

Data Protection and State Surveillance: A Critical Analysis of India's Legal Framework

Bhachra Jagruti Palubhai

Research scholar, (Department of law), Kranti guru Shyamji Krishna Varma Kachchh University

Abstract

India's legal framework for data protection and state surveillance is at a critical juncture, influenced by constitutional developments, technological advancements, and the competing demands of national security and individual privacy. The past decade has seen significant changes, notably the Supreme Court's recognition of privacy as a fundamental right and the enactment of the Digital Personal Data Protection Act, 2023. However, the balance between data protection and state surveillance remains contentious, highlighting the inherent tensions between individual autonomy and state power in the digital age. This paper critically analyzes India's data protection and surveillance regime. It examines the constitutional foundations, statutory frameworks, institutional mechanisms, and practical implications of this regime. The analysis aims to assess how adequately it safeguards fundamental rights and ensures democratic accountability.

In summary, the paper provides a critical examination of India's evolving legal and institutional mechanisms concerning data protection and state surveillance, emphasizing the ongoing challenges in balancing individual privacy with state interests in an increasingly digital society.

Keywords- Data Protection, State Surveillance, Right to Privacy, Legal Framework, Algorithmic Surveillance.

Introduction

India's legal framework governing data protection and state surveillance stands at a critical juncture, shaped by constitutional evolution, technological advancement, and competing imperatives of national security and individual privacy. The landscape has undergone profound transformation over the past decade, particularly following the landmark Supreme Court decision recognizing privacy as a fundamental right, and more recently through the enactment of the Digital Personal Data Protection Act, 2023. However, despite these formal legal developments, India's approach to balancing data protection with state surveillance remains deeply contested, reflecting fundamental tensions between individual autonomy and state power in an increasingly digital society. This critical analysis examines the constitutional foundations, statutory frameworks, institutional mechanisms, and practical implications of India's data protection and surveillance regime, while assessing its adequacy in safeguarding fundamental rights and maintaining democratic accountability.

Methods Used in This Paper

This paper employs a comprehensive analytical approach to critically evaluate India's legal framework regarding data protection and state surveillance. The primary methods utilized include:

Critical Legal and Policy Analysis- The study conducts a critical analysis of India's data protection and surveillance regime, examining its constitutional foundations, statutory frameworks, institutional mechanisms, and practical implications. This analysis assesses the adequacy of these frameworks in safeguarding fundamental rights and ensuring democratic accountability.

Examination of Constitutional Evolution - The paper traces the historical development of the `Right to Privacy` in India, detailing its emergence through judicial interpretation and its recognition as a fundamental right. It specifically highlights the landmark Supreme Court decision in **Justice K.S. Puttaswamy (Retd.) v. Union of India (2017)**, which established constitutional standards for surveillance and data processing, requiring legality, necessity, and proportionality .

Detailed Analysis of the Digital Personal Data Protection Act, 2023 (DPDP Act)- A significant method involves a detailed analysis of the `Digital Personal Data Protection Act, 2023` (DPDP Act). This includes scrutinizing its scope, framework, and inherent limitations, particularly how it attempts to balance individual privacy with national interests and economic development. The paper also examines the Act's provisions concerning consent, data minimization, storage limitation, transparency, security obligations, and the role of the Data Protection Board of India.

Analysis of Algorithmic Surveillance and AI Threats - The study investigates the emerging threats to privacy posed by `Artificial Intelligence` (AI) and `algorithmic surveillance` technologies. It details how AI-driven tools like facial recognition, predictive analytics, and behavioral profiling fundamentally alter the surveillance landscape, creating opaque and non-procedural systems. The paper also points out the inadequacy of existing legal frameworks in addressing these AI-driven surveillance challenges.

Comparative Analysis with International Frameworks - The paper performs a `comparative analysis` of India's data protection regime against international frameworks, specifically the European Union's General Data Protection Regulation (GDPR). This comparison reveals both areas of convergence and significant divergences, particularly in the treatment of state surveillance, regulatory independence, and enforcement mechanisms.

Assessment of Democratic Values Erosion- The paper examines how the concentration of surveillance power in India's digital governance framework, exemplified by systems like Aadhaar, challenges `democratic accountability` and the rule of law. It discusses how digital technologies are used to monitor citizens and suppress dissent, raising concerns about the erosion of privacy and democratic values.

In summary, the paper primarily uses a critical legal and policy analysis method, supported by historical tracing of constitutional rights, detailed statutory interpretation, identification of systemic flaws, analysis of technological impacts, and comparative legal studies to provide a comprehensive evaluation of India's data protection and surveillance landscape.

Constitutional Foundation: The Evolution of the Right to Privacy

The right to privacy in India represents one of the most significant achievements of Indian constitutional jurisprudence, emerging through decades of judicial interpretation and eventual recognition as a fundamental right. (Dubey and Singh 2025)The journey toward this recognition was neither linear nor inevitable.¹ Prior to the watershed moment of 2017, the Indian Supreme Court had repeatedly denied privacy protection as an explicit constitutional guarantee, with early judgments such as *M.P. Sharma v. Satish Chandra* and *Kharak Singh v. State of U.P.* explicitly rejecting privacy as a separate constitutional right. However, the constitutional framework evolved through progressive judicial reinterpretation, expanding the scope of Article 21, which guarantees the right to life and personal liberty, to encompass

unenumerated rights.(Raj Singh 2024).²

The transformative judgment came with Justice K.S. Puttaswamy (Retd.) v. Union of India (2017), which fundamentally recalibrated India's constitutional jurisprudence on privacy.(DIXIT 2026) In this landmark decision, a nine-judge Constitutional Bench unequivocally recognised privacy as a fundamental right inherent in human dignity and autonomy, establishing a broad framework for understanding privacy as multifaceted, encompassing informational, decisional, and bodily privacy.³ The Puttaswamy judgment established crucial constitutional standards that any surveillance measure or data processing activity must satisfy, specifically articulating the requirements of legality, necessity, and proportionality. (Yadav and - 2025)These constitutional tests became the touchstone for evaluating whether state action interferes disproportionately with

