# Navigating the Tension between Innovation and Data Privacy Laws in India and California


**Dr.Vartika Goyal***
**Dr.Gunjan Rawat****

## Abstract

*India's Digital Personal Data Protection Act, 2023 (DPDPA) marks a key step in protecting personal data while promoting the digital economy. Yet, balancing privacy with technological growth poses challenges, including broad government powers, no independent regulator, compliance pressures on smaller businesses, and unclear cross-border data rules. The article finds that while the law sets a solid base, its success hinges on transparent governance, accountable institutions, and regulations that protect privacy without hindering innovation.*

**Key Words**: *Data Privacy, Innovation vs. Regulation, Right to Privacy, Data Governance, Technological Advancement, Regulatory Challenges.*

## I. Introduction

In the 21st-century digital economy, data has emerged as one of the most valuable assets, driving innovation, economic growth, and governance efficiency. As India rapidly transitions into a digitally empowered society, propelled by initiatives like *Digital India*, *Startup India*, and the expansion of AI and fintech sectors, the collection and processing of personal data have become deeply embedded in everyday transactions. This digital transformation, however, has brought with it serious concerns about individual privacy, data misuse, and the unchecked power of both private companies and the state.The enactment of the Digital Personal Data Protection Act, 2023[1] (DPDPA) marks a significant legal milestone in India's efforts to address these concerns. Framed in the

*371 Lundy Place,Milpitas 95035,California,US.
**Assistant Professor,IIS University, Jaipur.

1. The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023.

aftermath of the Justice K.S. Puttaswamy (2017) judgment that recognized the right to privacy as a fundamental right, the Act aims to create a comprehensive framework for protecting personal data while also enabling the growth of a robust digital economy. The Act introduces concepts such as data fiduciaries, data principals, consent-based processing, and the creation of a regulatory authority—the Data Protection Board of India.

Despite these advancements, the implementation of the DPDPA raises several challenges. The law attempts to balance two potentially conflicting goals: protecting individual privacy rights and facilitating technological and economic innovation. This balancing act becomes particularly difficult given India's socio-economic diversity, digital infrastructure gaps, and the need to support emerging tech enterprises without imposing excessive compliance burdens. Furthermore, concerns have been raised over the Act's vague exemptions for government agencies, the limited independence of its regulatory framework, and ambiguities in cross-border data transfer provisions. This article critically examines the challenges that India faces in operationalizing its data protection law without stifling innovation. It explores the tension between privacy and progress, evaluates the strengths and shortcomings of the DPDPA, and draws comparisons with global regulatory models like the GDPR and CCPA. The goal is to identify pathways through which India can develop a rights-respecting yet innovation-friendly data governance regime.

## II. Historical Background

India's journey toward establishing a formal data protection regime has been both reactive and evolutionary, shaped by growing digital adoption, concerns over state surveillance, and judicial recognition of privacy as a fundamental right. For many years, India lacked a dedicated data protection law. Instead, personal data was loosely regulated through sectoral laws and provisions under the Information Technology Act, 2000, particularly under Section 43A and the IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. However, these measures were widely regarded as inadequate, particularly in the face of emerging technologies, increasing cyber threats, and the rapid expansion of the digital economy.

The watershed moment came in 2017, when the Supreme Court of India, in the landmark case of *Justice K.S. Puttaswamy (Retd.) v. Union of India*[2], unanimously held that the right to privacy is a fundamental right under Article 21 of the Constitution. This judgment not only recognized informational privacy as a constitutional value but also imposed an obligation on the State to enact

2. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1, 497 (India).

a comprehensive data protection framework. In response, the Government of India constituted the Justice B.N. Srikrishna Committee, which submitted a draft Personal Data Protection Bill in 2018. The bill went through multiple iterations over the years, reflecting ongoing debates on issues such as data localization, surveillance, state exemptions, and regulatory independence.

After years of consultations, revisions, and public discussions, the Digital Personal Data Protection Act, 2023 (DPDPA) was enacted. This law is the culmination of nearly a decade of policy deliberations and judicial influence. It seeks to create a legal framework that protects personal data while also facilitating the use of data for innovation, governance, and business efficiency. However, unlike the European Union's GDPR, which places individual rights at its core, or the California Consumer Privacy Act (CCPA), which focuses on consumer choice, India's DPDPA attempts a hybrid model—recognizing privacy while supporting data-driven innovation.

