GUARDING DIGITAL FRONTIERS: THE LEGAL EVOLUTION OF DATA PROTECTION IN INDIA

Sakshi Solanki, Gitarattan International Business School

INTRODUCTION

The evolution of data protection laws in India reflects the country's response to the complex challenges of safeguarding individual privacy in the digital age. With the increasing integration of digital technologies into everyday life—ranging from online banking and telemedicine to social media and e-governance—the collection and processing of personal data have become both ubiquitous and indispensable. However, this digital transformation has also heightened concerns about data misuse, surveillance, and the lack of adequate safeguards for personal information.

Historically, India lacked a dedicated legal framework for data protection. Early efforts were embedded within the broader provisions of the Information Technology Act, 2000, which primarily focused on cybercrime and electronic commerce rather than individual data rights. The introduction of Section 43A through an amendment in 2008 and the subsequent SPDI Rules of 2011 represented initial attempts to address data privacy. Yet these measures were narrow in scope, applying largely to corporate entities and offering limited protections to individuals.

A significant turning point came with the Supreme Court's 2017 judgment in Justice K.S. Puttaswamy v. Union of India, which unequivocally recognized the right to privacy as a fundamental right under the Indian Constitution. This judicial milestone not only underscored the urgent need for comprehensive data protection legislation but also laid the constitutional foundation for future reforms.

This article traces the legal and policy evolution of India's data protection framework—from its fragmented origins to the enactment of the Digital Personal Data Protection Act, 2023. It examines key legislative developments, judicial interventions, and regulatory mechanisms that have shaped the current regime. By analyzing the structural shift from sectoral regulations to a rights-based approach, the article highlights India's journey toward creating a secure,

transparent, and accountable digital environment that respects individual autonomy and privacy.

Early Legal Framework: Information Technology Act, 2000

India's initial attempt to address the digital ecosystem legislatively came with the Information Technology Act, 2000 which primarily dealt with cybercrime, digital signatures, and electronic governance. In response to growing concerns about data misuse and identity theft, Section 43A was introduced through an amendment in 2008. This provision made companies liable to pay compensation if they were negligent in implementing reasonable security practices while dealing with sensitive personal data. Despite its progressive intent, Section 43A was inherently limited in its scope. It applied only to "body corporates", thereby excluding government entities and individual data handlers from its purview. Furthermore, it did not clearly define what constituted reasonable security practices or what rights an individual held with respect to their data. The focus remained largely on corporate accountability rather than on the empowerment of individuals or the establishments of any enforceable data rights.

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011

(a) To give operational shape to Section 43A, the Government of India introduced the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (**"SPDI Rules"**). These rules marked India's first formal recognition of data privacy norms. They defined "sensitive personal data" to include information relating to passwords, financial information, health conditions, biometric data, and sexual orientation, among others.

(b) The SPDI Rules required body corporate to obtain consent from users before collecting or sharing such data and mandated them to publish a privacy policy outlining their data handling practices. While this was significant step forward, the rules remained limited in several aspects.

i) Limited Applicability - The rules applied only to commercial organizations, excluding government departments and agencies from their scope.

ii) Lack of Enforcement Authority – There was no dedicated regulatory authority

for monitoring or enforcing compliance with the SPDI Rules.

iii) No Individual Rights – The rules did not grant data subjects specific rights, such as the rights to access, correct, or delete their personal data.

iv) Inadequate for Modern Threats – The rules did not address emerging challenges such as algorithmic profiling, cross border data transfers, or data breaches at scale.

v) Thus, while the SPDI Rules established foundational principles of data protection in India, they fell short of establishing a comprehensive, rights-based, and enforceable legal regime.

Judicial Recognition- The Puttaswamy Judgement

(a) The landmark case titled "K.S.Puttaswamy v. Union of India" was decided on 24th August 2017, marked a watershed moment in Indian constitutional history. The issue emerged in the context of the Aadhaar scheme, a biometric identification system introduced by the Government of India streamline welfare benefits.

