The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

DATA PROTECTION IN INDIA: CHALLENGES UNDER THE IT ACT AND THE PENDING DIGITAL PERSONAL DATA PROTECTION BILL

-Vanshika Chauhan

1. ABSTRACT

This blog examines India's transition from a fragmented, security-focused data regime under the Information Technology Act to a rights-based framework proposed by the Digital Personal Data Protection Act. It outlines the IT Act's key gaps—legal uncertainty, weak individual remedies, fragmented enforcement, and operational burdens then summarises the new law's promises (enumerated data-subject rights, fiduciary duties, governance requirements) and the unresolved issues (broad state exemptions, regulator design, sensitive-data safeguards, and cross-border transfer rules). Practical priorities for organisations data-flow mapping, strengthened governance, contract updates, and regulatory preparedness are recommended to navigate the evolving landscape.

2. INTRODUCTION

India's data protection landscape is undergoing a significant transformation. The Information Technology Act and its associated rules established a fragmented, security-focused framework that resulted in gaps regarding individual rights and regulatory clarity. The Digital Personal Data Protection Act aims to establish a statutory framework centered on individual rights, yet crucial legal and operational issues still persist. This post outlines the background, highlights the main challenges posed by the IT Act, summarizes the proposals of the new legislation, and presents practical measures that organizations and advisers should prioritize at this moment.

3. CONSTITUTIONAL AND STATUTORY BACKGROUND

The Supreme Court's recognition of privacy as a fundamental right[1] established a constitutional foundation for statutory data protection. Until recently, however, India's legal response relied on the IT Act, sectoral regulations, and administrative orders.[2] that emphasised cybersecurity, intermediary liability, and mandatory reporting rather than a coherent set of individual rights and fiduciary duties. That legacy produced uncertainty for businesses, uneven protection for individuals, and multiple enforcement actors with overlapping mandates.

4. KEY CHALLENGES UNDER THE IT ACT REGIME

- **Fragmentation and legal uncertainty.** The IT Act and its associated rules focused on specific issues such as cybercrime, liability of intermediaries, and reasonable security measures, rather than developing a unified and comprehensive privacy framework. This lack of cohesion made it challenging to ascertain the applicable legal standard for various processing activities and resulted in inconsistent judicial decisions.
- **Weak individual remedies.** Legal actions addressing the misuse of personal data were primarily sought through tort, contract, or criminal laws. There was an absence of a formal list of enforceable rights for data subjects similar to contemporary privacy legislation, which restricted individuals' capacity to manage their data.
- **Administrative rule-making with limited safeguards[3].** Multiple administrative directives and announcements established requirements for reporting and the retention of data (such as incident reporting and data retention mandates) without providing comprehensive procedural safeguards or an analysis of proportionality. This method sparked worries regarding extensive data gathering and retention by both private entities and government authorities.
- **Multiple enforcement actors and uneven enforcement.** Enforcement duties were distributed among various agencies and ministries, resulting in differing enforcement priorities and solutions. The lack of a sole independent regulator with defined adjudicatory authority impeded the development of cohesive policies and reliable compliance results.

[1] K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India)
[2] Information Technology Act, No. 21 of 2000 (India)
[3] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, G.S.R. 313(E) (India)

- **Operational burdens without clarity.** Companies encountered responsibilities—like required reporting to regulatory bodies or adherence to specific directives—without explicit guidelines for compliance, heightening legal and operational risks.

5. WHAT THE DIGITAL PERSONAL DATA PROTECTION ACT PROPOSES

The new legislation signifies a transition from a security-oriented, sector-specific strategy to a legal structure that acknowledges the rights of data principals and places responsibilities on data fiduciaries. Notable aspects consist of:

- **Enumerated rights** for data principals, including the rights to access and make corrections, as well as a legal framework for grievance resolution.
- **Fiduciary duties** on organizations that define the objectives and methods of processing, which encompass obligations related to purpose limitation, data minimization, and security measures.
- **Governance requirements** such as assessments of the impact on data protection, maintaining records, and reporting incidents.
- **A central regulatory body** assigned with oversight, implementation, and regulation creation.

These modifications establish a more transparent legal framework and outline expectations for accountability and governance that were mostly lacking under the IT Act system.

6. REMAINING LEGAL AND POLICY GAPS

- **Broad state exemptions[4].** The statute retains broad carve-outs for state action, national security, and public order. The scope and procedural safeguards for these exemptions are not tightly circumscribed, raising constitutional questions about proportionality and judicial review.
- **Regulatory independence and enforcement design.** The success of the new system will heavily rely on the independence of the regulator, the processes for appointing officials, protections related to their tenure, and their enforcement authority. Any uncertainties in these design aspects could lead to a regulator that does not possess the necessary autonomy or resources to take assertive action.

[4] Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, No. 18 of 2016 (India)

- **Sensitive data and tiered protections.** The legislation does not implement a completely tiered framework for sensitive categories similar to certain international standards. This could result in especially sensitive data processing (such as health, biometric, and financial information) lacking the enhanced safeguards that many stakeholders anticipate.
- **Cross-border transfers and adequacy.** Regulations concerning international data transfers, adequacy assessments, and contractual protections need more clarification. Ambiguous transfer regulations lead to compliance uncertainties for global service and cloud providers.
- **Rule-making dependence.** Numerous operational specifics are delegated to lower-level regulations and guidance. The content of those regulations will influence the statute's practical application, and they will be the center of industry interactions and legal disputes.

7. PRACTICAL PRIORITIES FOR ORGANISATIONS AND ADVISERS

- **Map data flows and legal bases.** Carry out a thorough data-flow mapping process and record the legal grounds for each processing action. Justifications for purpose limitation and data retention should be noted.
- **Strengthen governance and accountability.** Implement or refine privacy governance: appoint responsible officers, adopt DPIA processes.[5]Maintain processing records, and build incident response playbooks.
- **Review contracts and vendor management.** Revise vendor agreements to incorporate fiduciary responsibilities, security criteria, and regulations for cross-border transfers. Confirm that subcontractor supervision and audit rights are established.
- **Prepare for regulatory engagement.** Create grievance redress systems and internal audit trails to show adherence to regulations. Prepare to interact with the regulator regarding rule formulation and to address inquiries related to enforcement.
- **Assess state-facing obligations.** When processing data involves government requests or legal frameworks (such as identity systems or access for law enforcement), it's important to document the legal grounds and procedural protections; also, think about litigation approaches where constitutional issues may arise.

8. CONCLUSION

[5] Information Technology Act, No. 21 of 2000 (India); Digital Personal Data Protection Act, 2023 (India)

The shift from the fragmented, security-focused framework of the IT Act to a comprehensive, rights-based approach marks a significant change in India's legal environment. The new legislation offers clearer responsibilities and entitlements, but its overall effect will depend on subordinate regulations, the design of regulatory frameworks, and judicial scrutiny—particularly regarding state exemptions and the enforcement structure. Organizations should view this period as an opportunity to establish compliance: implement governance structures now, participate in consultations for rule-making, and remain ready to adjust as the regulatory landscape and case law develop.