2026 Volume: 02 Issue: 11 www.ijrpa.com ISSN 2456-9995 Review Article

International Journal Research Publication Analysis

Page: 01-10

# DATA PROTECTION AND PRIVACY UNDER INDIAN LAW

***Jay Halpati**

Constitutional Foundations, Statutory Protection and Emerging Challenges.

**Article Received: 22 September 2026**
**Article Revised: 12 October 2026**
**Published on: 01 November2026**

***Corresponding Author: Jay Halpati**
Constitutional Foundations, Statutory Protection and Emerging Challenges.
DOI: https://doi-doi.org/101555/ijrpa.2948

## ABSTRACT

The rapid expansion of digital services has transformed personal data into an essential economic and social resource. In India, this transformation has also exposed individuals to surveillance, profiling, identity theft, data breaches and opaque forms of automated decision-making. The constitutional recognition of privacy in Justice K.S. Puttaswamy (Retd.) v. Union of India marked a decisive shift by treating privacy as an intrinsic part of dignity, liberty and autonomy under Article 21 and the broader scheme of fundamental rights. The Digital Personal Data Protection Act, 2023 (DPDP Act) represents India's principal legislative framework for digital personal data and establishes obligations for Data Fiduciaries, rights and duties of Data Principals, special protections for children, regulation of Significant Data Fiduciaries and an institutional mechanism through the Data Protection Board of India. The Digital Personal Data Protection Rules, 2025 provide the operational framework and introduce a phased commencement structure. This article examines the constitutional and statutory foundations of data protection in India, analyses the principal provisions of the DPDP Act, considers important judicial decisions, and identifies continuing concerns relating to state exemptions, consent, enforcement, cross-border transfers, surveillance, children's data and effective remedies. It argues that Indian privacy law must balance innovation and legitimate public interests with meaningful individual control, proportionality, transparency and institutional accountability.

**KEYWORDS:** Data Protection; Right to Privacy; DPDP Act 2023; Digital Personal Data; Data Fiduciary; Constitutional Law.

## 1. INTRODUCTION

Personal data has become one of the most valuable resources in the digital economy.

Banking, healthcare, education, e-commerce, telecommunications, social media and public welfare systems routinely depend upon the collection and analysis of information relating to individuals. A person's name, mobile number, location, financial information, photographs, identification details, online behaviour and biometric information can reveal aspects of personality and private life. When such information is aggregated, the resulting profile may be substantially more revealing than any single item of data.

The legal problem is therefore not merely the unauthorised disclosure of a secret. Modern data processing can affect an individual's autonomy even when information is lawfully collected. Continuous tracking, behavioural profiling, targeted advertising and algorithmic classification may influence opportunities, prices, access to services and social choices. Data protection law seeks to regulate this power relationship by imposing duties on organisations that process personal data and by giving individuals meaningful rights over information relating to them.

Indian privacy law has developed through constitutional adjudication as well as legislation. Before a comprehensive digital data protection statute was enacted, protection was distributed among constitutional rights, the Information Technology Act, 2000, sector-specific regulations, contractual principles and judicial remedies. The Supreme Court's nine-judge decision in Justice

K.S. Puttaswamy (Retd.) v. Union of India transformed this landscape by holding that privacy is a constitutionally protected right. The DPDP Act, 2023 subsequently created a dedicated statutory framework for digital personal data. The Rules notified in 2025 provide detailed implementation mechanisms and, importantly, establish a phased commencement timetable.

This article examines the evolution of Indian data protection law, the constitutional principles governing privacy, the architecture of the DPDP Act, the role of the Data Protection Board, and the principal challenges that will determine whether the new framework provides effective protection in practice.

## 2. CONSTITUTIONAL FOUNDATION OF THE RIGHT TO PRIVACY

The constitutional foundation of data protection lies principally in Article 21 of the Constitution of India, read with the guarantees of dignity, equality and freedoms contained in Part III. In Justice

K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, a nine-judge Bench unanimously recognised privacy as a constitutionally protected right. The Court connected

privacy with liberty, dignity, autonomy and the ability of an individual to make fundamental choices.

Puttaswamy rejected the idea that privacy is merely a narrow right to be left alone. It includes decisional, informational and spatial dimensions. Informational privacy is particularly important to data protection because it concerns an individual's ability to exercise control over information concerning the person. The Court also recognised that privacy is not absolute. Restrictions must satisfy constitutional requirements of legality, legitimate state aim, proportionality and procedural safeguards.

The proportionality principle has become an important constitutional tool for evaluating state interference with privacy. A restriction cannot be justified merely because the State identifies a desirable objective. There must be a lawful basis, a legitimate purpose and a rational and proportionate relationship between the measure and that purpose. Less restrictive alternatives may become relevant when assessing whether the interference is necessary.

