2026 Volume: 02 Issue: 09 www.ijrpa.com ISSN 2456-9995 Review Article

International Journal Research Publication Analysis

Page: 01-12

FROM CONSENT TO CONSTITUTIONAL CONTROL: REIMAGINING INFORMATIONAL PRIVACY UNDER INDIA'S DIGITAL PERSONAL DATA PROTECTION FRAMEWORK

***Jayshree Bhanushali**

India.

Article Received: 30 July 2026
Article Revised: 20 August 2026
Published on: 10 September 2026

***Corresponding Author: Jayshree Bhanushali**
India.

DOI: https://doi-doi.org/101555/ijrpa.9211

ABSTRACT

The digitalisation of governance, commerce and everyday life has transformed personal data into one of the most valuable resources in the modern economy. At the same time, the collection and processing of personal data creates significant risks to individual autonomy, dignity and liberty. In India, the constitutional recognition of privacy in *Justice K.S. Puttaswamy (Retd.) v. Union of India* marked a decisive shift from viewing privacy as merely a common-law interest to recognising it as a fundamental right. The enactment of the Digital Personal Data Protection Act, 2023 ("DPDP Act") and the subsequent notification of the Digital Personal Data Protection Rules, 2025 ("DPDP Rules") represent the legislative attempt to translate this constitutional principle into an operational regulatory framework.

This article argues that the success of India's data protection regime cannot be measured merely by the existence of consent notices, compliance programmes or monetary penalties. The deeper question is whether the framework meaningfully protects informational self-determination against both private and State power. The article examines the consent architecture, duties of Data Fiduciaries, rights of Data Principals, treatment of children's data, governmental exemptions and the institutional design of the Data Protection Board of India. It contends that the DPDP framework should be interpreted through the constitutional values of dignity, autonomy, proportionality, transparency and accountability. The article concludes by proposing a constitutional model of data protection in which consent is treated as one component of privacy protection rather than its complete substitute.

KEYWORDS: Data Protection, Informational Privacy, DPDP Act, Constitutional Law, Consent, Data Fiduciary, Data Principal, Digital Governance, Article 21, India.

I. INTRODUCTION

Personal data has become an indispensable component of contemporary social and economic life. A person's identity, location, financial transactions, browsing behaviour, educational history, health-related information and digital interactions can all be converted into data capable of being stored, analysed and monetised. The same digital infrastructure that enables faster public services, personalised commerce and technological innovation can also facilitate surveillance, profiling, manipulation and exclusion.

This transformation has created a fundamental legal question: **who should control information about an individual?**

For a considerable period, Indian law did not possess a comprehensive statutory framework governing the processing of personal data. Sector-specific legislation, contractual arrangements and provisions of the Information Technology Act, 2000 operated without forming a complete data protection architecture. The constitutional position, however, changed substantially with the Supreme Court's nine-Judge Bench decision in *Justice K.S. Puttaswamy (Retd.) v. Union of India*. The Court recognised privacy as a constitutionally protected right emerging principally from Article 21, while also connecting privacy with other fundamental freedoms and the values of dignity and autonomy. Informational privacy was expressly recognised as one of its important dimensions. [1]

The enactment of the Digital Personal Data Protection Act, 2023 was therefore more than a regulatory development. It represented an attempt to give statutory shape to a constitutional value. The Act declares its purpose to be the processing of digital personal data in a manner that recognises both the individual's right to protect personal data and the need to process such data for lawful purposes. [2]

The notification of the DPDP Rules, 2025 has subsequently provided greater detail regarding consent notices, security safeguards, children's data, grievance mechanisms, Consent Managers and the functioning of the Data Protection Board. The Rules were notified on 13 November 2025 and provide for phased implementation, with major substantive obligations scheduled to become operational after eighteen months. [3]

This transition raises a central question: **Will India's new data protection framework merely regulate data processing, or will it actually strengthen the constitutional right to informational privacy?**

This article argues that the answer depends on whether the DPDP framework is interpreted as a conventional economic-regulatory statute or as legislation operating within the constitutional architecture of privacy, dignity and autonomy.

