DATA FIDUCIARY VS DATA SOVEREIGNTY: ARE INDIA'S DIGITAL LAWS READY?

Bhavika Dhuria[*] Hitesh[*]

ABSTRACT

The intersection of data fiduciary responsibilities and data sovereignty imperatives presents one of the most complex legal and ethical challenges in India's evolving digital landscape. As personal data becomes the currency of the 21st century, the need to balance individual privacy rights, corporate obligations, and national interests has never been more urgent. This article critically examines India's legislative response to this challenge, with a focus on the Digital Personal Data Protection Act, 2023 (DPDPA), and its compatibility with constitutional guarantees, international standards, and technological realities. Adopting an academic yet humanised lens, the paper explores how the fiduciary model seeks to position entities that process data as trusted custodians of individual rights, while the sovereignty model asserts state control over data flows, especially in the context of national security and economic autonomy. Through a comparative analysis of global frameworks such as the EU's GDPR, China's PIPL, and the U.S. sectoral approach, the article situates India's framework in a global context. It highlights critical gaps in definitions, oversight mechanisms, cross-border data transfer norms, and the disproportionate exemptions granted to the state. The research argues that while India has made important strides towards recognising digital rights, the current framework remains lopsided—over-regulating private entities while under-regulating state surveillance. It concludes with a set of policy recommendations focused on legislative clarity, institutional independence, user empowerment, and digital literacy. Ultimately, the article calls for a rights-centric, transparent, and participatory model of digital governance—one that treats data not merely as a resource to be mined or a threat to be contained, but as an extension of human dignity and democratic life.

[*]LLB, THIRD YEAR, CHANDIGARH UNIVERSITY.
[*]LLB, THIRD YEAR, CHANDIGARH UNIVERSITY.

Keywords: Data Fiduciary, Data Sovereignty, Digital Personal Data Protection Act 2023, Privacy Rights.

INTRODUCTION

India is currently at a pivotal juncture in its data governance journey. With over 800 million internet users, a thriving startup ecosystem, and expansive government-led digital initiatives like Aadhaar, DigiLocker, and CoWIN, the stakes have never been higher. As data becomes the currency of the digital age, the question arises: who controls the data, and in whose interest? Two competing paradigms dominate this discourse. The first is data fiduciary, a concept that views data-handling entities as stewards of user information. They are bound permanently to trustees by duty of care, fairness and loyalty. This model is rooted in protecting the individual in a deeply asymmetrical digital ecosystem, where tech giants and state agencies wield immense power over personal data. The second is data sovereignty, a concept gaining traction among governments worldwide, including India. It posits that a nation has the right to govern and regulate data generated within its borders. This involves data localisation mandates, restrictions on cross-border data flows, and asserting state control in the name of national security, economic growth, and digital independence. India's attempt to walk the tightrope between these paradigms can be seen in its recent legislative initiatives. The Digital Personal Data Protection Act (DPDPA), 2023, is a landmark effort aimed at reconciling individual privacy with national interests. Yet, questions persist: Are the rights of the data principal clearly defined? Are data fiduciaries truly accountable? Do sovereignty claims erode individual autonomy?

This article aims to find out these concerns with the following key questions in mind:

- How does Indian law define and balance the roles of data fiduciaries and state actors?
- What tensions emerge between individual rights and national control?
- How do India’s frameworks compare with those of the EU, China, and the US?
- What reforms are needed to achieve a balanced, rights-protective, and sovereign data regime?

Through a critical, comparative, and human-centred lens, this paper aims to illuminate the path forward for India in its digital governance journey.

UNDERSTANDING DATA FIDUCIARY AND DATA SOVEREIGNTY

The conceptual heart of India's digital regulation lies in two divergent yet intertwined ideas: data fiduciary and data sovereignty.

Data Fiduciary: A data fiduciary is an entity that states the purpose and means of developing personal data. The term, borrowed from trust law, implies a higher standard of responsibility. Just as a lawyer must act in the best interest of a client, a data fiduciary must process data lawfully, fairly, and in a manner respectful of the data principal's rights. In India, this idea gained traction through the Justice B.N. Srikrishna Committee Report (2018), which argued for a trust-based framework.

The key principles underlying fiduciary duties are as follows-

- Informed consent from users
- Purpose limitation (data is used only for the purpose what is stated)
- Data minimisation (collect only what is necessary)
- Accountability for breach or misuse

However, without enforceability, these remain ideals. Real accountability demands strict regulatory oversight, independent grievance mechanisms, and meaningful penalties.

