BEHIND THE VEIL: STATE POWERS AND THE DISGUISED SURVEILLANCE REGIME IN DPDPA 2023

Amit Kumar Padhy, Research Scholar at National Law University, Nagpur

ABSTRACT

The Digital Personal Data Protection Act, 2023 (DPDPA) is an important milestone in India's data governance strategy, instituting an extensive framework for the regulation of personal data processing. The Act fundamentally acknowledges conflicting priorities - individual privacy rights in relation to legitimate state functions. Section 17(2)(a) of the DPDPA authorises the Central Government to exclude State instrumentalities from fundamental compliance requirements when data processing is considered vital for maintaining national sovereignty, integrity, security, amicable international relations, or public order. This exemption, supported by supplementary delegated authorities, enables the government to circumvent obligations such as notification, consent, and specific transparency responsibilities, ostensibly to avert disruption of essential state functions. Nonetheless, these exemptions provoke significant enquiries: Do they compromise the Act's declared dedication to personal autonomy and informational self-determination? Are the powers proportionality adequately protected by substantive and procedural safeguards? The exemptions are contingent upon the restrictions outlined in the Draft Rules of the Act, which restrict the data processed to what is necessary and require appropriate security measures; however, the breadth and discretionary authority remain extensive. Moreover, the Act exempts State bodies from obligatory deletion and retention constraints, diverging from international privacy standards. This article examines whether these exclusions create a potentially imbalanced framework that favours state interests over citizen rights, and evaluates the adequacy of the integrated legal, policy, and operational safeguards. It eventually examines how India's developing data protection framework reconciles the conflicts between strong governmental authority and an efficient, rights-oriented data privacy structure, referencing international norms and constitutional principles. The analysis aims to enhance the understanding of governmental authority under DPDPA, assessing its validity, need, and accountability within India's democratic framework.

Keywords: DPDPA, State Exemption, Surveillance, Public Order, Safeguards

I. Introduction

India's move to a regulated digital economy is marked by the enactment of the Digital Personal Data Protection Act, 2023 (DPDPA)[1]. Privacy rights, regulatory compliance, and sovereign imperatives have long been in tension in the Indian framework for data governance. The DPDPA arrives after a decade of policy drafts, Supreme Court verdicts, public consultations, and mounting international pressure to implement comprehensive data governance. Notably, the Act takes explicit cognizance of the difficult balance between state power and individual autonomy, codifying both citizen protections and significant exceptions for the government under Section 17(2)(a).

The surveillance powers reinforced by DPDPA cannot be seen in isolation. India's experiences with Aadhaar, Section 69 of the Information Technology Act[2], and evolving global privacy jurisprudence inform both the text and the public debate surrounding the Act. Recent global trends toward state-centric surveillance, justified by security and public order, mark the DPDPA as part of a broader reassertion of governmental authority over digital resources. This paper examines if the Act, especially through its exemption regime, crafts a surveillance structure that undermines its promise of privacy and self-determination. Broader questions arise: What are the legal and operational safeguards in place? How does India's regime stand in comparison with mature privacy infrastructures across Europe and North America? How is the proportionality of these powers measured and controlled?

II. Historical and Legislative Context

Evolution of Data Protection in India

India's pathway to modern data protection has involved successive committee reports, failed legislative attempts, sectoral guidelines (RBI, TRAI), and pivotal judicial interventions. The Justice Srikrishna Committee's 2018 proposals identified privacy risks in unregulated data handling and recommended stringent checks on state surveillance, transparency, and redress. The Supreme Court's 2017 judgment in Justice KS Puttaswamy v Union of India[3] was decisive,

[1] The Digital Personal Data Protection Act, No. 22 of 2023, Gazette of India, Extraordinary, Pt. II, Sec. 1 (Aug. 11, 2023), https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf.
[2] Vasudev Devadasan, Conceptualising India's Safe Harbour in the Era of Platform Governance, 19 Indian J.L. & Tech. 1 (2024), https://repository.nls.ac.in/ijlt/vol19/iss1/1/.
[3] AIR 2017 SC 4161.

holding privacy as an intrinsic component of Article 21 and limiting state encroachments without due process.

Policy Debates and Public Consultations

Multiple drafts of the data protection bill faced criticism for broad state exemptions and vague procedural safeguards. Civil society actors highlighted the necessity of robust parliamentary oversight and independent audit mechanisms. International actors, including EU representatives and global tech bodies, pressed for conformity with the General Data Protection Regulation (GDPR), especially regarding notice, consent, retention, and deletion norms.