II. From Privacy to Informational Self-Determination

Privacy is frequently misunderstood as a right to secrecy. Such an understanding is inadequate in the digital age. An individual may willingly disclose information to a hospital, bank, educational institution or online platform without intending that information to be used for unrelated purposes.

The constitutional conception of privacy is therefore broader. In *Puttaswamy*, the Supreme Court recognised informational privacy as involving an individual's ability to exercise control over the dissemination of information concerning oneself. [1] Privacy consequently concerns not merely whether information is secret, but also **who possesses it, why it is collected, how it is used, with whom it is shared and how long it remains available**.

This distinction is important because modern data processing often operates through aggregation. An individual may disclose dozens of apparently insignificant pieces of information. When combined, however, these fragments can create an extraordinarily detailed profile of that person.

For example, a shopping history may reveal economic circumstances; location data may reveal religious or political participation; search histories may reveal intimate concerns; and patterns of online behaviour may permit predictions about a person's preferences. Data processing can therefore affect individual autonomy even when no single item of information appears particularly sensitive.

The constitutional significance of informational privacy lies precisely here. The individual is not merely protecting a collection of isolated facts. The individual is protecting the ability to participate in society without becoming permanently subject to comprehensive digital observation and profiling.

The DPDP framework should accordingly be understood as a mechanism for protecting **informational self-determination** rather than merely preventing data theft.

III. The DPDP Act and the Shift from Consent to Accountability

Consent occupies a prominent position in the DPDP Act. The statutory framework distinguishes between processing based on consent and certain specified legitimate uses. It also imposes obligations upon Data Fiduciaries concerning notice, processing, security, grievance redressal and other aspects of data governance. [2]

The emphasis on consent is understandable. Consent reflects individual autonomy and allows a person to decide whether personal data may be processed.

However, consent alone cannot provide complete privacy protection.

The contemporary digital environment is characterised by unequal bargaining power. Individuals routinely encounter lengthy privacy policies before accessing essential services. The practical choice may not be between consenting and refusing, but between consenting and losing access to a platform or service. This phenomenon has produced what may be described as **consent fatigue**.

A person who clicks "I agree" after encountering a lengthy legal notice cannot necessarily be said to have exercised meaningful informational autonomy. Formal consent and substantive autonomy may therefore diverge.

The DPDP Rules attempt to address this problem by requiring notices to communicate relevant information in a clear and understandable manner, including an itemised description of personal data and the specified purpose of processing. [4] This is a positive development because meaningful consent requires meaningful information.

Nevertheless, the legal framework should move beyond the assumption that a properly drafted notice automatically produces genuine consent.

Consent should be viewed as only one element of a larger accountability framework. A Data Fiduciary should remain responsible for collecting only information reasonably connected to a legitimate purpose, maintaining appropriate security, preventing unauthorised processing and deleting information when retention is no longer justified.

In other words, **privacy should not become something that individuals must negotiate alone through a consent button**.

IV. Data Fiduciaries and the Responsibility of Power

The DPDP Act deliberately uses the concept of a "Data Fiduciary", reflecting the fact that organisations exercising control over personal data possess significant informational power. The Data Fiduciary is responsible for determining the purpose and means of processing personal data.

This allocation of responsibility is important because individuals ordinarily lack the technological capacity to monitor what happens to their information after disclosure.

A person may know that an online platform has collected their information, but may not know whether it has been copied, analysed, combined with other datasets, transferred to processors or retained indefinitely.

The fiduciary model therefore shifts the regulatory burden towards those who possess institutional and technological capacity.

