IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 5, May 2026
Impact Factor: 8.2

Review of the Data Protection and Privacy Law in India

Mr. Animeshsingh Pravinsingh Bayas
LL.M 1st Year (Corporate and Commercial Law)
School of Law, Sandip University, Nashik

Abstract: *Data protection and privacy have emerged as critical concerns of modern legal systems as personal information has become the most valuable resource in the digital economy. The recognition of privacy as a fundamental right under Article 21 in Justice K.S. Puttaswamy v. Union of India (2017) marked a decisive constitutional milestone in India. The enactment of the Digital Personal Data Protection Act, 2023 and the DPDP Rules, 2025 represents India's first comprehensive statutory framework for digital personal data protection. This paper undertakes an analytical and comparative study of India's data protection regime, examining its constitutional foundations, statutory structure, enforcement mechanisms, and contemporary challenges, comparing it with the EU's GDPR and the US sectoral model to identify gaps and reform priorities. The study concludes that while the DPDP Act is a landmark development, its effectiveness depends on institutional independence, meaningful consent, robust enforcement, and public awareness.*

Keywords: Data Protection, Privacy, DPDP Act 2023, GDPR, Data Fiduciary, Data Principal, Consent, Article 21, Fundamental Rights

I. INTRODUCTION

Data protection and privacy have emerged as central concerns of modern legal systems because personal information has become one of the most valuable resources in the digital economy. Globally, the rise of digital platforms, artificial intelligence, cloud computing, and internet-based services has created an environment in which data is continuously generated and processed. Governments use data for welfare delivery, taxation, policing, and national security, while private corporations use it for advertising, consumer profiling, and market expansion. While these developments have increased efficiency and convenience, they have also created serious legal and ethical concerns regarding consent, transparency, accountability, and misuse of personal information.

In India, the issue is especially significant due to rapid digitalisation, increasing internet penetration, expansion of digital payments, and growth of e-governance. The legal framework originally did not contain a comprehensive data protection statute — protection of personal information was scattered across constitutional provisions, the Information Technology Act, 2000, sectoral regulations, and judicial decisions. This fragmented approach became inadequate in light of the volume and sensitivity of personal data being processed. The recognition of privacy as a fundamental right in Justice K.S. Puttaswamy v. Union of India (2017) and the subsequent enactment of the Digital Personal Data Protection Act, 2023 (DPDP Act) mark a decisive shift towards structured statutory protection, seeking to regulate the relationship between the Data Principal and the Data Fiduciary in the digital age.

India's privacy law evolved gradually from limited judicial recognition to constitutional protection and finally to statutory regulation. The Constitution does not expressly mention privacy, yet courts progressively read it into Article 21 through cases such as Kharak Singh v. State of Uttar Pradesh (1963), Gobind v. State of Madhya Pradesh (1975), and Maneka Gandhi v. Union of India (1978), which broadened the meaning of personal liberty to include dignity, autonomy, and freedom from arbitrary interference.

The Information Technology Act, 2000 provided the first statutory framework for electronic records and data security, though it was primarily designed to facilitate e-commerce rather than protect privacy comprehensively. The SPDI

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 5, May 2026 Impact Factor: 8.2

Rules, 2011 introduced the first specific obligations on body corporates handling sensitive personal data — covering consent, purpose limitation, security practices, and privacy policies — but remained too narrow for the complexity of modern digital data processing. As digital platforms began collecting vast amounts of personal data beyond what these rules contemplated, the inadequacy of the fragmented framework became evident. The enactment of the DPDP Act, 2023 and the DPDP Rules, 2025 represents India's first comprehensive statutory attempt to regulate digital personal data in a rights-based manner, filling the long-standing legislative gap.

Legal Framework: The DPDP Act, 2023

The DPDP Act applies to digital personal data processed within India and, extraterritorially, to entities outside India that offer goods or services to Indian users. It defines personal data broadly as any data relating to an identifiable individual. The individual whose data is processed is termed the Data Principal, while the entity determining the purpose and means of processing is the Data Fiduciary — terminology reflecting a relationship of trust and legal responsibility rather than a merely transactional one.

