retd.) v. Union of India. The bench, in a landmark ruling, firmly declared privacy a fundamental right.[8] The Court also stressed the vital need for a comprehensive data protection

---

[5] *Id.* at §43A
[6] *Id.* at §72A
[7] *The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011,* G.S.R. 313(E), Apr. 11, 2011, https://upload.indiacode.nic.in/showfile?actid=AC_CEN_45_76_00001_200021_1517807324077&type=rule&filename=GSR313E_10511(1)_0.pdf
[8] *Puttaswamy, supra* note 2.

framework, stating clearly that informational privacy—especially in the digital world—is tied directly to human dignity and autonomy.[9]

After this judgment, the government formed the Justice B.N. Srikrishna Committee in 2017. This committee then submitted a thorough report along with a draft Personal Data Protection Bill in 2018, which effectively set the stage for new laws.[10] While the 2019 Bill developed from this initial draft, it was eventually withdrawn. This cleared the path for the Digital Personal Data Protection Act, 2023, which stands as India's first specific data protection law.

CURRENT LEGAL FRAMEWORK: THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023:

The enforcement of the Digital Personal Data Protection Act, 2023 (DPDP Act) truly stands as a key moment in India's efforts to legislate data privacy. After years of deliberation, pressure from courts, and analysing policies from other countries, this Act delivers India's first complete legal framework focused entirely on protecting personal data.

A. OVERVIEW AND SCOPE –

The DPDP Act applies broadly to the handling of digital personal data, regardless of whether it was collected online or converted from offline records.[11] It covers both Data Fiduciaries (the entities that decide the purpose and means of data processing) and Data Principals (the individuals the data relates to).[12] Notably, the Act even reaches beyond India's borders, applying to organisations outside the country if they process data while offering goods or services to people within India.[13]

The Act aims to strike a balance between individual rights and the legitimate requirements of both businesses and the government. Its structure is built on core principles: consent, purpose limitation, data minimisation, and accountability. These principles closely reflect established frameworks, like the European Union's General Data Protection Regulation (GDPR).

B. KEY PROVISIONS –

---

[9] *Id.* at ¶¶ 180–188

[10] *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians,* Committee of Experts under the Chairmanship of Justice B. N. Srikrishna, Ministry of Electronics & Information Technology (July 27, 2018), https://prsindia.org/files/bills_acts/bills_parliament/2019/Committee%20Report%20on%20Draft%20Personal%20Data%20Protection%20Bill,%202018_0.pdf

[11] The Digital Personal Data Protection Act, 2023, No. 22 of 2023, Acts of Parliament, 2023 (India), published Aug. 11, 2023, https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf

[12] *Id.* §§ 2(i), 2(j), 5.

[13] *Id.* § 3(b).

The Digital Personal Data Protection Act (DPDP Act) establishes stringent regulations concerning data processing and individual rights, diverging in certain aspects from international frameworks like the GDPR.

1. Consent and Notice Requirements –

   Under the DPDP Act, the processing of personal data necessitates explicit, informed, and unambiguous consent. This consent must be acquired through clear and easily comprehensible notices.[14] A right granted to Data Principals (individuals to whom the data relates) is the ability to revoke consent at any juncture, upon which data processing must immediately cease.[15]

2. Rights of Data Principals –

   The Act confers a comprehensive set of rights upon Data Principals. These include the right to access their data, the right to seek correction or erasure of inaccurate or outdated information, and the right to grievance redressal. Furthermore, the Act introduces a provision allowing Data Principals to nominate an individual to exercise these rights on their behalf in instances of incapacitation.[16]

3. Duties of Data Principals –

   A notable distinction of the DPDP Act, when compared to the GDPR, is the explicit imposition of duties on Data Principals. These duties include, but are not limited to, refraining from impersonation and the suppression of material information.[17]

4. Cross-Border Data Transfer –

   The DPDP Act permits cross-border data transfers to jurisdictions that have been officially notified by the central government.[18] Importantly, the final iteration of the Act does not mandate data localisation, a departure from earlier draft versions.

5. Data Breach Notification –

   In the event of a personal data breach, Data Fiduciaries (entities processing personal data) are obligated to promptly notify the Data Protection Board of India and the affected Data Principals.[19]

C. REGULATORY STRUCTURE AND ENFORCEMENT –

The Digital Personal Data Protection Act (DPDP Act) establishes the Data Protection Board of India (DPBI), which is designated as the primary adjudicatory body

[14] *Id.* § 6.
[15] *Id.* § 6(4).
[16] *Id.* §§ 11–14.
[17] *Id.* § 15.
[18] *Id.* § 16.
[19] *Id.* § 8(6).

responsible for addressing complaints, conducting inquiries, and enforcing the Act's provisions.[20] However, a closer examination reveals that the DPBI's structure may lack complete independence; its members are appointed and overseen by the Central Government, which consequently raises concerns regarding the institution's true autonomy.

