# DATA PRIVACY LAW IN INDIA: PAST PRESENT AND LEGAL FRAMEWORK

Manisha Nandan, Jharkhand High Court, Ranchi

**ABSTRACT**

India's data privacy landscape has evolved significantly, driven by the rise of digital technologies and the 2017 Puttaswamy judgment recognising privacy as a fundamental right. The Digital Personal Data Protection Act of 2023 emphasizes transparency, consent-based processing, and individual rights like data access and correction. While it aligns with global standards, challenges include compliance costs, digital divides, and concerns over government exemptions. As India navigates emerging technologies like AI, fostering public awareness and corporate accountability is vital. By balancing individual rights, national security, and economic growth, India aims to build a robust, trustworthy digital ecosystem.

## Introduction

In today's digital age, data privacy is one of the most pressing concerns globally. With personal information being collected, processed, and shared by various entities—such as governments, businesses, and online platforms—data privacy has moved beyond a mere policy concern to become a fundamental right in many countries, including India. Data privacy in India is particularly significant given the country's rapid digital transformation, marked by the widespread adoption of internet services, social media, and e-commerce. These advancements, however, have created new challenges as the volume of personal data online continues to grow, and the lines between public and private data are increasingly blurred.

The need for robust data privacy measures has grown as citizens become more aware of the risks associated with unregulated data access. From identity theft to data breaches, the potential harms of inadequate data security underscore the need for comprehensive protection. In response, India has gradually implemented various legal frameworks to ensure data security, the most recent being the Digital Personal Data Protection Act of 2023 (DPDP).

This article examines the evolution of India's data privacy laws, evaluates the current state of data protection, and considers future directions in India's journey toward securing digital rights for its citizens.

## Historical Evolution of Data Privacy Laws in India

### IT Act, 2000 and Early Legislation

The Information Technology Act of 2000 (IT Act) was a significant legislative milestone for India, marking its initial foray into data regulation and cyber law. This act was primarily aimed at combating cybercrime, which was becoming increasingly prevalent, and at promoting the growth of e-commerce as the Internet began to play a central role in business transactions. The IT Act included various provisions to penalise unauthorised access to data, thereby establishing a legal framework to address online offences. However, while it laid the groundwork for cyber security, the act's provisions regarding privacy protection were notably limited. In response to growing concerns about personal data safety and privacy, amendments were introduced in 2008. These amendments brought important changes, including Sections 43A and 72A of the IT Act. Section 43A requires companies to implement adequate security measures to protect

personal data. If a company failed to secure this data and an individual suffered, the company was liable to compensate the affected person. On the other hand, Section 72A introduced penalties for the unauthorized disclosure of personal information by individuals who had access to such data during their professional duties. Despite these advancements, the amendments revealed that the IT Act's measures only covered a limited range of issues related to data protection. Many significant gaps remained unaddressed, leaving individuals vulnerable and highlighting the ongoing need for comprehensive personal data privacy and protection regulations in the rapidly evolving digital landscape.

**The *Puttaswamy* Judgment (2017): Privacy as a Fundamental Right**

The 2017 Supreme Court ruling in Justice K.S. Puttaswamy (Retd.) v Union of India marked a transformative moment in India's data privacy landscape by affirming privacy as a fundamental right. The case arose in response to the government's Aadhaar program, a nationwide biometric identification initiative that made Aadhaar mandatory for accessing various public services and benefits. Concerns about excessive government surveillance, potential misuse of personal data, and the lack of adequate data protection frameworks led to this challenge. The nine-judge bench unanimously held that the right to privacy is integral to Article 21, which safeguards the Right to Life and Personal Liberty under the Indian Constitution.

This judgment laid the foundation for a more robust, constitutionally recognised mandate for data privacy, asserting that privacy encompasses personal autonomy, dignity, and the right to make choices without unwarranted interference. It highlighted the necessity for laws that balance citizens' rights to privacy with the state's interest in regulating data for national security, welfare, and governance purposes. In the wake of this decision, the urgency to introduce comprehensive data protection legislation became undeniable, leading to the creation of the Personal Data Protection (PDP) Bill. This bill aimed to establish a legal framework for data collection, processing, and storage by setting principles around consent, transparency, data minimisation, and accountability, thereby aligning India's data privacy framework with global standards. The PDP Bill eventually evolved into the Digital Personal Data Protection Act (DPDPA), reflecting the Puttaswamy judgment's enduring impact on privacy rights and underscoring the role of robust legal protections in preserving personal data security in a digitally connected India.

