J Euro Eco His.
ISSN : 0391-5115
Volume 7, Issue 2 (2026)
THE JOURNAL OF EUROPEAN ECONOMIC HISTORY

Digital Personal Data Protection in India: Examining the Tension Between State Surveillance and Informational Privacy

Ms. Pooja Kumari
Assistant Professor (Selection Grade), UPES, School of law, Dehradun.

Abstract
The enactment of the Digital Personal Data Protection Act (DPDPA), 2023, marked a paradigm shift in India's legal landscape, establishing the country's first comprehensive legislative framework for digital data governance.[Yadav, P. (2026). Privacy in the digital age: A critical study of the DPDP Act 2023 and its implications. Chinnu Ramaswamy College Law Research Journal.] Driven by the constitutional mandate of the Supreme Court's historic ruling in Justice K. S. Puttaswamy (Retd.) v. Union of India (2017),[Justice K. S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors., (2017) 10 SCC 1. The nine-judge bench unanimously held that privacy is a fundamental right under Article 21 of the Constitution of India.] the Act was designed to safeguard informational privacy under Article 21 of the Indian Constitution.[Sethi, M. I. S. (2025). The Digital Personal Data Protection Act 2023: Implications for mental healthcare practice in India. PubMed Central, PMC12423081.] However, its ultimate legislative design introduces a stark constitutional paradox. While the DPDPA constructs a robust compliance architecture for private entities ("data fiduciaries"), it simultaneously carves out expansive, unchecked exemptions for State instrumentalities under the banner of national security, public order, and sovereign functions.[Saurabh, S. (2024). The Digital Personal Data Protection Act of 2023: Strengthening privacy in the digital age. International Journal of Law in Changing World, 3(2), 77–94. https://doi.org/10.54934/ijlcw.v3i2.84]

This research paper critically examines the intensifying friction between state surveillance practices and individual informational privacy in India under the DPDPA regime. By assessing structural mechanisms such as Section 7 (legitimate uses) and Section 18 (state exemptions), this paper explores how the Act dilutes core data protection principles—namely purpose limitation, data minimization, and independent oversight. It further contextualizes these legislative gaps against the backdrop of India's expanding digital surveillance infrastructure, including the Central Monitoring System (CMS), Netra, and facial recognition technologies (FRTs). Ultimately, the paper argues that the DPDPA tilts the balance of power toward a state-centric model of control, failing the tripartite test of proportionality established in Puttaswamy. It concludes by outlining mandatory legislative, judicial, and systemic reforms necessary to reconcile sovereign security interests with the fundamental right to privacy in a digital democratic state.

Key Words: Privacy, DPDP, Central Monitoring System, Proportionality, Judicial.

Introduction

The digital transformation of the Indian political economy has fundamentally altered the structural relationship between the citizen, the market, and the State. With over 800 million active internet users and a state-led digital public infrastructure (DPI) spanning biometric authentication (Aadhaar), unified payments, and digitized public service delivery, India

J Euro Eco His.
ISSN : 0391-5115
Volume 7, Issue 2 (2026)
THE JOURNAL OF EUROPEAN ECONOMIC HISTORY

produces unparalleled volumes of digital data daily.[1] In this data-driven ecosystem, personal data is no longer merely an administrative byproduct; it has become a potent instrument of behavioral profiling, commercial extractivism, and state surveillance.[2][3]

For over two decades, India's primary cyber legislation—the Information Technology (IT) Act, 2000—proved structurally inadequate to handle these modern privacy crises. Its remedial provisions, notably Section 43A, offered narrow, compensatory mechanisms restricted solely to corporate failures in safeguarding "sensitive personal data."[4][5] This regulatory void became untenable following the landmark judgment in *Justice K. S. Puttaswamy (Retd.) v. Union of India* (2017), wherein a nine-judge bench of the Supreme Court unanimously declared the right to privacy an inalienable component of life and personal liberty under Article 21 of the Constitution.[6] The Court explicitly recognized "informational privacy"—the right of an individual to control the dissemination and processing of their personal characteristics—as a fundamental right requiring robust legislative protection.

The legislative journey toward realizing the *Puttaswamy* mandate was marked by intense deliberation, spanning multiple iterations of draft bills, beginning with the Justice B.N. Srikrishna Committee Report in 2018,[7] progressing through the heavily contested 2019 and 2022 draft bills, and culminating in the passage of the Digital Personal Data Protection Act (DPDPA) in August 2023.[8][9]

While hailed as a significant milestone that introduces cross-border data transfer regulations, strict financial penalties for private data breaches, and formalized rights for "Data Principals," the finalized Act has drawn sharp criticism from constitutional scholars and civil society.[10] The central fault line lies in its asymmetric application. While the Act imposes stringent

---

[2]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.
[3]Mohanty, S., Shah, A., & Patel, R. (2025). Legal safeguards for privacy and consumer protection in targeted advertising under the DPDP Act, 2023. Atlantis Press Legal Studies, 354–362.
[4]Tiwari, M. A. (2025). A step forward? Unpacking the gaps and government overreach in the Digital Personal Data Protection Act, 2023. Indian Journal of Integrated Research in Law, 5(9).
[5]Information Technology Act, 2000, Section 43A (inserted by the Information Technology (Amendment) Act, 2008). The provision applied only to corporate bodies and required compensation for negligence leading to wrongful loss of 'sensitive personal data.' Sensitive personal data was defined narrowly under the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

[7]Justice B. N. Srikrishna Committee, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians — Report of the Committee of Experts under the Chairmanship of Justice B. N. Srikrishna (2018), Ministry of Electronics and Information Technology, Government of India.

