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

Pratibha Jha, The Institute of Company Secretaries of India (ICSI)

ABSTRACT

The recognition of privacy as a fundamental right by the Supreme Court of India in *Justice K.S. Puttaswamy (Retd.) v. Union of India* marked a constitutional transformation in the understanding of individual autonomy, dignity and informational privacy. The Digital Personal Data Protection Act, 2023 (DPDP Act) subsequently sought to establish a statutory framework governing the processing of digital personal data. The notification of the Digital Personal Data Protection Rules, 2025 (DPDP Rules) represents the next stage in this regulatory development. This article examines whether India's emerging data-protection framework adequately transforms the constitutional promise of informational privacy into meaningful individual control over personal data. It particularly analyses consent, the obligations of Data Fiduciaries, rights of Data Principals, governmental processing, security safeguards and the institutional role of the Data Protection Board. It argues that consent, while important, cannot by itself constitute an adequate privacy safeguard in an environment characterised by information asymmetry, technological complexity and unequal bargaining power. The article therefore proposes a shift from a predominantly consent-oriented approach towards an accountability-based model grounded in data minimisation, purpose limitation, transparency, privacy-by-design and effective remedies. The phased commencement of the DPDP framework also creates an opportunity to strengthen institutional safeguards before substantive provisions become operational.

Keywords: Informational Privacy; Digital Personal Data Protection Act; Data Principal; Data Fiduciary; Consent; Article 21; Data Protection; Digital Rights.

I. INTRODUCTION

Personal data has become one of the most significant resources of the contemporary digital economy. Every online transaction, search query, social-media interaction, digital payment and location-based service can generate information about an identifiable individual. Such information can improve public services, facilitate innovation and enable businesses to provide personalised products. At the same time, extensive data collection creates risks of surveillance, profiling, discrimination, manipulation and loss of individual autonomy.

The constitutional dimension of this problem became clear with the Supreme Court's landmark judgment in *Justice K.S. Puttaswamy (Retd.) v. Union of India*. A nine-judge Constitution Bench unanimously recognised privacy as a constitutionally protected fundamental right, rooted in Article 21 and connected with dignity, liberty and autonomy.[1] The judgment transformed privacy from a contested constitutional concept into an express constitutional guarantee.

Informational privacy is particularly important in the digital age. An individual may disclose apparently insignificant pieces of information across different platforms, while the aggregation and analysis of those pieces may reveal intimate characteristics, preferences, behaviour and vulnerabilities. The constitutional concern therefore extends beyond the initial collection of information to its subsequent processing, combination and use.

The Digital Personal Data Protection Act, 2023 represents India's legislative response to this challenge. The Act seeks to regulate the processing of digital personal data while recognising both the right of individuals to protect their personal data and the need to process such data for lawful purposes.[2] The Digital Personal Data Protection Rules, 2025 subsequently supplied detailed mechanisms for implementing the statutory framework.[3]

The central issue, however, is not simply whether India now possesses a data-protection statute. The more fundamental question is whether the statutory framework can translate the constitutional right to privacy into meaningful informational control. This article argues that although the DPDP framework constitutes an important regulatory development, its success cannot depend primarily upon formal consent. Meaningful privacy protection requires a broader accountability architecture in which organisations bear substantial responsibility for limiting unnecessary collection, protecting information and ensuring effective remedies.

II. CONSTITUTIONAL FOUNDATIONS OF INFORMATIONAL PRIVACY

Before the development of a dedicated data-protection statute, Indian privacy law evolved substantially through constitutional adjudication.

In *Puttaswamy*, the Supreme Court rejected the proposition that privacy was not protected by the Constitution. The Court located privacy within the guarantees of liberty, dignity and personal autonomy contained in Part III.[4] Privacy was understood not merely as freedom from physical intrusion but as a broader constitutional interest protecting decisional autonomy and the individual's ability to control aspects of personal life.

The importance of this constitutional recognition extends beyond the relationship between citizens and the State. In a society increasingly dependent upon private digital platforms, corporations possess significant capacity to collect and process personal information. Consequently, the protection of informational privacy cannot be reduced to protection against governmental surveillance alone.

