# Informational Autonomy and Statutory Limits: Re-examining India's Data Governance Architecture

*ROHIT SAINI, DR MUNESH KUMAR*

**Abstract**: *The ubiquity of network architecture has drastically reconfigured how personal metrics are aggregated, processed, stored, and monetized across modern markets. Modern tech networks, financial mechanisms, state entities, and automated analytical models depend continuously on individual data streams to deliver operational capabilities and enforce systemic governance. These structural shifts have amplified the constitutional importance of informational self-determination, especially following the landmark ruling of the Supreme Court of India in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017). The introduction of the Digital Personal Data Protection Act, 2023 (DPDP Act) serves as the state's primary legislative response to build a comprehensive data governance structure. Nevertheless, codifying statutory rules does not automatically validate that basic fundamental rights are fully preserved.*

*This study evaluates whether the DPDP Act effectively translates the constitutional directives set*

*forth in Puttaswamy into robust, practical protections. Utilizing a doctrinal and comparative framework, the paper investigates the statutory design, consent mechanics, duties of data fiduciaries, rights accorded to data principals, regulatory oversight bodies, and statutory broad exemptions. It further measures the tension between individual sovereignty, state authority, and commercial data exploitation against the doctrine of constitutional proportionality. The findings highlight significant gaps between statutory intent and actual privacy preservation, specifically caused by expansive executive carve-outs, institutional dependency of the regulator, and structural flaws in reliance on user consent. Ultimately, the paper advocates for a structural accountability paradigm grounded in strict legality, institutional independence, and enforceable remedies.*

**Keywords:** Informational Privacy; Digital Personal Data Protection Act, 2023; Puttaswamy Doctrine; Data Governance; Constitutional Proportionality; Data Fiduciary; Fundamental Rights.

Rohit Saini (singodiyarohit70@gmail.com) Senior Research Scholar, Pandit Deendayal Upadhyay Shekhawati University Sikar, (Raj.)332001
Dr Munesh Kumar (kumarmunesh09@gmail.com) Principal Govt Law College Churu (Raj.)

**Introduction**

The contemporary expansion of pervasive computing has fundamentally reordered the dynamic connecting individuals, administrative bodies, and corporate entities. Personal information has evolved into a primary engine driving global markets, public delivery systems, technical innovation, and civic interaction. Daily activities—including electronic banking, web-based commerce, social networking, digital health monitoring, and remote education—generate dense digital footprints. These footprints reveal sensitive details concerning personal choices, economic statuses, behavioral patterns, associations, real-time locations, and core aspects of personal identity. The expanding systemic capability to capture, cross-reference, and evaluate such information creates unparalleled forms of institutional power.

This structural transformation challenges traditional definitions that restrict privacy to mere physical boundaries or non-disclosure of intimate facts. Within digital ecosystems, privacy fundamentally concerns the structural conditions under which individual metrics are collected, evaluated, held, inferred, and deployed to influence life choices. A breach of individual autonomy occurs even without overt public exposure. Continuous tracking, opaque algorithmic profiling, indefinite storage, and unauthorized secondary processing pose direct risks to individual agency, non-discrimination, human dignity, and freedom of expression.

In India, the jurisprudential underpinning for confronting these technological vulnerabilities was consolidated by the unanimous nine-judge Bench decision in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017). The Supreme Court affirmed that privacy is a core constitutional guarantee anchored primarily within Article 21 and reinforced by Part III liberties. Crucially, the bench established informational privacy as a crucial dimension of personal autonomy, recognizing that threats stem from both state apparatuses and non-state commercial entities. The ruling explicitly mandated the creation of a balanced statutory framework capable of reconciling private liberty with valid public objectives.

The enactment of the Digital Personal Data Protection Act, 2023 represents the formal legislative realization of this directive. The statutory architecture establishes standard criteria for handling digitized data, specifying the legal responsibilities of data fiduciaries while codifying formal entitlements for data principals. The statute aims to provide legal certainty for commercial data operations while supporting India's expanding digital economy.

However, statutory codification is not inherently equivalent to genuine privacy enforcement. The crucial analytical issue is whether the regulatory mechanisms actively restrain public and corporate bodies from abusing informational dominance. A statute may grant formal access or deletion rights while simultaneously embedding broad carve-outs and procedural barriers that render those rights ineffective. Thus, evaluating a data protection statute requires measuring its substantive checks, regulatory autonomy, procedural clarity, and remedial efficacy.

This paper contends that the DPDP Act must be evaluated strictly against the constitutional test set by Puttaswamy, rather than administrative expediency or market preferences. Realizing

informational privacy requires a legal regime where all data handling remains legally justified, necessary, proportionate, and subject to effective oversight.