¹ Dubey, K. K., & Yadav, S. K. (2025). The Right to Privacy in India: Evolution and Developments. *International Journal for Multidisciplinary Research*, 7(2). <https://doi.org/10.36948/ijfmr.2025.v07i02.42002>

² Law, U. (March 31, 2024). RIGHT TO PRIVACY IN INDIA: CONSTITUTIONAL BASIS AND IMPLICATIONS ON MODERN ISSUES. Unique Law. <https://www.uniquelaw.in/post/right-to-privacy-in-india-constitutional-basis-and-implications-on-modern-issues>

³ Dixit, A. (2026). *Data protection in India after the digital personal data protection act, 2023: a critical evaluation of privacy and state power*. <https://doi.org/10.65393/ldeo6679>

privacy rights, thereby creating a normative baseline against which all subsequent legislation and executive action must be measured.⁴

This constitutional recognition was not merely symbolic but represented a foundational shift in the relationship between the state and the individual in the digital age. The judgment acknowledged that privacy is integral to democracy itself, essential for preserving individual dignity, autonomy, and democratic participation in a society increasingly characterized by data collection and technological intrusion. (Jindal n.d.)⁵ However, the recognition of privacy as a fundamental right simultaneously raised critical questions about how this right would be protected, particularly in light of rapid digitalization, the expansion of state surveillance capabilities, and the commercial interests in personal data exploitation. The Supreme Court's affirmation of privacy as fundamental thus created a constitutional imperative for legislative action to create robust safeguards, leading eventually to the enactment of comprehensive data protection legislation.

The Digital Personal Data Protection Act, 2023: Scope and Framework

The Digital Personal Data Protection Act, 2023 (DPDP Act) represents India's first comprehensive legislative effort to establish a structured legal framework for the protection of personal data, enacted in the aftermath of the Puttaswamy decision to address a constitutional and legislative vacuum that had persisted despite recognition of privacy as a fundamental right. (DIXIT 2026) The DPDP Act adopts a consent-based regulatory approach, attempting to balance individual privacy protection with national interests and economic development.⁶ The legislation establishes fundamental principles governing data processing, including requirements for consent, data minimization, storage limitation, transparency, and

security obligations on data fiduciaries—entities that determine the purpose and means of data processing.

⁴ Ijfmr. (2025a). E-ISSN: 2582-2160 • Website: www.ijfmr.com • Email: editor@ijfmr.com. Ijfmr. <https://www.ijfmr.com/papers/2025/6/59991.pdf>

⁵ Jindal, T. (n.d.). Unknown title. <https://doi.org/10.36948/ijfmr.2024.v06i06.31832>

⁶ Dixit, A. (2026). *Data protection in India after the digital personal data protection act, 2023: a critical evaluation of privacy and state power*. <https://doi.org/10.65393/ldeo6679>

The Act's scope is defined by its focus on "digital personal data," encompassing information collected, processed, stored, or transmitted in digital form that relates to an identified or identifiable natural person. (Mahajan 2026) Critically, the Act applies to the processing of personal data in India, even if the data is digitized after offline collection, and extends to processing conducted outside India when the purpose involves offering services or products within India.⁷ The legislation establishes a Data Protection Board of India as an institutional mechanism for enforcement and dispute resolution, vesting it with powers to investigate violations, adjudicate complaints, and impose penalties for non-compliance. (Naithani 2025) The Act also recognizes a range of data principal rights, including the right to access personal data held by data fiduciaries, the right to correction of inaccurate data, the right to erasure, and importantly, the right to grievance redress.⁸

However, the practical architecture of the DPDP Act reveals significant structural limitations that fundamentally constrain its effectiveness in protecting informational privacy. The consent-based model, while ostensibly empowering individuals to control personal data processing, operates within a highly asymmetrical power dynamic where individuals often face take-it-or-leave-it consent interfaces, lack meaningful ability to understand data processing implications, and encounter coercive digital architectures that make non-consent practically infeasible. (Collaco, 2025) The Act permits data fiduciaries broad discretion to determine purposes of processing and often fails to account for structural inequalities and coercive digital environments that undermine genuine informed consent, particularly affecting vulnerable populations.⁹ Furthermore, the legislation does not prescribe specific mechanisms for algorithmic decision-making accountability, nor does it establish robust requirements for algorithmic transparency and

⁷ Mahajan., & Gaurav. (2026). India's emerging data protection framework : A critical analysis of legal reform and global interoperability. *Journal of Data Protection & Privacy*. <https://doi.org/10.69554/XLLB8520>

⁸ 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>

⁹ Collaco., & Mitchelle, A. (2025). The Illusion of Choice: Re-imagining digital consent in India through a feminist lens. *Journal of Data Protection & Privacy*. <https://doi.org/10.69554/KIHH4415>

explain ability, creating significant governance gaps at precisely the point where data processing produces the most significant impacts on individual autonomy and life chances.

