© Volume 2, Issue 11, November 2026 | JATIR
e-ISSN: 2839-5786, p-ISSN: 3139-8464

Reconciling State Authority and Informational Autonomy: A Constitutional Appraisal of India's Digital Personal Data Protection Act, 2023

Rohit Saini
Pandit Deendayal Upadhyay Shekhawati University Sikar

***Abstract*—The rapid digitization of public administration has fundamentally transformed the relationship between the State, corporate entities, and citizens. While aggregating personal datasets enhances governance efficiency and public security, it simultaneously intensifies concerns regarding informational autonomy, state surveillance, and constitutional accountability. In India, these challenges acquired significant legal weight following the Supreme Court's declaration of privacy as a fundamental right in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017). The Digital Personal Data Protection Act, 2023 (DPDP Act) represents India's baseline legislative framework to regulate personal data handling. However, its broad state exemptions under Section 17, administrative structure, and distribution of executive power raise critical questions regarding its constitutional adequacy. Addressing key literature gaps, this study evaluates the statutory framework through the constitutional principles of legality, legitimate state purpose, necessity, and proportionality. It proposes a three-tier constitutional accountability model to reconcile administrative state interests with individual dignity.**

***Index Terms*—DPDP Act 2023; Right to Privacy; Puttaswamy Framework; Constitutional Proportionality; Informational Autonomy; Executive Surveillance; Institutional Accountability.**

I. INTRODUCTION

Contemporary governance relies heavily upon the systematic collection, storage, analysis, and exchange of personal information for welfare delivery, public safety, financial regulation, and statutory enforcement. While such practices enhance operational efficiency, they expand the State's capacity to observe and influence individual behavior. Consequently, personal

information functions not merely as an administrative resource, but as a core dimension of individual liberty and constitutional autonomy.

The landmark judgment in Puttaswamy (2017) established that privacy is an intrinsic element of life and personal liberty under Article 21 of the Indian Constitution. The nine-judge Constitution Bench rejected narrow views of constitutional liberty, affirming that informational self-determination protects citizens from arbitrary state intrusion. The Court established a strict constitutional standard: any state restriction on privacy must have legal authorization, pursue a legitimate objective, and satisfy the principle of proportionality.

The enactment of the Digital Personal Data Protection Act, 2023 represents India's central legislative response to digital data processing. While the statute codifies rights for Data Principals and obligations for Data Fiduciaries, its statutory exemptions raise a crucial constitutional question: to what extent does the Act constrain state power when the government itself acts as both primary data controller and regulator?

II. CONCEPTUAL FOUNDATIONS AND LITERATURE REVIEW

The theoretical foundations of privacy jurisprudence stem from Warren and Brandeis (1890), who established privacy as a protectable interest safeguarding personal autonomy beyond physical property. Modern scholarship adapted this to technological growth: Solove (2006) developed a taxonomy demonstrating how data aggregation, processing, and disclosure compromise individual freedom. Furthermore, Nissenbaum (2010) formulated the theory of contextual integrity, emphasizing that privacy violations occur when data collected for one specific purpose is diverted to another without authorization.

In Indian jurisprudence, Puttaswamy (2017) affirmed individual control over personal data, supported by procedural frameworks in cases like Modern Dental College (2016) regarding structured proportionality tests. Recent scholarship (Jha & Lakra, 2026) highlights additional statutory concerns, including the exclusion of publicly available personal data from statutory protection, underscoring the need for rigorous constitutional scrutiny.

III. RESEARCH METHODOLOGY AND FOUR-PRONGED FRAMEWORK

This study employs a qualitative doctrinal legal methodology combined with comparative constitutional analysis. Primary materials include the Constitution of India, the DPDP Act (2023), the DPDP Rules (2025), and key Supreme Court decisions. Comparative perspectives draw from the European Union's General Data Protection Regulation (GDPR, 2016).

State data actions are systematically evaluated across four constitutional dimensions:

- Legality: Data processing must be authorized by clear, accessible, and specific statutory provisions.
- Legitimate Aim: The public objective pursued must fall strictly within constitutionally permissible state functions.

