DATA PROTECTION AND PRIVACY IN CYBERSPACE: LEGAL CHALLENGES IN INDIA

Simran Najmal, St. Joseph's College of Law, Bangalore

ABSTRACT

The rapid expansion of digital technologies in India has intensified concerns surrounding data protection and informational privacy, necessitating a robust legal framework to safeguard individual rights in cyberspace. The recognition of the right to privacy as a fundamental right by the Supreme Court in *Justice K.S. Puttaswamy (Retd.) v. Union of India* marked a constitutional turning point, compelling legislative action in the realm of personal data protection. Against this backdrop, the Digital Personal Data Protection Act, 2023 (DPDP Act) was enacted with the objective of regulating the processing of digital personal data and institutionalising privacy protections. This paper undertakes a critical doctrinal analysis of the DPDP Act to examine whether it effectively translates the constitutional mandate of privacy into enforceable statutory safeguards. The study analyses key provisions relating to consent, cross-border data transfers, institutional enforcement mechanisms, and government exemptions. It argues that despite its progressive intent, the Act suffers from significant structural deficiencies, including broad state exemptions, ambiguous transfer frameworks, and limited independent oversight. These shortcomings, when read alongside existing surveillance laws, create constitutional concerns regarding proportionality and accountability. By comparing the DPDP Act with international standards such as the GDPR, the paper highlights regulatory gaps that undermine individual autonomy and privacy. The study concludes that while the DPDP Act represents an important legislative advancement, substantive reforms are required to ensure effective protection of privacy rights in India's evolving digital ecosystem.

Keywords: Digital Personal Data Protection Act, 2023; Right to Privacy; State Surveillance; Cross-Border Data Transfers; Institutional Oversight.

Introduction

The rapid proliferation of digital technologies has positioned India as a major global player in the digital economy, fostering innovation but simultaneously escalating the challenges associated with data protection and individual privacy.[1] As digital platforms—ranging from social media and banking applications to government services—collect, process, and transfer massive volumes of personal data, the necessity for a robust legal framework has become paramount.[2] Recognizing this global trend and spurred by domestic judicial mandates, India has embarked on a legislative journey aimed at transitioning from a fragmented regulatory system to a comprehensive data protection regime.[3] This process culminated in the enactment of the Digital Personal Data Protection Act, 2023 (DPDP Act).[4] This research paper conducts a critical, doctrinal analysis of this shift, identifying the inherent legal challenges that undermine the realization of constitutionally mandated privacy rights within India's cyberspace.[1]

1.2. Existing Legal Situation

The Constitutional Foundation

The legal status of privacy in India underwent a transformative change with the landmark decision of the Supreme Court in *Justice K. S. Puttaswamy (Retd.) v. Union of India*.[5] A nine-judge bench unanimously held that the right to privacy is a constitutionally protected fundamental right, deeply entrenched in Article 21 (the Right to Life and Liberty) of the Constitution of India.[6] This judgment established a fundamental benchmark: any state action infringing upon privacy must satisfy the rigorous test of proportionality, ensuring it is grounded in law, serves a legitimate aim, employs the least restrictive means, and is balanced appropriately.[7]

The Pre-2023 Patchwork

Prior to the DPDP Act, India's data protection framework was largely confined to the

5 Justice K. S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
6 *Id.* at 405 (stating that the right to privacy is an intrinsic part of Article 21).
7 *Id.* at 414.
8 Information Technology Act, 2000, No. 21 of 2000, INDIA ACTS OF PARLIAMENT; Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Ministry of Communications and Information Technology, INDIA.
9 IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, R. 3.
10 Rajagopal, S. & Sharma, A., *India's Privacy Paradox: Analysing the IT Rules, 2011*, 8 J. LEGAL STUD. 33, 40 (2018).