The Aadhaar litigation further demonstrated the tension between welfare objectives and informational privacy. In K.S. Puttaswamy (Retd.) v. Union of India, (2019) 1 SCC 1, the Supreme Court examined the constitutional validity of the Aadhaar framework and applied proportionality to different forms of data use and authentication. The decision illustrates that data protection is not only a matter of private contracts; state collection and use of personal data must also conform to constitutional standards.

Privacy has also informed decisions concerning autonomy and personal choice. In Navtej Singh Johar v. Union of India, (2018) 10 SCC 1, and Common Cause v. Union of India, (2018) 5 SCC 1, the Supreme Court linked privacy with dignity and decisional autonomy. These cases reinforce a broader proposition: personal information is closely connected with the ability of individuals to shape their identities and lives free from unjustified interference.

## 3. THE PRE-DPDP LEGAL FRAMEWORK

Before the DPDP Act, India's principal statutory provision specifically addressing compensation for failure to protect sensitive personal data was section 43A of the Information Technology Act, 2000, supported by the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. The earlier framework was important but limited in scope and structure. It did not provide the comprehensive rights-and-obligations model now associated with modern data protection regimes.

The Information Technology Act also contains provisions relevant to unauthorised access,

disclosure and misuse of information. Section 72A, for example, addresses disclosure of information in breach of lawful contract in specified circumstances. These provisions demonstrate that Indian law recognised information-related harms before the DPDP Act, but regulation was fragmented.

The constitutional position supplied another layer of protection. Individuals could invoke Articles 14, 19 and 21 where state action unjustifiably interfered with privacy. Contract law and sectoral rules could also regulate particular relationships. However, the rapid growth of digital platforms made a general data protection statute increasingly necessary.

The DPDP Act therefore represents a shift from a primarily sectoral and reactive model toward a general framework based on accountability, specified purposes, consent and lawful uses. At the same time, the Act differs from some foreign models because of its terminology and design. It uses the concepts of 'Data Principal' and 'Data Fiduciary' rather than data subject and controller, and it adopts a comparatively concise legislative structure.

## 4. THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

The Digital Personal Data Protection Act, 2023 is intended to regulate the processing of digital personal data while recognising both the individual's interest in protecting personal data and the need to process data for lawful purposes. The Act received Presidential assent on 11 August 2023. It defines the individual to whom personal data relates as the Data Principal and the person who determines the purpose and means of processing as the Data Fiduciary.

The Act applies to processing of digital personal data within India where the processing is in connection with offering goods or services to Data Principals within India, and it can also apply to certain processing outside India connected with such activity. This gives the legislation an important extraterritorial dimension.

A central feature is the distinction between consent and certain legitimate uses. Consent must be free, specific, informed and unambiguous, and must involve clear affirmative action. The Act also recognises circumstances where processing may occur without ordinary consent, including specified public functions, legal obligations, medical emergencies, employment-related purposes and other enumerated legitimate uses. This approach attempts to balance individual control with practical requirements of governance and commerce.

Section 5 requires notice before or at the time of requesting consent. The notice model is significant because meaningful consent is impossible where individuals do not understand what information is being collected and why. The 2025 Rules strengthen this requirement by requiring clear, standalone and understandable notices that identify the personal data being

processed and the purposes for which it is processed.

Section 8 imposes general obligations on Data Fiduciaries. These include responsibility for compliance, implementation of technical and organisational measures, reasonable security safeguards, breach notification, deletion when the specified purpose is no longer being served subject to legal retention requirements, publication of contact information and an effective grievance-redress mechanism.

The Act also creates additional obligations for Significant Data Fiduciaries. Such entities may be designated based on factors including the volume and sensitivity of data, risks to individuals, impact on sovereignty and integrity, electoral democracy, security of the State and public order. Significant Data Fiduciaries must appoint a Data Protection Officer, appoint an independent data auditor and undertake periodic Data Protection Impact Assessments and audits.

Children receive special protection. Processing of children's personal data is subject to additional safeguards, including verifiable parental consent and restrictions on processing that is likely to cause detrimental effects on children's well-being. The framework also addresses tracking, behavioural monitoring and targeted advertising involving children.

The Act grants Data Principals rights including access to information about personal data, correction and erasure, grievance redressal and nomination. These rights are balanced by duties, such as complying with applicable law, not impersonating another person, not suppressing material information and not filing false or frivolous grievances. The inclusion of duties reflects the Act's emphasis on reciprocal responsibility.