- Necessity: The measure must be strictly required, ensuring no less intrusive alternative can achieve the objective.
- Proportionality: The degree of infringement on individual rights must not be excessive relative to the public benefit.

STRUCTURAL CONSTITUTIONAL EVALUATION OF THE DPDP ACT

Puttaswamy Core Test	DPDP Act Vulnerabilities	Proposed Reform Model
Legality, Legitimate Objective, Necessity, & Proportionality.	Broad Sec. 1 7 state exemptions & executive influence over Board.	Independent supervision, narrow exceptions, & direct judicial remedies.

IV. CRITICAL ANALYSIS OF THE DPDP ACT, 2023

4.1. State Exemptions under Section 1 7

Section 17(2) authorizes the Central Government to exempt state instrumentalities from core provisions in the interest of state security, public order, and sovereignty. While these objectives are legitimate, framing exemptions broadly without statutory safeguards or independent prior review risks arbitrary execution. Statutory exemptions cannot override constitutional duties under Article 21

4.2. Independence of the Data Protection Board

The Data Protection Board of India (DPBI) is tasked with enforcing statutory compliance. However, executive control over appointments, tenure, and operational procedures creates institutional vulnerability. When state agencies themselves process data, the regulatory authority must possess structural independence to deliver impartial adjudication.

4.3. Limitations of Consent in Public Governance

Consent mechanisms are structurally asymmetric when citizens interact with public authorities. When access to essential welfare, healthcare, or civil documentation requires data submission, consent is rarely voluntary. Consequently, formal consent cannot serve as the sole legal justification for state processing; it must be backed by objective necessity and proportionality.

V. COMPARATIVE CONSTITUTIONAL PERSPECTIVE (GDPR VS. DPDP)

The European Union's GDPR (2016) provides a useful comparative baseline, embedding principles of data minimization, purpose limitation, and mandatory impact assessments. While the GDPR accommodates national security exemptions, it requires explicit legislative parameters and independent judicial supervision. India's path requires adapting these global standards into its domestic constitutional framework established in Puttaswamy.

VI. PROPOSED THREE-LEVEL CONSTITUTIONAL ACCOUNTABILITY MODEL

To align digital statecraft with fundamental rights, this research formulates a structured three-level accountability model:

Accountability Level	Core Objective	Operational Requirements
Level I: Substantive Legality	Ensure explicit statutory backing and narrow purpose specification.	Clear legislation defining specific data categories, processing scope, and explicit statutory boundaries.
Level II: Institutional Supervision	Establish independent administrative check on state processing powers.	Autonomous DPBI oversight, mandatory data protection impact assessments, and written administrative justification.
Level III: Judicial Remedies	Guarantee constitutional enforcement and citizen redress.	Direct access to statutory appellate review and constitutional writ jurisdiction under Articles 32 and 226.

VII. CONCLUSION

A constitutionally legitimate digital state is defined not by the volume of information it can extract, but by the restraints it enforces upon its own power. The DPDP Act, 2023 establishes a valuable legislative foundation, but its state exemptions and regulatory architecture must be brought into strict alignment with the constitutional standards of Puttaswamy. Protecting individual dignity and informational autonomy remains essential to constitutional democracy in the digital age.

REFERENCES

[1]. Analysis of India's Digital Personal Data Protection Act, 2023. (2024). International Journal ofLaw and Management, 66(4), 410–428. https://doi.org/10.1108/IJLMA-05-2024-0174
[2]. European Parliament and Council ofthe European Union. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation). Official Journal ofthe European Union, L 119, 1 –88.
[3]. Jha, N., & Lakra, R. (2026). Reevaluating publicly available data under the DPDPA Act 2023: A constitutional challenge.
[4]. Indian Law Review, 10(1), 31 –50. https://doi.org/10.1080/24730580.2026.2619382
[5]. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).
[6]. Modern Dental College and Research Centre v. State of Madhya Pradesh, (2016) 7 SCC 353 (India).
[7]. Nissenbaum, H. (2010). Privacy in context: Technology, policy, and the integrity ofsocial life. Stanford University Press.
[8]. Solove, D. J. (2006). A taxonomy ofprivacy. University ofPennsylvania Law Review, 154(3), 477–564.
[9]. Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. Harvard Law Review, 4(5), 193–220.