Information Technology Act, 2000 (IT Act), and the subordinate Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules).[8] This regime focused narrowly on sensitive personal data or information (SPDI), including passwords, financial data, and health information.[9] Critically, the framework was often criticized for being reactive and limited in scope, lacking the comprehensive, rights-based architecture necessary to address modern data processing complexities. Consent under the SPDI Rules was often governed by ambiguous contract law principles rather than the specific, rights-based requirements of contemporary data protection law.[10]

1.3. Research Problem

The central legal challenge in India's data protection regime resides in the fundamental friction between the expansive, rights-based constitutional guarantee established by the *Puttaswamy* ruling and the specific mechanisms codified in the DPDP Act, 2023. Specifically, the legislation grants broad exemptions to government agencies for data processing, relies on ambiguous terms like "deemed consent," and subjects vital regulatory mechanisms, such as cross-border data transfer, to executive discretion. This legislative structure raises concerns about whether the DPDP Act sufficiently upholds the constitutional mandate of proportionality, particularly in contexts involving state surveillance and accountability mechanisms.

1.4. Hypothesis

The Digital Personal Data Protection Act, 2023 inadequately safeguards individual privacy due to expansive state exemptions, regulatory ambiguities, and weak enforcement mechanisms.

1.5. Research Questions

The study is guided by the following three research questions:

1. **Constitutional Foundations and Statutory Evolution**

How effectively does the DPDP Act, 2023 codify the constitutional right to privacy established in *K.S. Puttaswamy v. Union of India*, and what critical legal lacunae persist from the previous IT Act, 2000 regime?

2. **Regulatory Gaps and Implementation Challenges**

What are the primary regulatory and structural challenges—including those related to defining consent, regulating cross-border data flows, and establishing the Data Protection Board—that undermine the practical enforcement of the DPDP Act, 2023?

3. **State Surveillance and Proportionality Review**

To what extent do the broad exemptions for government processing under the DPDP Act and existing surveillance laws (e.g., IT Act, Section 69) contravene the constitutional requirement of proportionality, and what mechanisms for judicial or independent oversight are critically absent?[2]

1.6. Scope and Objectives

The scope of this study is focused exclusively on the legal and constitutional analysis of the protection of *digital* personal data within the jurisdiction of India. The primary objective is to conduct a doctrinal assessment of the DPDP Act, 2023, by systematically comparing its key provisions against the constitutional standard of proportionality mandated by the Supreme Court. Furthermore, the study aims to identify existing gaps in institutional enforcement and recommend necessary legislative harmonization, particularly concerning surveillance laws.

1.7. Research Methodology

This research employs a doctrinal legal methodology, involving systematic analysis of primary legal sources (the Constitution of India, the IT Act, 2000, and the DPDP Act, 2023) and secondary sources, including judicial interpretations, academic journals, and legal commentaries.[11] A critical comparative analysis is performed, benchmarking the Indian legal framework against international standards, such as the EU's General Data Protection Regulation (GDPR), to highlight regulatory strengths and weaknesses.[3]

11S. R. Ranganathan, Doctrinal Legal Research: Method and Scope, 25 Law Q. 1, 5 (1988).
12 [12] Justice K. S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
[13] Dr. Srinivas Katkuri, A Critical Analysis of the Digital Personal Data Protection Act, 2023, 11 I NT'L J. L. 22, 23 (2025).
[14] Vrinda Bhandari & Karan Lahiri, The Surveillance State: Privacy and Criminal Investigation, 3 U. OXF. HUM. RTS. J. 1, 1 (2021).
[15] Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).
[16] Justice K. S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

1.8. Literature Review

Scholarly literature reviewed for this analysis spans three key areas. The first involves the constitutionalization of privacy, centering on the profound impact of *Puttaswamy* in transforming privacy from a derivative right to an independently enforceable fundamental right.[12] The second body of work focuses on the critical assessment of the DPDP Act, examining its provisions regarding consent, cross-border data transfer, and the establishment of the Data Protection Board (DPB).[13] The third area critiques the existing legal basis for state surveillance, scrutinizing the extent to which executive authorization aligns with constitutional principles of necessity and proportionality.[14]

1.9. Limitations

A primary limitation of this study stems from the nascent status of the DPDP Act, 2023. While the Act has been notified, its operationalization is phased, with many critical sections—including enforcement timelines and the full establishment of the Data Protection Board—subject to subordinate rules yet to be fully framed and enacted.[15] [4]Consequently, the analysis relies heavily on statutory interpretation and scholarly projection of the Act's practical implications, as concrete jurisprudence and enforcement history remain absent.