**The Personal Data Protection (PDP) Bill, 2019**

The Personal Data Protection Bill, 2019, introduced in the Lok Sabha by the Minister of Electronics and Information Technology, Mr. Ravi Shankar Prasad, on December 11, 2019, represents a significant step in India's efforts to safeguard personal data and privacy. It establishes protections for individuals' data and creates a Data Protection Authority to oversee compliance. The Bill governs the processing of personal data by entities including (i) the government, (ii) companies incorporated in India, and (iii) foreign companies handling the personal data of individuals within India. Personal data includes information related to an individual's identity, characteristics, or traits, which can identify them. The Bill also classifies certain types of personal data as "sensitive," including financial and biometric information, caste, religious or political beliefs, and other categories specified by the government in consultation with relevant regulatory bodies.

As defined by the Bill, a data fiduciary is any entity or individual responsible for determining the purposes and methods for processing personal data. Such data processing is subject to strict rules, ensuring it is conducted only for lawful, specific, and transparent purposes. Fiduciaries must adopt accountability measures, such as implementing security safeguards (e.g., data encryption) to protect data and establishing grievance redressal mechanisms to address individuals' complaints. Furthermore, they must implement age verification systems and obtain parental consent when handling children's sensitive personal data.

The Bill grants individuals, referred to as data principals, specific rights concerning their data. These rights include (i) confirming if their data has been processed, (ii) requesting corrections of inaccurate or outdated information, (iii) transferring personal data to other data fiduciaries in some instances, and (iv) restricting or withdrawing consent for data disclosure when no longer necessary. Data fiduciaries must generally obtain an individual's consent before processing their data; however, some exceptions allow data processing without consent for purposes such as state-provided benefits, legal proceedings, or emergencies.

Social media intermediaries—defined as platforms enabling user interaction and information sharing online—must provide a voluntary user verification system if they exceed a specified user threshold and significantly impact electoral democracy or public order.

To ensure compliance with data protection standards, the Bill establishes a Data Protection

Authority tasked with safeguarding individual interests and preventing data misuse. This Authority will include a chairperson and six members with expertise in data protection and IT, and its decisions can be appealed to an Appellate Tribunal, with further appeals directed to the Supreme Court. Sensitive personal data may be transferred outside India for processing with the individual's explicit consent, provided it remains stored within India. Certain types of "critical" personal data, as designated by the government, must be processed exclusively within India. The Bill also provides certain exemptions, allowing the central government to excuse agencies from its requirements for national security, public order, sovereignty, and foreign relations. Exemptions also apply to personal, domestic, and journalistic purposes as long as data processing follows lawful, specific, and secure standards. Non-compliance with the Bill's requirements, such as unauthorised processing or transfer of personal data, can result in fines up to Rs 15 crore or 4% of the fiduciary's annual turnover. Failure to conduct data audits may lead to penalties of up to Rs 5 crore or 2% of turnover. Additionally, re-identifying anonymised data without authorisation can incur penalties of up to three years' imprisonment, fines, or both. The government may require data fiduciaries to share anonymised or non-personal data to improve service targeting and ensure that such data cannot identify individuals. Finally, the Bill amends the Information Technology Act of 2000, removing provisions on company compensation for failure to protect personal data.

**Criticisms of the PDP Bill**

The Personal Data Protection (PDP) Bill was largely considered a significant advancement in safeguarding personal data rights in India. However, it did not go without its criticisms. One major point of contention was the requirement for data localization, which mandates that certain types of data must be stored and processed within Indian borders. Critics argued that this provision could impose substantial financial burdens on multinational companies that operate in India, as they may need to invest in local data infrastructure or alter their existing data management practices to comply with these regulations. Furthermore, concerns were raised regarding the government's authority to exempt itself from certain privacy obligations outlined in the bill. While these exemptions were framed as necessary measures for national security, critics feared that they could lead to excessive and unchecked powers for the government. The broad discretion granted to authorities to determine when and how these exemptions could be applied sparked worries about potential misuse and erosion of individual

privacy rights. Overall, while the PDP Bill aimed to enhance data protection, these issues prompted a robust debate about its implications for both businesses and citizens.