### 1.1 Problem Statement

The key problem lies in the disconnect between the constitutional protection of informational privacy and the statutory mechanics created under the DPDP Act. Although the statute grants specific rights, critical concerns remain regarding broad government exemptions, the practical friction of user consent, the functional autonomy of the Data Protection Board, and the availability of accessible legal remedies. These vulnerabilities are especially severe when data is processed by state authorities or powerful digital monopolies.

### 1.2 Significance of the Inquiry

This analysis holds value across three key dimensions: First, it examines statutory data governance through the prism of constitutional rights and personal liberty. Second, it assesses how systemic data practices alter power relations between citizens, government bodies, and commercial firms. Third, it offers a constitutional accountability model designed to inform statutory interpretation, administrative rules, and judicial evaluation.

### 1.3 Literature Gap

Current academic works have evaluated the statute's compliance models, consent provisions, and comparative positioning alongside foreign statutes like the GDPR. For instance, Naithani (2025) presents a doctrinal review highlighting uncertainties in enforcing data principal protections. Furthermore, scholarly critique by Kolanu et al. (2025) points out institutional risks introduced by the 2025 subordinate rules, particularly regarding executive exemptions. This study builds on those insights by putting constitutional proportionality and systemic oversight at the center of the inquiry, assessing whether the statutory framework sufficiently limits informational dominance.

## Literature Review

Privacy theory has evolved from early legal protections of physical spaces toward controlling institutional information processing. The foundational formulation by Warren and Brandeis (1890) defined privacy as the "right to be let alone." While conceived in response to early print photography, its core standard remains vital: technical capacity must not justify unconstrained intrusion into personal life.

Subsequent scholarship moved beyond mere secrecy and physical intrusion. Solove (2006) conceptualized privacy as a complex web of distinct systemic harms occurring across data collection, processing, dissemination, and intrusion. This taxonomy is vital for digital environments where risk emerges from data pooling and secondary analysis rather than isolated exposures.

Additionally, Nissenbaum (2010) introduced the concept of contextual integrity, arguing that privacy violations occur when data transfers violate contextual norms. Information shared within a clinical environment should not be repurposed for commercial scoring without

justification. This demonstrates why consent alone is insufficient: initial consent in one context does not validate subsequent processing across unrelated domains.

Indian privacy jurisprudence underwent a major shift following Puttaswamy (2017), which established privacy as fundamental to human dignity and individual freedom, while subjecting state interference to legality, legitimate state aim, and strict proportionality.

Recent studies focusing on the DPDP Act concentrate on statutory mechanics and compliance burdens. Naithani (2025) compares statutory features with global models, while Kolanu, Lakra, and Shrivastava (2025) analyze the DPDP Rules, 2025, highlighting risks concerning administrative exemptions and regulatory independence. Furthermore, Tandon and Gupta (2025) examine data protections against automated intelligence systems, emphasizing automated profiling risks.

**Research Questions**

- To what degree does the DPDP Act, 2023 satisfy the constitutional metrics established in the Puttaswamy ruling?
- Does the statutory framework achieve a balanced alignment between user sovereignty, state power, and corporate data processing?
- Are notice-and-consent mechanics and statutory rights robust enough to shield citizens from non-transparent profiling?
- Do executive exemptions and regulatory enforcement structures meet constitutional requirements of necessity and proportionality?
- What structural, legal, and interpretative adjustments are required to strengthen digital privacy protections in India?

**Research Objectives**

- To analyze the constitutional parameters governing digital privacy in India.
- To dissect the legal architecture and statutory mechanisms of the DPDP Act, 2023.
- To evaluate the operational strength of consent and statutory rights granted to data principals.
- To critique state exemptions and the independence of enforcement bodies.
- To compare the Indian framework against European Union data governance standards.
- To formulate an actionable constitutional accountability model for digital data processing.

**Methodology**

This paper uses a doctrinal legal research methodology combined with constitutional analysis and comparative evaluation. Primary sources analyzed include the Constitution of India, the DPDP Act, 2023, the DPDP Rules, 2025, and relevant Supreme Court jurisprudence. The core constitutional standard relies on Puttaswamy (2017), alongside earlier precedents such as Maneka Gandhi v. Union of India (1978), PUCL v. Union of India (1997), and Modern Dental

College v. State of M.P. (2016). Secondary sources include peer-reviewed journals, legal treatises, and comparative references to the EU General Data Protection Regulation (GDPR).

## Constitutional Foundations of Privacy In India

### 6.1 Fundamental Guarantee and Jurisprudence

Indian privacy jurisprudence developed progressively through case law. Early rulings like Kharak Singh (1963) and Gobind (1975) recognized partial protections against physical surveillance under personal liberty. However, the definitive shift arrived with Puttaswamy (2017), which established privacy as an inherent fundamental right protected under Article 21 and Part III freedoms. The Court affirmed that privacy protects individual dignity, agency, and informational autonomy against both state and private intrusion.