The Constitutional Foundation and Legislative Evolution (Addressing RQ I)

2.1. The Judicial Mandate and the Right to Informational Privacy

2.1.1. *Puttaswamy* and Privacy as an Inherent Right

The *K.S. Puttaswamy v. Union of India* judgment fundamentally redefined the relationship between the state and the individual's personal data. The Supreme Court recognized privacy as extending beyond physical space to include "informational privacy," acknowledging that an individual possesses a right to control the dissemination and use of their personal data.[16] This recognition was essential for addressing the challenges posed by the modern digital age, where personal data is constantly collected and processed.

2.1.2. Establishing the Proportionality Doctrine

Central to the *Puttaswamy* decision was the establishment[5] of the doctrine of proportionality as the yardstick against which all invasions of the fundamental right to privacy must be measured.[17] The Court stipulated a four-pronged test: first, the restriction must be sanctioned by law; second, it must pursue a legitimate aim of the State; third, it must be necessary for achieving that aim; and fourth, it must employ means that are proportional to the objective sought, ideally choosing the least intrusive method.[18] This doctrinal toolkit serves as the constitutional filter for assessing the legality and validity of all subsequent privacy legislation, including the DPDP Act.

2.2. The Inadequacies of the Previous Regime

The prior regime, anchored in the Information Technology Act, 2000, and the SPDI Rules, was widely considered deficient. These laws applied primarily to corporate bodies handling specific categories of data, such as passwords and health records.[19] The criticism focused on the fact that this framework was based on limited statutory provisions (Section 43A of the IT Act) and addressed data breaches through compensation rather than establishing comprehensive data subject rights and accountability obligations.[20] Furthermore, the lack of a clear, high standard for informed consent meant that data processing was often governed by vague contractual provisions, failing to guarantee autonomy to the individual Data Principal.[21]

2.3. Analysis of the Digital Personal Data Protection Act, 2023

2.3.1. Scope and Applicability

The Digital Personal Data Protection Act, 2023, represents a decisive move toward a comprehensive data protection law, replacing the disparate rules that preceded it.[22] The Act is structured around the obligations of the Data Fiduciary (equivalent to a data controller) and the rights and duties of the Data Principal (the individual whose data is processed).[23] The Act

[17] Id.
[18] Id.
[19] Information Technology (Reasonable security practices and procedures and sensitive personal data or Information) Rules, 2011, cl. 3 (India).
[20] S. Katkuri, supra note 13, at 23.
[21] M.P. Sharma, supra note 10, at 115.
[22] Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).
[23] Id.
[24] Id.
[25] Prabhash Dalei, The Digital Personal Data Protection Act, 2023: A Legal Analysis in Light of Global Data Protection Standards, 11 I NT'L J. L. 1, 5 (2025).

possesses clear extraterritorial reach, applying to the processing of digital personal data outside India if that processing relates to the offering of goods or services to Data Principals within India.[24]

2.3.2. Limitation to Digital Data

A notable feature, and a key point of legal debate, is the Act's restrictive scope: it applies solely to digital personal data—either data collected digitally or physical data subsequently digitized.[25] Furthermore, the Act explicitly excludes personal data that is already publicly available either by the Data Principal or by any other person under a legal obligation to make that data public.[26] This limited scope creates a dual standard of protection. If the right to privacy, as established by the Supreme Court, is inherently linked to human dignity and applies universally, the statutory protection should not cease merely because data exists in a physical form or is legally accessible through other means, such as the Right to Information Act.[27] This suggests a legislative prioritization of regulating the digital economy and simplifying administrative compliance over providing holistic constitutional protection, exposing non-digitized data and legally public data to lesser safeguards.

