THE EVOLVING LANDSCAPE OF DATA PRIVACY LAW IN INDIA: CONSTITUTIONAL FOUNDATIONS, THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023, AND THE 2025 RULES

Dr. K. Sangeetha, Associate Professor, Department of International Law, The Tamil Nadu Dr. Ambedkar Law University, Tharamani Campus, Tharamani, Chennai. October 2026.

ABSTRACT

Personal Data has become a central resource in India's Digital Economy, Public Administration and delivery of essential services. Its collection and use can enable innovation, financial inclusion and efficient governance, but can also expose individuals to surveillance, profiling, discrimination, identity theft and loss of autonomy. Indian Data Privacy law has developed through constitutional adjudication, information technology legislation, sectoral regulation and, most significantly, the Digital Personal Data Protection Act, 2023 (DPDP Act). The Digital Personal Data Protection Rules, 2025, notified on 14 November 2025, supply important operational detail while adopting a phased commencement schedule. This article examines the constitutional basis of informational privacy, the principal statutory instruments, the rights and obligations created by the DPDP framework, relevant judicial decisions, implementation challenges and possible reforms. It argues that effective privacy protection depends not only on formal legal rights but also on independent and accessible enforcement, proportionate state access, transparent digital systems and practical remedies for individuals.

Keywords: Data Privacy; Informational Privacy; DPDP Act 2023; DPDP Rules 2025; Constitutional Law; Consent; Data Protection Board; Cyber Security.

Introduction:

Digital Transactions routinely generate information about identity, location, health, education, employment, finances, communications and behaviour. Government platforms, banks, hospitals, universities, e-commerce services and social media intermediaries may process personal data at significant scale. Data processing can improve services, but the same information can be misused or exposed through insecure systems, opaque profiling, excessive retention or unauthorised disclosure. Data privacy is therefore both an individual rights issue and a matter of Institutional Accountability.

India's framework has moved from a fragmented model centered on the Information Technology Act, 2000 and Subordinate rules to a dedicated Statute for Digital Personal Data. The DPDP Act received assent in August 2023. The Central Government notified the DPDP Rules, 2025 on 14 November 2025, with different provisions taking effect at different times. Consequently, it is important to distinguish enactment and notification from the commencement of each substantive obligation. The current position should be checked against the Official Gazette and Enforcement timeline before advising on a particular compliance deadline.[1]

Constitutional Foundation: Privacy as a Fundamental Right:

The Constitution does not expressly use the phrase 'Data Protection'. Nevertheless, Privacy is protected through the guarantees of life, personal liberty and dignity under Article 21, read with the freedoms and equality guarantees in Part III. In Justice K.S. Puttaswamy (Retd.) v Union of India, a nine judge Bench of the Supreme Court unanimously recognised privacy as a constitutionally protected Fundamental Right. The Judgment treated Privacy as intrinsic to liberty, dignity and autonomy, while recognising that the right is not absolute and those restrictions require Constitutional Justification.[2]

The Constitutional approach has consequences for both Public and Private data practices. State Collection and use of information must satisfy applicable requirements of legality, legitimate purpose, necessity and proportionality. The Judgment also identified

[1] Ministry of Electronics and Information Technology, 'Digital Personal Data Protection Rules, 2025', Gazette of India, G.S.R. 846(E), 13 November 2025; 'Digital Personal Data Protection Rules 2025' and 'Enforcement Timeline for the DPDP Act', Official Portal.
[2] (2017) 10 SCC 1; AIR 2017 SC 4161.

informational privacy as a core dimension of Privacy and acknowledged the risks created by large scale Data aggregation. Parliament's subsequent Legislation should therefore be read in harmony with Constitutional rights, and not as displacing them. In K.S. Puttaswamy (Aadhaar) v Union of India, the Supreme Court considered the Constitutional validity of the Aadhaar framework and placed limits on aspects of compulsory use and private sector access to Aadhaar Authentication Data.[3] The decision illustrates the need to balance welfare delivery and identity verification against privacy, exclusion and proportionality concerns. In Anuradha Bhasin v Union of India,[4] the Court also emphasised Constitutional scrutiny of restrictions affecting internet access and required publication of relevant orders, reinforcing the importance of Transparency where Digital infrastructure and Rights intersect.