Data Sovereignty: On the other hand, Data sovereignty states the idea that data—especially of citizens should be governed by the laws of the country where it originates. This concept is not new, but it has gained urgency in the context of -

- Global tech giants are dominating the Indian data markets
- Geopolitical tensions (e.g., with China)
- National security and cybersecurity imperatives
- Economic aspirations to build local data infrastructure

India's policy direction on sovereignty is evident in multiple proposals and rules—such as the Draft e-Commerce Policy (2019) and the RBI's data localisation circular (2018)—which require that financial data and sensitive personal data be stored within the country. However, unchecked sovereignty may undermine individual freedoms. Data localisation, for example, may not necessarily improve data security or privacy; instead, it could expose data to domestic surveillance and fragment global digital flows.

Intersection and Friction: While fiduciary duty is fundamentally user-centric, sovereignty is state-centric. At times, they can align for instance, in ensuring that foreign firms don't exploit Indian users' data without responsibility. At other times, they clash—particularly when state interests override consent or data rights in the name of public interest or security.

This friction raises essential questions-

- Can a government simultaneously be a regulator and a data fiduciary?
- What safeguards ensure that sovereign control doesn't become digital authoritarianism?
- How can policy preserve both individual agency and national interest?

India's legal answers to these questions lie—imperfectly—in the DPDPA 2023, which we explore next.

INDIA'S DIGITAL LEGAL FRAMEWORK: AN OVERVIEW

India's journey toward a comprehensive data protection regime has been long, often fragmented, and reactive to judicial, social, and political stimuli. Unlike jurisdictions that evolved with single, unifying privacy legislation, India's data protection architecture has developed through a patchwork of laws, regulatory circulars, and judicial pronouncements. This section outlines the key pillars of India's digital data framework prior to and alongside the Digital Personal Data Protection Act, 2023.

Constitutional Foundation (The Puttaswamy Judgment): The landmark **Justice K.S. Puttaswamy v. Union of India (2017)** judgment of the Supreme Court recognised the right to privacy as a fundamental right under Article 21 of the Constitution. This decision served as the constitutional anchor for all future data protection legislation. It not only established privacy as intrinsic to dignity and autonomy but also laid down the "three-fold test" for any state interference with personal data: legality, necessity, and proportionality. This judgment shifted the policy narrative—data protection was no longer a luxury but a constitutional obligation. It was a watershed moment that gave birth to the Srikrishna Committee in 2017, whose report in 2018 became the intellectual and ethical foundation for India's data protection law.

Information Technology Act, 2000 (and Amendments): Prior to 2023, the Information Technology Act, 2000 (IT Act) was India's primary statute governing electronic data. Section 43A of the IT Act, along with the Information Technology (Reasonable Security Practices and

Procedures and Sensitive Personal Data or Information) Rules, 2011, provided some protections.

However, the IT Act-

- Focused on corporate responsibility, not user rights
- Covered only sensitive personal data (e.g., health, financial info)
- Lacked enforcement independence
- Did not contain comprehensive rights like correction, portability, or erasure
- The lack of harmonisation between data security practices across sectors (e.g., finance vs. telecom vs. health) made compliance burdensome and user protections inconsistent.

Sectoral Regulations: Several regulators have issued their own rules for data handling such as RBI requires payment system operators to store data locally. IRDAI commands insurers to safeguard policyholder data with strict access protocols. TRAI issues directives for telecom operators especially under Do Not Disturb (DND) and KYC regimes. Ministry of Health, through the National Digital Health Mission guidelines, attempted to develop a framework for electronic health records. These efforts, though well-meaning, often overlap or conflict, leading to ambiguity for data fiduciaries. Worse, they often lack a unified rights-based lens or recourse for ordinary citizens.

Aadhaar and State-led Digital Projects: India's biggest data project is Aadhaar, the biometric identity system governed by the Aadhaar Act, 2016. Though promoted for welfare delivery, its implementation raised concerns around consent, exclusion, and surveillance. The Puttaswamy (Aadhaar-2) judgment (2018) limited Aadhaar's use but upheld it for welfare schemes. Yet, state-led digitisation programs—from CoWIN to DigiLocker—have steadily expanded data collection without consistent oversight. This dual role of the state—as both data fiduciary and regulator—raises serious concerns about conflict of interest. The lack of independent oversight mechanisms—akin to the European Data Protection Board under the GDPR—limits accountability.

THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

The long-awaited *Digital Personal Data Protection Act, 2023 (DPDPA),* finally codified a country's privacy system. It attempts to balance individual rights (via fiduciary obligations) and

sovereign authority (via exemptions and localisation flexibility). While progressive in several respects, the DPDPA has also attracted critique for vagueness and executive overreach.