This background highlights the broader challenge India now faces: implementing a law that must uphold constitutional privacy rights, align with international data protection standards, and simultaneously encourage technological progress in a rapidly expanding digital economy.

## III. Legislative Trends

The legislative evolution of data protection laws in India reflects a growing recognition of the need to balance the imperatives of individual privacy with the demands of technological innovation and economic development. Globally, data protection frameworks have taken different forms—some prioritizing privacy as a fundamental right, others emphasizing commercial regulation. India's legislative journey has drawn from both approaches, resulting in a hybrid legal framework in the Digital Personal Data Protection Act, 2023 (DPDPA).

### A. From Sectoral Regulations to Comprehensive Legislation

India's early approach to data protection was fragmented and sector-specific, primarily governed by the Information Technology Act, 2000 and the IT Rules, 2011. These frameworks offered minimal safeguards and lacked enforcement teeth. As digital technologies evolved—especially with the rise of e-governance, fintech, and social media platforms—the limitations of the existing regime became increasingly apparent. This prompted a shift in legislative intent towards a unified, purpose-built law, especially after the Puttaswamy judgment (2017), which held that privacy is a fundamental right.

## B. Emergence of Rights-Oriented Drafts

Following judicial guidance, the Justice B.N. Srikrishna Committee submitted the Personal Data Protection Bill, 2018, which drew heavily from the European Union's General Data Protection Regulation (GDPR). The draft emphasized individual rights, strict processing norms, and proposed an independent Data Protection Authority. However, subsequent versions of the bill—particularly the 2019 draft and finally the 2023 Act—revealed a gradual dilution of some rights-based principles, reflecting the government's effort to balance privacy with innovation, national security, and economic concerns.

## C. Executive Flexibility and State-Centric Control

A key legislative trend in the DPDPA, 2023 is the centralization of rule-making powers in the executive. The Act empowers the central government to notify significant portions of its framework through delegated legislation. While this allows flexibility to adapt to technological change, it also raises concerns about legal certainty, transparency, and regulatory independence—critical for both protecting citizens' rights and ensuring investor confidence.

## D. Focus on Innovation and Ease of Doing Business

Unlike its earlier drafts, the 2023 Act relaxes data localization requirements, simplifies compliance for startups and small entities, and introduces broad exemptions for state functions. These trends reflect the government's strategic shift to make the law business-friendly, encouraging investment in India's digital ecosystem while maintaining a basic privacy framework. However, this shift has sparked debates about the adequacy of privacy protections, especially in the absence of strong, independent oversight.

## E. Alignment with Global Trends

India's legislative trend mirrors the global movement toward hybrid models of data governance. Like the California Consumer Privacy Act[3] (CCPA), which emphasizes consumer choice and commercial compliance, the DPDPA incorporates flexible obligations for data fiduciaries. At the same time, it adopts elements from rights-centric models like the GDPR, such as data principal rights and the requirement of consent. The challenge lies in operationalizing these principles in a way that does not stifle innovation but still upholds constitutional values.

The legislative trends surrounding India's data protection law reflect a nuanced attempt to create a context-sensitive framework—one that protects

3. The California Consumer Privacy Act, 1798.100–1798.199 Cal. Civ. Code (2018).

individual privacy without obstructing digital growth and innovation. The shift from strict regulatory proposals to a more adaptive and innovation-friendly legal architecture suggests a deliberate effort to balance constitutional obligations with developmental aspirations. However, the true test of this legislation lies not just in its drafting but in its implementation, interpretation, and enforcement, which must address both citizen rights and the demands of a rapidly evolving digital economy.

## IV. Various Aspects

The implementation of the Digital Personal Data Protection Act, 2023 (DPDPA) presents a multidimensional challenge as it seeks to strike a fine balance between individual privacy rights and the economic need for digital innovation. This balance is crucial in an era where data is not only a resource but also a matter of personal dignity and national interest. The key dimensions in this balancing act include:

### A. Legal and Constitutional Dimension

The right to privacy, recognized as a fundamental right under Article 21 of the Indian Constitution (Puttaswamy Judgment, 2017), is the legal backbone of data protection. However, the law must also account for reasonable restrictions, particularly for national security, public order, and innovation. The DPDPA attempts to uphold privacy while granting the State broad discretionary powers, such as exemptions from consent in certain cases. This raises questions about the constitutionality and proportionality of such provisions.