Consent is a cornerstone of the Act. It must be free, specific, informed, unconditional, and unambiguous, with a clear affirmative action and the right of withdrawal. Data Principals are granted rights of access to information about their data, correction, erasure, grievance redressal, and the right to nominate another person to exercise rights in the event of death or incapacity. Correspondingly, the Act also imposes duties on Data Principals, creating a balanced rights-and-duties model.

Data Fiduciaries bear the primary obligations: providing clear notice, maintaining data accuracy in decision-making contexts, implementing reasonable security safeguards, notifying the Data Protection Board and affected individuals of breaches, and erasing data once the purpose is fulfilled or consent is withdrawn. Certain entities classified as Significant Data Fiduciaries — based on volume, sensitivity, and risk — face additional duties including appointment of a Data Protection Officer, independent audits, and Data Protection Impact Assessments. The Data Protection Board of India serves as the enforcement authority empowered to inquire into breaches, issue directions, and impose substantial monetary penalties to ensure compliance.

Constitutional Foundation and Judicial Approach

The Puttaswamy judgment (2017), decided by a nine-judge bench, unanimously recognised privacy as a fundamental right under Article 21 of the Constitution. The Court identified bodily, decisional, and informational privacy as distinct but interconnected dimensions. Informational privacy — the right to control one's personal data — is especially significant for data protection law as it establishes that personal data is not merely a commercial asset but is constitutionally connected to the personality, dignity, and autonomy of the individual.

The judgment established that state restrictions on privacy must satisfy three conditions: there must be a law authorising the restriction; it must pursue a legitimate state aim; and the measure must be necessary and proportionate. This proportionality doctrine is now central to evaluating all forms of surveillance, biometric data collection, and state access to personal information. The Aadhaar case (2019) applied this test, upholding biometric identity for welfare delivery while significantly limiting its private use, and emphasising that state data collection must be accompanied by strong safeguards.

Other significant decisions include Karmanya Singh Sareen v. Union of India, which raised critical questions about platform data-sharing policies and meaningful user consent; Selvi v. State of Karnataka (2010), which affirmed protection against compelled personal disclosure under Articles 20(3) and 21; and R. Rajagopal v. State of Tamil Nadu (1994), which recognised the right to privacy against unauthorised publication of personal information. Together, these decisions provide the normative foundation upon which the DPDP framework must be interpreted and applied.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 5, May 2026 Impact Factor: 8.2

Issues and Concerns

Several significant challenges persist in India's data protection framework. First, limited digital literacy means many users accept consent requests without understanding their implications, reducing consent to a procedural formality rather than a meaningful exercise of autonomy. This is particularly acute for vulnerable groups including children, elderly persons, rural users, and first-time internet users who may not understand how their data is collected, stored, or used.

Second, data breaches and cybersecurity risks remain serious threats. The undefined standard of 'reasonable security safeguards' creates compliance uncertainty, and breaches may arise not only from hacking but also from weak internal access controls, negligent employees, misconfigured databases, or insecure third-party vendors. Third, consent fatigue and dark patterns — interface designs that hide opt-out options, pre-select consent, or repeatedly prompt users until they accept — structurally undermine voluntary consent, making it appear valid in form but defective in substance.

Fourth, the DPDP Act's broad exemptions for national security, public order, and state functions may, if applied widely, insulate government agencies from accountability, conflicting with the proportionality doctrine established in Puttaswamy. Fifth, unlike the SPDI Rules, 2011 and the GDPR, the Act lacks a distinct sensitive personal data category, potentially treating biometric, health, and financial data with insufficient differentiation. Finally, concerns about the Data Protection Board's institutional independence from executive control, technical expertise, and accessibility for ordinary citizens remain significant obstacles to effective enforcement.