The DPDP Rules strengthen this architecture through requirements concerning reasonable security safeguards. These include measures such as encryption, masking or tokenisation, access controls, logging and monitoring, backups and other organisational and technical safeguards. [5]

This represents an important conceptual shift. Data protection should not begin after a breach occurs. It should be embedded into the design and operation of systems from the beginning.

The idea is particularly important for artificial intelligence and algorithmic decision-making. As automated systems become increasingly capable of drawing conclusions from personal information, the distinction between data collection and decision-making becomes less meaningful.

A privacy-protective framework should therefore ask not only whether an organisation lawfully collected data, but also whether the resulting processing produces disproportionate effects upon individuals.

For example, if data is used to determine eligibility for credit, employment, insurance or access to services, an apparently neutral processing system may reproduce existing social inequalities. Privacy protection must consequently interact with the constitutional principles of equality and non-arbitrariness.

V. Rights of Data Principals: From Formal Rights to Effective Remedies

The DPDP Act recognises several rights for Data Principals, including rights relating to access to information about personal data, correction and erasure, grievance redressal and nomination. [2]

These rights are essential because privacy without a remedy is largely theoretical.

Yet the effectiveness of these rights depends on accessibility. A right that requires complex technological knowledge, repeated correspondence or expensive litigation will disproportionately benefit sophisticated users while leaving ordinary citizens behind.

The DPDP Rules attempt to strengthen accessibility by requiring Data Fiduciaries and relevant Consent Managers to publish mechanisms through which individuals may exercise their rights and submit grievances. [6]

The next challenge is enforcement.

The establishment of the Data Protection Board of India represents a significant institutional development. The Act provides for the Board as the principal regulatory body responsible for functions assigned under the legislation. The Board was formally established by notification in November 2025. [7]

The institutional independence of the Board will be crucial. A regulator dealing with powerful technology companies and State instrumentalities must possess sufficient expertise, procedural independence and credibility.

The Board's effectiveness should therefore not be measured merely by the number of penalties imposed. Its legitimacy will depend upon transparent procedures, reasoned decisions, accessible complaint mechanisms and consistent interpretation of statutory rights.

A rights-based data protection system must make the citizen's journey from “I believe my privacy has been violated” to “I can obtain an effective remedy” as simple as possible.

VI. Children's Data and the Principle of Vulnerability

Children require heightened protection in the digital environment because their capacity to understand long-term consequences of data disclosure is developing.

The DPDP Act consequently establishes special provisions governing the processing of children's personal data and places additional restrictions upon certain forms of processing. [2]

The Rules provide mechanisms for obtaining verifiable parental consent and identify circumstances in which certain obligations may be relaxed for specified classes of Data Fiduciaries or purposes. [8]

The challenge, however, lies in balancing child protection with the legitimate use of digital services.

Overly rigid systems may make educational, health or communication technologies difficult for children to access. Conversely, weak safeguards may allow platforms to build persistent profiles of minors.

The appropriate approach should therefore be based on the principle of **best interests of the child**. The objective should not simply be to verify age but to minimise unnecessary collection and prevent the creation of long-term behavioural profiles.

The law should also recognise that today's child's digital identity may remain accessible for decades. A seemingly harmless data point collected at age fourteen can potentially influence opportunities much later in life.

Children's privacy is therefore not merely a specialised data-protection issue; it is a question of preserving future autonomy.

VII. State Processing and the Constitutional Question

Perhaps the most significant constitutional issue within India's data protection framework concerns processing by the State.

Governments possess legitimate reasons to process personal data. Welfare delivery, taxation, public health, law enforcement and administration all require information.

At the same time, State access to large databases creates risks that are qualitatively different from ordinary commercial data processing. The State possesses coercive authority and can combine information across multiple institutions.

The DPDP Act permits specified forms of processing by the State and its instrumentalities for purposes including the provision of subsidies, benefits, services, certificates, licences and permits, subject to statutory conditions. [9]

The Rules require such processing to satisfy standards relating to lawful purpose, necessity, accuracy, retention, security, transparency and accountability. [10]

The constitutional question is whether these safeguards are sufficient when State processing substantially interferes with privacy.