### B. Technological Dimension

Innovation in artificial intelligence (AI), big data analytics, cloud computing, and machine learning heavily relies on large-scale data processing. A stringent data protection regime could stifle such innovation if compliance burdens are too high. On the other hand, weak safeguards could lead to misuse of personal data. Therefore, the law must support privacy-by-design frameworks, data minimization principles, and technological safeguards like encryption to allow innovation without compromising personal data.

### C. Economic and Business Dimension

Startups, digital platforms, and global tech companies view data as a strategic asset. The DPDPA provides compliance relaxations for smaller entities, but the ambiguity around consent, cross-border data transfer, and data fiduciary

obligations may deter investment. The challenge lies in ensuring ease of doing business while maintaining a trust-based digital economy, especially as India aspires to become a global data hub.

## D. Regulatory and Institutional Dimension

The Act proposes the establishment of a Data Protection Board of India, but concerns exist about its independence and effectiveness due to the high degree of executive control. A truly independent and well-resourced regulatory body is essential for fair enforcement, grievance redressal, and compliance oversight. Weak regulation could undermine both user trust and corporate accountability.

## E. Social and Ethical Dimension

In a country with low digital literacy, informed consent and awareness about data rights remain limited. This gives rise to ethical issues around manipulation, surveillance, profiling, and algorithmic bias. Balancing privacy with innovation also means protecting vulnerable populations from digital exploitation, while ensuring inclusive access to data-driven services.

## F. Global and Geopolitical Dimension

India's data protection law must also align with international standards to facilitate cross-border data flow and trade negotiations. Striking a balance between data sovereignty and global interoperability (with laws like GDPR and CCPA) is crucial for India's position in global digital governance. Overly restrictive laws could lead to data localization demands that hamper international collaborationBalancing innovation and privacy is not a one-time legislative act but a dynamic, evolving process. The success of India's data protection law depends on how well it manages these overlapping dimensions—protecting personal dignity, encouraging responsible innovation, ensuring regulatory fairness, and maintaining global credibility. The law must evolve in response to emerging technologies, citizen expectations, and global standards, making adaptive governance the key to its long-term success.

# V. Constitutional Aspects

The constitutional framework of India provides the guiding principles for balancing innovation with the fundamental right to privacy. After the Supreme Court's landmark judgment in *Justice K.S. Puttaswamy v. Union of India* (2017), privacy was firmly established as an intrinsic part of Article 21,

meaning that any restriction on personal data must satisfy the tests of legality, necessity, and proportionality. At the same time, the Constitution also protects the freedom of trade, expression, and equality under Articles 19 and 14, which support technological development, digital entrepreneurship, and innovation in the larger public interest. The Digital Personal Data Protection Act, 2023 attempts to harmonize these competing claims by recognizing the right of individuals to safeguard their data while enabling lawful use of data for governance, research, and economic growth. However, the Act's broad government exemptions, vague definitions such as "public interest," weak regulatory independence, and high compliance burdens for startups pose serious constitutional and practical challenges. These issues raise concerns of arbitrariness under Article 14, possible violation of proportionality under Article 21, and potential chilling effects on freedom of trade and innovation under Article 19. Thus, the real constitutional test lies not merely in the passage of the law but in its implementation—ensuring that privacy is meaningfully protected while innovation is fostered within the boundaries of constitutional safeguards. **Directive Principles of State Policy (Articles 38, 39, 43, 47)** The State has a duty to promote welfare, scientific development, and access to information while protecting citizens' dignity. Data-driven innovation in areas like health, education, and fintech aligns with **directive principles**, but must be harmonized with fundamental rights. India's Constitution provides a robust foundation to balance **privacy** and **innovation**: **Privacy (Article 21)** must be protected as a core fundamental right.**Innovation and economic growth (Articles 19, 38, 39, 43)** are legitimate state interests.The real challenge lies in **implementation**—ensuring that the DPDP Act and its rules uphold **legality, necessity, and proportionality**, while enabling a thriving digital economy.

Courts, regulators, and policymakers will need to **continuously calibrate** this balance to prevent privacy from being sacrificed in the name of progress, or innovation from being stifled by rigid regulation.