[9]Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023). The Act received Presidential assent on August 11, 2023, and was published in the Gazette of India Extraordinary, Part II, Section 1.

J Euro Eco His.
ISSN : 0391-5115
Volume 7, Issue 2 (2026)
THE JOURNAL OF EUROPEAN ECONOMIC HISTORY

obligations of consent, transparency, and accountability on commercial entities, it systematically immunizes the State from those very same standards.[11]

Today, India boasts over 800 million active internet users, making it the second-largest online market globally. This digital expansion is built upon the foundation of India's Digital Public Infrastructure (DPI)—famously known as the "India Stack"—consisting of Aadhaar (a centralized biometric database covering over 1.3 billion residents), the Unified Payments Interface (UPI), and the Account Aggregator consent framework.[12] While this ecosystem has improved public welfare delivery, it has created unprecedented vulnerabilities in personal, behavioral, and biometric data.[13][14]

When the IT Act was amended in 2008, Section 43A was introduced requiring corporate entities to compensate for negligence in maintaining "reasonable security practices."[15] However, this provision suffered deep structural limitations: it applied exclusively to corporate entities, exempting government databases entirely; it was reactive rather than proactive; and its definition of "sensitive personal data" was too narrow to cover everyday behavioral metadata.
The finalized DPDPA introduces a formalized terminology, categorizing individuals as Data Principals and entities that determine the purpose of processing as Data Fiduciaries.[16] The Act establishes clear rules for the commercial sector, requiring free, specific, and informed consent backed by detailed privacy notices, and imposes significant financial penalties—up to ₹250 crore ($30 million)—for corporate data breaches.[17][18] However, through mechanisms like Section 18 and Section 7, the Act systematically immunizes government entities from the very accountability frameworks it imposes on corporations.[19][20][21]

---

[16]Digital Personal Data Protection Act, 2023, Section 2(i) (definition of 'Data Fiduciary') and Section 2(j) (definition of 'Data Principal'). The terminology loosely mirrors the GDPR's 'data controller' and 'data subject' categories.

[18]Digital Personal Data Protection Act, 2023, Section 9 (Data Erasure) and Schedule I (penalty provisions). The maximum penalty of ₹250 crore applies to breaches of the obligation to implement reasonable security safeguards under Section 8(5).

[20]Digital Personal Data Protection Act, 2023, Section 18(2). The provision states: 'The Central Government may, by notification, exempt from the application of all or any of the provisions of this Act, the processing of personal data—(a) by such instrumentalities of the State as it may specify in the interests of the sovereignty and integrity of India, security of the State, friendly relations with foreign States, maintenance of public order or preventing incitement to any cognisable offence relating to any of these.'

2. The Constitutional Evolution of Informational Privacy in India

To understand the legal friction embedded within the DPDPA, it is necessary to chart the evolution of privacy jurisprudence within Indian constitutional law. The Indian Constitution does not explicitly list "privacy" as a fundamental right. Consequently, its recognition was achieved through decades of judicial interpretation, shifting from a rigid, property-centric view to an expansive, rights-based doctrine.

Year	Case / Phase	Major Constitutional Development
1954	M.P. Sharma v. Satish Chandra	Privacy was NOT recognized as a Fundamental Right; search and seizure powers were upheld.
1962	Kharak Singh v. State of U.P.	Domiciliary visits declared unconstitutional, but privacy as a Fundamental Right was still rejected.
1975–1997	Gobind & PUCL Era	Courts gradually expanded privacy protections through the 'Compelling State Interest' doctrine and safeguards against arbitrary wiretapping.
2017	Justice K.S. Puttaswamy v. Union of India	Privacy was declared an inalienable Fundamental Right under Article 21 of the Constitution.