(b) Justice K.S.Puttaswamy, a retired judge of theHon'ble Karnataka High Court, filed a writ petition before the Hon'ble Supreme Court challenging the constitutional validity of Aadhaar, asserting that it violated the fundamental right to privacy.

(c) The core legal issue was whether the Indian Constitution guarantees a fundamental right to privacy. This was crucial because earlier decisions by the Hon'ble Supreme Court, most notably M.P. Sharma v. Satish Chandra and Kharak Singh v. State of Uttar Pradesh, had held that privacy was not a fundamental right. Therefore, to resolve the matter conclusively, a nine judge Constitution Bench was constituted to re-examine the position of privacy under the Constitution.

The issues which were interpreted by the Hon'ble apex court were

i. Is the right to privacy a fundamental right under the Indian Constitution?

ii. If affirmative, under which provisions of the Constitution is it protected?

iii. How does this right co-exist with other competing interests, such as national security and state welfare programs?

Key Findings and Principles Established

(a) The Hon'ble Supreme Court delivered a unanimous verdict, affirming that the right to privacy is a fundamental right, intrinsic to life and personal liberty under Article 21 of the Constitution. The core principles established in the case are given below:

(i) Privacy as a Fundamental Right – The Hon'ble Supreme Court held that privacy is not a standalone right but is derived from existing guarantees under Part III of the Constitution of India, particularly, Article 14 (Right to Equality) Article 19 (Right to Freedom), and Article 21 (Right to Life and Personal Liberty). Privacy, according to the Hon'ble apex court, includes a wide range of aspects such as bodily, autonomy, personal information, freedom of thought, family life and international self-determination.

(ii) Overruling Previous Judgements – The judgements provided in landmark cases like M.P Sharma and Kharak Singh were expressly overruled. The Hon'ble Supreme Court clarified that these judgements were rendered in an era when the understanding of privacy was limited and not developed in the manner required in a modern democratic society.

(iii) Facets of Privacy Recognized – The judgement elaborated that privacy has multiple facets including bodily privacy, decisional privacy and informational privacy. This categorization broadened the scope of privacy to include both tangible and intangible aspects of personal life.

(iv) Privacy is not absolute - While privacy is fundamental, it is not absolute. The Hon'ble Supreme Court laid down a three-part test to determine when the state can lawfully infringe on privacy. Those included legality test which stated that there must be a law in existence to justify the encroachment, necessity test which stated that the law must be made for a legitimate reason, and the proportionality test which further stated that the law must be proportionate.

(v) Impact on Aadhaar and Beyond –The judgement ultimately upheld the constitutionality of the Aadhaar scheme, finding that it passes the tests of legitimate state aim, necessity, and proportionality when used for the purpose of providing welfare benefits to citizens.

(b) The Puttaswamy judgement represents a paradigm shift in Indian constitutional law. It elevated privacy from a peripheral concern to a central pillar of constitutional governance, placing individual autonomy and dignity at the heart of the Indian legal system. The decision underscored the need for legal safeguards in the digital age and laid the intellectual and constitutional foundation for the DPDP, 2023 which now governs the collection, processing and protection of personal data in India.

OVERVIEW AND KEY FEATURES OF THE DPDP ACT, 2023

The DPDP Act is one of the biggest leaps for India in its journey to assure robust data governance and privacy protection. This legislation was enacted on August 11, 2023, to deal with the increasing complexities of managing digital data with the rapid evolution of technology. While the act has been enacted, the government is yet to announce the enforcement date. The implementation timeline is expected to be phased, with exact dates to be determined through government notifications.

Balancing the fundamental right to privacy of an individual with the legitimate need for data-driven innovation, the DPDP Act creates a comprehensive framework for the collection, processing, storage, and sharing of personal data in digital formats.

The new legislation, once implemented, will be transformative as it provides clarity to data fiduciary's responsibilities, enhances individual control over personal data, and provides a transparent mechanism for grievance redressed. It harmonizes the data protection laws of India with international standards while taking into account the unique socio-economic dynamics of the country.