The answer should be informed by the proportionality framework developed by the Supreme Court. A privacy restriction must have a lawful basis, pursue a legitimate objective, maintain a rational connection between the measure and objective, satisfy necessity and maintain a proper balance between the competing interests. [1]

Consequently, statutory authorisation should not automatically be treated as constitutional justification.

A government database containing extensive personal information may technically operate under statutory authority while still raising questions concerning necessity, retention, access controls and proportionality.

The constitutional principle should therefore be:

The State must not collect or retain more personal information than is reasonably necessary to achieve a legitimate public purpose.

This principle is particularly important as India expands digital public infrastructure.

VIII. The Exemption Problem

No data protection law can operate without exemptions. National security, law enforcement, research, legal obligations and other public interests may require departures from ordinary privacy obligations.

The danger, however, lies in exemptions becoming so broad that they undermine the rule itself.

The constitutional status of privacy means that exemptions affecting fundamental rights cannot be evaluated solely as matters of administrative convenience. They must remain consistent with constitutional limitations upon State power.

This is particularly important because the DPDP Act contains provisions permitting exemptions from specified obligations in defined circumstances. [11]

A rights-protective interpretation requires that exemptions be construed narrowly rather than expansively.

The principle should be that an exemption is an exception to ordinary accountability, not an alternative regulatory regime in which accountability disappears.

Independent review, purpose limitation, retention controls and safeguards against secondary use should remain central wherever possible.

IX. The Data Protection Board and Institutional Independence

The Data Protection Board is intended to provide a specialised institutional mechanism for implementing the statutory framework. The Board's establishment and operational provisions were brought into force in the first phase of implementation beginning in November 2025. [7]

The institutional structure presents an important question of regulatory independence.

Data protection regulation frequently involves conflicts between powerful private entities and public authorities. A regulator that lacks sufficient independence may struggle to command public confidence.

The Board should therefore cultivate three forms of independence.

First, it requires **functional independence**, enabling it to investigate and adjudicate matters without inappropriate external influence.

Second, it requires **technical independence**, including access to personnel capable of understanding cybersecurity, artificial intelligence, data architecture and algorithmic systems.

Third, it requires **procedural independence**, meaning that affected parties should receive fair notice, an opportunity to be heard and reasoned decisions.

The use of a digital office model can improve accessibility and efficiency, but digitisation should not eliminate procedural fairness. Individuals must remain able to understand proceedings and meaningfully participate in them.

X. A Constitutional Reading of the DPDP Framework

The central argument of this article is that the DPDP Act should not be interpreted in isolation from constitutional privacy jurisprudence.

Three constitutional principles should guide its interpretation.

1. Dignity

Personal information can expose intimate aspects of a person's life. Uncontrolled processing may reduce individuals to data profiles rather than recognising them as autonomous persons.

2. Autonomy

The individual must retain meaningful control over personal information. Consent, access, correction and erasure rights should therefore be interpreted in a manner that strengthens rather than weakens individual agency.

3. Proportionality

Privacy restrictions must remain proportionate to legitimate objectives. This principle is particularly important for State processing and broad statutory exemptions.

These principles transform data protection from a technical compliance exercise into a constitutional project.

XI. Beyond Compliance: Towards Privacy by Design

The future of Indian data protection cannot depend exclusively on lawyers and compliance departments reviewing privacy policies.

Privacy must become a design principle.

Organisations should conduct data mapping, minimise unnecessary collection, establish retention schedules, separate sensitive datasets, restrict internal access and integrate privacy considerations into product development.

The DPDP Rules' emphasis on technical and organisational safeguards supports this direction. [5]

Privacy by design also has an economic advantage. Preventing unnecessary collection reduces the volume of data that can be compromised during a breach. It can also reduce storage costs, improve data quality and increase consumer trust.