### 6.2 The Threefold Proportionality Test

Under Puttaswamy, any state intrusion into individual privacy must pass three strict constitutional hurdles: (1) Legality (backed by clear statutory authority); (2) Legitimate State Purpose (serving a valid constitutional goal); and (3) Proportionality (ensuring the least intrusive means are used). The court also highlighted the state's positive obligation to protect citizens from private party infringements. Mere statutory authorization does not validate intrusive processing; the nature, purpose, necessity, and scope of data collection must meet constitutional scrutiny.

### 6.3 Informational Privacy and Democratic Liberty

Informational privacy is directly tied to core democratic rights including free speech, association, and personal conscience. Unchecked monitoring creates a chilling effect that leads individuals to alter their behavior and self-censor. Protecting informational privacy is therefore essential for vibrant democratic participation, requiring robust shields against excessive data capture, discriminatory profiling, and unauthorized secondary processing.

## The Digital Personal Data Protection Act, 2023: Structural Analysis

### 7.1 Scope and Application

The DPDP Act governs the processing of digital personal data within India, covering both native digital records and physical data subsequently digitized. Extraterritorial jurisdiction applies when overseas operations involve offering goods or services to individuals in India. While supporting legitimate commercial and administrative data processing, these activities must strictly respect constitutional privacy limits.

### 7.2 Consent Architecture and Operational Reality

The statute relies heavily on user consent, requiring it to be free, specific, informed, unconditional, and explicit. Data Fiduciaries must issue clear notices detailing collected parameters and specific processing goals. However, in digital markets, users face long notices, complex terms, and forced choices where access to essential services requires agreeing to broad data collection. In such asymmetrical environments, consent can become illusory, failing to

account for automated inferences or future secondary uses. Consequently, user consent must not replace strict statutory limits on data processing.

### 7.3 Statutory Rights of Data Principals

The statute accords Data Principals rights to access summary data, request correction or deletion, utilize grievance channels, and designate representatives during incapacity. While these rights acknowledge user agency, their practical value depends on accessibility. Complex administrative hurdles and technical opacity often prevent users from exercising these rights effectively without institutional support and strict regulatory enforcement.

### 7.4 Duties of Data Fiduciaries

The Act mandates data accuracy, security measures, storage limits, and breach notifications, with additional requirements for Significant Data Fiduciaries—such as data protection officers and mandatory privacy audits. While this shifts responsibility onto data controllers, practical protection depends on rigorous oversight rather than passive procedural compliance.

### 7.5 Regulatory Oversight: The Data Protection Board

The statute establishes the Data Protection Board of India (DPBI) to manage compliance, investigate breaches, and impose civil penalties (formally notified on November 13, 2025). However, true regulatory effectiveness requires functional independence, technical expertise, and procedural transparency. If executive control influences appointments or budgets, public confidence and enforcement against state entities will be compromised.

### 7.6 Executive Exemptions and State Power

Section 17 contains broad state exemptions for national security, public order, and crime prevention. While security exceptions exist in democratic states, statutory carve-outs must remain strictly proportionate. Broad exemptions risk creating unmonitored surveillance channels that bypass basic constitutional protections.

### 7.7 Phased Implementation Schedule

Pursuant to Gazette Notification G.S.R. 843(E) (November 13, 2025), key provisions follow a staggered timeline: basic organizational elements took immediate effect, secondary rules activate after 12 months, and core substantive rights and duties (Sections 3–17) take effect 18 months post-publication (May 13, 2027). Similarly, the DPDP Rules, 2025 (G.S.R. 846(E)) follow a phased rollout. As of late 2026, substantive operational enforcement remains prospective.

## Critical Analysis of The Dpdp Act

### 8.1 Fallacy of Consent as Primary Defense

Relying on consent as the primary privacy defense fails to address institutional power imbalances. Users routinely accept unread privacy policies out of economic necessity. Furthermore, initial consent cannot anticipate future algorithmic profiling or data aggregation. Consent must therefore be supplemented by non-negotiable statutory duties of data minimization, purpose limitation, and algorithmic transparency.

### 8.2 Constitutional Vulnerability of State Carve-Outs

Broad state exemptions under Section 17 challenge the proportionality principles of Puttaswamy. Executive exemptions must be narrowly construed and bound by independent judicial oversight, strict retention limits, and mandatory audits. Statutory authorization does not override fundamental constitutional rights.

### 8.3 Institutional Autonomy of the Regulator

The DPBI's credibility depends on its operational autonomy from political and corporate influence. Robust tenure protections, independent funding, transparent procedures, and clear judicial review pathways are essential for effective enforcement against powerful actors.