Upon its commencement, the DPDP Act will supersede Section 43A of the Information Technology Act, 2000, and SPDI Rules. These rules derive their statutory authority from Section 43A of the Information Technology Act, 2000, which mandates body corporates to implement reasonable security practices for handling sensitive personal data. However, the omission of Section 43A in the DPDP Act effectively nullifies the legal foundation of the SPDI Rules, rendering them inoperative. While the DPDP Act does not explicitly override the SPDI Rules, the absence of their enabling statutory provision implicitly repeals them.

The key elements of the Act include universal consent, special protection for children, restrictions on cross-border data flow, and provisions for government use of data for public services. The Act is interdependent on DPDP Rules, 2025, and thus, lays the foundation for a secure and accountable digital ecosystem, fostering trust among citizens and businesses alike.

Key Features of the DPDP Act, 2023

The DPDP Act, 2023 has been introduced to outline the procedures for the collection and usage of personal data of Indian citizens by organizations and governments. The Act covers personal data acquired either in digital format or initially in non-digital format, which are then digitalized subsequently. The Act also applies to the processing of digital personal data outside of India if there is a connection of offering goods or services to data principals within the territory of India.

The Act specified its non-applicability on the following types of data:

(a) Non-digital data

(b) Data used for personal or household purposes

(c) Data that is publicly accessible due to legal obligation.

The other important principles provided in the DPDP Act 2023, are as follows:

(a) Stakeholders

The Act expressly defines “Data Principal” as an individual to whom the personal data belongs. It establishes a direct relationship between data and the person providing it. In certain circumstances, where a data principal is a child or disabled person, the definition extends to include the parents or the lawful guardians, who are entrusted with their well-being.“Data Fiduciary” is a person determining the purpose and means of processing the personal data. Data fiduciary is different from “Data processor” because the latter interprets or determines the data on behalf of the data fiduciary in accordance with the directions, objectives, and methods prescribed by the data fiduciary. In order to

determine whether a person is a data fiduciary or data processor, the amount of influence or control over each other must be analyzed.

(b) Consent (Section 6)

The Act provides that a request for consent shall be accompanied by a notice by the data fiduciary to the data principal, highlighting the purpose of processing the data, the manner in which rights can be exercised as provided u/s 6 (consent) and u/s 13 (grievance redressal) of the Act, and the manner in which a complaint can be made to the Data Protection Board of India ("Board").

It is further provided in the Act that the consent provided by the Data Principal must be out of free consent and should be specific and unconditional. It shall signify an agreement to the processing of personal data of the Data Principal for the specified purpose only. In case the consent leads to a contradiction of any provisions of the said Act or rules made thereunder, then the same shall be considered to be invalid.

Also, the Data Principal shall have the right to withdraw the given consent at any time, the consequences of which shall be borne by the Data Principal, and such withdrawal will not affect the legality of processing personal data based on consent before its withdrawal.

(c) Legitimate Use (Section 7)

The Act outlines the following instances of "legitimate use" where Data Fiduciary can process the personal data given by the Data Principal:

The Data Principal willingly provides their personal data to the Data Fiduciary for a specified purpose and has not objected to the utilization of their personal data.

i. To avail any benefit, subsidy, certificate, etc. from the state or its instrumentalities.

ii. To comply with any judgment, decree or order under Indian law, as well as any judgment, decree, or order of civil/ contractual nature in accordance with foreign laws.

iii. To protect the interest of the sovereignty and integrity of India.

(d) Processing of Personal Data of Children (Section 9)

As per the Act, a Data fiduciary shall obtain verifiable consent of a lawful guardian in order to process personal data of a child or a person with a disability. Also, a data fiduciary shall not undertake tracking or behavioral monitoring of children.

(e) Rights & Duties of Data Principal (Section 11)

i. Right to Access: Individuals can access their data held by organizations.

ii. Right to Correction: Individuals can request corrections to inaccurate or incomplete data.

iii. Right to Erasure: Individuals can demand deletion of data no longer necessary for processing.

iv. Right to Grievance Redressal: Mechanisms are in place for resolving complaints related to data processing.