State Exemptions and Surveillance Powers: The Erosion of Privacy Safeguards

One of the most contentious and constitutionally problematic aspects of the DPDP Act concerns its treatment of state data processing, which is characterized by extraordinarily broad exemptions that fundamentally undermine the protective intent of the legislation. Section 17 of the DPDP Act provides that the Act does not apply to personal data processing undertaken by the state for purposes such as national security, public order, public health, safety, or official functions related to governance, welfare schemes, and law enforcement. (DIXIT 2026) These exemptions are formulated with such breadth that they effectively transfer vast swaths of state surveillance activity outside the purview of data protection guarantees, creating a parallel legal universe where state agencies operate with minimal constraints on data processing, collection, and retention.¹⁰

The exemptions are particularly troubling because they lack meaningful safeguards: there is no requirement for judicial authorization of state surveillance measures, no mandatory proportionality assessment, no temporal limitations on data retention, and minimal transparency or public accountability mechanisms. The state may invoke national security or public order justifications without demonstrating necessity or proportionality, and without subjecting its surveillance to independent judicial oversight. (Tyagi and Dutt 2026) This structure represents a fundamental departure from the constitutional standards articulated in *Puttaswamy*, which explicitly required that any interference with privacy must satisfy strict tests of legality, necessity, and proportionality.¹¹ The exemptions effectively exempt the state from these constitutional tests, creating a dangerous gap between the constitutional promise of privacy protection and the legislative reality of state surveillance.

¹⁰ Dixit, A. (2026). *Data protection in India after the digital personal data protection act, 2023: a critical evaluation of privacy and state power*. <https://doi.org/10.65393/ldeo6679>

¹¹ Tyagi, R. D., & Dutt, O. (n.d.). Unknown title. <https://doi.org/10.36948/ijfmr.2026.v08i01.67398>

The backdrop to these exemptions lies in India's complex surveillance legal architecture, which predates the DPDP Act and has evolved through various statutes granting expansive surveillance powers. The Telecommunications Act 2023 and the Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules 2024 authorize wide-ranging data interception and dragnet surveillance while exempting government agencies from meaningful oversight. (Ramaswamy 2024) The Information Technology Act 2000, while predating contemporary digital surveillance capabilities, has been interpreted to permit extensive executive discretion in surveilling digital communications, with minimal procedural safeguards. These legal frameworks, anchored in expansive executive powers, opaque data practices, and minimal judicial oversight, have been compounded by artificial intelligence technologies such as facial recognition and predictive policing tools that enable mass surveillance capabilities unprecedented in scope and intrusiveness.¹²

The absence of meaningful constraints on state surveillance is particularly concerning in light of India's emerging "digital authoritarianism," characterized by increasing state surveillance, data control, and restrictions on digital freedoms. (MOHAPATRA 2025) ¹³The Indian government leverages digital

technologies, including biometric identification systems through Aadhaar, artificial intelligence, and internet shutdowns, to monitor citizens and suppress dissent. Case studies of Aadhaar, the Pegasus spyware controversy, and internet shutdowns reveal the intersection of technology and state power, demonstrating how India's digital governance is evolving in ways that challenge constitutional freedoms and threaten democratic values. The normalization of mass surveillance through these legal and technological mechanisms raises profound concerns about the erosion of privacy as a lived reality, even as it remains recognized as a constitutional right on paper.

¹² Ramaswamy, Samyukta (2024) "The Evidence Machine: Rethinking Admissibility and Privacy in India's AI Surveillance State," *Indian Journal of Law and Technology*: Vol. 20: Iss. 2, Article 4.

¹³ Ijfmr. (2025a). E-ISSN: 2582-2160 • Website: www.ijfmr.com • Email: editor@ijfmr.com. Ijfmr. <https://www.ijfmr.com/papers/2025/3/48656.pdf>

Artificial Intelligence and Algorithmic Surveillance: Emerging Threats to Privacy

The rapid integration of artificial intelligence into state surveillance mechanisms represents one of the most significant and inadequately addressed challenges to privacy protection in India. AI-driven surveillance technologies, including facial recognition systems, predictive analytics, and behavioral profiling tools, fundamentally alter the surveillance landscape by enabling pervasive monitoring and data-driven decision-making that operates through opaque, non-procedural systems producing what has been termed a "black box" effect. (Ramaswamy 2024) These technologies disproportionately target marginalized populations due to inherent risks of algorithmic bias, and the opacity of machine learning systems creates a fundamental incompatibility with due process, procedural fairness, and individual autonomy.¹⁴

India's existing legal framework is inadequate to address these AI-driven surveillance challenges. The Information Technology Act 2000 and the DPDP Act 2023, while representing important steps, fail to establish comprehensive frameworks for algorithmic accountability, transparency, and fairness. The regulatory gaps are particularly acute in relation to government deployment of AI systems, where the state exemptions in the DPDP Act permit unchecked algorithmic surveillance without requirements for algorithmic audits, fairness assessments, or transparency mechanisms. Major initiatives like Safe City programs, DigiYatra, and the National Digital Health Mission employ AI-driven surveillance and profiling without adequate safeguards for informational privacy or protection against algorithmic bias and discrimination.

Furthermore, AI-generated outputs from surveillance systems are increasingly introduced as evidence in criminal proceedings without clear standards for reliability, admissibility, or constitutional compliance, creating potential for evidentiary abuse and violations of due process. (Ramaswamy 2024) The criminal justice system lacks established frameworks for evaluating the admissibility of AI-generated evidence, for assessing the reliability of algorithmic outputs, or for ensuring that algorithmic decision-making complies with constitutional protections. This gap creates a troubling scenario where individuals are subjected to algorithmic profiling, algorithmic decision-making, and algorithmic evidence within criminal proceedings without meaningful

¹⁴ Ramaswamy, Samyukta (2024) "The Evidence Machine: Rethinking Admissibility and Privacy in India's AI Surveillance State," Indian Journal of Law and Technology: Vol. 20: Iss. 2, Article 4.

opportunity to challenge the underlying algorithmic logic or to contest the reliability of algorithmic outputs.