Non-compliance with the Act incurs substantial penalties, with fines for significant breaches potentially reaching up to ₹250 crore.[21] Notably, the legislation also incorporates provisions for voluntary undertakings and various alternative dispute resolution mechanisms. This inclusion suggests a shift towards a more responsive and perhaps less adversarial approach to regulatory compliance.

CRITICAL ANALYSIS OF THE DPDP ACT, 2023:

1. STRENGTHS OF THE DPDP ACT, 2023 –

The Digital Personal Data Protection Act (DPDP Act) institutes several critical advancements in India's data privacy landscape:

- Formal Codification of Privacy Principles: A significant step involves the Act's formal adoption of core privacy principles. These include purpose limitation, data minimisation, storage limitation, and the requirement for lawful consent, all of which demonstrate alignment with established international frameworks, notably the EU General Data Protection Regulation (GDPR). This represents a marked improvement over the more fragmented and largely outdated provisions found within the Information Technology Act, 2000.
- Empowerment of Data Principal Rights: The legislation explicitly confers upon individuals a suite of rights concerning their data. These encompass the right to access, rectify, and erase their information, alongside the crucial ability to withdraw previously granted consent. Such provisions are designed to enable users to exert greater agency over the management and processing of their data.[22]
- Enhanced Cross-Border Data Transfer Flexibility: Departing from earlier, more restrictive stances, the Act removes mandatory data localisation requirements. Instead, it permits the transfer of data to jurisdictions that have received official notification from the Central Government. This revised approach aims to facilitate

[20] *Id.* §§ 18–23.
[21] *Id.* § 33(1).
[22] *Id.* §§ 11–14

international trade and digital commerce while concurrently preserving sovereign regulatory control.[23]

- Establishment of a Dedicated Data Protection Board: The creation of the Data Protection Board of India (DPBI) lays essential groundwork for the adjudication of privacy infringements and the robust enforcement of compliance. While the extent of its institutional autonomy remains a subject of ongoing debate, the very presence of a specialised oversight body marks a clear progression from prior regulatory regimes that notably lacked such dedicated mechanisms.[24]
- Streamlined Compliance for Emerging Enterprises: The Act reduces certain burdensome obligations, such as the mandatory appointment of Data Protection Officers (DPOs) and the conduct of Data Impact Assessments (DIAs), particularly for smaller businesses and startups. This simplification aims to mitigate regulatory friction, thereby fostering an environment conducive to innovation and growth within these sectors.[25]

2. WEAKNESSES AND GAPS IN THE DPDP ACT, 2023 –

India's current data protection law, while a step towards safeguarding personal information, raises several critical concerns that could undermine its effectiveness and public trust.

- Government Exemptions: The law gives the Central Government vast authority to bypass its own rules. It can exempt any agency from data protection obligations based on broad, undefined terms like "public order" or "sovereignty." This sweeping power is worrying because it risks creating a loophole for unchecked mass surveillance, bypassing the crucial checks and balances from courts and lawmakers that are fundamental to a healthy democracy. Such broad exemptions go against principles of limited government power, as highlighted in the landmark Puttaswamy judgment.[26]
- Data Protection Board: The very body tasked with enforcing data protection, the Data Protection Board, lacks true independence. Since the government appoints its members, controls its funding, and oversees its operations, there's a real concern that it might struggle to fairly rule against government actions that

[23] *Id.* § 16.
[24] *Id.* §§ 18–23.
[25] *Id.* § 17.
[26] *Justice K.S. Puttaswamy (Retd.) v. Union of India,* AIR 2017 SC 4161, ¶ 180.

violate data privacy. This inherent lack of autonomy could severely compromise its ability to be an impartial arbiter of justice for citizens.[27]

- Sensitive Data: A significant drawback of the current law is its failure to distinguish between different types of data. Unlike previous drafts and international standards, it doesn't recognise "sensitive personal data" such as health records, biometric information, or financial details. By treating all data uniformly, the law overlooks the vastly different levels of harm that can arise from the misuse of highly sensitive information. This "one-size-fits-all" approach weakens protections precisely where they are needed most.[28]
- Grievance Redressal: While the law promises ways for citizens to complain about data breaches, the actual grievance redressal framework is weak. It lacks clear deadlines for resolving complaints, defined paths for escalating issues, or truly independent processes. Moreover, the absence of a dedicated appellate tribunal means that unresolved citizen complaints could get stuck, creating a significant bottleneck and making it harder for individuals to seek effective recourse.[29]
- Algorithmic Harms: The law, unfortunately, overlooks the growing impact of algorithmic profiling, AI-driven decision-making, and other automated systems. These technologies are increasingly influencing everything from public services to policing and advertising. Given India's rapid adoption of technology, this omission is a serious concern, as it leaves citizens vulnerable to potential harms from opaque and unchecked algorithmic processes.[30]
- Limited Scope: Finally, the current law primarily focuses on "vertical" relationships—meaning it governs how the state or businesses handle individual data. However, it largely ignores the misuse of personal data by private individuals, informal groups, or even political actors outside of traditional institutional structures. This "limited horizontal application" means that many