2.3.3. Codification of Rights and Duties

The DPDP Act establishes specific rights for Data Principals, including the right to access information, the right to correction and erasure, and the right to grievance redressal.[28] Correspondingly, it imposes duties on Data Fiduciaries, mandating lawful processing, adherence to security safeguards, and transparency regarding data usage.[29]

Critical Analysis: DPDP Act and the Regulatory Lacunae (Addressing RQ II)

3.1. The Dilution of Consent and the Role of 'Legitimate Uses'

3.1.1. The Standard of Consent

The DPDP Act mandates that consent for data processing must be free, informed, specific, unambiguous, and accompanied by the right for the Data Principal to withdraw consent at any time.[30] Data Fiduciaries must provide clear privacy notices specifying the purposes for collection.[31]

3.1.2. The Introduction of 'Deemed Consent' and Legal Base[6]s

A significant structural departure from globally established data protection regimes is the reliance on "Legitimate Uses" (Section 7), which permits processing without the explicit consent of the Data Principal under specified circumstances.[32] These circumstances include compliance with legal or judicial obligations, providing medical treatment or health services during an epidemic, addressing employment needs, and securing public order.[33] This concept is often equated with "deemed consent" in legal discourse, allowing for processing that facilitates easier administration and provision of services, presenting a flexible, state-centered paradigm.[34]

However, the DPDP Act notably omits standard legal bases found in comparable global frameworks like the GDPR, specifically "Contractual Necessity" and "Legitimate Interests."[35] Excluding "Legitimate Interests" deprives Data Fiduciaries of a common and flexible tool for justifying commercial processing that does not strictly rely on explicit consent but where balancing tests confirm the low risk to privacy. By relying primarily on explicit consent and vague "legitimate uses," the DPDP Act creates an imbalance: it is simultaneously too restrictive on businesses (lacking a common commercial processing basis) and too broad on state functions (using "legitimate uses" and "deemed consent" to cover state needs).[36] This structural choice is viewed as reflecting a state-centric bias in the legislative design, potentially subjecting essential commercial and administrative activities to less transparent legal justifications.

3.2. Institutional Shortfalls and Enforcement Weaknesses

3.2.1. Operationalizing the Data Protection Board (DPB)

The enforcement mechanism of the DPDP Act relies heavily on the establishment of the Data Protection Board of India (DPB). While sections pertaining to the appointment of the DPB chairperson and members have come into force immediately, the majority of compliance

[26] Id. at 6.
[27] Id. at 7.
[28] S. Katkuri, supra note 13, at 24.
[29] Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).
[30] S. Katkuri, supra note 13, at 24.
[31] Hogan Lovells, India's Digital Personal Data Protection Act 2023 Brought into Force, H OG. LOV. (Aug. 2023).
[32] Digital Personal Data Protection Act, 2023, § 7, No. 22, Acts of Parliament, 2023 (India).
[33] Id.
[34] M. Singh, The DPDPA and the 'Deemed Consent' Paradigm, 15 I NT'L J. L. 51, 55 (2024).

provisions (such as those concerning notice and consent) are subject to a phased implementation, with timelines extending up to 18 months from the date of notification.[37] This tiered approach grants the ecosystem necessary preparation time but simultaneously creates an immediate implementation challenge, as the enforcement body's full operational capacity is crucial for guiding compliance efforts and ensuring accountability.[38]

3.2.2. The Accountability Gap in Record-Keeping

A significant omission in the DPDP Act, when compared to international standards like the GDPR, is the lack of a mandatory obligation for Data Fiduciaries to maintain detailed records of their data processing activities.[39] The GDPR explicitly requires both controllers and processors to maintain such logs to ensure transparency and aid regulatory investigations.[40] The absence of a similar record-keeping mandate in the DPDP Act compromises the DPB's investigative capacity. Accountability—a core stated principle of the DPDP Act—cannot be reliably enforced if the underlying mechanisms required for proving compliance, such as systematic processing documentation, are not legally required. While this may reduce [7]administrative burdens for companies, it introduces a major transparency deficit and increases risk exposure for Data Principals.[41]

3.2.3. Financial Penalties

To ensure deterrence, the DPDP Act includes provisions for significant financial penalties, with fines for serious failures to protect data reaching up to ₹250 crore (approximately $28 million) per contravention.[42] This penalty structure, while high, is generally considered less severe compared to the maximum penalties imposed by the GDPR.[43]