II. SUGGESTIONS AND CONCLUSION

To strengthen India's data protection framework, the following measures are recommended. First, the law should progressively recognise additional rights including data portability and objection to harmful automated decision-making, as AI-driven processing increasingly influences access to credit, insurance, employment, and public services. Second, a risk-based sensitive personal data category should be reintroduced, imposing stricter obligations for biometric, health, financial, and children's data. Third, the institutional independence of the Data Protection Board must be ensured through transparent, merit-based appointments insulated from excessive executive control, accompanied by adequate funding, technical staffing, and accessible multilingual complaint mechanisms.

Fourth, consent interfaces should be mandated to be clear, concise, and free of dark patterns, with privacy notices available in regional languages. Fifth, state exemptions must be interpreted narrowly in conformity with the constitutional proportionality test from Puttaswamy, ensuring that national security is not used as a blanket justification for unrestricted data collection. Sixth, sector-specific data protection standards should be developed in coordination with regulators such as RBI, SEBI, and TRAI. Finally, digital literacy campaigns must be actively promoted across schools, rural communities, and vulnerable populations so that individuals can meaningfully exercise their statutory rights.

India's data protection framework has entered a transformative new phase with the DPDP Act, 2023 and DPDP Rules, 2025. The constitutional foundation of the Puttaswamy judgment provides the enduring normative basis, while the statute creates a rights-and-duties model suited to the digital economy. However, the true effectiveness of this framework will depend not merely on the text of the law but on institutional integrity, credible enforcement, meaningful public awareness, and a regulatory culture that treats privacy not as a compliance burden but as a constitutional value. Data protection in the digital age is ultimately a necessity linked to human dignity, individual autonomy, and democratic accountability.

REFERENCES

A. Case Laws

1. *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.
2. *K.S. Puttaswamy v. Union of India (Aadhaar Case)*, (2019) 1 SCC 1.
3. *Maneka Gandhi v. Union of India*, (1978) 1 SCC 248.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 5, May 2026 Impact Factor: 8.2

4. *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295.
5. *Gobind v. State of Madhya Pradesh*, (1975) 2 SCC 148.
6. *R. Rajagopal v. State of Tamil Nadu*, (1994) 6 SCC 632.
7. *Selvi v. State of Karnataka*, (2010) 7 SCC 263.
8. *Karmanya Singh Sareen v. Union of India*, W.P.(C) 7663/2016 (Delhi HC).

B. Books

9. M.P. Jain, *Indian Constitutional Law* (LexisNexis, 8th edn., 2019).
10. Daniel J. Solove, *Understanding Privacy* (Harvard University Press, 2008).
11. Nandan Kamath, *Law Relating to Computers, Internet and E-Commerce* (Universal Law Publishing, 2014).
12. Rishab Bailey and Smriti Parsheera, *Data Protection in India: A Practitioner's Guide* (Eastern Book Company, 2023).
13. D.D. Basu, *Commentary on the Constitution of India* (LexisNexis, 9th edn., 2014).

C. Statutes and Regulations

14. Digital Personal Data Protection Act, No. 22 of 2023, India.
15. Digital Personal Data Protection Rules, 2025 (MeitY Notification).
16. Information Technology Act, No. 21 of 2000, India.
17. IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
18. General Data Protection Regulation (EU) 2016/679 [GDPR].
19. California Consumer Privacy Act (CCPA), 2018; California Privacy Rights Act (CPRA), 2020.

D. Reports and General References

20. Justice B.N. Srikrishna Committee Report on Data Protection (Ministry of Electronics and Information Technology, 2018).
21. Internet Freedom Foundation, 'Analysis of the Digital Personal Data Protection Act, 2023' (2023), available at <https://internetfreedom.in>.
22. European Data Protection Board, 'Guidelines 05/2020 on Consent under Regulation 2016/679' (May 2020).
23. Personal Data Protection Bill, 2019 (Lapsed) — Joint Parliamentary Committee Report (2021).
24. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2013 Revised Edition).
25. Ministry of Electronics and Information Technology (MeitY), Annual Report 2022–23, Government of India.
26. Telecom Regulatory Authority of India (TRAI), 'Recommendations on Privacy, Security and Ownership of Data in the Telecom Sector' (2018)