**The Digital Personal Data Protection Act, 2023**

The Digital Personal Data Protection (DPDP) Act, 2023 represents India's first dedicated legislative step toward protecting personal data in the digital age. This comprehensive law aligns with the Supreme Court's 2017 judgment in *Justice K.S. Puttaswamy vs. Union of India*, which upheld the right to privacy as intrinsic to the fundamental right to life. Following earlier iterations in 2019 and 2022, which encountered issues around data localisation and compliance burdens, the DPDP Act 2023 provides a structured, balanced approach that considers individual privacy rights alongside economic development and security demands.

**Key Objectives and Scope**

The DPDP Act targets digital personal data processing regulation, extending its jurisdiction beyond India for companies that handle data from Indian residents. The Act is designed to foster a secure environment for data usage within a lawful and transparent framework while laying a foundation for data protection norms that could interact with broader legislative frameworks like the Digital India Act.

**Fundamental Principles and Features**

The DPDP Act rests on essential principles:

- Lawfulness and Transparency: Entities must process data transparently and for specific, informed purposes.
- Purpose Limitation and Data Minimization: Only essential data is collected and used for designated purposes, ensuring no excessive collection.
- Consent-Based Processing: Data processing is allowed only with clear, informed, and revocable consent from the individual (or "Data Principal"). Consent exceptions include state security, public order, health emergencies, and certain state services.

The Act incorporates a groundbreaking feature by using gender-neutral pronouns, "she/her," as

a standard, symbolising inclusivity. Individuals, termed Data Principals, have rights to access, correct, and request deletion of their data. Additionally, they can transfer data between service providers and withdraw consent anytime. Importantly, individuals have the right to nominate representatives to manage their data rights if they become incapacitated. Along with it, Entities that manage data, known as Data Fiduciaries, must:

- Protect data with security measures to prevent unauthorised access.
- notify affected individuals and the Data Protection Board (DPB) in case of breaches.
- Erase data once the purpose is fulfilled unless legal requirements dictate otherwise.

Significant Data Fiduciaries—entities that manage large volumes of sensitive data—are subject to additional scrutiny, including regular audits and risk assessments. Additionally, the DPDP Act allows data transfers to countries that meet approved data standards. This provision balances national security interests with the operational flexibility needed for multinational businesses, making the compliance process easier for companies engaged in cross-border transactions.

**Regulatory Framework and Enforcement**

The Data Protection Board of India (DPB), created under the Act, is a civil authority empowered to monitor compliance, handle grievances, and impose penalties up to INR 500 crore for severe violations. The DPB's decisions can be appealed to the Telecommunications Dispute Settlement and Appellate Tribunal (TDSAT), and further appeal rights can be extended to the Supreme Court.

**While the Act signifies progress, specific provisions raise concerns:**

1. Surveillance Concerns: Broad powers granted to the central government (Section 36) may permit extensive surveillance, and Section 17 exempts state entities from compliance for security or public order reasons.
2. RTI Amendment Impact: The Act amends the Right to Information (RTI) Act, potentially limiting transparency by allowing public information officers to withhold data if classified as personal.

So, The DPDP Act, with its emphasis on privacy and regulatory structure, advances India's digital landscape, protecting individual privacy while encouraging responsible data use. As rules evolve and courts interpret the law, its practical impact on privacy protection and regulatory efficiency will become more apparent.

**Implementation Challenges in India**

India's digital infrastructure remains significantly underdeveloped in various regions, which creates substantial challenges for the enforcement of data privacy regulations. This inadequacy in infrastructure can hinder the effective monitoring and compliance required under the DPDP Act, especially in rural and remote areas where internet connectivity and technological access are limited. Small and medium enterprises (SMEs) face particular difficulties in navigating the complexities of these regulations due to their limited technical expertise and financial resources. Many SMEs may find it challenging to invest in the necessary tools, systems, and training needed to adhere to the stringent standards established by the DPDP Act.

A fundamental and ongoing debate within India's data privacy framework revolves around the balance between the protection of individual privacy rights and the needs of national security. The government possesses the authority to exempt certain data processing activities from compliance under the guise of national security, which raises concerns about the potential for overreach and abuse of power. Citizens and advocacy groups are increasingly anxious about the implications of such measures, fearing that they may infringe upon personal freedoms and privacy rights. Thus, it is crucial to find a harmonious balance that maintains the integrity of individual privacy while addressing the legitimate security concerns that the government may have. Moreover, effective implementation of data privacy laws goes beyond merely having legislative frameworks in place; it necessitates a concerted effort to educate the public about their rights and responsibilities under the DPDP Act. Initiatives such as public awareness campaigns and comprehensive digital literacy programs are essential to empower individuals with the knowledge they need to understand their rights. These programs should focus on providing citizens with information about what constitutes their personal data, their rights to access and control that data, and the mechanisms available for reporting violations. By fostering a privacy-conscious society, we can encourage greater public engagement and accountability in data privacy matters, ultimately benefiting both individuals and the broader community.