The convergence of AI and surveillance thus represents a second-order threat to privacy, adding layers of opacity, bias, and automation to state surveillance that exceed what traditional legal frameworks can adequately regulate. The proposed AI Regulation Act, 2025 represents a step toward addressing some of these concerns through risk-based regulation frameworks, but remains nascent in development and uncertain in scope. The absence of comprehensive AI regulation, combined with broad state exemptions from the DPDP Act, means that India's most intrusive and consequential surveillance practices—those employing artificial intelligence—operate with minimal legal constraint and accountability mechanisms.¹⁵

Institutional Design and Enforcement Limitations

The institutional architecture established by the DPDP Act to enforce privacy protections reveals critical weaknesses that constrain the legislation's practical effectiveness. The Data Protection Board of India, conceived as the primary enforcement and adjudicatory body, suffers from structural limitations that undermine its independence and effectiveness. (DIXIT 2026) The Board lacks explicit judicially insulated status, meaning its independence from executive influence remains uncertain.¹⁶ The Board operates within a framework providing limited avenues for redress, with constrained powers to provide remedies to aggrieved individuals and limited capacity to impose meaningful sanctions that would deter violations by powerful state or corporate actors.

The absence of an independent, robustly constituted data protection authority represents a critical institutional failure that distinguishes India's framework unfavorably from international benchmarks like the European Union's General Data Protection Regulation. (DIXIT 2026) The GDPR establishes independent data protection authorities in each member state, with explicit

¹⁵ Verma, A., Mittal, B., & Bala, A. (n.d.). Unknown title. <https://doi.org/10.36948/ijfmr.2025.v07i05.58572>

¹⁶ Dixit, A. (2026). *Data protection in India after the digital personal data protection act, 2023: a critical evaluation of privacy and state power*. <https://doi.org/10.65393/ldeo6679>

constitutional protection against removal or interference by executive authorities, comprehensive investigative powers, and authority to impose substantial penalties including fines up to four percent of global turnover. India's Data Protection Board, by contrast, operates within a more constrained institutional space, lacking clear independence guarantees and operating with limited financial and human resources relative to the scale of India's digital economy.

Moreover, the enforcement mechanisms established by the DPDP Act remain underdeveloped and untested. The rules governing the Board's procedures have been delayed, resulting in significant uncertainty regarding practical implementation. (Mahajan 2026)¹⁷ The timeline for complaint adjudication, the procedures for investigating violations, the standards for assessing data fiduciary compliance, and the mechanisms for imposing and enforcing penalties all remain inadequately specified. This institutional ambiguity creates compliance uncertainty for data fiduciaries and undermines confidence among data principals regarding redress availability, while simultaneously enabling continued violations during the critical early implementation period.

Comparative Analysis: Learning from International Frameworks

A comparative analysis of India's data protection regime with international frameworks, particularly the European Union's General Data Protection Regulation (GDPR), reveals both areas of convergence and significant divergences that illuminate strengths and critical weaknesses in India's approach. Both frameworks recognize personal data protection as a fundamental right and establish consent-based processing models requiring transparency and accountability. Both frameworks establish independent regulatory authorities tasked with enforcement and protection of data subjects' rights. (Kumar 2025) Both frameworks recognize rights to data access, correction, and erasure, attempting to empower individuals with control over personal information.¹⁸

¹⁷ Mahajan., & Gaurav. (2026). India's emerging data protection framework : A critical analysis of legal reform and global interoperability. Journal of Data Protection & Privacy. <https://doi.org/10.69554/XLLB8520>

¹⁸https://www.researchgate.net/publication/399837145_Evolving_Jururisprudence_of_Digital_Privacy_A_Comparative_Study_of_Global_Data_Protection_Frameworks

However, critical divergences emerge in the treatment of state surveillance, regulatory independence, and enforcement mechanisms. The GDPR contains no categorical exemptions for state surveillance comparable to the sweeping exemptions in the DPDP Act Section 17. Instead, the GDPR subjects state data processing to the same proportionality requirements applicable to private sector processing, with some sector-specific variations but without wholesale exemption of state agencies. (Naithani 2025)¹⁹ The GDPR establishes explicit proportionality constraints on surveillance, requiring that interference with privacy be necessary and proportionate to legitimate aims. The GDPR authorizes independent data protection authorities with explicit constitutional protection and substantial enforcement powers, including capacity to impose meaningful penalties that deter violations.

Furthermore, international frameworks increasingly recognize algorithmic accountability as a discrete regulatory concern requiring specific safeguards beyond traditional data protection mechanisms. The EU's proposed AI Act establishes risk-based regulation of artificial intelligence systems, with heightened requirements for high-risk algorithmic systems deployed in critical decision-making contexts. (Abraham and Dev 2025a)²⁰ The Canadian AI and Data Act similarly addresses algorithmic bias, transparency, and accountability. These international frameworks recognize that algorithmic systems require specialized regulatory approaches distinct from traditional data protection, yet India's legal framework fails to establish comprehensive algorithmic accountability mechanisms, creating a critical gap in protection

against AI-driven harms.

The comparative analysis also reveals that India's framework is weaker in its treatment of vulnerable populations and intersectional privacy concerns. While the GDPR contains specific provisions protecting children's data with heightened consent requirements and restrictions on targeted marketing toward minors, India's DPDP Act provides less robust protection for minors and fails to address gendered privacy concerns, despite evidence that women and children face

¹⁹ 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>

²⁰ Abraham., Mariyan, M., Dev., & Shampa. (2025). AI-driven surveillance in India: Reconciling privacy, national security and legal oversight. *Journal of Data Protection & Privacy*. <https://doi.org/10.69554/BZBZ5748>

disproportionate privacy violations through digital surveillance, harassment, and data misuse. (Kaur and Nath 2025b) The absence of intersectional privacy protections means that India's formal rights on paper fail to adequately address how surveillance, data exploitation, and algorithmic discrimination operate differentially across social groups based on gender, caste, religion, and other social positions.²¹

Digital Governance and the Erosion of Democratic Values

The concentration of surveillance power in India's digital governance framework represents a profound challenge to democratic accountability and the rule of law. The digitalization of governance through platforms like Aadhaar, Digital India, and increasingly AI-driven welfare delivery systems has created massive systems of data collection and algorithmic decision-making that determine access to essential services and benefits. (Madaan and Mohanty 2025)²² These systems concentrate unprecedented power in state and corporate hands while diminishing citizen agency and democratic oversight. The asymmetrical control of digital infrastructure creates scenarios where surveillance is normalized, where resistance is ineffective, and where individuals experience limited capacity to contest algorithmic determinations affecting their life chances.