The Supreme Court's Aadhaar judgment further examined the constitutional implications of large-scale collection and aggregation of personal information and considered privacy alongside the requirements of legality and proportionality.[5] The constitutional framework therefore establishes an important principle: an interference with privacy must not be assessed merely by asking whether information was technically available or voluntarily disclosed. The purpose, extent, necessity and consequences of processing remain relevant.

III. THE DPDP ACT: FROM CONSTITUTIONAL RIGHT TO STATUTORY RIGHT

The DPDP Act introduces a statutory vocabulary that distinguishes between the individual whose personal data is processed and the entity determining the purpose and means of processing.

The individual is designated as the Data Principal, while the organisation determining the purpose and means of processing is designated as the Data Fiduciary.[6] This terminology is significant because it conceptualises the relationship as one involving responsibility rather than unrestricted ownership of personal information.

Section 4 establishes that personal data may be processed only in accordance with the Act

and for a lawful purpose, subject to the statutory grounds for processing.[7] Consent is one such ground, while the Act also recognises specified legitimate uses. Section 5 establishes a notice-based framework requiring the Data Fiduciary to provide information relating to the personal data and the purpose for which it is proposed to be processed.[8]

On paper, these provisions strengthen individual autonomy. In practice, however, their effectiveness depends upon whether individuals can understand and meaningfully exercise their choices.

IV. THE ILLUSION OF INFORMED CONSENT

Consent occupies a central position in privacy law. The underlying assumption is straightforward: an individual who understands how personal data will be used should be able to decide whether to permit such processing.

The difficulty is that digital consent frequently does not resemble meaningful decision-making. A user may be presented with lengthy privacy policies containing technical terminology and multiple cross-references. Most users do not possess the time, expertise or bargaining power to negotiate these terms. In many cases, refusing consent may effectively prevent access to a digital service.

This creates an important distinction between formal consent and meaningful consent. Formal consent asks whether the individual clicked an acceptance button or otherwise expressed agreement. Meaningful consent asks whether the individual understood what information was being collected, whether the purpose was clear, whether consent was genuinely voluntary, whether it could later be withdrawn and whether a realistic alternative existed.

The DPDP Rules, 2025 seek to improve this position by requiring clearer notices and mechanisms through which Data Principals can exercise rights and withdraw consent.[9] Nevertheless, implementation must ensure that notice does not become merely another lengthy compliance document.

The fundamental problem is structural. A large technology company can possess extensive legal, technical and financial resources, while an ordinary individual may possess little information about what happens to personal data after it is submitted. A privacy regime that

transfers the entire burden of protection onto the individual therefore risks reproducing the very information asymmetry it seeks to address.

V. FROM CONSENT TO ACCOUNTABILITY

A more effective approach requires a shift from an exclusively consent-oriented model to an accountability-based model.

The Data Fiduciary is generally better positioned than the Data Principal to understand the data lifecycle. It knows what information is collected, where it is stored, which processors receive it, how long it is retained and how it is analysed. Accordingly, responsibility should follow capacity.

The principle can be expressed simply: the greater an organisation's capacity to collect and process personal data, the greater its responsibility to prevent unnecessary or harmful processing.

This approach is particularly important in artificial intelligence systems. Modern algorithms can infer information that an individual never expressly disclosed. Seemingly ordinary behavioural data may be used to generate predictions about preferences, financial circumstances, health-related characteristics or other sensitive aspects of an individual's life.

Consequently, privacy protection cannot focus exclusively on the moment of collection. It must also consider subsequent processing, data aggregation, automated inference, profiling, sharing with processors, retention periods and consequences for the individual.

The DPDP Act's obligations upon Data Fiduciaries provide a foundation for this accountability model.[10] The effectiveness of those obligations, however, will ultimately depend upon enforcement and institutional practice.

VI. THE DIGITAL PERSONAL DATA PROTECTION RULES, 2025: AN OPPORTUNITY FOR STRONGER IMPLEMENTATION

The notification of the DPDP Rules in November 2025 represents an important stage in India's data-protection journey.[11] However, the implementation framework is deliberately phased.