3.3. Cross-Border Data Flows and Digital Sovereignty

The DPDP Act permits the transfer of personal data outside India, subject to restrictions that the government may impose by way of notification.[44] This approach contrasts sharply with

[35] Hogan Lovells, supra note 31.
[36] Id.
[37] Pavan Duggal, Digital Personal Data Protection Rules 2025 Explained, I NDIAN EXPRESS (Nov. 2025).
[38] Latham & Watkins, India's Digital Personal Data Protection Act 2023 vs. the GDPR: A Comparison, L ATHAM & W ATKINS (Dec. 2023).
[39] P. Dalei, supra note 25, at 8.
[40] Id.
[41] Id.

previous draft proposals that mandated data localization (maintaining a "serving copy" in India) and empowered the government to declare certain categories of data as "critical personal data," prohibiting cross-border transfer entirely.[45]

Critique of Executive Discretion[8]

The current reliance on unilateral executive notification for permitting or restricting data transfers is a major source of legal uncertainty.[46] Globally, decisions on cross-border flows are typically made based on legislative guidelines regarding "reciprocity" or "adequacy" (the presence of comparable safeguards in the destination country).[47] The DPDP Act remains silent on these substantive considerations, delegating "unchecked power" to the executive branch.[48] Submitting decisions on cross-border data flows entirely to executive discretion introduces profound legal and operational uncertainty for global Data Fiduciaries and subjects the fundamental right to informational privacy to the shifting priorities of data diplomacy, thereby risking the transfer of data to jurisdictions with inadequate or weak data protection standards.[49]

Feature	India's DPDP Act (2023)	EU's GDPR (2018)	Regulatory Challenge
Legal Basis for Processing	Consent and limited "Legitimate Uses" (e.g., state functions, medical emergency)[1]	Six lawful bases including Contractual Necessity and Legitimate Interests	Rigidity and state-centric nature of legal bases limits flexibility for common commercial/processing activities.
Data Types Covered	Digital Personal Data only. Excludes publicly available data by law [3]	Personal Data (digital and hard copy)	Leads to inconsistent protection levels, potentially contradicting the constitutional mandate for holistic privacy protection.
Record Keeping of Processing	No explicit mandate for Data Fiduciaries to maintain records	Mandates Controllers and Processors to	Severely impedes the Data Protection Board's ability to

[42] Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).
[43] Global Network Initiative, DPDP Act 2023: Key Provisions and Criticisms, G NI. ORG. (July 2023).
[44] Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).
[45] Malavika Raghavan, Cross-Border Data Flows and India's Digital Sovereignty, V ERFASSUNGSBLOG (Sept. 2023).
[46] P. Dalei, supra note 25, at 7.
[47] M. Raghavan, supra note 45.
[48] Id.
[49] Id.

Feature	India's DPDP Act (2023)	EU's GDPR (2018)	Regulatory Challenge
	of processing activities [4]	maintain detailed records	monitor compliance and investigate breaches transparently.
Cross-Border Transfer	Permitted to notified countries; relies heavily on executive discretion [5]	Requires "Adequacy Decisions" based on comparative safeguards	High executive discretion introduces political uncertainty and risks transferring data to weak protection regimes.

The Legal Status of State Surveillance and Exemptions (Addressing RQ III)[9]

4.1. The Surveillance Framework: A Statutory Conflict

4.1.1. Existing Interception Powers

State surveillance in India is governed by two principal, overlapping statutes: the archaic Indian Telegraph Act of 1885 (regulating the interception of traditional communications) and Section 69 of the Information Technology Act, 2000.[50] Section 69 grants sweeping authority to the Central or State Governments to intercept, monitor, or decrypt *any* information transmitted, stored, or received in *any computer resource*.[51] These powers can be invoked on broad grounds, including the interests of the sovereignty and integrity of India, the security of the State, public order, and preventing incitement to the commission of an offense.[52]

4.1.2. The Overlap and Maximization of Discretion

The IT Act expanded surveillance authority by regulating interception on a "computer resource" (which includes computers and individual devices), whereas the Telegraph Act focuses on "telegraphs" (transmission devices).[53] This overlap is particularly critical concerning mobile phones, which are classified under both statutes.[54] The existence of two parallel interception regimes allows the state to choose the legal route offering the highest degree of executive flexibility and the lowest level of scrutiny. This maximization of executive