[27] *Comments on the Draft Digital Personal Data Protection Bill, 2022*, Vidhi Centre for Legal Policy (Jan. 5, 2023), https://vidhilegalpolicy.in/research/comments-on-the-draft-digital-personal-data-protection-bill-2022/
[28] *IFF's First Read of the Draft Digital Personal Data Protection Bill, 2023,* Internet Freedom Foundation (Aug. 2023), https://internetfreedom.in/iffs-first-read-of-the-draft-digital-personal-data-protection-bill-2023/
[29] *Id.*
[30] *Privacy in Practice: Strategies for Data Management in India,* Kazim Rizvi & Shravishtha Ajaykumar, eds., Observer Research Foundation (Jan. 24, 2025), https://www.orfonline.org/public/uploads/posts/pdf/20250118170914.pdf

forms of data exploitation by non-institutional entities could go unchecked, leaving significant gaps in overall data protection.[31]

COMPARATIVE PERSPECTIVE:

To truly grasp where India stands with its data protection laws, it's helpful to see them through a global lens. This comparison quickly shows us what India has done well and where it still urgently needs to improve. We can look at two very different international approaches: the European Union's comprehensive General Data Protection Regulation (GDPR) and the United States' more fragmented, industry-specific system.

A. THE EUROPEAN UNION – GDPR (COMPREHENSIVE & RIGHTS-BASED):

Setting the Bar High Since May 2018, the GDPR has been the global benchmark for protecting personal data. It’s built on the idea that individuals have fundamental rights over their information, and these rules apply consistently across all EU countries. Some of its standout features include:

- Clear Permission: Companies must get explicit "yes" from individuals before using their data.
- Dedicated Data Guardians: Many organisations, especially public bodies and those handling lots of data, must appoint a Data Protection Officer (DPO) to oversee compliance.
- Proactive Risk Checks: Before undertaking risky data activities, organisations need to conduct Data Protection Impact Assessments (DPIAs) to identify and mitigate potential harms. Empowering Individuals: People have rights like asking for their data to be erased ("the right to be forgotten") or moving their data from one service to another (data portability).
- Serious Consequences: Breaking these rules can lead to hefty fines, up to €20 million or 4% of a company's worldwide revenue.
- Independent Watchdogs: Each EU country has an independent authority to ensure these rules are followed without undue influence.

Now, when we look at India’s DPDP Act of 2023, we see it has adopted some good ideas from the GDPR, like the importance of consent, giving notice, and recognising individual rights. However, it doesn't quite match the GDPR's muscle when it comes

[31] *Understanding India’s New Data Protection Law,* Carnegie Endowment for International Peace (Oct. 3, 2023), https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law?lang=en

to enforcement. India also lacks the truly independent oversight bodies seen in Europe and doesn't have the same detailed risk-based categories for data (like "sensitive personal data").[32] What's more, India doesn't require organisations to have DPOs, and broad allowances for government surveillance significantly weaken the universal data protection that the GDPR aims for.[33]

B. UNITED STATES – SECTORAL AND SELF-REGULATORY MODEL:

In stark contrast to the EU's comprehensive approach, the U.S. doesn't rely on a single, overarching federal law for data protection. Instead, it operates under a more sectoral and often self-regulatory model, meaning different rules apply to different industries or types of data. This leads to a patchwork of legislation, such as:

- HIPAA (Health Insurance Portability and Accountability Act): Specifically governs health-related data.
- COPPA (Children's Online Privacy Protection Act): Focuses solely on children's online privacy.
- GLBA (Gramm-Leach-Bliley Act): Pertains to financial institutions.
- FTC Act § 5: This broad provision underpins much of the Federal Trade Commission's (FTC) power, allowing it to act against "unfair or deceptive acts or practices" in commerce, which often includes data privacy issues.

While a growing number of U.S. states – with California leading the charge through its California Consumer Privacy Act (CCPA) and subsequent California Privacy Rights Act (CPRA) – have indeed enacted GDPR-inspired privacy laws, the overall landscape of protections remains fragmented and inconsistent across jurisdictions.[3] This means what's protected in one state might not be in another.