The Aadhaar biometric identification system exemplifies these concerns. Conceived as a financial inclusion and governance efficiency tool, Aadhaar has evolved into a comprehensive identification and surveillance infrastructure enabling unprecedented scope of state monitoring. (Yadav and - 2025)²³ While the Supreme Court in *Puttaswamy v. Union of India* ultimately upheld Aadhaar's constitutional validity, the judgment articulated significant concerns about surveillance risks and established constitutional constraints on Aadhaar's deployment, including requirements that Aadhaar usage be limited to specific welfare and tax purposes, with prohibition on generalized usage for law enforcement and surveillance absent legislative authorization. Yet

²¹ Kaur, D., & Nath, A. (n.d.). Unknown title. <https://doi.org/10.63363/aijfr.2025.v06i05.1462>

²² Madaan, A. M., & Mohanty, A. (2025). Identity Theft in the Digital Age: Legal Challenges and the

Evolving Role of Law Enforcement in India. *Cyber Law Reporter*. <https://doi.org/10.55662/CYLR.2025.4102>

²³ Yadav, E., & Khanna, P. G. (n.d.). Unknown title. <https://doi.org/10.36948/ijfmr.2025.v07i06.59991>

despite these constitutional constraints, Aadhaar usage has progressively expanded beyond the constitutionally sanctioned scope, integrated into increasingly diverse governance functions without corresponding legislative authorization or proportionality assessments.

The absence of meaningful democratic oversight over surveillance and data processing represents a critical failure in India's governance architecture. Legislative scrutiny of surveillance expansions remains sporadic and reactive rather than systematic and preventive. Parliamentary debates on surveillance legislation often lack the detailed technical expertise necessary to adequately scrutinize surveillance proposals, resulting in sweeping surveillance powers approved with minimal deliberation. (J N and N 2025)²⁴ The judiciary, while providing important safeguards through constitutional interpretation, operates at a remove from the immediate governance of surveillance, intervening primarily through reactive litigation rather than proactive oversight. Civil society and public discourse remain inadequately informed regarding surveillance expansion, constrained by classifications of surveillance tools as "national security matters" resistant to public scrutiny.

Implementation Challenges and Enforcement Gaps

Despite the formal enactment of the DPDP Act, the practical implementation landscape remains characterized by significant uncertainty, delay, and institutional incapacity. The Act was passed in August 2023, yet critical rules necessary for implementation were not finalized until late 2024, creating a prolonged period of implementation ambiguity during which the Act's requirements remained unclear to data fiduciaries and data principals alike. (Saha and Mukhopadhyay 2024) This extended implementation timeline has enabled continued data processing practices contrary to the Act's intent, with organizations operating under uncertainty regarding compliance requirements and with limited fear of enforcement given the Data Protection Board's nascent state and unclear enforcement protocols.²⁵

²⁴ N, S. K. J., & N, M. (n.d.). Unknown title. <https://doi.org/10.36948/ijfmr.2025.v07i02.40059>

²⁵ Saha, S., & Mukhopadhyay, S. (2024). A New Age of Data Privacy Laws in India: Review of Digital Personal Data Protection Act, 2023. *International Journal of Law and Social Sciences*. <https://doi.org/10.60143/ijls.v10.i1.2024.114>

The enforcement challenges are compounded by the complexity of investigating and adjudicating data protection violations in the context of large-scale commercial and governmental data processing. The Data Protection Board lacks resources, expertise, and institutional capacity adequate to address the scale of potential violations across India's digital economy. (Mahajan 2026) The volume of potential complaints exceeds the Board's adjudicatory capacity, creating backlogs and delays that render remedies ineffective.²⁶ The Board faces significant challenges in investigating violations involving sophisticated technical systems, algorithmic decision-making, and cross-border data flows, requiring technical expertise that may exceed the institution's current capacities.

Furthermore, compliance by organizations remains incomplete and often performative rather than substantive. Organizations frequently adopt "privacy by policy" approaches, establishing formal data protection frameworks while maintaining extraction and surveillance practices that contravene the Act's protective intent. (Singh and Simon 2025)²⁷ The sophisticated asymmetries in bargaining power between individuals and organizations, combined with the limited penalties for violations relative to the

commercial value of personal data, create insufficient incentives for genuine compliance. When penalties are imposed, they often prove inadequate to deter recurrence, with commercial entities absorbing fines as a cost of data exploitation business models.

Gendered Dimensions of Surveillance and Data Protection

Women and girls face distinctive privacy vulnerabilities through surveillance and data collection that existing legal frameworks inadequately address. The gendered nature of digital surveillance, harassment, and data misuse remains undertheorized and inadequately protected within India's

²⁶ Mahajan., & Gaurav. (2026). India's emerging data protection framework : A critical analysis of legal reform and global interoperability. Journal of Data Protection & Privacy. <https://doi.org/10.69554/XLLB8520>

²⁷ Singh., Pushpit., Simon., & Tomy, S. (2025). Personal data monetisation model in India : Reimagining the contours of the Digital Personal Data Protection Act, 2023 through a market-oriented approach analysis. Journal of Data Protection & Privacy. <https://doi.org/10.69554/XDRR7205>

legal framework. (Kaur and Nath 2025a) ²⁸ Women face disproportionate risks of cyber harassment, non-consensual intimate image sharing, digital stalking, and surveillance abuse, yet the legal framework addressing these harms remains fragmented and inadequately resourced. The Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013 addresses workplace harassment but provides limited specific protections for digital workplace monitoring and surveillance that increasingly characterizes employment relationships.