### 8.4 Automated Profiling and AI Integration

Advanced machine learning models process personal data to derive sensitive behavioral insights for automated credit, employment, and risk decisions. The DPDP Act must be interpreted to require algorithmic transparency, human intervention options, and clear channels to dispute automated decisions.

## Comparative perspective: dpdp act vs. Eu gdpr

Comparing the Indian framework with the European Union's General Data Protection Regulation (GDPR) highlights key differences in regulatory architecture and enforcement philosophy.

**Table 1:** Architectural Comparison Between Indian DPDP Act and EU GDPR

| Dimension | DPDP Act, 2023 (India) | GDPR (European Union) |
|---|---|---|
| **Regulatory Body** | Data Protection Board of India (Adjudicative board) | Independent Supervisory Authorities per Member State |
| **Legal Bases** | Consent-centric model supplemented by statutory legitimate uses | Six equal legal grounds (Art. 6), including legitimate interests |
| **Principal Rights** | Access, correction, erasure, and grievance redressal | Extensive rights: portability, restriction, and automated profiling objection |
| **State Carve-Outs** | Broad statutory executive exemptions under Section 17 | Strict, narrow derogations bounded by EU judicial review |
| **Governance Mandates** | Audits required primarily for Significant Data Fiduciaries | Mandatory Data Protection Impact Assessments (DPIA) & structural logs |

Note: Comparative analysis synthesized from DPDP Act 2023 text and EURegulation 2016/679.

**Discussion & Proposed Framework**

The analysis demonstrates that statutory rights alone do not guarantee privacy without strong institutional checks. To address these vulnerabilities, this paper proposes a Three-Tiered Constitutional Accountability Model for data governance.

**Table 2:** Proposed Three-Tiered Constitutional Accountability Architecture

| Level | Core Pillar | Operational Requirements |
|---|---|---|
| **Tier I** | Substantive Legality & Proportionality | Strict purpose limitation, data minimization, narrow exemptions, mandatory necessity testing. |
| **Tier II** | Institutional Oversight | Independent regulatory appointments, administrative autonomy, mandatory privacy audits, public reporting. |
| **Tier III** | Remedial Efficacy | Accessible grievance channels, judicial review access, enforceable deletion, prompt statutory remedies. |

**Key Findings**

1. Statutory vs. Constitutional Sufficiency: Enacting statutory rules does not automatically satisfy the constitutional proportionality standards set in Puttaswamy.
2. Inadequacy of Consent: Notice-and-consent mechanics fail to protect users in structurally unequal digital environments.
3. Need for Narrow Carve-outs: Executive exemptions must remain strictly subject to judicial review and proportionality testing.
4. Regulatory Independence: The Data Protection Board must operate with complete functional and political autonomy to enforce rules effectively.
5. Enforceable Remedies: Statutory rights remain theoretical without accessible, low-friction legal remedies for affected users.
6. Emerging AI Threats: Automated profiling requires proactive regulation beyond basic data collection rules.
7. Constitutional Primacy: Fundamental privacy guarantees under Article 21 must override administrative convenience.

**Conclusion**

Informational privacy is an essential condition for personal dignity, individual autonomy, and democratic freedom. While the DPDP Act, 2023 provides a statutory framework for digital data regulation in India, its ultimate success depends on aligning its operational rules with the constitutional standards of Puttaswamy. Preserving digital privacy requires moving beyond consent mechanics toward independent institutional oversight, narrow state exemptions, robust algorithmic transparency, and accessible legal remedies.

**References**

Kolanu, M., Lakra, R., & Shrivastava, A. (2025). Data, control, and power: Decoding India's Digital Personal Data Protection Act, 2023. Global Privacy Law Review, 6(4), 136-155. https://doi.org/10.54648/gplr2026002

Naithani, P. (2025). Analysis of India's Digital Personal Data Protection Act, 2023. International Journal of Law and Management, 67(5), 543-553. https://doi.org/10.1108/IJLMA-05-2024-0174

Nissenbaum, H. (2010). Privacy in context: Technology, policy, and the integrity ofsocial life. Stanford University Press.

Solove, D. J. (2006). A taxonomy of privacy. University ofPennsylvania Law Review, 154(3), 477-564.

Tandon, U., & Gupta, N. K. (2025). Informational privacy in the age of artificial intelligence: A critical analysis of India's DPDP Act, 2023. Legal Issues in the Digital Age, 6(2), 87-117. https://doi.org/10.17323/2713-2749.2025.2.87.117

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. Harvard Law Review, 4(5), 193-220.

Gobind v. State of Madhya Pradesh, (1975) 2 SCC 148.

Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295.

Maneka Gandhi v. Union of India, (1978) 1 SCC 248.

Modern Dental College & Research Centre v. State of Madhya Pradesh, (2016) 7 SCC 353.

People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301.