## VI. Judicial Scenario

The Indian judiciary has played a pivotal role in shaping the discourse around data protection and privacy, especially in the absence of a dedicated legislative framework until recently. While courts have largely emphasized the primacy of the right to privacy, they have also acknowledged the legitimate interests of the State and industry in promoting innovation and economic growth. The evolving jurisprudence reveals a careful attempt to balance individual rights with collective technological advancement.

### 1.2 K.S. Puttaswamy (Aadhaar-5J) & Others v. Union of India (Supreme Court)

- The Aadhaar judgment is a touchstone for privacy jurisprudence in India. It upheld the constitutional validity of the Aadhaar scheme but also imposed limits, particularly on which uses of Aadhaar are mandatory.
- Important rulings include striking down Section 57 of Aadhaar Act insofar as it permits private entities to use Aadhaar authentication compulsorily, limiting retention of authentication (and other) metadata, and insisting on minimality, purpose limitation, and proportionality. The dissent (by Justice Chandrachud) raised concerns of the risks of profiling, aggregation of data silos, and surveillance architecture.

### 2. High Court Cases Around Aadhaar Location / Usage Data Disclosure

- There is a case (Bengaluru High Court) where the court held that UIDAI can be required, via a High Court order, to share Aadhaar authentication / usage / location data in a missing persons investigation. The Court balanced the need for data for law enforcement with the Aadhaar Act's safeguards.
- Such cases are significant because they test the boundaries of "exemptions" or lawful access to what is typically sensitive personal data under Aadhaar / related regime.

### 3. Supreme Court & Election Commission — Aadhaar as Proof of Identity but Not Citizenship [4](Bihar SIR)

- The Supreme Court has recently clarified that Aadhaar may serve as a proof of identity in the Special Intensive Revision (SIR) of electoral rolls in Bihar, but **not** as proof of citizenship.
- This case is relevant to data protection and constitutional safeguards: it draws a line between permissible uses of identity data and uses that may strain or overburden privacy or citizenship rights. It also reflects judicial scrutiny on how state bodies require or accept Aadhaar in various administrative settings.

4. Association for Democratic Reforms v. Election Commission of India, W.P.(C) No. 640 of 2025 (India).

**4. PhonePe & Information Sharing Case** (Karnataka High Court)

- Karnataka HC rejected PhonePe's plea against a notice under CrPC Section 91 for sharing transaction information in a criminal investigation. The Court held that user privacy must yield where there is a lawful investigative necessity. This is important in balancing privacy (especially of financial transactions) with law enforcement and public safety needs.

**5. Karthick Theodore / Ikanoon Software Development Pvt. Ltd & Ors** (Madurai Bench, Madras High Court; stayed by SC)

- This addresses whether personal / sensitive information in judgments published online must be redacted, especially for individuals acquitted. The Madurai Bench held that litigants have a discretionary right not to have their identity or "sensitive personal info" published, but that decision has been stayed by the Supreme Court.
- It shows tensions between transparency / public record (innovation in access to legal records, open justice) vs privacy of persons involved.

**6. Association for Democratic Reforms v. Election Commission of India[5] (2024, Supreme Court, Electoral Bonds case)**

- While not strictly a "data protection" case, it intersects privacy, free speech, transparency: the Court struck down the Electoral Bonds Scheme over right to information issues, highlighting constitutional norms of transparency, accountability, and how financial data (donor identity) implicates democratic values.

**7. ABC v. State (NCT of Delhi) (Nov 2024)**

The Delhi High Court ruled that individuals cleared of guilt in quashed criminal proceedings have a "right to be forgotten" to protect their dignity. It directed Google and other search engines to mask the petitioner's name in online records.

**8. Exonerated Banker Case (Dec 2025)**

The Delhi High Court held that the right to dignity and reputation under Article 21 can override media freedom once a person is exonerated in high-profile cases.

**9. WhatsApp LLC v. Competition Commission of India (CCI) (2024–2025)**

The NCLAT (Dec 2025) clarified that WhatsApp must provide opt-out rights and transparent safeguards for all data sharing with Meta, including for advertising purposes.

5. Association for Democratic Reforms v. Union of India, 2024 INSC 113.

The Supreme Court had previously directed WhatsApp to publicize that Indian users do not have to accept its 2021 privacy policy to continue using the platform.