[50] Indian Telegraph Act, 1885, No. 13, Acts of Parliament, 1885 (India).
[51] Information Technology Act, 2000, § 69, No. 21, Acts of Parliament, 2000 (India).
[52] Indian Telegraph Act, 1885, No. 13, Acts of Parliament, 1885 (India).
[53] Global Network Initiative, supra note 43.
[54] Id.
[55] Dr. Rumi Dhar & Ms. Sonia Nath, Digital Surveillance and Civil Rights, 2 I JCNLU 41, 45 (2025).

discretion significantly undermines the constitutional safeguard that requires restrictions on privacy to be narrowly tailored and subject to clear legal procedures.

4.1.3. Apparatus of Mass Surveillance

The broad statutory powers have facilitated the normalization of digital monitoring through sophisticated government systems.[55] Agencies utilize instruments like the Central Monitoring System (CMS), which monitors calls, text messages, and online activity, and the Advanced Application for Social Media Analytics (AASMA), which collects live user data, conducts sentiment analysis, and tracks locations.[56] This shift toward mass surveillance, often undertaken without statutory basis or external oversight,[10] poses an alarming threat to civil liberties and the right to expression, often resulting in a chilling effect.[57]

4.2. Government Exemptions in the DPDP Act

4.2.1. The National Security and Public Interest Carve-outs

Section 17 of the DPDP Act explicitly grants substantial exemptions to government entities.[58] Specifically, it permits government agencies to bypass core obligations regarding consent, notice, and Data Principal rights when processing personal data for purposes such as national security, law enforcement, investigation, and maintaining public order.[59]

The expansive nature of these national security and public interest carve-outs means that government entities can effectively disregard the fundamental data protection requirements that commercial entities must follow.[60] The legislative structure, therefore, implies that the state is statutorily insulated from the constitutional requirement of protecting privacy whenever it asserts a claim of "public interest" or national security. This grants government processing blanket immunity, undermining the integrity of the rights framework established by the Act itself.

---

[56] A. Sharma, The New Normal: Digital Surveillance in India, 10 G IGA F OCUS 1, 3 (2024).
[57] Id.
[58] Digital Personal Data Protection Act, 2023, § 17, No. 22, Acts of Parliament, 2023 (India).
[59] P. Dalei, supra note 25, at 9.
[60] Id.
[61] Justice K. S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
[62] V. Bhandari & K. Lahiri, supra note 14, at 3.
[63] Id. at 5.
[64] Id. at 1.

4.2.2. The Proportionality Deficit

These broad statutory exemptions critically fail to satisfy the Proportionality Doctrine laid out in *Puttaswamy*.[61] The doctrine requires that the state employ the *least intrusive means* necessary to achieve its legitimate aim.[62] Granting wide, unspecified statutory immunity—which allows government agencies to conduct data processing and surveillance without mandatory consent or notice—is demonstrably the *most* restrictive and intrusive means available. Legal analysis suggests that the vagueness and generality of these exemptions contravene the 'necessity' and 'balancing' limbs of the proportionality test, creating a constitutional deficit where executive discretion supersedes constitutional rights.[63]

4.3. Judicial Oversight and the Erosion of the Rule of Law

4.3.1. Absence of Independent Oversight

A defining legal challenge in India's surveillance regime is the severe lack of independent inter-branch oversight.[64] Currently, the authority to authorize surveillance under the Telegraph Act and IT Act rests almost entirely with the executive branch. There is no statutory requirement for mandatory pre-interception judicial authorization or warrants, which would serve as a critical counterweight to executive power.[65] This concentration of power increases the risk of disproportionate state action, misuse, and subsequent rights violations, moving India toward a rights-restrictive "surveillance democracy."[66]