The commencement notification provides that the institutional provisions concerning the Data Protection Board came into force upon publication, while several other provisions—including the core obligations contained in Sections 3 to 5, Sections 7 to 17 and related provisions—are scheduled to commence eighteen months after publication.[12]

This phased structure creates both a challenge and an opportunity. The challenge is that statutory rights and obligations will not operate simultaneously with the establishment of the institutional framework. The opportunity is that the intervening period can be used to strengthen institutional capacity, educate Data Principals, develop compliance systems and clarify regulatory procedures.

The Rules contain mechanisms concerning consent managers, security safeguards, breach notifications, retention, rights of Data Principals, significant Data Fiduciaries and cross-border transfers.[13] These provisions indicate an attempt to move beyond abstract recognition of privacy towards practical governance.

Reasonable security safeguards are intended to prevent personal-data breaches through organisational and technical measures.[14] The framework also provides mechanisms through which Data Principals can exercise statutory rights. The success of these provisions will depend on whether they are implemented as genuine rights or reduced to procedural checkboxes.

VII. DATA MINIMISATION AND PURPOSE LIMITATION

One of the weaknesses of a consent-centred model is that it may allow organisations to collect extensive quantities of information so long as the individual technically agrees. A stronger privacy framework must therefore incorporate data minimisation.

Data minimisation requires organisations to collect only information reasonably necessary for the stated purpose. It recognises that every additional piece of information collected creates another potential point of misuse, breach or unauthorised access.

Similarly, purpose limitation requires data to remain connected to the legitimate purpose for which it was collected. These principles are particularly significant in an environment where businesses frequently seek to transform personal information into commercial insights.

Suppose a consumer provides a mobile number solely for delivery of an online purchase.

The fact that the number has been voluntarily provided does not necessarily mean that the consumer expects it to be used for unrelated marketing, profiling or data-sharing purposes. The legal framework must therefore distinguish between the fact of disclosure and the reasonable expectations surrounding that disclosure.

VIII. GOVERNMENT ACCESS AND CONSTITUTIONAL SAFEGUARDS

Data protection also raises difficult questions concerning governmental access to personal information. The State may legitimately require information for purposes including law enforcement, public administration, taxation and delivery of welfare benefits. Privacy cannot be understood as an absolute prohibition on governmental processing.

However, governmental access to personal data must remain subject to constitutional safeguards. The Supreme Court's privacy jurisprudence emphasises that privacy is not an absolute right, but an intrusion upon it must satisfy constitutional requirements.[15] The principle of proportionality is therefore important in assessing restrictions upon privacy.

The concern becomes particularly acute where large databases are combined or where information collected for one purpose is subsequently used for another. The legal system should consequently insist upon clear statutory authority, legitimate objectives, procedural safeguards and proportionality wherever State action significantly interferes with informational privacy.

A data-protection framework should not create a false dichotomy between privacy and governance. The objective should instead be to enable legitimate governmental functions while preventing unnecessary and disproportionate intrusion.

IX. THE ROLE OF THE DATA PROTECTION BOARD

No rights-based regulatory framework can function effectively without an institution capable of enforcing those rights.

The DPDP Act establishes the Data Protection Board of India and provides for its powers and functions.[16] The commencement notification has brought several institutional provisions into operation ahead of the substantive obligations.[17]

The Board's effectiveness will depend upon accessibility, expertise, procedural fairness and public confidence. For ordinary Data Principals, the regulatory system should not become so complicated that exercising a statutory right requires extensive legal assistance.

The principle of access to justice must therefore inform data-protection enforcement. A person whose data has been misused should be able to understand where to complain, how to submit a complaint, what evidence is required, how the complaint will be investigated and what remedy may be available.

X. PRIVACY BY DESIGN: THE NEXT STEP

India's data-protection framework should increasingly adopt a privacy-by-design approach. Privacy should not be added after a digital product has already been developed. It should be integrated into the architecture of the product from the beginning.

Such measures can include collecting fewer categories of personal data, limiting employee access, encrypting sensitive information, establishing automatic deletion mechanisms, maintaining auditable records, restricting secondary use and ensuring simple mechanisms for withdrawal of consent.

These measures reduce dependence on individual vigilance. An ordinary user should not have to become a data-security expert to enjoy the constitutional protection of privacy.

XI. RECOMMENDATIONS

Make Consent Understandable. Consent notices should use plain and accessible language. Legal compliance should not be measured by the volume of information provided but by whether the information enables genuine understanding.