Key Definitions and Structure-

The DPDPA defines the following:

Data Principal: Individual to whom the personal data pertains

Data Fiduciary: Entity states the purpose and means of processing

Consent: Free, specific, informed, unconditional, and revocable

It classifies certain fiduciaries as Significant Data Fiduciaries (SDFs) based on volume and sensitivity of data handled, subjecting them to heightened obligations like Data Protection Impact Assessments (DPIAs), grievance redressal officers, and audits.

Rights of the Data Principal

The Act provides several rights to data principals, including-

- Right to Access Information (about processing)
- Right to Correction and Erasure
- Right to Grievance Redressal
- Right to Nominate (a person in case of incapacity or death)
- These echo global best practices, though enforcement and awareness will determine their real-world efficacy.

Duties of the Data Fiduciary: Data fiduciaries must Obtain valid consent, maintain purpose limitation, Implement security safeguards and notify data breaches and respect children's data with parental consent. Non-compliance can lead to penalties ranging from ₹10 crore to ₹250 crore, as the case may be.

Government Exemptions and Concerns: One of the most controversial sections of the DPDPA is Section 17, which entitles the Central Government to exempt any emergent "instrumentality of the state" in the guise of national security, public order, or sovereignty from the provisions of the Act. This creates a broad escape route for surveillance or non-transparent use. It blurs the boundary between legitimate state interests and arbitrary overreach. The

proportionality test prescribed by the Supreme Court in Puttaswamy is avoided. Furthermore, the Data Protection Board, while an adjudicatory body, lacks the independence of a constitutional authority and is appointed by the government itself—raising concerns about autonomy and checks.

Sovereignty via Localisation: The 2023 DPDPA did not prescribe exclusive localisation of data, permitting cross-border movement of data. This is a pragmatic shift, aligned with India's desire for trade agreements (e.g., with the EU or US), but it softens the sovereignty push—raising questions on enforcement and reciprocity.

GLOBAL MODELS: EU, CHINA, AND THE US

India's attempt to balance data fiduciary obligations and sovereignty over data is not unique. Globally, jurisdictions have approached this balance through different legal and political frameworks—ranging from rights-centric regimes to state-driven control. A comparative analysis of the European Union (EU), China, and the United States (US) highlights key lessons and warning signs.

The European Union: Rights and Regulation: The General Data Protection Regulation (GDPR) is often hailed as the gold standard in data protection. It is based on a fundamental rights approach, treating personal data as an extension of individual autonomy and dignity.

Key features-

- Priority on user rights: access, correction, deletion, portability, and opposition.
- Strict consent frameworks, including opt-in models and granular control.
- Data fiduciary-like duties are imposed on data controllers and processors.
- Cross-border transfer restrictions: data can only be transferred to jurisdictions ensuring "adequate" protection.
- Data Protection Authorities (DPAs) in each member state and a coordinating European Data Protection Board (EDPB).

Lessons for India: A robust, independent oversight mechanism ensures rights are not merely theoretical. Provisions like "privacy by design" and "data protection *impact assessments* (DPIA)" are critical in preventing harm before it occurs. India's DPDPA, while inspired by the GDPR, lacks the same degree of regulatory independence and judicial oversight.

China (Sovereignty First): China's data protection framework is driven primarily by state control and security imperatives, though recent reforms reflect growing concerns about consumer privacy.

Key Instruments

Personal Information Protection Law (PIPL): This 2021 addition reads like GDPR with a Chinese flavour inside a state-supervised model.

Data Security Law and Cybersecurity Law: assert data localisation, national security vetting, and state surveillance mechanisms. China mandates Local storage of critical data, Security assessments for cross-border transfers, Vague but expansive state access rights, often without court oversight.

Lessons for India

- Excessive state control may achieve sovereignty, but it undermines civil liberties.
- Without independent redressal, consent can be reduced to a formality.
- India's broader democratic framework calls for transparency and proportionality, which China's regime lacks.

United States (A Patchwork of Protections): US does not have a single data protection law. Instead, it follows a sectoral model, with laws like HIPAA (healthcare), GLBA (finance), COPPA (children) and CCPA/CPRA (California's consumer protection laws).

Features

- Business-driven flexibility rather than rights-based rigidity.
- The federal government has limited control; most initiatives are state-led.
- Emphasis on self-regulation and industry codes of conduct.

Lessons for India

- The fragmented US model results in inconsistent protections and limited accountability.
- India's unified law is preferable—but it must not sacrifice substance for simplicity.
- Sector-specific regulators in India must be aligned under the broader DPDPA framework.