4.3.2. The Chilling Effect

The history of misapplication of existing laws underscores the dangers of unchecked executive power. For instance, despite the Supreme Court repealing [11]Section 66A of the IT Act in 2015, police continued to use it for unconstitutional arrests related to social media posts.[67] Similarly, Section 69A has been used extensively for content moderation and website blocking.[68] When surveillance functions and data interception powers are perceived as opaque and easily deployable, they generate a profound chilling effect on freedom of expression and dissent in

[65] Id. at 6.
[66] A. Sharma, supra note 56, at 1.
[67] Id.
[68] Id.
[69] Id.

the digital public sphere.[69]

Statute/Instrument	Authorization Scope	Constitutional Challenge	Judicial Oversight Status
Indian Telegraph Act, 1885	Interception of communications for national security/public order [6]	Archaic, prone to over-breadth, and disproportionate application in the digital age.	Executive authorization; criticized for lacking independent judicial review. [8]
Information Technology Act, 2000 (S. 69)	Monitoring/decryption of any information on any computer resource [7]	Grants vast power across all digital platforms; constitutionality challenged post-*Puttaswamy*. [10]	Executive discretion; pending Supreme Court adjudication on proportionality. [10]
DPDP Act, 2023 (Section 17 Exemptions)	Bypassing consent/notice requirements for national security/law enforcement [11]	Fails the 'necessity' limb of the *Puttaswamy* proportionality test by granting broad, unspecified immunity.	Minimal, relying on post-facto review; significantly weakens regulatory efficacy.

Chapter 5: Jurisdictional Dilemmas and Future Reform Pathways

5.1. Transnational Data Governance and Enforcement

5.1.1. Extraterritorial Application

Both the IT Act and the DPDP Act assert extraterritorial jurisdiction. The IT Act grants Indian law enforcement authority to prosecute cybercriminals operating outside India if the offense involves electronic resources within the country.[70] Similarly, the DPDP Act applies to [12]data

[70] Information Technology Act, 2000, § 75, No. 21, Acts of Parliament, 2000 (India).
[71] Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).
[72] R. Pandey, supra note 11, at 554.
[73] Dr. K. Verma, Why We Need Data Protection Laws for AI in India, 1 D EFACTO L. J. 1, 2 (2024).
[74] S. Katkuri, supra note 13, at 25.
[75] Dr. K. Verma, supra note 73, at 3.
[76] Id.
[77] V. R. Mistry, The DPDPA, 2023 and Challenges in the Medical Ecosystem, 1 P. MED. CARE 1, 2 (2025).
[78] Id.
[79] Id. at 1.

[13]processing outside India if it relates to offering goods or services to Data Principals in India.[71] This necessary extraterritoriality creates transnational jurisdictional complexities.

5.1.2. The Need for International Cooperation

The rise of transnational cybercrimes and data breaches necessitates clear legal mechanisms for international cooperation. The current framework does not comprehensively articulate how India will address complex jurisdictional hurdles or utilize instruments like Mutual Legal Assistance Treat[14]ies (MLATs) to effectively prosecute offenses involving foreign actors.[72] Clarity on international agreements is crucial for ensuring that the DPDP Act's provisions can be enforced against global entities.

5.2. Regulating Advanced Technologies (AI and Health Data)

5.2.1. The AI Gap

The proliferation of Artificial Intelligence (AI) and automated decision-making systems presents unique privacy risks, including algorithmic bias, opaque processing, and lack of transparency.[73] While the DPDP Act addresses broad personal data handling, it is largely silent on specific regulatory mechanisms for AI technologies.[74] There is an absence of direct provisions regulating algorithmic bias, ensuring transparency, or mandating explainability (the right to an explanation for automated decisions)—safeguards prominently featured in the GDPR.[75] This limits the law's ability to "future-proof" privacy protection and ensure algorithmic accountability in rapidly evolving sectors like fintech and criminal investigation.[76]

5.2.2. Health Sector Ambiguities

Healthcare data constitutes sensitive personal data requiring high security measures.[77] Digital health, encompassing telemedicine and electronic health records, is rapidly expanding.[78] However, the DPDP Act's implications for medical personnel and the healthcare ecosystem remain ambiguous.[79] Although the Act provides exceptions for processing related to medical treatment during an epidemic,[80] the general implementation of the DPDP Act on clinicians and digital health platforms needs specific amendments and subordinate rules to ensure that providers can discharge their duties efficiently without being unduly burdened by the threat of litigation.[81]