2.1 Pre-Puttaswamy Jurisprudence: The Fragmented View

The early constitutional view of privacy was profoundly restrictive. In *M. P. Sharma v. Satish Chandra* (1954), an eight-judge bench of the Supreme Court rejected the existence of a fundamental right to privacy, holding that the framers of the Constitution did not intend to limit the State's power of search and seizure by reading an implied right to privacy into the text.[22] This property-oriented, literalist approach was reinforced by a majority of a six-judge bench in *Kharak Singh v. State of Uttar Pradesh* (1962), which upheld a state regulation allowing police domiciliary visits, declaring that "the right of privacy is not a guaranteed right under our Constitution."[23]

However, a powerful dissent by Justice K. Subba Rao in *Kharak Singh* sowed the seeds for modern privacy jurisprudence, observing that the right to personal liberty under Article 21 encompasses "the right to be let alone."[24] Over subsequent decades, smaller benches increasingly relied on this dissent:

[21]Digital Personal Data Protection Act, 2023, Section 7(b). The provision permits processing of personal data without consent for 'the State' or any of its instrumentalities for providing or issuing any subsidy, benefit, service, certificate, licence or permit.' This effectively removes the consent requirement for all state-administered welfare and civic services.
[22]M. P. Sharma and Ors. v. Satish Chandra, District Magistrate, Delhi, AIR 1954 SC 300. An eight-judge bench rejected the existence of a fundamental right to privacy under the Constitution of India.
[23]Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295. A six-judge bench upheld most surveillance regulations, with the majority holding that 'the right of privacy is not a guaranteed right under our Constitution.'

J Euro Eco His.
ISSN : 0391-5115
Volume 7, Issue 2 (2026)
THE JOURNAL OF EUROPEAN ECONOMIC HISTORY

***Gobind v. State of Madhya Pradesh* (1975):** The Court recognized a limited right to privacy but subjected it to a standard of "compelling state interest."[25]

***People's Union for Civil Liberties (PUCL) v. Union of India* (1997):** Confronted with unregulated wiretapping, the Court declared telephonic conversations an essential aspect of private life and established procedural safeguards against arbitrary wiretapping under the Indian Telegraph Act, 1885.[26][27]

The earliest challenge in *M. P. Sharma* arose from massive coordinated searches during a fraud investigation. The eight-judge bench held that an implied right to privacy could not be read into the Constitution to limit statutory powers of search and seizure, establishing a precedent viewing privacy as a secondary, non-constitutional interest.[28]

In *Kharak Singh*, the petitioner was subjected to secret monitoring of his movements, midnight domiciliary visits, and periodic police inquiries among his neighbors. While the majority struck down nocturnal domiciliary visits, it upheld all other forms of surveillance and explicitly rejected privacy as a guaranteed constitutional right.[29]

In *PUCL*, the Court recognized that a telephonic conversation is an intimate expression of private life and that wiretapping violates Article 21 unless conducted under a strict, legally sanctioned procedure. Because the Telegraph Act lacked internal checks, the Court established mandatory administrative guardrails, including Home Secretary authorization, bimonthly executive review, and 180-day data retention limits.[30][31] While the *PUCL* guidelines introduced procedural discipline, they contained a major institutional vulnerability: they relied entirely on executive self-regulation, with no judicial warrant required to authorize a wiretap.

2.2 The Puttaswamy Revolution and the Tripartite Test

By 2015, challenges to the biometric Aadhaar enrollment program brought the older, fragmented precedents into direct conflict, prompting a referral to a historic nine-judge bench. On August 24, 2017, the bench issued a unanimous verdict in *Justice K. S. Puttaswamy (Retd.) v.*

[25]Gobind v. State of Madhya Pradesh, AIR 1975 SC 1378. A three-judge bench acknowledged a limited right to privacy derivable from Articles 19 and 21, but subject to a 'compelling state interest' standard.
[26]People's Union for Civil Liberties (PUCL) v. Union of India, (1997) 1 SCC 301. The Supreme Court held that telephonic conversations are an essential aspect of private life under Article 21 and established procedural safeguards against arbitrary wiretapping under the Indian Telegraph Act, 1885, Section 5(2).
[27]Indian Telegraph Act, 1885, Section 5(2). The PUCL guidelines required that interception orders be personally authorized by the Union Home Secretary or a State Home Secretary, reviewed by a committee every two months, and subject to a 180-day data retention limit. Critically, no judicial warrant was required.

J Euro Eco His.
ISSN : 0391-5115
Volume 7, Issue 2 (2026)
THE JOURNAL OF EUROPEAN ECONOMIC HISTORY

Union of India, explicitly overruling *M.P. Sharma* and the majority view in *Kharak Singh*, and elevating privacy to an inalienable, foundational right under Article 21.[32]

Constitutional Provision	**Privacy Dimension Protected**
Article 14	Protects against arbitrary and opaque state classifications.
Article 19	Safeguards the spatial dimensions of privacy in speech and movement.
Article 21	Protects human dignity, bodily autonomy, and informational privacy/control.

Crucially, *Puttaswamy* moved beyond older concepts of spatial and bodily privacy to explicitly define informational privacy—the right of an individual to control their personal data, asserting that an individual does not lose their privacy simply because they use a public utility or transact on a commercial platform. The Court then replaced the permissive "compelling state interest" standard from *Gobind* with a strict, four-pronged proportionality test:[3334]
Legality: The state's intrusion must be authorized by an explicit, accessible, and valid legislative statute.
Rational Connection (Necessity): The state must demonstrate a clear, logical connection between data collection and a legitimate state objective.
Least Intrusive Means (Proportionality): The state must prove that the chosen method is the least restrictive option available to achieve its objective.
Procedural Safeguards (Balancing): The law authorizing the intrusion must incorporate robust, independent structural safeguards to prevent executive abuse.
The *Puttaswamy* judgment created an immediate legislative mandate: the Union of India was constitutionally required to construct a comprehensive data protection regime meeting all four prongs of this proportionality test.[3536]
The fragmented and contradictory positions of *M. P. Sharma* and *Kharak Singh* were thus definitively overturned. The DPDPA, 2023, must therefore be evaluated against this exact constitutional yardstick: does it faithfully implement or actively bypass the *Puttaswamy* tripartite test?[37]

[32]Justice K. S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors., (2017) 10 SCC 1, para. 645 (Chandrachud, J.). The judgment overruled M. P. Sharma and the majority view in Kharak Singh, anchoring privacy within Articles 14, 19, and 21 of the Constitution.