The Principal Legal Framework

Digital Personal Data Protection Act, 2023

The DPDP Act is the Central, dedicated Statute governing the processing of Digital Personal Data within its scope. It applies to digital personal data processed in India and, subject to statutory conditions, to processing outside India connected with offering goods or services to individuals in India. It also addresses personal data collected offline and subsequently digitised. The Act contains exclusions and exemptions, so its application must be assessed against the facts and the text of the relevant provisions.[5]

The Act uses the terms 'Data Principal' for the individual to whom personal data relates and 'Data Fiduciary' for a person who, alone or with others, determines the purpose and means of processing. A Data Processor processes data on behalf of a Data Fiduciary. The framework generally requires a lawful basis for processing, notice and consent where consent is relied upon, subject to specified 'legitimate uses' and other statutory provisions. Consent must be free, specific, informed, unconditional and unambiguous, expressed through a clear affirmative action. A request for consent must be accompanied by notice describing the personal data and purpose of processing. Individuals must be able to withdraw consent with ease comparable to the ease with which it was given. Withdrawal does not automatically make

[3] (2019) 1 SCC 1.
[4] (2020) 3 SCC 637.
[5] Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023), especially Sections 3 to 17 and the Schedule.

prior lawful processing unlawful, but future processing must have another valid legal basis if it is to continue.

Section 8 establishes general obligations for Data Fiduciaries, including responsibility for processing undertaken on their behalf, reasonable security safeguards, breach related duties, erasure in specified circumstances and grievance redressal. The Act also provides rights to access information about personal data, seek correction and erasure, use grievance redressal mechanisms and nominate another person to exercise rights in the event of death or incapacity. Rights are subject to Statutory conditions and do not amount to unrestricted access to every record or an absolute right to erase all Data.

The Act establishes the Data Protection Board of India to inquire into breaches and exercise powers assigned by the statute. Monetary penalties may be substantial, with the maximum amounts specified for different contraventions in the Schedule. The Scheme is primarily regulatory and monetary; it should not be mistaken for a general statutory right to claim compensation for every privacy harm. The Act also authorises exemptions in defined circumstances, including certain State functions and other specified situations. The scope and safeguards surrounding exemptions are central to the practical strength of the framework.

Digital Personal Data Protection Rules, 2025

The Digital Personal Data Protection Rules, 2025 were notified in the Gazette of India on 13 November 2025 and published by the Ministry of Electronics and Information Technology. They set out operational requirements on matters including notices, consent mechanisms, security safeguards, breach notifications, children's data, significant Data Fiduciaries and the functioning of the statutory framework.[6]

The Rules have a phased commencement structure. Rules 1, 2 and 17–21 came into force upon publication; Rule 4 is scheduled to commence One year after publication; and Rules 3, 5 to 16, 22 and 23 are scheduled to commence Eighteen months after publication. Accordingly, as of 10th October 2026, the provisions whose commencement is immediate are in force, while the One year and Eighteen month groups have not yet reached their scheduled commencement dates. Compliance planning should use the exact commencement clauses and

[6] Digital Personal Data Protection Rules, 2025, especially rules 1 to 3 and the rule specific commencement provisions; see also the Official Meit Corrigendum published 16th December 2025.

any later corrigendum or notification rather than assuming that all obligations became operative on the date of notification.[7]

The Rules seek to make notices understandable independently of other information and to identify the categories of personal data and purposes involved. They prescribe security-related measures and a framework for notifying affected individuals and the Board of personal-data breaches. They also contain provisions concerning verifiable parental consent for children and verifiable consent of lawful guardians where applicable. These requirements aim to translate broad statutory duties into practical Organisational processes.

Information Technology Act, 2000 and SPDI Rules, 2011

The Information Technology Act, 2000 remains an important part of India's digital law framework. Section 43A historically addressed compensation for failure by a body corporate to protect sensitive personal data or information, while section 72A concerns disclosure of information in breach of a lawful contract with the requisite wrongful intent or knowledge. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 prescribe requirements for covered bodies corporate in relation to specified sensitive information, privacy policies, consent, disclosure, transfer and security practices.

The DPDP Act contains provisions addressing the amendment or omission of earlier provisions, including section 43A of the IT Act. Because commencement and transitional details matter, organisations should not assume that every legacy provision has the same continuing operation after the relevant commencement date. The IT Act's other provisions, rules and sectoral requirements may still apply independently. Legal review should therefore map each processing activity to the provisions currently in force.

Cybersecurity Directions and Sectoral Regulation

Privacy and Cyber Security overlap but are not identical. The Indian Computer Emergency Response Team (CERT-In), acting under the IT Act, issued directions in April 2022 requiring covered entities to report specified Cyber incidents within prescribed timelines

[7] Information Technology Act, 2000, including sections 43A and 72A as relevant to the applicable commencement and transition position; Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

and to maintain certain logs for a specified period. These directions address incident response and Cyber resilience, rather than replacing the DPDP framework.