Synthesis (Where India Stands): India's DPDPA borrows principles from the GDPR but allows for China-style state exemptions. Unlike the US, it seeks a unified framework, but its challenge lies in weak enforcement, independence and state overreach clauses. To balance fiduciary duty with sovereign control, India must- create independent regulatory institutions**,** define public interest and national security narrowly and transparently and enable judicial oversight over exemptions.

SECTORAL CASE STUDIES IN INDIA

To assess the real-world effectiveness of India's data laws, we must explore how fiduciary obligations and sovereignty claims play out in specific sectors. The following case studies illustrate recurring themes: conflicting duties, blurred lines of consent, and institutional vacuum.

Healthcare (Consent in Crisis): During the COVID-19 pandemic, platforms like *Aarogya Setu and CoWIN* became central to public health surveillance. These platforms collected sensitive personal data: location, health status, contact history, and vaccination status.

Key concerns-

- Consent was bypassed in emergency use.
- No clear sunset clauses on data retention.
- Lack of clarity on data-sharing with private entities.
- Aarogya Setu's privacy policy was vague, and the platform was initially claimed to be voluntary but later mandated for travel and employment.

Implications: State acted as both fiduciary and sovereign—but with minimal transparency. The absence of judicial oversight or grievance redress exposed the limits of user protection. If Data Protection Board existed, it could have held authorities accountable.

Fintech and Financial Data

Localisation v Innovation: The Reserve Bank of India (RBI) has ensured that all data generated in the payment systems should be stored within the country. This will impact players like Google Pay, PhonePe, Paytm and Razorpay.

Challenges

- Foreign firms argue localisation increases costs and reduces innovation.
- Domestic firms worry about unclear compliance expectations.
- Users are unaware of how and where their financial data is stored.
- The fiduciary duties of these platforms are shaped by RBI circulars, but without a unified framework for consent, erasure, or portability, users remain powerless.
- Sovereignty is invoked in the name of national security, but it is not always clear what data poses a risk or how oversight is ensured.

Cloud Services and Cross-border Transfers: Many Indian businesses rely on foreign cloud providers (e.g., Amazon AWS, Microsoft Azure). These platforms store and process large volumes of user data across multiple jurisdictions.

Issues

- Uncertainty about cross-border data sharing rules post-DPDPA.
- Companies fear legal ambiguity when choosing providers outside India.
- The absence of a whitelist of trusted jurisdictions leads to over-compliance or non-compliance.

India must balance the following:

- Economic pragmatism (via partnerships and trade)
- Sovereignty mandates (ensuring Indian legal authority over its citizens' data)
- Fiduciary responsibilities (transparency with users)

Without clarity, companies default to restrictive interpretations, stifling cloud-based innovation.

Government as Fiduciary-The DigiLocker Case

DigiLocker, the national cloud-based document wallet, stores KYC documents, academic certificates, and IDs. It represents the State-as-Fiduciary, managing individual documents for welfare and ease of access. While user experience has improved, following concerns remain-

- Are audit trails publicly available?
- Can users delete or transfer data?
- How are breaches managed?

When the government performs dual roles—as regulator and fiduciary there must be institutional safeguards to prevent misuse.

Summary of Sectoral Lessons

- Fiduciary obligations in India are weakly enforced and poorly understood.
- Sovereignty is frequently invoked, but its boundaries remain undefined.
- Users have few remedies and limited awareness of their rights.
- Regulatory silos between RBI, TRAI, MeitY, and others lead to overlapping or contradictory compliance mandates.
- India's digital future depends on harmonising these tensions through clear legal definitions, regulatory cooperation, and citizen empowerment.

CHALLENGES AND GAPS IN THE CURRENT FRAMEWORK

Despite the enactment of the Digital Personal Data Protection Act, 2023, India's data protection landscape remains riddled with structural, legal, and ethical challenges. While the Act lays down a foundation for reconciling data fiduciary responsibilities with sovereign interests, its implementation framework raises several concerns.

Regulatory Overlaps and Fragmentation: India's data governance continues to suffer from regulatory fragmentation. The coexistence of sectoral regulators like RBI, TRAI, IRDAI, and MeitY—each issuing their data norms—creates conflicting mandates for data fiduciaries. For example, A fintech app may be required by the RBI to localise data, while also being subject to DPDPA obligations for cross-border processing, raising confusion over which takes precedence. In the absence of a central coordination mechanism, fiduciaries face legal uncertainty and compliance fatigue. Moreover, the Data Protection Board (DPB), though

envisioned as the nodal adjudicatory body, lacks true independence. Unlike the GDPR's supervisory authorities, the DPB is structurally tied to the executive, undermining the credibility of enforcement.