Apart from the above-mentioned rights, it is also provided that data principals must not submit false information and must cooperate in verifying their identity when exercising rights.

(f) Cross-Borders Data Transfers (Section 16)

The Act restricts data transfer from India to any other country due to weak data protection laws. The Act employs a "blacklisting" approach, which includes that the movement of data transfers will not have been interrupted except when the receiving territory has been blacklisted by the government.

(g) Penalties for Non-Compliance (Section 33)

The Act imposes significant financial penalties for non-compliance, including up to INR 250 Cr. for failing to prevent data breaches, INR 200 Cr. for non-compliance with the provision for children, and INR 10,000 if a data principal fails to perform his duty.

DIGITAL PERSONAL DATA PROTECTION RULES, 2025

The draft of rules proposed to be made by the Central Government in exercise of the powers

conferred by sub-sections (1) and (2) of section 40 of the DPDP Act was published vide notification dated 03.01.2025. The proposed rules are referred to as the Digital Personal Data Protection Rules, 2025 ("DPDP Rules") and are proposed towards efficient implementation of the DPDP Act. These rules simplify the act by explaining substantial obligations, processes, and technical requirements for compliance. The rules aim to standardize the practices for data protection, ensuring all organizations follow uniform and fair procedures. The rules also detail the functioning of the Data Protection Board in case of violations and appeals. The government has invited stakeholders to share feedback/comments on the draft rules latest by 18th February 2025.

The rules strike a balance between protecting privacy and promoting innovation and improving growth in India's digital economy while safeguarding individual's rights.

(a). Notices to Users: Organizations must issue a clear, standalone, and understandable notice to the data principal. It should contain itemized list of the personal data collected, along with a clear description of the purpose of collecting such data and an itemized explanation of the goods, services, or uses of such processing.

(b) Consent Managers**:** Those who are facilitating individuals to manage their consent on the use of data should operate according to rigorous security, transparency, and independence standards. To be a consent manager, a company should have sound business capacity along with a fair reputation, a minimum net worth of INR 2 Cr., and a certified interoperable platform where data principals can manage their consent.

(c) Government Use of Data: Public agencies may collect data for the delivery of services like benefits or certificates, subject to strict security and transparency standards.

(d) Security Measures: Data handlers must protect data using tools like encryption and secure storage. The aim of these safeguards is to ensure confidentiality, integrity, and prevention of data breaches.

(e) Data Breach Notification: If a data breach occurs, organizations must promptly notify affected users and regulators about the breach's nature, timing, extent, and steps taken to prevent future occurrences. The data fiduciary is also responsible for informing the board about the breach within 72 hours of the incident.

(f) Unused Data: If users stop engaging with a service, their data must be deleted after notifying them unless such data is needed for legal compliance. Before erasing the data, the data principal must be informed at least 48 hours in advance about the erasure of their data.

(g) Contact Information: Organizations must provide easy-to-find contact details for user queries about data use. Usually, contact of the Data Protection Officer (DPO) is given in case the Data Principal wants to exercise their rights.

(h) Children's Data Consent: Special measures ensure only verified parents or guardians give consent for children's or persons with disabilities' data processing, respectively.

(i) Exemptions for Children's Data: Some organizations (e.g., schools, healthcare providers) can process children's data for specific purposes like education or safety in accordance with Section 9 of the said Act. This is done for the sake of the well-being of children.

(j) Significant Data Fiduciaries: Big organizations shall audit annually and ensure that their tools do not infringe on the rights of users. The Significant Data Fiduciaries must conduct a Data Protection Impact Assessment (DPIA), whose results shall be reported to the Board.

(k) User Rights: Users have the right to access or erase their data through simple, public procedures.

(l) Transfer of Data outside India: Specific government regulations apply to the transfer of data outside India to ensure protection.

(m) Research Exemption: Data used for research, statistics, or archiving is exempt if safeguards are followed.