Financial entities may also be subject to Reserve Bank of India requirements; regulated securities market entities to applicable Securities and Exchange Board of India requirements; and Telecom providers to Telecom Specific Laws and Directions. Health, Employment, Education and Public sector organisations may face additional confidentiality, record retention, professional or Statutory Duties. The result is a layered system in which the DPDP Act is Central but not the only relevant instrument.

Transparency, Purpose Limitation and Data Minimisation

Organisations should identify why each category of Personal Data is needed, collect no more than is reasonably required for the stated purpose, and avoid reusing information for incompatible purposes without a valid Legal basis. Privacy notices should explain processing in plain language and distinguish essential processing from optional uses such as targeted advertising or analytics. A long, generic notice may Technically disclose information but fail to support meaningful understanding.

Security and Personal Data Breaches

Reasonable safeguards should be proportionate to the nature and volume of data, the likely harm from compromise and the organisation's technical capacity. Practical measures include access controls, encryption where appropriate, secure development, vendor oversight, staff training, tested backups, retention limits, incident response plans and documented risk reviews. Breach response should be coordinated across legal, security, communications and operational teams, with reporting performed under the applicable legal timeline.

Children's Personal Data

The DPDP Act establishes special protections for Children, including verifiable parental consent requirements and restrictions on specified processing practices, subject to statutory exceptions and the Rules. This has particular significance for Schools, Universities, Gaming services, Social networks, Educational Technology and Health Services. Organisations should design age appropriate notices, minimise collection, verify consent

proportionately and avoid practices that expose Children to tracking or behavioural manipulation where prohibited.

Significant Data Fiduciaries and Accountability

The Act permits the Central Government to designate certain Data Fiduciaries as Significant Data Fiduciaries based on factors such as the volume and sensitivity of personal data, risks to individuals, sovereignty and integrity of India, electoral democracy, security of the State and Public order. Additional duties can include appointing an India based Data Protection Officer, engaging an independent data auditor and undertaking periodic impact assessments and audits. Organisations potentially within this category should monitor designation decisions and maintain evidence of Governance and Risk management.

Cross Border Processing

The Act does not establish a universal rule that all Personal Data must remain in India. It allows cross border processing subject to restrictions that may be specified by the Central Government and to other applicable Indian Laws. Sector specific localisation or transfer conditions may operate separately. Organisations should therefore maintain a data-flow inventory, identify vendors and hosting locations, and assess both DPDP requirements and any sectoral restrictions before transferring data internationally.

Judicial Decisions shaping Privacy and Digital Rights

- **Justice K.S. Puttaswamy (Retd.) v Union of India, (2017) 10 SCC 1.** Established Privacy as a fundamental right under the Constitution, including informational privacy, and supplied the principal constitutional foundation for Data Protection Law.

- **K.S. Puttaswamy (Aadhaar) v Union of India, (2019) 1 SCC 1.** Considered the Aadhaar architecture and imposed limits on aspects of compulsory use and private sector access, demonstrating the importance of proportionality and safeguards.

- **Shreya Singhal v Union of India, (2015) 5 SCC 1.** Struck down section 66A of the IT Act and read down aspects of intermediary liability, underscoring the Constitutional limits on digital regulation and online speech restrictions.

- **Anuradha Bhasin v Union of India, (2020) 3 SCC 637.** Addressed internet restrictions and transparency of orders; relevant to digital rights and the need for reviewable, legally justified State action.

- **People's Union for Civil Liberties v Union of India, (1997) 1 SCC 301.** Recognised privacy concerns in Telephone tapping and emphasised procedural safeguards against arbitrary interception.

- **District Registrar and Collector, Hyderabad v Canara Bank, (2005) 1 SCC 496.** Recognised privacy interests in bank documents and rejected intrusive access to private records without adequate legal justification. These decisions predate or sit alongside the DPDP Act and do not all interpret its provisions directly. Their continuing importance lies in the constitutional standards they provide for interpreting privacy, state power, digital regulation and procedural safeguards. Future litigation will likely clarify how these principles apply to exemptions, Government processing, automated decisions, breach remedies and the relationship between the Board's regulatory role and Constitutional Judicial Review.