## 5. DATA PROTECTION BOARD AND ENFORCEMENT

The institutional mechanism under the Act is the Data Protection Board of India. The Board is intended to inquire into personal data breaches and complaints, issue directions and impose monetary penalties for contraventions. The enforcement design is significant because a data protection statute is effective only when individuals and organisations have access to a credible and accessible remedy.

The Act adopts a financial penalty framework rather than criminalising ordinary regulatory non-compliance. The Schedule permits substantial penalties, with the highest category reaching up to ■250 crore for specified failures, including failure to take reasonable security safeguards. Other categories cover failures concerning breach notification, children's data, Significant Data Fiduciaries and other contraventions.

The penalty structure should nevertheless be understood as a maximum framework rather

than an automatic fine. The Board is required to consider statutory factors when determining the amount. Effective enforcement will depend on the Board's independence, technical expertise, procedural fairness and ability to handle large volumes of complaints.

The Rules notified in November 2025 are especially important to implementation. They establish requirements concerning notices, Consent Managers, security safeguards, breach intimation and other operational matters. The commencement notification adopts a phased approach. Certain institutional and definitional provisions took effect on 13 November 2025; another group is scheduled one year after publication, while the principal operational provisions are scheduled eighteen months after publication. Accordingly, the legal position in September 2026 is transitional rather than one in which every substantive provision of the Act is already operative.

## 6. CROSS-BORDER DATA AND THE ROLE OF THE STATE

Digital services routinely transfer data across national borders. Cloud computing, international payments, social media and multinational business operations may involve processing in several jurisdictions. The DPDP Act does not adopt a blanket localisation requirement. Instead, section 16 permits the Central Government to restrict the transfer of personal data outside India to such countries or territories as may be notified.

This approach provides regulatory flexibility but raises questions concerning certainty and international interoperability. Businesses need predictable rules to structure cross-border processing, while individuals require assurance that data transferred abroad remains subject to meaningful safeguards.

A more difficult issue concerns exemptions available to the State and other specified purposes. The Act permits exemptions in circumstances connected with sovereignty and integrity, security of the State, public order and prevention, detection, investigation or prosecution of offences, among others. Such purposes can be legitimate, but privacy requires that even legitimate objectives be pursued through lawful, necessary and proportionate measures.

The constitutional framework developed in Puttaswamy remains relevant here. Statutory power to process data does not necessarily answer every constitutional question. Where state action substantially interferes with privacy, courts may examine legality, legitimate aim and proportionality. Transparency and independent oversight therefore remain important even where confidentiality is necessary for national security or law enforcement.

## 7. IMPORTANT JUDICIAL DEVELOPMENTS

Indian courts have progressively developed principles that support modern data protection.

In R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632, the Supreme Court recognised aspects of the right to privacy and discussed the limits of publication of private facts. Although decided before the digital data economy expanded, the judgment remains relevant to the relationship between privacy and dissemination of personal information.

In PUCL v. Union of India, (1997) 1 SCC 301, the Supreme Court imposed procedural safeguards in relation to telephone interception. The decision demonstrates that communications surveillance must not be treated as an unlimited executive power.

Puttaswamy elevated these principles by expressly constitutionalising privacy. The judgment also recognised informational privacy as an important component of individual autonomy. Its reasoning provides a constitutional foundation against excessive collection and use of personal information.

In Shreya Singhal v. Union of India, (2015) 5 SCC 1, the Court struck down section 66A of the Information Technology Act, emphasising the importance of constitutional freedoms in the digital environment. Although the case primarily concerned freedom of speech, it established an important judicial willingness to scrutinise technologically mediated restrictions.

K.S. Puttaswamy (Aadhaar) further demonstrates the relevance of proportionality when government databases and identification systems affect fundamental rights. The judgment is particularly significant for understanding the relationship between authentication, welfare delivery, exclusion risks and privacy.

Taken together, these decisions show that Indian privacy law is not limited to the DPDP Act. The statute operates within a wider constitutional framework, and judicial review remains an essential safeguard against disproportionate interference.

## 8. CHALLENGES IN THE INDIAN DATA PROTECTION REGIME

The first challenge is meaningful consent. In many digital environments, users encounter lengthy privacy notices and have little practical bargaining power. Consent may therefore become formal rather than genuinely informed. The effectiveness of the DPDP framework will depend on whether notices are understandable and whether withdrawal of consent is realistically available.

Second, data minimisation must be taken seriously. Organisations often collect information because it may be useful in the future. A strong privacy culture requires collection to be

connected to a legitimate and defined purpose rather than speculative future uses.

Third, data breaches remain a major concern. Security obligations are meaningful only when supported by appropriate technical controls, access management, encryption, monitoring, incident response and employee training. Legal compliance should therefore be integrated with cybersecurity governance rather than treated as a purely documentation exercise.