## Global Comparison

India's data privacy landscape is rapidly evolving, prominently marked by the enactment of the Data Protection and Digital Personal Data Protection (DPDP) Act. This legislation draws substantial inspiration from two influential frameworks: the General Data Protection Regulation (GDPR) in the European Union and the California Consumer Privacy Act (CCPA) in the United States. While the foundational principles of these regulations are clear similarities, significant differences exist, particularly concerning enforcement mechanisms and government exemptions. The GDPR sets a high benchmark for data protection across the globe. It is characterized by strong provisions that empower individuals with rights such as data portability, which allows users to transfer their data from one service provider to another; rectification, which enables individuals to correct inaccurate or incomplete data; and erasure (often referred to as the "right to be forgotten"), which allows individuals to request the deletion of their personal data in certain circumstances. In addition to these rights, the GDPR enforces strict penalties for non-compliance, including heavy fines that can reach up to 4% of a company's global annual revenue. These stringent measures ensure that organizations are held accountable for safeguarding personal data and enhancing consumer trust. The DPDP Act mirrors these principles but adopts a more centralized and government-oriented framework. Certain government entities are exempt from the exact stringent requirements placed on private companies, leading to concerns about consistency and fairness in accountability. Additionally, the penalty structure within the DPDP Act is less rigorous than that of the GDPR, potentially reducing the deterrent effect on organisations that mishandle personal data. Conversely, the CCPA takes a more consumer-centric approach, primarily focusing on enhancing consumers' rights regarding their personal information. The CCPA aims to make data rights accessible and compliance straightforward, particularly benefiting small businesses that might struggle with the more complex requirements of other regulations. It enables consumers to request information on what personal data is being collected about them and to whom it is being sold and provides the right to opt out of the sale of their personal information. These clear and manageable guidelines could be beneficial for India in crafting a balanced approach to data privacy, ensuring that robust protections do not hinder economic growth.

India could significantly enhance its data privacy framework by integrating the stringent enforcement mechanisms seen in the GDPR with the practical, consumer-focused principles of the CCPA. This dual approach could empower individuals with more substantial rights over

their personal data while ensuring that compliance remains feasible for businesses of all sizes, fostering trust, security, and innovation in the digital economy. Such a strategy would protect consumers and support India's ambition to be a global player in the digital landscape.

**Case Study 1: Aadhaar and Biometric Data Protection**

*Background:* The introduction of Aadhaar, India's unique identification program, brought forth significant concerns about the security of biometric data. This case examines how India's data privacy laws, particularly the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, address the complex issues of safeguarding biometric data.

*Comparative Analysis:* The GDPR and CCPA take distinct approaches to protecting biometric data. The GDPR treats biometric data as a sensitive category that demands enhanced safeguards, while the CCPA grants consumers the right to opt out of the sale of such data.

*Outcome:* India's current legal framework has faced criticism for its limited protections for biometric data. This case study highlights the need for a more refined approach to align with global standards for biometric data protection.

**Case Study 2: Cross-Border Data Transfer in E-commerce**

*Background:* A multinational e-commerce company operating in India encounters challenges related to cross-border data transfers. This case investigates how India's data privacy laws compare to GDPR and CCPA in supporting smooth and compliant data flow across borders.

*Comparative Analysis:* The GDPR enforces strict conditions on cross-border transfers, requiring explicit consent or specific mechanisms like Standard Contractual Clauses. The CCPA mandates that businesses disclose if they sell consumers' personal information, influencing practices in cross-border data handling.

*Outcome:* This case highlights the complexities businesses face in navigating cross-border data regulations, emphasizing the importance of aligning Indian and international standards to enhance compliance and foster customer trust.

**Case Study 3: Consent Mechanisms in Social Media Platforms**

*Background:* A social media platform in India is being scrutinised regarding its methods for obtaining user consent. This case looks into how India's data privacy laws, particularly the proposed Personal Data Protection Bill, 2019, address the complexities of securing meaningful consent from users.