Challenges in Implementation

First, phased commencement creates a transition period in which organisations must distinguish current obligations from provisions scheduled to commence later. Compliance programmes should use a dated legal register and update it when commencement notifications, corrigenda or sectoral directions change the position. Second, meaningful consent is difficult where services are essential, notices are lengthy, or individuals have little bargaining power. Consent cannot be a substitute for sound system design, purpose limitation and accountability. Interface design should avoid dark patterns and should make refusal or withdrawal practical where consent is the Legal basis. Third, the breadth of exemptions and State processing powers raises questions about necessity, oversight and effective remedies. Public bodies often process data at scale to deliver welfare, identity, taxation, education and health services. Clear purpose statements, access controls, independent audits, retention schedules and accessible grievance mechanisms are particularly important in these settings. Fourth, smaller organisations may lack the expertise and budget to implement sophisticated privacy programmes. Proportionate compliance guidance, standard templates, sector specific codes and capacity building can improve compliance without weakening protection. Fifth, individuals may not know how to exercise rights or may face language, disability,

connectivity or digital literacy barriers. Offline and regional language channels are essential if statutory rights are to be practically accessible. Finally, data protection and Cyber security require distinct but coordinated approaches. An organisation can prevent a data leak yet still process data unfairly; conversely, lawful processing can be undermined by weak security. Governance must address legality, fairness, security, retention, vendor management and redressal together.

Recommendations:

1. Publish and maintain a clear, consolidated commencement tracker identifying the operative provisions of the DPDP Act and Rules, with plain language compliance guidance.

2. Require privacy by design reviews for high-risk processing, including data minimisation, retention limits, role based access, audit trails and documented vendor oversight.

3. Ensure that notices and grievance channels are available in accessible formats and relevant Indian languages, with offline alternatives where digital access is limited.

4. Develop Transparent, proportionate procedures for Government data processing, including defined purposes, necessity assessments, independent review where appropriate and meaningful remedies for unlawful use.

5. Provide practical guidance for Schools, Universities, Hospitals, Small businesses and Public authorities on Children's data, sensitive contexts, breach response and records management.

6. Promote independent audits and risk assessments for high impact processing, while ensuring that compliance mechanisms are not merely documentary exercises.

7. Clarify coordination among the Data Protection Board, sectoral regulators, CERT-In and Courts, so that individuals and organisations can identify the correct reporting and redressal route.

8. Build public awareness about phishing, identity theft, consent withdrawal, grievance redressal and safe handling of personal information.

Conclusion:

India's Data Privacy regime represents a significant shift from a fragmented set of Information Technology rules towards a dedicated framework for Digital Personal Data. The Constitutional foundation established by Puttaswamy remains essential: Privacy protects dignity, autonomy and the ability to participate freely in Society. The DPDP Act, 2023 and the Rules, 2025 create a structure of notices, consent, fiduciary duties, individual rights, safeguards and regulatory enforcement, but their practical impact depends on careful implementation and effective oversight.

As of 10 October 2026, the Rules' phased commencement must be treated as a substantive compliance issue, not a Technical detail. The strongest approach for organisations is to map data flows, identify lawful purposes, minimise collection, protect information, prepare for breach reporting and establish accessible grievance systems while monitoring official notifications. For Lawmakers and Regulators, the priority should be to ensure that innovation and legitimate public purposes are pursued consistently with Constitutional rights, Transparency and Proportionate safeguards.

Bibliography

Legislation and Official Instruments

- Constitution of India. 1950.
- Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023).
- Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), Gazette of India, 13 November 2025.
- Information Technology Act, 2000.
- Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
- Indian Computer Emergency Response Team (CERT-In), Directions under section 70B(6) of the Information Technology Act, 2000, 28 April 2022.

Cases

- Anuradha Bhasin v Union of India, (2020) 3 SCC 637.
- District Registrar and Collector, Hyderabad v Canara Bank, (2005) 1 SCC 496.
- Justice K.S. Puttaswamy (Retd.) v Union of India, (2017) 10 SCC 1.
- K.S. Puttaswamy (Aadhaar) v Union of India, (2019) 1 SCC 1.
- People's Union for Civil Liberties v Union of India, (1997) 1 SCC 301.
- Shreya Singhal v Union of India, (2015) 5 SCC 1.

Official Online Resources

- Ministry of Electronics and Information Technology, Digital Personal Data Protection Rules, 2025 and related notifications, https://www.meity.gov.in/
- India Code, Digital Personal Data Protection Act, 2023, https://www.indiacode.nic.in/
- Press Information Bureau, 'Government notifies DPDP Rules to empower citizens and protect privacy', 14 November 2025, https://www.pib.gov.in/