[34]The proportionality framework adopted in Puttaswamy draws from the structured test applied in Modern Dental College & Research Centre v. State of Madhya Pradesh, (2016) 7 SCC 353, and is consistent with the proportionality doctrine developed in German and European constitutional jurisprudence.

J Euro Eco His.
ISSN : 0391-5115
Volume 7, Issue 2 (2026)
THE JOURNAL OF EUROPEAN ECONOMIC HISTORY

3. Anatomy of the DPDPA, 2023: Corporate Accountability vs. State Immunity

The structural architecture of the DPDPA is split into two conflicting paradigms: a highly regulated, consent-driven marketplace for private entities, and an ecosystem of sweeping exemptions for government agencies.[38]

3.1 Corporate Compliance and Data Principals' Rights

For commercial operations, the DPDPA introduces an expansive compliance framework modeled loosely on global standards like the European Union's General Data Protection Regulation (GDPR), though significantly trimmed down.[39] It categorizes entities that determine the purpose and means of processing as Data Fiduciaries, while individuals to whom the data belongs are termed Data Principals.[40][41]

The Act institutes clear baseline obligations for private fiduciaries:

Informed Consent: Processing must be anchored to consent that is free, specific, informed, unconditional, and unambiguous, preceded or accompanied by a detailed notice written in plain, accessible language.[42]

Purpose Limitation: Data can only be collected for the specific, lawful purpose explicitly stated during the consent process.[43]

Data Erasure: Fiduciaries are required to erase personal data as soon as the specified purpose has been fulfilled or when the data principal withdraws consent.[44][45]

Violations of these provisions carry severe financial penalties, reaching up to ₹250 crore ($30 million) for failing to implement reasonable security safeguards to prevent data breaches.[46][47]

3.2 The State Exemption Regime: Deconstructing Section 18 and Section 7

[42]Digital Personal Data Protection Act, 2023, Sections 5–8. Section 6 mandates that consent be 'free, specific, informed, unconditional and unambiguous,' accompanied by an itemised notice in clear, plain language. Section 11 provides the Data Principal the right to withdraw consent at any time.

THE JOURNAL OF EUROPEAN ECONOMIC HISTORY

The stringent standards of accountability applied to the private sector erode when applied to the State. The operational core of state surveillance and data access under the DPDPA is found in Section 18 and Section 7.

Section 18: Blanket Sovereign Immunity

Section 18(2) of the DPDPA empowers the Central Government to exempt any instrumentality of the State from the application of the Act's core provisions. These exemptions can be granted by mere notification in the interest of wide, vaguely defined grounds—the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, and maintenance of public order.[48]

Once an agency is exempted under Section 18, it is no longer bound by obligations to obtain consent, issue notice, ensure data accuracy, implement data erasure timelines, or respect the rights of data principals.[49] This creates a legal environment where state intelligence, law enforcement, and administrative bodies can process and retain vast amounts of personal information indefinitely, completely shielded from public scrutiny or regulatory oversight.

Provision / Section	Tax Treatment / Rule
Section 18(2) — Blanket State Exemptions	Central Government may exempt any instrumentality of the State from all or any provisions of the Act by mere executive notification.
Section 7(b) — Legitimate Uses (No Consent)	Permits state processing of personal data without consent for provision of subsidies, benefits, services, licences, or permits.
Section 19 — DPBI Governance	Chairperson and members appointed, compensated, and removable by the Central Government — no independent selection process.

Section 7: "Legitimate Uses" and the Death of Consent

Further weakening the position of the individual is Section 7, which outlines conditions under which personal data may be processed without the data principal's consent for certain "legitimate uses." Specifically, Section 7(b) permits the State to process personal data without consent for the provision of any subsidy, benefit, service, certificate, licence, or utility issued by the Government.[50]

Because the state acts as the sole provider of essential social security benefits, welfare subsidies, and basic civic identification (such as Aadhaar or public distribution systems), this section effectively legalizes a coercive trade-off: citizens must surrender their informational privacy and accept unconsented data processing simply to access the public services necessary for survival.[51][52]

J Euro Eco His.
ISSN : 0391-5115
Volume 7, Issue 2 (2026)
THE JOURNAL OF EUROPEAN ECONOMIC HISTORY

4. The Surveillance Architecture in India: Operational Reality vs. Legal Gaps

The legal immunities embedded within the DPDPA do not operate in a vacuum. They serve to reinforce and shield an extensive, pre-existing digital surveillance apparatus that has expanded rapidly across India over the past decade.