[80] Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

5.3. Recommendations for Legislative Harmonization and Judicial Activism

5.3.1. Surveillance Reform

The most crucial requirement for harmonizing statutory law with the *Puttaswamy* constitutional mandate is the overhaul of the existing surveillance framework. The fragmented regime under the Indian Telegraph Act and Section 69 of the IT Act must be repealed and replaced with a single, technology-neutral **Surveillance Act**.[82] This new statute must fundamentally incorporate the Proportionality Doctrine by mandating *ex-ante* judicial authorization—a prerequisite judicial warrant—for all forms of interception, monitoring, or decryption of data.[83] This would provide the necessary independent inter-branch oversight currently lacking.

5.3.2. Amending the DPDP Act for Balance

To ensure the DPDP Act is effective and constitutional, specific legislative adjustments are necessary:

- **Narrowing Exemptions:** Section 17, concerning government exemptions, must be refined through subordinate rules to specify legitimate purposes narrowly and introduce mandatory independent review mechanisms for state data processing that bypasses consent.[84]
- **Institutional Accountability:** Legislative mandates must be introduced requiring Data Fiduciaries to maintain comprehensive records of processing activities, thereby enhancing transparency and bolstering the DPB's investigative capacity.[85]
- **Addressing the AI Gap:** The government must introduce specific rules to regulate automated decision-making, profiling, and algorithmic bias, incorporating principles of transparency, explainability, and the r[15]ight to human intervention.

5.3.3. Judicial Role

The judiciary holds a vital role in preserving the rule of law and acting as a counterweight

[81] V. R. Mistry, supra note 77, at 4.
[82] V. Bhandari & K. Lahiri, supra note 14, at 7.
[83] Id.
[84] P. Dalei, supra note 25, at 10.
[85] Id.
[86] V. Bhandari & K. Lahiri, supra note 14, at 1.
[87] Id. at 8.

against executive overreach.[86] Continued judicial vigilance, leveraging the rigorous standard of proportionality established in *Puttaswamy*, is essential to challenge vague statutory exemptions and administrative actions that infringe on privacy, ensuring that constitutional rights are genuinely preserved in cyberspace.[87]

Conclusion

The enactment of the Digital Personal Data Protection Act, 2023, is an indispensable legislative step that officially codifies India's commitment to the fundamental right to privacy established by the Supreme Court. The Act addresses many lacunae of the previous regime by defining rights, duties, and accountability standards, and by introducing substantial financial penalties.

However, the analysis confirms the central hypothesis: the efficacy of the DPDP Act in safeguarding privacy is fundamentally limited by significant statutory compromises. Specifically, the regulatory framework suffers from structural weaknesses, including the reliance on ambiguous 'deemed consent' mechanisms, institutional deficits such as the lack of mandatory processing records, and a transfer mechanism highly dependent on executive discretion.

Most critically, the persistence of broad, unchecked surveillance powers under existing laws and the expansive exemptions granted to government agencies under the DPDP Act itself create a profound constitutional friction. These broad carve-outs allow the state to bypass core data protection principles without mandatory independent oversight, thereby failing to satisfy the 'necessity' and 'least restrictive means' requirements of the Proportionality Doctrine. India has successfully achieved the *recognition* of the right to privacy, but the effective *safeguarding* of this right remains incomplete due to these legislative and institutional deficits.

Suggestions:

To genuinely safeguard fundamental privacy rights in India's cyberspace and align statutory law with constitutional requirements, comprehensive structural reforms are urgently necessary. This requires: (1) the immediate enactment of a consolidated, rights-centric Surveillance Act that mandates *ex-ante* judicial authorization for all interception activities; (2) the issuance of subordinate rules under the DPDP Act that narrowly define and constrain government exemptions (Section 17) through mandatory proportionality safeguards; and (3) legislative strengthening of the Data Protection Board's independence and accountability mechanisms, including mandating record-keeping for all Data Fiduciaries.