III. Structure of DPDPA

The DPDPA institutionalises a catalogue of rights (access, correction, erasure, consent), obligations (security, purpose limitation, breach notification), and sanctions for non-compliance. The Data Protection Board is set up as a quasi-judicial regulator, though its independence is debated, especially considering government appointment powers and reporting lines. The Act contains over 30 delegated rulemaking provisions, making its true contours heavily reliant on executive notifications.

Section 17(2)(a) - Text, Scope, and Rationale

Section 17(2)(a) stands as a broad authorisation for the Central Government to exempt "any instrumentality of the State".[4] The text allows bypassing nearly every significant compliance requirement if "necessary or expedient" for sovereignty, integrity, security, friendly relations, or public order. This goes beyond targeted agency lists (as in the RTI Act), potentially enabling vast categories of ministries, regulatory bodies, public banks, and state enterprises to fall within its scope upon notification.

Rationale for Exemptions

State agencies argue an operational necessity for rapid information processing during investigations, counterterrorism, international diplomacy, and disaster management. The government justifies broad exemptions by referencing persistent threats, cyber-attacks,

[4] Section 17 of DPDPA, 2023.

misinformation, terrorist financing, where delays could be detrimental. These rationales echo global security discourses, but critics highlight the risk: the lack of clear criteria, transparency, and third-party/independent review.

Potential for Expansive Discretion

Unlike the GDPR's limited and specific derogations under Article 23[5], Section 17(2)(a) allows expansive and ongoing notification powers with minimal statutory restraint. The Indian context is made even more controversial by recent episodes where surveillance measures (telephone interception, mass facial recognition) have been deployed without judicial warrants or post-facto reporting.

IV. Section 17 in Practice: Case Studies and Comparative Analytical Deep Dive

State Agency Coverage

The range of "state instrumentalities" covered by Section 17(2)(a) is potentially enormous: law enforcement agencies, intelligence agencies, public health authorities, regulatory bodies, and even financial institutions. Controversial exemptions granted to agencies such as the Unique Identification Authority of India (UIDAI), Central Bureau of Investigation, and SEBI could mean longitudinal data collection, biometrics, financial records, communication logs, beyond the reach of regular privacy controls.[6]

Judicial Scrutiny and Executive Accountability

Historically, judicial scrutiny of surveillance in India is ex-post and limited. Even under previous statutes (e.g., Telegraph Act, IT Act), warrants and oversight mechanisms were rarely implemented. Parliamentary committees recommended ongoing audits, impact assessments, and annual reporting to mitigate executive overreach. However, DPDPA delegates much of its substantive detail to future rules, delaying meaningful checks.

V. Draft Rules and Security Safeguards: A Critical Perspective

Draft Rules accompanying DPDPA prescribe that data processed under exemptions must be

[5] Article 23 of General Data Protection Regulation, 2016.
[6] Pameela George, India's Surveillance Landscape After the DPDPA, IAPP (last updated Sept. 2025), https://iapp.org/news/a/india-s-surveillance-landscape-after-the-dpdpa.

"strictly necessary" and be subject to "reasonable security safeguards", encryption, access control, breach logging, and periodic reviews. Breach notification is required, but only if unauthorised access occurs, not for lawful state processing.

Despite these requirements, experts warn of implementation gaps. There is little clarity on oversight, enforcement, or sanctions for non-compliance. Security standards are not harmonised with global best practices, nor is there a mandate for external data audits or third-party vulnerability assessments. Government agencies, especially those in national security domains, are known for opaque reporting and resistance to external checks. The effectiveness of internal and external accountability in the surveillance regime remains questionable.

Data Retention, Deletion, and the Right to be Forgotten

DPDPA's state exemption regime is marked by its explicit removal of "right to erasure" and "time-bound retention" constraints for notified government agencies. Compared to the GDPR's Article 17 (right to be forgotten)[7] and Article 5 (purpose limitation)[8], India's framework allows indefinite retention based on broad "public interest" justifications.

Implications for Citizens

Longitudinal and indefinite data retention exposes citizens to vulnerabilities, identity theft, profiling, misuse by public or private actors, and erosion of informational self-determination. In the absence of periodic review or automatic deletion policies, surveillance becomes embedded not only in the policy regime but also in the quotidian experiences of Indian digital citizens.