Conversely, India has made a deliberate move towards a unified national data protection model with the DPDP Act. While this undeniably offers a welcome degree of legal clarity, the Indian model currently lacks robust private enforcement mechanisms, such as the ability for individuals to bring class-action lawsuits. Moreover, its newly established Board doesn't quite possess the same level of independent regulatory power and established authority that the U.S. Federal Trade Commission (FTC) wields.[34]

---

[32] European Union, *General Data Protection Regulation (GDPR),* Regulation (EU) 2016/679, https://gdpr.eu/
[33] *Digital Personal Data Protection Act, supra* note 11, §17.
[34] *California Consumer Privacy Act (CCPA),* Office of the Attorney General of California (last updated July 2025), https://oag.ca.gov/privacy/ccpa

RECOMMENDATIONS FOR REFORM:

India's Digital Personal Data Protection Act of 2023 marks a crucial first step toward safeguarding personal data. Yet, its present design, appearing to favour governmental interests and ease of compliance, necessitates refinement. To genuinely uphold constitutional rights and align with global benchmarks, the Act requires targeted reforms and clarifications.

A. NARROW THE SCOPE OF GOVERNMENT EXEMPTIONS –

A key area of concern lies in Section 17, which broadly permits the Central Government to exempt any agency based on ill-defined grounds like "public order" or "sovereignty."[35] This effectively establishes a separate data framework where state entities can sidestep fundamental obligations of transparency, proportionality, and consent. To address this, reforms should focus on:

- Refining the language of Section 17: This would entail making the criteria for exemptions far more specific and less open to broad interpretation.
- Implementing robust oversight mechanisms: Introducing judicial review or independent oversight bodies would ensure accountability in state data processing.
- Mandating statutory safeguards: Clear limits on data retention and precise specifications for data usage would further protect individual privacy.

These adjustments would bring the DPDP Act in line with the "proportionality test" established in the landmark Puttaswamy judgment, thereby restoring public trust in how the state handles data.[36]

B. STRENGTHEN INSTITUTIONAL INDEPENDENCE –

The Data Protection Board of India must operate with genuine functional and financial autonomy. Its appointment processes ought to be transparent and based purely on merit, with strong safeguards against arbitrary dismissals.[37] Learning from the experiences of international bodies like the UK's Information Commissioner's Office or France's CNIL, India must ensure that data protection enforcement remains impartial, especially when government entities are implicated in violations.

C. REINTRODUCE RISK-BASED FRAMEWORK -

[35] *Digital Personal Data Protection Act, supra* note 11, §17.
[36] *Puttaswamy, supra* note at 26, ¶ 180.
[37] *Vidhi Comments, supra* note 27.

The Act, in its present form, doesn't differentiate between various types of personal data. Reintroducing classifications like sensitive personal data and critical personal data, which were part of earlier proposals, would allow us to implement protection measures that scale with risk. This means data categories prone to greater misuse, such as biometrics and health records, would receive the heightened protection they inherently require.

D. EXPAND HORIZONTAL PROTECTIONS –

Currently, the law's focus is somewhat limited, primarily addressing data misuse by corporations and government bodies. However, to genuinely reflect the intricate nature of India's data landscape, the legislation needs to explicitly extend its reach to cover private misuse by non-corporate entities. This includes, but isn't limited to, political parties, private data brokers, and various intermediaries who frequently handle vast amounts of personal information. Without this broader scope, the law overlooks significant avenues of potential harm in the real world.[38]

E. INTRODUCE AI AND PROFILING SAFEGUARDS –

As India increasingly integrates advanced technologies, its data protection framework must evolve to tackle the growing concerns surrounding automated profiling, AI-based decision-making, and algorithmic discrimination. While the European Union's General Data Protection Regulation (GDPR) has already addressed these issues under Article 22, India's law needs to adapt these principles to its unique context. This is particularly crucial given the state's expanding reliance on AI in sensitive areas like policing and welfare distribution, where algorithmic biases could have profound impacts on individuals' lives.[39]

CONCLUSION:

The Digital Personal Data Protection Act, 2023, while a pivotal step, harbours critical shortcomings. Its broad government exemptions, coupled with weak enforcement and a lack of institutional independence, prevent it from meeting the constitutional standards established in Puttaswamy or aligning with global frameworks like the GDPR. For the law to be more than a symbolic gesture, we must critically address its accountability deficits, implement risk-based protections for different data categories, and confront the distinct challenges of AI-driven

[38] *Understanding India's New Data Protection Law, supra* note 31.
[39] *GDPR, supra* note 32.

technologies. The credibility of India's digital future depends on our ability to craft a truly robust and citizen-centric legal framework.