*Comparative Analysis:* The GDPR's principles for promoting transparent, explicit consent mechanisms are similar. At the same time, the CCPA gives users an additional layer of control through the right to opt out of personal data sales.

*Outcome:* The case underscores the need for evolving consent frameworks that align with global standards, ensuring users are well-informed and empowered in the digital age.

**Future of Data Privacy in India**

India's data privacy and protection future is on the brink of significant advancement, with the Digital Personal Data Protection Act (DPDPA) and Information Technology (IT) Rules poised for essential updates. These amendments are designed to tackle the challenges introduced by emerging technologies, such as artificial intelligence (AI), the Internet of Things (IoT), and big data. As India accelerates toward digital transformation in sectors like smart cities, healthcare, and customer service, these laws must address pressing issues related to data ownership, user consent, cybersecurity, and real-time protection. For instance, smart city projects will generate vast quantities of personal data, necessitating robust protections around data ownership and accountability to ensure individual privacy in these public data ecosystems.

The upcoming legislative amendments aim to expand the DPDPA's reach to new AI and data-driven technologies risks. Anticipated enhancements include the right to data portability, stricter rules around biometric data, and transparency in AI-powered decision-making. These measures will enhance user control over personal information and enforce accountability on AI systems, especially those affecting sensitive areas like healthcare diagnostics or financial services. As digital interactions grow, these updates will address data-sharing concerns, ensuring data remains secure and private even across connected devices. On the technological front, India is leveraging advanced tools like AI and machine learning for proactive data protection, especially for real-time threat detection and prevention. Technologies such as

blockchain and advanced encryption, including the Advanced Encryption Standard (AES), are expected to secure data transactions and storage, preserving data integrity and preventing unauthorized access. This technology integration with policy reflects India's forward-looking approach to data privacy, aiming to adapt continuously to the digital landscape's evolving challenges.

Internationally, India's alignment with global data frameworks, like the EU's General Data Protection Regulation (GDPR), is becoming essential for seamless cross-border data flows. Partnerships, such as an EU-India Data Transfer Agreement, could establish India as a credible partner in data privacy, attracting investment from foreign businesses and strengthening India's digital economy. Global interoperability standards could also foster trust, facilitating Indian businesses' international operations while adhering to privacy regulations.

Finally, there's a growing emphasis on data ethics and corporate responsibility in India. With responsible AI practices becoming an industry standard, India will likely encourage corporate transparency, including regular data audits and public reports on data handling. Policies may mandate companies to train employees on ethical data handling, creating an ecosystem that values user privacy and builds trust. By focusing on ethical data practices, responsible AI, and corporate accountability, India is proactively shaping a framework that balances innovation with protecting individual rights in the digital age.

## Conclusion

India has made significant strides in data privacy with recent advancements and amendments to the Digital Personal Data Protection Act (DPDPA), reflecting a commitment to safeguarding personal information in an increasingly digital society. This evolving legislative framework underscores the importance of regular updates to stay ahead of rapid technological changes, ensuring that data protection laws can effectively address new challenges posed by AI, IoT, and big data. The collective efforts of citizens, businesses, and the Data Protection Board are pivotal in upholding these laws, as they foster a culture of accountability, empower individuals with control over their data, and enable businesses to prioritise ethical data practices. Such active participation strengthens the domestic digital economy and positions India as a critical player in the global digital landscape. As India aligns with international privacy standards, its data protection laws contribute to a trustworthy digital ecosystem that reinforces national values of

privacy and integrity while bolstering economic growth and enhancing its appeal as a responsible data partner worldwide.

## REFERENCES

1) Data protection and data privacy laws in IndiData protection and data privacy laws in India

2) K.S. Puttaswamy v. Union of India (2017): Recognizing Privacy as a Fundamental Right in India – Legal blend

3) Justice K.S.Puttaswamy(Retd) vs Union Of India on 26 September, 2018

4) The Personal Data Protection Bill, 2019

5) Digital Personal Data Protection Act 2023 | Ministry of Electronics and Information Technology, Government of India

6) [The Viewpoint] Digital Personal Data Protection Act, 2023 – A Brief Analysis bar and bench

7) Data Privacy Laws Comparison: Indian DPDP vs. GDPR vs. CCPA - Privacy Protection - Privacy - India

8) Data Privacy Laws in India: A Comparative Study with Global Standards

9) https://www.freelaw.in/legalarticles/Data-Protection-Laws-in-India-Current-Scenario-and-Future-Prospects

10) Data privacy in India: Current outlook and the future