4.1 Structural Surveillance Systems

Long before the DPDPA was drafted, the Indian executive established several large-scale network surveillance systems that operate with minimal legislative oversight or judicial review:[53][54][55]

System Name	Operating Agency	Primary Objective / Capabilities
Central Monitoring System (CMS)	Telecom Enforcement Resource and Monitoring (TERM) / Intelligence Agencies	Direct, real-time interception of telephonic calls, text messages, and internet data traffic across the nation by bypassing telecom service providers.
Netra (Network Traffic Analysis)	Defence Research and Development Organisation (DRDO)	A mass internet surveillance system designed to scan, intercept, and analyze domestic web traffic using specific keyword filters across emails, blogs, and forums.
National Intelligence Grid (NATGRID)	Ministry of Home Affairs	An integrated intelligence data link that connects databases from multiple government agencies, combining immigration records, banking transactions, tax returns, airline travels, and vehicle registrations into a unified profile.

4.2 Facial Recognition and Biometric Expansion

[53]The Central Monitoring System (CMS) was developed by the Centre for Development of Telematics (C-DOT) and deployed by the Telecom Enforcement Resource and Monitoring (TERM) cell. It enables direct, real-time access to voice calls, SMS, and internet traffic without requiring telecom operators to process individual interception orders. See Internet Freedom Foundation, 'Explained: India's Surveillance Infrastructure' (2022).

[54]Netra (Network Traffic Analysis) was developed by the Defence Research and Development Organisation (DRDO). It scans internet communications for pre-set trigger words across emails, social media posts, and online forums. Its legal basis, operational scope, and data retention policies have never been publicly disclosed by the Government of India.

[55]The National Intelligence Grid (NATGRID) was established under the Ministry of Home Affairs following the 2008 Mumbai terrorist attacks. It is designed to aggregate data from 21 government databases including immigration records, bank transactions, income tax filings, telecom records, and travel data. See Ministry of Home Affairs, Annual Report 2021–22.

J Euro Eco His.
ISSN : 0391-5115
Volume 7, Issue 2 (2026)
THE JOURNAL OF EUROPEAN ECONOMIC HISTORY

Beyond telecommunications interception, the state-wide deployment of Automated Facial Recognition Systems (AFRS) by law enforcement agencies—most notably the National Crime Records Bureau (NCRB) and various state police departments—has normalized mass biometric surveillance in public spaces.[56]

Under standard data protection regimes such as the GDPR, biometric data is classified as a "special category" of sensitive personal data, requiring high thresholds of protection and explicit bans on mass processing without consent.[5758] However, the DPDPA explicitly avoided establishing separate, heightened categories for sensitive or biometric data, treating all digital information under a flat, uniform standard.[596061] Consequently, when state agencies deploy facial recognition technologies under the "public order" or "sovereign function" exemptions of Section 18, there are no statutory safeguards within the Act to protect citizens against algorithmic bias, false positives, or permanent tracking.[6263]

5. The Proportionality Deficit: Evaluating the DPDPA under the Puttaswamy Doctrine

When the state exemptions and surveillance practices authorized by the DPDPA are measured against the constitutional standards established in *Puttaswamy*, a deep proportionality deficit becomes apparent. The Act systematically fails to satisfy the elements of the Supreme Court's tripartite test.[64]

5.1 The Legality and Legitimate Goal Standard

The DPDPA technically passes the first two prongs of the test. The state's processing of data is backed by an explicit statute passed by Parliament, fulfilling the requirement of legality. Furthermore, protecting national security, preventing cybercrime, and maintaining public

[56]National Crime Records Bureau (NCRB), Request for Proposal for Automated Facial Recognition System (AFRS) (2019). The NCRB's proposed national AFRS would aggregate data from CCTV networks, crime records, and passport/visa databases. No dedicated legislation governing its deployment, retention standards, or error-rate accountability has been enacted.

[57]European Union, General Data Protection Regulation (GDPR), Regulation (EU) 2016/679, Article 9, which designates biometric data used for unique identification as 'special category data' requiring explicit consent or a specific statutory derogation. Article 35 mandates a Data Protection Impact Assessment (DPIA) prior to large-scale biometric processing.

[61]Digital Personal Data Protection Act, 2023, Sections 3 and 4. Section 4 applies the Act to the processing of digital personal data within India, and to processing outside India if it involves offering of goods or services to Data Principals in India. The Act does not create separate categories of 'sensitive personal data' as the earlier 2019 Personal Data Protection Bill had proposed.