The DPDP Act fails to address gendered surveillance concerns or intersectional privacy vulnerabilities. The consent-based framework, while superficially neutral, operates differentially for women in contexts characterized by structural power asymmetries and gendered coercion. (Collaco 2025)²⁹ The feminist critique of digital consent reveals that individualistic consent frameworks fail to account for structural inequalities, coercive digital architectures, and gendered power dynamics that shape women's digital experiences and constrain meaningful consent. The framework's failure to recognize collective and relational models of agency means that it inadequately protects women's informational autonomy, particularly in contexts involving intimate data, reproductive information, and domestic surveillance.

Furthermore, surveillance of women's bodies and behaviors perpetuates historical patterns of patriarchal control digitized through contemporary technology. Facial recognition surveillance, behavioral profiling, and location tracking systems enable monitoring of women's movements and social participation, with particular risks for women activists, journalists, and political opponents. (Khaladkar 2025)³⁰ The absence of specific protections for women's privacy within India's legal framework means that gendered surveillance harms remain largely remediable only through general privacy provisions that inadequately capture the specific nature and consequences of gendered privacy violations.

²⁸ Kaur, D., & Nath, A. (n.d.). Unknown title. <https://doi.org/10.63363/aijfr.2025.v06i05.1462>

²⁹ Collaco., & Michelle, A. (2025). The Illusion of Choice: Re-imagining digital consent in India through a feminist lens. Journal of Data Protection & Privacy. <https://doi.org/10.69554/KIHH4415>

³⁰ Satyavati Rajesh Khaladkar (2025). Right to Privacy for Women: Legal Framework and Social Imperatives TTASSH. 5(3), 1-6. doi.org/10.36647/TTASSH/05.03.A001.

The Right to Information Act and Transparency Tensions

A critical but often underexamined tension exists between the Right to Information Act, 2005 (RTI Act) and privacy protections, with implications for how data protection law should accommodate transparency and accountability imperatives. (PADMAJA 2026a)³¹ The RTI Act represents one of India's most transformative democratic achievements, institutionalizing government transparency as a means of ensuring accountability, controlling corruption, and enabling informed democratic participation. However, the RTI Act's access framework applies to information held by government bodies, potentially including personal data, creating scenarios where privacy and transparency values conflict. The DPDP Act's enactment has recalibrated the legal landscape governing this interface, raising critical questions regarding how personal data protection obligations should reconcile with transparency obligations.

The legal resolution of this tension remains inadequately developed. The RTI Act contains exemptions for information that would constitute an invasion of privacy, yet the scope and application of these exemptions remain contested and inconsistently applied. (PADMAJA 2026b) An overly expansive application of data protection norms to personal data held by government could substantially dilute the RTI Act's transformative potential and weaken democratic accountability by enabling government bodies to withhold information relevant to scrutinizing state action under privacy justifications. Conversely, an unduly narrow application of privacy exemptions to RTI requests could result in indiscriminate disclosure of personal data, eroding privacy protections. This tension requires nuanced jurisprudential development to establish principles of proportionality, public interest, and harmonious statutory interpretation that recognize both privacy and transparency as foundational democratic values requiring balanced protection.

Sectoral Privacy Concerns: Healthcare, Finance, and Governance

The DPDP Act establishes a general framework for personal data protection but inadequately addresses the distinctive privacy concerns arising in critical sectors where data collection is intensive and consequences of data misuse are severe. Healthcare data processing, which

³¹ PRIVACY VIS-À-VIS TRANSPARENCY: RECONCILING THE RIGHT TO INFORMATION ACT, 2005 WITH THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023 – Indian Journal of Legal Review [ISSN – 2583-2344] (n.d.). Doi. <https://doi.org/10.65393/GMEO4129>

involves intimate information regarding physical and mental health, genetic predispositions, and therapeutic relationships, requires heightened privacy protections and specific safeguards beyond general data protection principles. (Singh and Singh 2024) The National Digital Health Mission and emerging electronic health record systems process vast quantities of sensitive health data with limited privacy safeguards and inadequate constraints on secondary use of health data for purposes distinct from clinical care.³²

Similarly, fintech and e-commerce sectors process extensive personal financial data, creating risks of profiling, discrimination, and exclusion based on algorithmic determinations regarding creditworthiness, purchasing behavior, and financial reliability. (Samraat Singh and Dr. Ajeet Kumar 2026)³³ The DPDP Act's framework, while addressing some fintech privacy concerns, permits data processing for

commercial profiling and algorithmic decision-making that may perpetuate discrimination and restrict consumer autonomy. The absence of specific sectoral safeguards means that data protection requirements apply uniformly across sectors with fundamentally different risk profiles and requiring different levels of protection.