For regulators, the objective should similarly be preventive rather than purely punitive.

A mature data protection system should encourage organisations to identify risks before harm occurs.

XII. The Road Ahead

The phased implementation of the DPDP Act and Rules provides organisations with time to build compliance systems. Under the notified framework, major operational provisions are scheduled to come into force eighteen months after notification, while the Consent Manager framework has a separate one-year commencement period. [3]

This transition period should not be treated as a reason to postpone privacy governance.

Instead, it should be used to develop:

1. comprehensive data inventories;
2. purpose-based data collection policies;
3. effective consent and withdrawal mechanisms;
4. data retention and deletion systems;
5. breach-response procedures;
6. children's data safeguards;
7. grievance-redressal mechanisms;
8. vendor and processor controls; and
9. internal privacy accountability structures.

For the State, the transition period should similarly be used to review databases and determine whether existing practices satisfy necessity, proportionality and purpose limitation. The objective should be to prevent the DPDP regime from becoming a paperwork exercise.

XIII. CONCLUSION

India's journey towards data protection has moved from constitutional recognition to legislative implementation. *Puttaswamy* established that privacy is intrinsic to dignity, liberty and autonomy. The DPDP Act attempts to translate that constitutional recognition into enforceable statutory responsibilities, while the DPDP Rules provide the operational architecture necessary for implementation.

Yet the success of the regime will depend on more than the existence of legislation.

A privacy framework becomes meaningful only when individuals can understand how their information is used, exercise genuine control over it and obtain effective remedies when their rights are violated. Similarly, organisations must understand that compliance is not simply a matter of obtaining consent or publishing privacy policies. It requires accountability throughout the data lifecycle.

The greatest challenge will be maintaining this balance in relation to State power. Digital governance can produce enormous public benefits, but efficiency cannot become a substitute for constitutional safeguards. The fact that information is digitally accessible does not make it constitutionally insignificant.

India therefore needs to move from a **consent-centric conception of privacy towards an accountability-centric conception of informational autonomy**.

Consent should remain important, but it should not carry the entire burden of privacy protection. The stronger principle is that every exercise of informational power must be justified by purpose, limited by necessity, constrained by proportionality and accompanied by accountability.

The DPDP framework provides the statutory foundation for such a system. Its ultimate success, however, will depend upon how courts, regulators, businesses and public institutions interpret and implement it.

The constitutional promise of privacy will be fulfilled not when citizens become better at clicking “I agree”, but when the legal system ensures that their personal information cannot be used against their autonomy, dignity and liberty without lawful and proportionate justification.

India's next chapter in privacy law should therefore not be about **who has consented**.

It should be about **who has power over personal information—and whether that power can be justified**.

REFERENCES

1. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1, Supreme Court of India. The judgment recognises privacy as a constitutionally protected right and identifies informational privacy as a dimension of the right.
2. The Digital Personal Data Protection Act, 2023, Act No. 22 of 2023, India Code.
3. Digital Personal Data Protection Rules, 2025, Ministry of Electronics and Information Technology, notified 13 November 2025.
4. DPDP Rules, 2025, provisions concerning notice by Data Fiduciaries and communication of information to Data Principals.
5. DPDP Rules, 2025, provisions concerning reasonable security safeguards and organisational and technical measures.
6. DPDP Rules, 2025, provisions concerning exercise of Data Principal rights and grievance redressal.

7. Government of India notification establishing the Data Protection Board of India, 13 November 2025.
8. DPDP Rules, 2025, provisions concerning verifiable consent and processing of children's personal data.
9. Digital Personal Data Protection Act, 2023, Section 7, concerning certain legitimate uses by the State and its instrumentalities.
10. DPDP Rules, 2025, Schedule II, concerning standards for processing personal data by the State and its instrumentalities.
11. Digital Personal Data Protection Act, 2023, Section 17, concerning exemptions.