[64]Puttaswamy (2017) 10 SCC 1, paras 310–325 (Chandrachud, J.). The Court held that any state action restricting privacy must satisfy four requirements: (i) it must be sanctioned by law; (ii) it must be necessary for a legitimate state aim; (iii) the extent of such interference must be proportionate to the need; and (iv) there must be procedural guarantees against abuse of such interference.

order are recognized by constitutional jurisprudence as legitimate state goals that can justify reasonable restrictions on fundamental freedoms.[65]

5.2 The Failure of Proportionality Strictu Sensu

The DPDPA fails on the crucial third prong: proportionality and narrow tailoring. The *Puttaswamy* doctrine requires that any state infringement on privacy must employ the least intrusive means necessary to achieve its objective. Section 18(2) violates this principle by deploying blanket, all-or-nothing exemptions instead of narrowly tailoring exemptions to protect specific, ongoing counter-terrorism operations or active criminal investigations.[6667] Furthermore, the statutory terms used to trigger these exemptions—particularly "public order"—are notoriously broad and elastic under Indian law. By utilizing expansive executive language without embedding strict statutory definitions, the DPDPA permits state instrumentalities to reclassify routine political dissent, peaceful assembly, or digital journalism as threats to "public order," justifying intrusive data collection and behavioral profiling without consent or notice.[6869]

6. Regulatory Capture: The Structural Weakness of the Data Protection Board

A foundational pillar of any effective data protection framework is an independent, autonomous regulatory authority capable of enforcing compliance against private corporations and state institutions alike. The DPDPA establishes the Data Protection Board of India (DPBI) to serve as its primary enforcement mechanism.[7071] However, a structural analysis of the DPBI's institutional design reveals a high risk of regulatory capture and executive dominance.

6.1 Institutional Dependency

Under Section 19 of the Act, the Central Government retains near-total control over the composition and operations of the DPBI: the chairperson and all members are appointed directly by the Central Government; salaries, allowances, and conditions of service are

[69]Digital Personal Data Protection Act, 2023, Section 18(2)(a). The use of the term 'public order' mirrors Article 19(2) of the Constitution, which the Supreme Court has consistently required to be narrowly construed. See Ram Manohar Lohia v. State of Bihar, AIR 1966 SC 740, where the Court held that 'public order' connotes an absence of disorder involving breaches of local significance, not every act of dissent or civil disobedience.

determined entirely by the executive; and the Central Government possesses the unilateral authority to remove Board members under broadly defined administrative grounds.[72]
This complete dependency on the executive violates the core principles of institutional independence affirmed in *Puttaswamy*. An enforcement board whose appointments, funding, and tenure are controlled by the state cannot realistically function as an impartial arbiter when a citizen files a complaint against a state surveillance agency or an intelligence bureau.[73][74]

6.2 Omission of Structural Safeguards

The structural weakness of the DPBI is further exacerbated by the legislative omission of classic data protection principles found in global frameworks.[75] The Act does not grant the DPBI proactive, independent investigative powers (*suo motu* powers) to audit state databases or inspect surveillance centers for structural privacy compliance. The Board functions primarily as a post-facto adjudicatory body for data breaches, leaving it structurally unequipped to prevent or regulate ongoing, systemic state-led surveillance.[76]

7. Comparative Analysis: India's DPDPA vs. Global Data Protection Models

To understand the exceptional nature of India's state-centric data model, it is valuable to contrast the DPDPA with the two dominant global frameworks of data protection: the European Union's General Data Protection Regulation (GDPR) and the United States' sector-specific, national-security framework.[77][78][79]

---

[72]Digital Personal Data Protection Act, 2023, Section 19 (Establishment of Data Protection Board of India). The section provides that the Chairperson and Members shall be appointed by the Central Government, their salaries and service conditions shall be as the Central Government prescribes, and the Central Government may remove the Chairperson or any Member on specified grounds.
[73]Supreme Court of India, Secretary, Ministry of Information & Broadcasting, Govt. of India v. Cricket Association of Bengal, (1995) 2 SCC 161, establishing that statutory regulatory bodies must be insulated from executive control to maintain impartiality. See also the principles of institutional independence affirmed in Union of India v. R. Gandhi, (2010) 11 SCC 1.

[77]European Union, Law Enforcement Directive (Directive 2016/680/EU), which governs the processing of personal data by competent authorities for law enforcement purposes. Unlike the GDPR, it imposes distinct, tailored obligations on state agencies while preserving core data subject rights. No analogous bifurcated framework exists under the DPDPA.
[78]United States, Privacy Act of 1974, 5 U.S.C. § 552a (regulating federal agency data processing), and Foreign Intelligence Surveillance Act of 1978 (FISA), 50 U.S.C. § 1801 et seq. (requiring judicial warrants from the Foreign Intelligence Surveillance Court (FISC) for electronic surveillance targeting foreign intelligence).
[79]Legal, B. (2026). Consent in the digital age: A comparative study of the GDPR and the Digital Personal Data Protection Act, 2023. White Black Legal. The study identifies fundamental divergences in enforcement independence, sensitive data classification, and state exemption scope between the two frameworks.