Governance contexts, including welfare administration, taxation, and law enforcement, involve state access to sensitive personal data with potential for abuse and discrimination. (Annappa 2022)³⁴ The DPDP Act's state exemptions mean that government agencies operate with minimal constraints in processing personal data for governance functions, creating opportunities for surveillance, discrimination based on protected characteristics, and abuse of administrative power. The absence of meaningful constraints on state data processing for governance purposes

³² Singh, R., & Singh, V. (2024). Beyond Consent: Ensuring Meaningful Protection of Genetic Data Under India's Digital Personal Data Protection Act, 2023. *Journal of Indian Academy of Forensic Medicine*, 46(4), 562–567. <https://doi.org/10.1177/09710973251328785>

³³ Singh, S., & Kumar, D. A. (2026). THE RIGHT TO PRIVACY AND THE DIGITAL ECONOMY: AN EXAMINATION OF THE IMPACT OF INDIA'S DATA PROTECTION REGIME ON E-COMMERCE AND FINTECH. *EPRA International Journal of Research & Development (IJRD)*. <https://doi.org/10.36713/epra25992>

³⁴ Annappa, N. (2022). The State's access to data and internet intermediary response – an assessment of India's attempt to reallocate the legal framework to ensure national security. *International Review of Law, Computers & Technology*, 36(3), 404–430. <https://doi.org/10.1080/13600869.2022.2030038> undermines both privacy protection and equal protection principles that should constrain administrative action.

Recommendations for Legal and Structural Reform

Addressing the inadequacies in India's data protection and surveillance framework requires comprehensive legal and structural reforms that strengthen privacy protections, constrain state surveillance, ensure institutional independence, and establish meaningful accountability mechanisms. First, the DPDP Act requires amendment to narrow the state exemptions in Section 17, establishing that state data processing for national security and public order purposes must satisfy strict constitutional tests of legality, necessity, and proportionality, with mandatory judicial authorization of surveillance measures affecting communications or location data. (DIXIT 2026)³⁵ The state exemptions should be restructured to require that any surveillance interference with privacy must be subject to independent judicial authorization, undergo proportionality assessment demonstrating necessity of the surveillance measure, and be subject to meaningful oversight and auditing.

Second, India requires comprehensive algorithmic governance legislation establishing requirements for algorithmic transparency, fairness, explain ability, and accountability specific to AI systems deployed in consequential decision-making contexts. (Abraham and Dev 2025b)³⁶ Such legislation should establish algorithmic impact assessments as prerequisites for deploying high-risk algorithmic systems, require fairness testing and bias auditing, establish mechanisms for contesting algorithmic determinations, and create institutional infrastructure for algorithmic accountability separate from traditional data protection regulation.

Third, the Data Protection Board of India requires structural reinforcement to ensure institutional independence, including explicit constitutional protection against removal or interference by executive authorities, adequate financial and human resource allocation, and authority to impose

³⁵ Dixit, A. (2026). *Data protection in India after the digital personal data protection act, 2023: a critical evaluation of privacy and state power*. <https://doi.org/10.65393/ideo6679>

³⁶ Abraham., Mariyan, M., Dev., & Shampa. (2025). AI-driven surveillance in India: Reconciling privacy, national security and legal oversight. *Journal of Data Protection & Privacy*. <https://doi.org/10.69554/BZBZ5748>

meaningful penalties capable of deterring violations. (DIXIT 2026) The Board should be restructured with appointment procedures ensuring insulation from executive control, fixed tenures protecting member independence, and enhanced powers to investigate violations, compel testimony, and impose penalties adequate to deter violations by powerful state and corporate actors.

Fourth, India should establish comprehensive sectoral privacy protections addressing distinctive risks in healthcare, finance, and governance contexts, with tailored safeguards reflecting different risk profiles and sensitivity levels across sectors. Healthcare data should be subject to heightened privacy protections restricting secondary use and algorithmic processing without explicit informed consent. Fintech and e-commerce regulation should constrain profiling and algorithmic discrimination in access to financial services. Government data processing should be subject to transparency requirements, auditing, and oversight adequate to ensure that surveillance does not exceed constitutional bounds.

Fifth, gendered privacy protections should be integrated throughout India's data protection framework, recognizing distinctive privacy vulnerabilities faced by women and establishing specific safeguards for intimate data, reproductive information, and protection against gender-based surveillance and harassment. Feminist legal theory should inform development of privacy frameworks acknowledging power asymmetries, structural inequalities, and gendered modes of coercion that constrain meaningful consent.

Sixth, civil society participation and democratic deliberation regarding surveillance and data processing should be strengthened through transparency regarding surveillance infrastructure, public participation in surveillance policy development, and civil society access to information regarding state surveillance practices. Parliamentary scrutiny of surveillance legislation should be enhanced through establishment of legislative committees with adequate technical expertise to evaluate surveillance proposals and through mandatory public consultation on surveillance policy changes.

Conclusion

India's legal framework governing data protection and state surveillance remains inadequate to the task of protecting informational privacy and maintaining democratic accountability in a rapidly digitalizing society. While the constitutional recognition of privacy as a fundamental right in *Puttaswamy v. Union of India* represents a profound achievement in human rights jurisprudence, and the enactment of the DPDP Act represents an important step toward formal data protection legislation, the practical architecture of India's legal framework reveals critical gaps that undermine effective privacy protection and create opportunities for expansive state surveillance. The broad state exemptions in the DPDP Act, the absence of comprehensive algorithmic governance, the inadequate institutional

infrastructure for enforcement, and the failure to address distinctive privacy vulnerabilities of marginalized populations collectively render India's data protection framework insufficient to satisfy the constitutional standards articulated in Puttaswamy or to align with international human rights norms regarding privacy protection.

The emergence of artificial intelligence-driven surveillance represents a second-order threat to privacy that existing legal frameworks inadequately address, creating a situation where India's most intrusive and technologically sophisticated surveillance practices operate with minimal legal constraint and accountability. The digital authoritarianism increasingly characterizing India's governance through normalized surveillance, pervasive data collection, and algorithmic decision-making threatens fundamental democratic values including individual autonomy, democratic participation, and equal citizenship. Addressing these threats requires not only amendment of existing legislation but also a fundamental reconceptualization of the relationship between state power and individual rights in the digital age, one that privileges privacy protection, constrains surveillance power, ensures institutional accountability, and restores democratic agency in technological governance. Only through comprehensive legal reform, institutional restructuring, and genuine commitment to privacy as a cornerstone of democratic society can India transform its formal legal recognition of privacy rights into meaningful lived protections for all citizens in an increasingly digital world.