Make Withdrawal as Easy as Consent. If consent can be provided through one simple digital action, withdrawal should not require navigating multiple screens or contacting customer support.

Strengthen Data Minimisation. Organisations should justify the collection of categories of personal data that are not demonstrably necessary for the stated purpose.

Introduce Stronger Scrutiny for High-Risk Processing. Artificial intelligence, biometric

processing, large-scale profiling and other high-risk forms of processing should receive enhanced regulatory attention.

Strengthen Institutional Independence. The enforcement institution must possess sufficient expertise, resources and procedural independence to protect Data Principals effectively.

Improve Public Awareness. Privacy rights have limited practical value if individuals do not know that those rights exist. Public awareness programmes should therefore accompany implementation.

Adopt a Rights-Based Interpretation. The DPDP Act should be interpreted consistently with the constitutional values of dignity, autonomy and privacy established by the Supreme Court.

XII. CONCLUSION

India's data-protection journey represents a significant constitutional and legislative transition. The Supreme Court's recognition of privacy in *Puttaswamy* established that privacy is inseparable from dignity and individual autonomy. The DPDP Act subsequently transformed this constitutional principle into a statutory regulatory framework, while the DPDP Rules, 2025 seek to operationalise that framework.

Yet the existence of legislation does not automatically produce meaningful privacy. The central challenge lies in the gap between formal consent and genuine control.

In the digital economy, individuals routinely encounter situations where they possess limited understanding of data practices and little practical ability to negotiate the conditions upon which services are provided. Treating consent as the complete answer risks placing an unrealistic burden upon individuals.

India should therefore move towards a broader accountability-based approach. Data Fiduciaries must assume responsibility for limiting unnecessary collection, protecting information, restricting secondary uses and providing accessible remedies. The State must ensure that governmental access to personal information remains subject to constitutional principles. Regulatory institutions must remain accessible and effective.

The phased implementation of the DPDP framework provides India with an important opportunity. Before substantive provisions become fully operational, policymakers and regulators can strengthen institutional safeguards and develop a culture of responsible data governance.

Ultimately, the success of India's privacy regime should not be measured by the number of consent forms accepted, privacy policies published or compliance mechanisms created. The real measure is whether an ordinary individual can reasonably understand what happens to their personal data, exercise meaningful control over it, and obtain an effective remedy when that control is violated.

The constitutional promise of privacy therefore requires a movement from consent to control, and from individual responsibility to institutional accountability.

ENDNOTES:

1. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
2. Digital Personal Data Protection Act, 2023, No. 22 of 2023, pmbl.
3. Digital Personal Data Protection Rules, 2025, G.S.R. 846(E) (Nov. 13, 2025).
4. *Puttaswamy*, (2017) 10 SCC 1.
5. *K.S. Puttaswamy (Retd.) v. Union of India*, (2019) 1 SCC 1.
6. Digital Personal Data Protection Act, 2023, § 2.
7. Id. § 4.
8. Id. § 5.
9. Digital Personal Data Protection Rules, 2025, r. 3.
10. Digital Personal Data Protection Act, 2023, §§ 8–10.
11. Digital Personal Data Protection Rules, 2025, G.S.R. 846(E) (Nov. 13, 2025).
12. Notification, G.S.R. 843(E) (Nov. 13, 2025).
13. Digital Personal Data Protection Rules, 2025, rr. 3–23.
14. Id. r. 6.
15. *Puttaswamy*, (2017) 10 SCC 1.
16. Digital Personal Data Protection Act, 2023, §§ 18–27.
17. Notification, G.S.R. 843(E) (Nov. 13, 2025).

BIBLIOGRAPHY

Primary Sources: Constitution of India, 1950; Digital Personal Data Protection Act, 2023; Digital Personal Data Protection Rules, 2025; *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1; *K.S. Puttaswamy (Retd.) v. Union of India*, (2019) 1 SCC 1.

Government Materials: Ministry of Electronics and Information Technology, Government of India, Digital Personal Data Protection Rules, 2025; Ministry of Electronics and Information Technology, Government of India, Enforcement Timeline for the DPDP Act.

Submission Reference: Indian Journal of Law and Legal Research, Call for Papers and Submission Guidelines.