Lack of User Awareness and Digital Literacy: One of the most under-discussed challenges is the **digital illiteracy of Indian users**. Terms like "consent," "data minimisation," or "purpose limitation" are alien to many users, especially in rural or marginalised communities. Even if fiduciaries obtain consent, it is often **uninformed and symbolic**—presented through dense privacy policies that most users do not read. This makes it easier for state or corporate actors to use consent as a shield for unethical data processing. Digital empowerment must go hand in hand with regulation. Without awareness, the rights granted under DPDPA may remain paper tigers.

Broad State Exemptions: Section 17 of the DPDPA allows the central government to **exempt any state entity** from compliance if deemed necessary for public order, national security, or sovereignty. While some degree of flexibility is warranted, the **lack of judicial or parliamentary oversight** over such exemptions opens the door for arbitrary surveillance. For example, law enforcement agencies could theoretically collect personal data without consent or transparency under a blanket exemption—bypassing the proportionality test laid down in Puttaswamy. Such unchecked sovereign power directly undermines the fiduciary principle of trust and fairness, and has **chilling effects on democratic rights**.

Vague Terminology and Undefined Principles: Key concepts in the DPDPA like "public interest," "reasonable expectation," "harm," or even "significant data fiduciary" are left undefined or under-defined.

This creates the following:

- Legal uncertainty for companies
- Ambiguity for courts
- Loopholes for misuse

Without clear definitions, enforcement becomes inconsistent, and rights become hard to defend.

Weak Enforcement Mechanisms-

The success of any data protection regime depends on enforcement, deterrence, and trust. Currently, the DPDPA:

- Lacks clear timelines for redressal
- Gives discretionary powers to the Board
- Doesn't offer class-action remedies for affected communities
- Has limited provisions for independent audits or inspections

The imbalance of power between users and large data fiduciaries remains unaddressed, making remedies inaccessible and diluted.

Cross-Border Challenges and Global Non-Alignment-

With data increasingly flowing across borders, India's failure to define *"trusted"* jurisdictions for cross-border data transfer creates uncertainty. Multinational companies fear investing in Indian infrastructure without clarity on:

- Where can they send data?
- How to sign Standard Contractual Clauses (SCCs)
- What penalties do they face for violations?

At the same time, India's insistence on retaining sovereign control makes ***international data transfer agreements*** difficult, delaying potential trade pacts and digital services growth.

RECOMMENDATIONS

Legislative Reforms-

Narrow State Exemptions Amend Section 17 to ensure exemptions are granted only after the following:

- Legislative approval or
- Review by an independent oversight body.

Defined Key Terms: It provided clarity on Public interest, National security, significant data fiduciary and Harm. This will reduce regulatory discretion and improve transparency.

Judicial Oversight: Introduce a system where state-led data processing is subject to **judicial review or warrants**, especially in cases involving surveillance or sensitive personal data.

Institutional Recommendations

Independent Regulator: Upgrade the **Data Protection Board** into an **autonomous authority**, akin to the Election Commission or CAG. Independence is critical to win public trust.

Sectoral Harmonisation: Create a **National Data Governance Council** to coordinate between MeitY, RBI, TRAI, IRDAI, and others—ensuring uniformity in standards, rights, and duties.

Capacity Building: Train data protection officers, the judiciary, and law enforcement on privacy ethics, user consent, and global compliance norms.

Public-Centric Interventions-

Awareness and Literacy Campaigns to run multilingual public campaigns (like voter awareness or health drives) to:

- Educate users about their rights
- Explain grievance mechanisms
- Promote ethical data use

Privacy-by-Design in Tech: Encourage developers to embed privacy features into apps and services by design, rather than as post-facto add-ons.

Youth and School Curriculum: Include data ethics, cyber hygiene, and privacy rights in school curricula—building a future-ready digital citizenry.

CONCLUSION

In 2025, data is not just digital code—it is the heartbeat of human identity, livelihood, and dignity. For someone like Aarti, a gig worker in Delhi relying on digital wallets for income, data misuse could mean financial exclusion. For Mohammad, a farmer from Bihar, unauthorised access to land documents or biometric records could lead to dispossession. For millions of others, digital footprints leave a trail that is deeply human—vulnerable, intimate,

and permanent. India stands at the cusp of becoming a global digital leader. But that leadership must rest on **ethical scaffolding**, not just infrastructure. Laws must not only serve corporate ease or government control—they must serve the people, with accountability, empathy, and foresight. To answer the question: Are India's digital laws ready? — The honest response is: not yet. But with reform, resolve, and rights at the centre, they can be. The future of India's data governance lies not just in its statutes, but in the spirit of its constitutional promise to protect liberty, dignity, and justice in every byte of digital life.