References

1. Dubey, K. K., & Yadav, S. K. (2025). The Right to Privacy in India: Evolution and Developments. *International Journal For Multidisciplinary Research*, 7(2). <https://doi.org/10.36948/ijfmr.2025.v07i02.42002>
2. Law, U. (March 31, 2024). RIGHT TO PRIVACY IN INDIA: CONSTITUTIONAL BASIS AND IMPLICATIONS ON MODERN ISSUES. Unique Law.
3. <https://www.uniquelaw.in/post/right-to-privacy-in-india-constitutional-basis-and-implications-on-modern-issues>
4. Dixit, A. (2026). *Data protection in India after the digital personal data protection act, 2023: a critical evaluation of privacy and state power*. <https://doi.org/10.65393/ldeo6679>
5. Ijfmr. (2025a). E-ISSN: 2582-2160 • Website: www.ijfmr.com • Email: editor@ijfmr.com.
6. Ijfmr. <https://www.ijfmr.com/papers/2025/6/59991.pdf>
7. Jindal, T. (n.d.). Unknown title. <https://doi.org/10.36948/ijfmr.2024.v06i06.31832>
8. Mahajan., & Gaurav. (2026). India's emerging data protection framework : A critical analysis of legal reform and global interoperability. *Journal of Data Protection & Privacy*. <https://doi.org/10.69554/XLLB8520>
9. Collaco., & Michelle, A. (2025). The Illusion of Choice: Re-imagining digital consent in India through a feminist lens. *Journal of Data Protection & Privacy*. <https://doi.org/10.69554/KIHH4415>
10. Tyagi, R. D., & Dutt, O. (n.d.). Unknown title. <https://doi.org/10.36948/ijfmr.2026.v08i01.67398>
11. Ramaswamy, Samyukta (2024) "The Evidence Machine: Rethinking Admissibility and Privacy in India's AI Surveillance State," *Indian Journal of Law and Technology*: Vol. 20: Iss. 2, Article 4.
12. Ijfmr. (2025a). E-ISSN: 2582-2160 • Website: www.ijfmr.com • Email: editor@ijfmr.com. Ijfmr. <https://www.ijfmr.com/papers/2025/3/48656.pdf>
13. Verma, A., Mittal, B., & Bala, A. (n.d.). Unknown title. <https://doi.org/10.36948/ijfmr.2025.v07i05.58572>

14. https://www.researchgate.net/publication/399837145_Evolving_Jururisprudence_of_Digital_Privacy_A_Comparative_Study_of_Global_Data_Protection_Frameworks
15. 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>
16. Madaan, A. M., & Mohanty, A. (2025). Identity Theft in the Digital Age: Legal Challenges and the Evolving Role of Law Enforcement in India. *Cyber Law Reporter*. <https://doi.org/10.55662/CYLR.2025.4102>
17. Yadav, E., & Khanna, P. G. (n.d.). Unknown title. <https://doi.org/10.36948/ijfmr.2025.v07i06.59991>
18. N, S. K. J., & N, M. (n.d.). Unknown title. <https://doi.org/10.36948/ijfmr.2025.v07i02.40059>
19. Saha, S., & Mukhopadhyay, S. (2024). A New Age of Data Privacy Laws in India: Review of Digital Personal Data Protection Act, 2023. *International Journal of Law and Social Sciences*. <https://doi.org/10.60143/ijls.v10.i1.2024.114>
20. Singh., Pushpit., Simon., & Tomy, S. (2025). Personal data monetisation model in India : Reimagining the contours of the Digital Personal Data Protection Act, 2023 through a market-oriented approach analysis. *Journal of Data Protection & Privacy*. <https://doi.org/10.69554/XDRR7205>
21. Kaur, D., & Nath, A. (n.d.). Unknown title. <https://doi.org/10.63363/aijfr.2025.v06i05.1462>
22. Satyavati Rajesh Khaladkar (2025). Right to Privacy for Women: Legal Framework and Social Imperatives *TTASSH*. 5(3), 1-6. doi.org/10.36647/TTASSH/05.03.A001.
23. PRIVACY VIS-À-VIS TRANSPARENCY: RECONCILING THE RIGHT TO INFORMATION ACT, 2005 WITH THE DIGITAL PERSONAL DATA PROTECTION ACT,
24. 2023 – Indian Journal of Legal Review [ISSN – 2583-2344] (n.d.). Doi. <https://doi.org/10.65393/GMEO4129>
25. Singh, R., & Singh, V. (2024). Beyond Consent: Ensuring Meaningful Protection of Genetic Data Under India's Digital Personal Data Protection Act, 2023. *Journal of Indian Academy of Forensic Medicine*, 46(4), 562–567. <https://doi.org/10.1177/09710973251328785>
26. Singh, S., & Kumar, D. A. (2026). THE RIGHT TO PRIVACY AND THE DIGITAL ECONOMY: AN EXAMINATION OF THE IMPACT OF INDIA'S DATA PROTECTION
27. REGIME ON E-COMMERCE AND FINTECH. *EPRA International Journal of Research & Development (IJRD)*. <https://doi.org/10.36713/epra25992>
28. Annappa, N. (2022). The State's access to data and internet intermediary response – an assessment of India's attempt to reallocate the legal framework to ensure national security. *International Review of Law, Computers & Technology*, 36(3), 404–430. <https://doi.org/10.1080/13600869.2022.2030038>
29. Abraham., Mariyan, M., Dev., & Shampa. (2025). AI-driven surveillance in India: Reconciling privacy, national security and legal oversight. *Journal of Data Protection & Privacy*. <https://doi.org/10.69554/BZBZ5748>