J Euro Eco His.
ISSN : 0391-5115
Volume 7, Issue 2 (2026)
THE JOURNAL OF EUROPEAN ECONOMIC HISTORY

Regulatory Domain	European Union (GDPR)	United States (FISA / Privacy Act)	India (DPDPA, 2023)
State Exemption Framework	Narrowly Tailored: State processing for law enforcement is strictly governed by a separate, specific directive (Directive 2016/680), preserving core data principles.	Bifurcated Regime: The Privacy Act of 1974 regulates federal agencies, but intelligence surveillance is conducted under FISA, requiring specialized judicial warrants.	Blanket Exemptions: Section 18 allows complete, unreviewable statutory immunity for state agencies via executive notification.
Independent Regulatory Authority	High Autonomy: Data Protection Authorities (DPAs) are constitutionally independent of executive control, possessing deep audit and fine enforcement powers.	Decentralized / Judicial: Enforced via the FTC for commerce, and specialized courts (FISC) for state surveillance warrants.	Executive Dependent: The DPBI is appointed, compensated, and regulated directly by the Central Government, risking institutional capture.
Data Minimization & Profiling	Strict Regulation: Explicit prohibitions on processing sensitive personal data (biometrics, political views) without strict necessity and prior impact assessments.	Constitutional Restraints: The Fourth Amendment restricts generalized data seizures, requiring probable cause for targeted tracking.	Unregulated: No specialized categories for sensitive data; mass algorithmic profiling and biometric tracking by state agencies remain largely unmonitored.

The comparative matrix illustrates that while the European Union treats privacy as a fundamental human right that must be defended against state overreach, and the United States relies on a combination of market regulation and constitutional judicial warrants, India has institutionalized a state-centric architecture of control.[80][81][82] The DPDPA uses the vocabulary of data protection to formalize market dynamics while systematically clearing a legal path for expanding executive surveillance.[83]

[81]Joshi, U. (2026). AI ethics in Indian healthcare: a scoping review of national and international guidelines on privacy, data protection, and security. PubMed Central (PMC). The review highlights the absence of sector-specific data protection rules for AI-driven biometric and health data processing in India.
[82]Sharma, A. K. (2026). Effect of new technologies on the right to privacy in India: With special reference to Artificial Intelligence. Naveen International Journal of Multidisciplinary Sciences (NIJMS). The paper argues that the DPDPA's flat regulatory approach is structurally inadequate to address AI-driven profiling and automated decision-making.
[83]Patel, A. (2026). The evolution of data privacy laws in India and constitutional jurisprudence.

J Euro Eco His.
ISSN : 0391-5115
Volume 7, Issue 2 (2026)
THE JOURNAL OF EUROPEAN ECONOMIC HISTORY

8. The Way Forward: Legislative, Judicial, and Systemic Reforms

The current structural imbalance within the DPDPA poses an ongoing risk to the democratic health of the Indian polity. If informational privacy is to coexist with the legitimate security interests of the State, the data protection framework must undergo deep structural and systemic reforms.

8.1 Legislative Amendments: Narrowing Section 18

The blanket exemption mechanism under Section 18(2) must be replaced with a system of proportional, activity-based exemptions rather than entity-wide immunities.[84][85]

The Principle of Specificity: Exemptions granted to security or intelligence agencies must be restricted strictly to data processing directly linked to active counter-terrorism, espionage, or serious criminal investigations. Administrative, human resource, and routine civil data processing within these agencies must remain fully subject to the DPDPA.

Statutory Definitions: The term "public order" must be strictly defined within the statute to prevent its use as an umbrella clause for processing the data of political dissidents, activists, or journalists.[86]

8.2 Introduction of Independent Judicial Oversight

A critical flaw in India's current surveillance architecture is that interception orders and data demands are authorized internally by executive officers under the IT Act or Telegraph Act. This makes the executive the judge, jury, and executioner of its own surveillance programs.[87][88][89]

Surveillance Warrants: No state agency should be permitted to bypass data protection rules or intercept personal communication without a prior judicial warrant issued by an independent, specialized judicial authority or a dedicated division within the High Courts, specifying the target, the exact scope of data collection, and a strict expiration timeline.[90]

8.3 Restructuring the DPBI for True Independence

Supremo Amicus, 40. The article traces the legislative genealogy from the IT Act, 2000, through the Srikrishna Committee recommendations, to the DPDPA, 2023, identifying the progressive erosion of state accountability across successive drafts.

J Euro Eco His.
ISSN : 0391-5115
Volume 7, Issue 2 (2026)
THE JOURNAL OF EUROPEAN ECONOMIC HISTORY

To transform the DPBI into an effective, impartial data regulator, its institutional design must be insulated from executive influence:[9192][93]

Independent Selection Committee: The appointment of the DPBI Chairperson and members should be conducted by a tripartite selection committee consisting of the Prime Minister, the Leader of the Opposition, and the Chief Justice of India (or a nominated Supreme Court Judge).
Financial Autonomy: The DPBI's budget should be drawn directly from the Consolidated Fund of India rather than being dependent on discretionary ministerial allocations.