Aadhaar and Retention Controversies

The Aadhaar regime, prior to DPDPA, exhibited similar vulnerabilities. Large-scale breaches revealed how biometric and demographic records could be used for surveillance and denial of services (e.g., pension, welfare) with little accountability. The absence of clear erasure rights

[7] Prashant Mali, Privacy Law: Right to Be Forgotten in India, 7 NLIU L. Rev. 17 (2018), https://nliulawreview.nliu.ac.in/wp-content/uploads/2022/01/Volume-VII-17-33.pdf.
[8] Asia J. Biega & Michèle Finck, Purpose Limitation and Data Minimization in Data-Driven Systems, Woodstock '18: ACM Symposium on Neural Gaze Detection, June 3–5, 2018, Woodstock, NY, https://asiabiega.github.io/papers/biega-finck-tutorial-facct22.pdf.

and retention limits now finds statutory reinforcement in DPDPA.[9]

VI. International Comparisons and Global Surveillance Regimes

European Union

The EU's General Data Protection Regulation (GDPR) establishes a rights-centric regime, subjecting national security derogations to explicit necessity, proportionality, parliamentary scrutiny, and judicial review. Data protection authorities function independently, and periodic public reporting is mandated.

United States

US state privacy laws (California, Colorado, Virginia, Connecticut) typically carve out exemptions for governmental agencies, but these are narrow, context-specific, and balanced by sectoral statutes and legislative oversight. The Federal Trade Commission (FTC) polices consumer privacy, and judicial recourse is readily available for abuse.[10]

China and Other Jurisdictions

China's Personal Information Protection Law (PIPL) grants broad state powers over digital surveillance but also requires periodic reviews and data impact assessments. The lack of transparency is offset, to some extent, by sectoral reporting obligations. India's regime is similar to China's in breadth but weaker in formal oversight.[11]

VII. Safeguards: Constitutional and Policy Analysis

Constitutional Mandates

Indian constitutional jurisprudence (Art 21, Puttaswamy)[12] posits privacy as a facet of dignity and self-determination. Legitimate encroachments by the state must meet tests of legality,

[9] Vaishnaw Asks UIDAI to Revise Aadhaar Law to Gel with Personal Data Protection Act, The Hindu (Apr. 9, 2025), https://www.thehindu.com/news/national/vaishnaw-asks-uidai-to-revise-aadhaar-law-to-gel-with-personal-data-protection-act/article69431330.ece.

[10] Privacy and Security Enforcement, Fed. Trade Comm'n, https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement (last visited Sept. 23, 2025).

[11] Julia Zhu, The Personal Information Protection Law: China's Version of the GDPR?, Colum. J. Transnat'l L. Bulletin Blog (Nov. 12, 2021), https://www.jtl.columbia.edu/bulletin-blog/the-personal-information-protection-law-chinas-version-of-the-gdpr.

[12] AIR 2017 SC 4161.

necessity, proportionality, and due process. The DPDPA's broad executive delegation and indefinite data retention conflict with these constitutional standards.

Policy Recommendations

Leading think tanks and policy groups recommend:

- Narrowly tailored notification powers
- Transparent publication of exemption orders
- Parliamentary review of delegated legislation
- Mandatory data protection impact assessments for state agencies
- Independent audit and reporting mechanisms
- Periodic legislative sunsets and judicial review triggers on broad exemptions

Enforcement and Remedies

The Data Protection Board retains limited powers to review state notifications, with most remedies available only after harm is proven. Preemptive injunctions, independent complaints, and external audit authorisations are weakly defined or missing entirely under both the Act and Draft Rules.

Civil Society, Judicial Oversight, and Media Advocacy

Civil society organisations, Internet Freedom Foundation, Centre for Internet and Society, have documented surveillance and privacy abuses, pushing for more transparency, user education, and independent audits. India's courts have started to demand justification for intrusive state action, but piecemeal litigation lacks the teeth required for systemic oversight. Media, investigative journalism, and advocacy campaigns serve as informal accountability checks, revealing instances of undue surveillance, data misuse, and executive overreach. However, the absence of clear statutory standards limits their effectiveness in inducing policy change.

VIII. Conclusion and Recommendations

The DPDPA is a landmark in India's digital policy. However, its surveillance regime, embodied

in Section 17(2)(a) and corresponding delegated rule-making, appears to construct a legal infrastructure favouring executive power over individual rights. The detailed analysis confirms crucial gaps:

- Weak procedural and substantive safeguards,
- Absence of parliamentary, independent, or judicial review for exemption orders,
- Minimal oversight in data retention, access, and erasure,
- Vulnerabilities to arbitrary and unaccountable surveillance.

India's evolving digital landscape demands a privacy architecture that meaningfully reconciles security interests with constitutional principles. Necessary reforms include the narrowing of exemption powers, adoption of global best practices in oversight, and the strengthening of remedies for affected individuals. India's position on the global stage, as both a data hub and a democracy, will be shaped by how these issues are resolved. The development and future implementation of DPDPA should be closely monitored to ensure a robust, rights-based digital future.