## 10. RBI Master Direction (2024)

Effective April 1, 2024, it mandates regulated entities (banks, NBFCs) to institute rigorous IT governance and report cyber incidents to the RBI and CERT-In within 6 hours.

## 11. SEBI Cloud Framework (2023)

Required SEBI-regulated entities to ensure that data processed via public or hybrid clouds is stored within India's legal boundaries by March 2024.

## 12. Summary of Data Principal Rights (2025)

Under the current regime, individuals ("Data Principals") have the right to:

Access and Correction: Request a summary of their data and correct inaccuracies.

Erasure: Request deletion of data once the purpose is served or consent is withdrawn.

Grievance Redressal: File complaints online via a dedicated portal/app for resolution within 90 days.

Nomination: Appoint a representative to exercise rights in case of death or incapacity.

These cases bring out several constitutional/implementation challenges for India's Data Protection framework (including the DPDP Act, 2023):

- **Defining and Limiting Exemptions / Mandatory Uses**: The Aadhaar case shows courts are ready to strike down or limit statutory provisions that make certain usages (by private parties, or compulsion) mandatory. The DPDP Act will need clear boundaries for what states/private actors can be compelled to do, with strong legal safeguards.

- **Lawful Access vs Privacy Safeguards**: Cases involving law enforcement access (PhonePe, Aadhaar location data) show courts balancing privacy against investigation/public interest. But these often hinge on strong procedural safeguards (judicial orders, limited scope). The DPDP regime must ensure similar procedural checks.

- **Transparency, Redaction, Public Access vs Right to Privacy**: The Karthick Theodore case shows that publication of judgments and legal data is one area where innovation (access to case law, legal databases)

collides with privacy claims (especially for acquitted persons or those who have their identities exposed unfairly).

- **Data Minimization, Purpose Limitation and Retention Periods**: Aadhaar judgment (majority & dissent) emphasized minimal data collection and storage, limited retention of authentication logs, etc. Implementation and any legal rules (including DPDP rules) must enforce these principles, else they risk constitutional infirmity.
- **Identity vs Citizenship vs Rights**: The Bihar SIR case clarifies that identity proof can be different from proof of citizenship. This matters in preventing overreach that may infringe rights of non-citizens or marginalized persons. The state's use of identity systems must not be conflated with heavier legal statuses unless legally valid.
- **Institutional Readiness & Regulatory Enforcement**: Many judgments implicitly point out lack of strong oversight, ambiguity in mechanisms. For example, concerns in Aadhaar case about UIDAI's responsibilities for security, about grievance redress, about data misuse. DPDP Act will be judged not only on paper but on whether oversight body (Data Protection Board) is effective.

Courts will likely be called upon to interpret these provisions in light of constitutional values and international privacy standards, particularly when balancing innovation with individual autonomy. The Indian judiciary has so far taken a balanced and nuanced approach to privacy and innovation. It has neither ignored the importance of technological advancement nor allowed it to trample upon individual rights. As India navigates the implementation of its data protection law, the courts will continue to play a critical role in ensuring that innovation is pursued responsibly, and that privacy remains a non-negotiable cornerstone of India's digital future.

## VII. Conclusion

The enactment of the Digital Personal Data Protection Act, 2023 marks a significant step in India's efforts to safeguard personal data in an increasingly digitized economy. However, the true test lies in how effectively the law can balance the competing demands of individual privacy and technological innovation. While the legislation provides a long-awaited legal framework for data protection, its success will depend on the clarity of subordinate rules, the independence of regulatory bodies, the enforcement of compliance, and the protection of fundamental rights.

India's aspirations to become a global digital hub require a data regime that is not only business-friendly but also rights-respecting. Overly rigid rules can stifle innovation, especially among startups and smaller enterprises, whereas insufficient safeguards may undermine public trust and constitutional liberties. Therefore, a flexible yet robust regulatory approach is essential.

Judicial precedents have consistently emphasized proportionality, necessity, and transparency as guiding principles for any restriction on privacy. Moving forward, India must ensure that the implementation of its data protection law aligns with these principles, while also encouraging responsible data-driven growth. Striking the right balance between innovation and privacy is not a one-time achievement but an ongoing process—one that must evolve with technology, public expectations, and global norms. As India builds its digital future, the ability to protect personal data while enabling innovation will define the credibility, fairness, and sustainability of its digital ecosystem.