Fourth, children's privacy requires particular attention. Young users may not understand long-term consequences of data disclosure. Parental consent is useful but cannot by itself solve the problems of platform design, behavioural profiling and persuasive technology. Age assurance mechanisms also create their own privacy risks if they require collection of additional identity information.

Fifth, state exemptions require careful constitutional scrutiny. National security and law enforcement are legitimate objectives, but broad powers without effective safeguards can undermine the informational autonomy that privacy law seeks to protect. Independent oversight, clear purpose limitations and proportionate procedures are therefore essential.

Sixth, enforcement capacity will determine the practical value of rights. A specialised Board must have adequate expertise in technology, cybersecurity, administrative law and adjudication. It must also be accessible to ordinary individuals, not only large corporations.

Finally, the relationship between the DPDP framework and other Indian laws will require continuing judicial and administrative clarification. Sectoral regulators in banking, telecommunications, health, insurance and securities may impose additional requirements. Harmonisation will be necessary to prevent contradictory obligations and excessive compliance burdens.

## 9. WAY FORWARD

India should treat privacy as both a constitutional value and a governance principle. Organisations should adopt privacy-by-design practices, conduct data inventories, restrict access on a need-to-know basis, establish retention schedules and test incident-response plans. Consent interfaces should be simple enough for ordinary users to understand.

The Data Protection Board should develop transparent and predictable enforcement practices. Published guidance, reasoned decisions and accessible complaint procedures can improve legal certainty. Penalties should be proportionate to the seriousness of the breach while being sufficiently meaningful to create incentives for compliance.

The government should also clarify the interaction between data protection, cybersecurity and sectoral regulation. Cross-border data transfers require predictable rules that protect

individuals without unnecessarily isolating India from global digital commerce.

Most importantly, privacy should not be understood as an obstacle to innovation. Strong privacy standards can increase trust in digital services. Businesses that minimise unnecessary data collection and maintain effective security are likely to face fewer regulatory, reputational and operational risks. Privacy-respecting innovation can therefore support, rather than hinder, the growth of India's digital economy.

## 10. CONCLUSION

Data protection in India has moved from a fragmented statutory landscape toward a dedicated legal framework. The constitutional recognition of privacy in Puttaswamy established the normative foundation, while the DPDP Act, 2023 provides a general statutory architecture governing digital personal data. The 2025 Rules add important operational detail and the phased commencement framework marks the transition from legislation to implementation.

The central question is not simply whether India has a data protection law, but whether individuals can exercise meaningful control over personal information and whether institutions can be held accountable for misuse. The answer will depend on the quality of consent, security safeguards, grievance mechanisms, Board enforcement and constitutional oversight of state action.

Indian data protection law should therefore be understood as an evolving field. The DPDP framework provides an important foundation, but its success will be measured by implementation in real-world situations involving citizens, businesses, government agencies and digital platforms. A rights-respecting approach requires the law to preserve a careful balance between privacy, innovation, public interest and national security. Ultimately, effective data protection is not merely about controlling information; it is about protecting human dignity and autonomy in an increasingly data-driven society.

## REFERENCES AND FOOTNOTES

1. Constitution of India arts. 14, 19, 21.
2. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC
3. K.S. Puttaswamy (Retd.) v. Union of India, (2019) 1 SCC 1.
4. R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632.
5. People's Union for Civil Liberties (PUCL) v. Union of India, (1997) 1 SCC 301.
6. Shreya Singhal v. Union of India, (2015) 5 SCC 1.
7. Navtej Singh Johar v. Union of India, (2018) 10 SCC 1.

8. Common Cause v. Union of India, (2018) 5 SCC 1.
9. Information Technology Act, 2000, §§ 43A, 72A.
10. Digital Personal Data Protection Act, 2023, §§ 3–17, 18–37 & Schedule.
11. Digital Personal Data Protection Rules, 2025, Gazette of India, G.S.R. 846(E), 13 Nov. 2025.
12. Digital Personal Data Protection Act, 2023, commencement notification, G.S.R. 843(E), 13 Nov. 2025.
13. Ministry of Electronics and Information Technology, Government of India, Digital Personal Data Protection Rules, 2025 and Explanatory Note.
14. Supreme Court of India, Justice K.S. Puttaswamy (Retd.) v. Union of India, W.P. (C) No. 494 of 2012, judgment dated 24 Aug. 2017.
15. Digital Personal Data Protection Act, 2023, § 8 (general obligations of Data Fiduciary), § 10 (Significant Data Fiduciary), §§ 11–15 (rights and duties of Data Principal), § 33 & Schedule (penalties).