9. Conclusion

The Digital Personal Data Protection Act, 2023, represents a watershed moment in India's legal history, but it remains a deeply flawed instrument. In its current form, the Act functions as a double-edged sword: it builds a structured regulatory wall around commercial data processing while simultaneously handing the executive a legal blank check to conduct surveillance across the digital lives of Indian citizens.[94][95]
By granting blanket exemptions under Section 18 and allowing non-consensual processing for state services under Section 7, the DPDPA fails to satisfy the tripartite test of proportionality established in *Justice K. S. Puttaswamy v. Union of India* (2017).[96][97] It tips the constitutional scales decisively away from individual informational autonomy and toward an opaque, state-centric model of data control.[98] National security and public order are undeniably compelling state interests, but a democratic society cannot preserve its security by dismantling the privacy of its citizens.
As India's digital ecosystem continues to expand, the lack of systemic guardrails, judicial warrants, and an independent regulatory board creates an environment ripe for executive overreach.[99] The enactment of the DPDPA signals the formal end of an era of unregulated data extraction and establishes the country's first unified legislative framework for the digital age.[100]

---

[93]Saini, S. (2025). Workplace Monitoring, Digital Tracking and Employee Privacy: A Legal Assessment. International Journal of Research & Technology, 13(4). The paper documents the absence of any DPDPA provision specifically governing employer surveillance of employees, creating a further regulatory gap.

J Euro Eco His.
ISSN : 0391-5115
Volume 7, Issue 2 (2026)
THE JOURNAL OF EUROPEAN ECONOMIC HISTORY

By standardizing obligations of notice, specific consent, and financial liability for data breaches, the Act provides essential consumer protections within the commercial marketplace.[101102]
The fundamental flaw of the DPDPA lies in its asymmetric design. The Act divides the Indian digital landscape into two completely different regulatory zones: a highly scrutinized, transparent market for private data fiduciaries, and an opaque ecosystem of immunity for the state and its instrumentalities.[103104] By failing to establish separate, heightened protections for biometric and sensitive personal data,[105106] the DPDPA does not check the expansion of surveillance tools like the CMS, Netra, and AFRS. Instead, it provides a legal shield, allowing mass behavioral profiling, algorithmic tracking, and continuous data aggregation to proceed without individual consent or institutional transparency.[107108109]

To bring the DPDPA into true compliance with the *Puttaswamy* doctrine, the state's immunity must be narrowed from blanket entity exemptions to strict, case-specific activity exemptions; independent judicial warrants must become a mandatory requirement before any government agency intercepts personal communications; and the DPBI must be insulated from executive control through a balanced, independent appointment process.[110111112]
Ultimately, national security and public order are vital state interests, but a democratic society cannot preserve its security by dismantling the constitutional liberties of its citizens. The true measure of a data protection law is its ability to protect the citizen not just from commercial extraction, but from the unchecked power of the state. Until the DPDPA brings state instrumentalities under the rule of law, its promise to safeguard informational privacy will remain unfulfilled, and the tension between state surveillance and individual freedom will continue to challenge the democratic fabric of the Indian republic.

References

1. Gobind v. State of Madhya Pradesh, AIR 1975 SC 1378.
2. Joshi, U. (2026). AI ethics in Indian healthcare: a scoping review of national and international guidelines on privacy, data protection, and security. PubMed Central (PMC).
3. Justice K. S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors., (2017) 10 SCC 1.
4. Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295.
5. 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.
6. Legal, B. (2026). Consent in the digital age: A comparative study of the GDPR and the Digital Personal Data Protection Act, 2023. White Black Legal.
7. M. P. Sharma and Ors. v. Satish Chandra, District Magistrate, Delhi, AIR 1954 SC 300.
8. Mohanty, S., Shah, A., & Patel, R. (2025). Legal safeguards for privacy and consumer protection in targeted advertising under the DPDP Act, 2023. Atlantis Press Legal Studies, 354–362.
9. Patel, A. (2026). The evolution of data privacy laws in India and constitutional jurisprudence. Supremo Amicus, 40.
10. People's Union for Civil Liberties (PUCL) v. Union of India, (1997) 1 SCC 301.
11. Saini, S. (2025). Workplace Monitoring, Digital Tracking and Employee Privacy: A Legal Assessment. International Journal of Research & Technology, 13(4).
12. Saurabh, S. (2024). The Digital Personal Data Protection Act of 2023: Strengthening privacy in the digital age. International Journal of Law in Changing World, 3(2), 77–94. https://doi.org/10.54934/ijlcw.v3i2.84
13. Sethi, M. I. S. (2025). The Digital Personal Data Protection Act 2023: Implications for mental healthcare practice in India. PubMed Central, PMC12423081.
14. Sharma, A. K. (2026). Effect of new technologies on the right to privacy in India: With special reference to Artificial Intelligence. Naveen International Journal of Multidisciplinary Sciences (NIJMS).
15. Tiwari, M. A. (2025). A step forward? Unpacking the gaps and government overreach in the Digital Personal Data Protection Act, 2023. Indian Journal of Integrated Research in Law, 5(9).
16. Yadav, P. (2026). Privacy in the digital age: A critical study of the DPDP Act 2023 and its implications. Chinnu Ramaswamy College Law Research Journal.