(n) Data Protection Board: A government-appointed board oversees data protection compliance, including appointing members and ensuring transparency.

(o) Board Salaries: Members receive fixed salaries without extra benefits like housing or cars. The chairperson is entitled to a consolidated salary of INR 4,50,000 per month, and each member receives INR 4, 00,000 per month.

(p) Board Meetings: Meetings follow structured rules, with decisions made by voting. Urgent matters can be addressed immediately and confirmed later. The chairperson shall have the

casting vote in the event of a tie.

(q) Digital Operations: The Board operates digitally to make processes faster and reduce the need for physical meetings. With the help of digital office [defined u/s 2(m) of the Act], the board can adopt techno-legal measures to undertake its functions.

(r) Board Staff: This rule outlines the process for the appointment and service terms of officers and employees working for the board. Such officers and employees can be appointed either on deputation or from the National Institute for Smart Government.

(s) Appeals: Users can appeal board decisions through a digital process to the Telecom Disputes Settlement and Appellate Tribunal within 60 days from the date of receipt of the order.

(t) Government Data Requests: Authorities can request data for national security or legal purposes, following safeguards. Under Section 36 of the act, fulfillment of such a request is a part of legal obligation.

CONCLUSION

The enactment of the Digital Personal Data Protection Act, 2023 marks a significant turning point in India's legal landscape concerning data governance. In an age where digital technologies shape nearly every aspect of life—from financial transactions and social media to healthcare and e-governance—the regulation of personal data has evolved from a policy choice to a constitutional mandate, firmly rooted in the right to privacy as recognized in Justice K.S. Puttaswamy v. Union of India. This article has analyzed the Act through legal, structural, and comparative perspectives, tracing India's journey from the limited safeguards of the IT Act, 2000 and SPDI Rules, 2011, through the judicial acknowledgment of privacy as a fundamental right in 2017, to the introduction of a dedicated and comprehensive legal framework in 2023. The DPDP Act introduces a consent-driven and principles-based model that grants enforceable rights to data principals, establishes clear obligations for data fiduciaries, and creates an independent oversight body—the Data Protection Board of India. Provisions such as the designation of Significant Data Fiduciaries, mechanisms for grievance redressal, and a structured approach to cross-border data transfers reflect a shift from voluntary compliance to a rights-oriented, enforceable regime. At the same time, the Act's success will depend on its implementation, clarity of subordinate legislation, digital infrastructure, public awareness, and

the autonomy of the regulatory authority. Concerns around government exemptions and state surveillance remain areas that demand further judicial and academic engagement. Nonetheless, the DPDP Act stands as a foundational step toward building a secure, transparent, and constitutionally anchored data protection regime. Its effectiveness will rest on the nation's commitment to interpreting and applying it in a manner that upholds the democratic values of dignity, autonomy, and accountability in the digital era.

REFERENCES

- *Information Technology Act, 2000*, No. 21 of 2000.
- See: World Economic Forum, *Personal Data: The Emergence of a New Asset Class*, 2011.
- Information Technology Act, 2000 (No. 21 of 2000).
- Information Technology (Amendment) Act, 2008; Section 43A.
- SPDI Rules, 2011; criticism discussed in various policy briefs (e.g., NASSCOM, CIS Reports).
- *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
- B.N. Srikrishna Committee Report on Data Protection, 2018.
- Digital Personal Data Protection Act, 2023.
- Justice B.N. Srikrishna Committee Report – *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians*, Government of India, July 2018.
- White Paper of the Committee of Experts on a Data Protection Framework for India, Ministry of Electronics and Information Technology, Nov 2017.
- Report of the Group of Experts on Privacy, chaired by Justice A.P. Shah, Planning Commission of India, October 2012.
- General Data Protection Regulation (GDPR), Regulation (EU) 2016/679.
- Graham Greenleaf, "Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance," *Privacy Laws & Business International Report*, Issue 169.
- Organisation for Economic Co-operation and Development (OECD), *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 2013.