International Journal of Creative and Open Research in Engineering and Management
ISSN: 3108-1754 (Online)
Volume 02 Issue 09 September-2026 | Impact Factor: 3.5

The Evolving Jurisprudence of Data Protection and Privacy in India: A Critical Analysis of the Digital Personal Data Protection Act, 2023

Author: **Satish Kumar Dodiya**
Affiliation: Aurora University, Second Year LL.B.
Date: September 2026

How to Cite this Article:

Dodiya, S. K. (2026). The Evolving Jurisprudence of Data Protection and Privacy in India: A Critical Analysis of the Digital Personal Data Protection Act, 2023. International Journal of Creative and Open Research in Engineering and Management, 02(9), 1-9. https://doi.org/10.55041/ijcope.v2i9.166

https://doi.org/10.55041/ijcope.v2i9.166

ABSTRACT

The enactment of the Digital Personal Data Protection Act, 2023 (DPDP Act) marks a watershed moment in India's data protection jurisprudence, codifying the fundamental right to informational privacy recognised in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017). This paper provides a critical, chapter-wise analysis of the DPDP Act, examining its structural framework, the rights of data principals, the obligations of data fiduciaries, and the institutional architecture of the Data Protection Board of India. While the Act introduces a principles-based regime aligned with global standards—including consent as the cornerstone of lawful processing, purpose limitation, data minimisation, and stringent penalties up to ₹250 crore—it faces substantial criticism for legislative minimalism, expansive state exemptions under Section 17 on national security and public order grounds, and the absence of robust safeguards against automated decision-making and profiling. Through doctrinal analysis and comparative evaluation against the EU GDPR, this study identifies key deficiencies including excessive executive discretion, dilution of consent through "legitimate uses," and the omission of data portability rights. The paper concludes with recommendations for legislative amendments to strengthen judicial oversight, narrow state exemptions, and enhance data principal rights, ensuring the DPDP Act fulfils its constitutional promise of balancing technological advancement with the fundamental right to privacy.

Keywords: Data Protection, Privacy, DPDP Act 2023, Puttaswamy Case, Informational Privacy, Data Fiduciary, Data Principal, State Exemptions, India

CHAPTER I: INTRODUCTION

1.1 Background and Context

The digital revolution has fundamentally transformed how personal data is collected, stored, processed, and monetised. In India, the proliferation of digital services—from Aadhaar-based authentication to e-commerce platforms, social media, and fintech applications—has resulted in the unprecedented datafication of everyday life. This transformation, while enabling technological innovation and economic growth, has simultaneously exposed individuals to significant privacy risks, including unauthorised data collection, profiling, surveillance, and data breaches.

Prior to 2023, India's data protection framework was fragmented and inadequate, primarily governed by Section 43A of the Information Technology Act, 2000, and the accompanying Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules). These provisions

imposed limited obligations on body corporates to implement "reasonable security practices" and provided compensation for negligence in protecting sensitive personal data. However, the regime lacked comprehensive coverage, failed to recognise individual rights over personal data, and did not establish an independent regulatory authority.

The constitutional landscape shifted dramatically on 24 August 2017, when a nine-judge Constitution Bench of the Supreme Court unanimously held in *Justice K.S. Puttaswamy (Retd.) v. Union of India* that the right to privacy is a fundamental right protected under Articles 14, 19, and 21 of the Constitution. This landmark judgment established informational privacy as an essential facet of the right to privacy in the digital age, imposing a constitutional obligation on the State to enact comprehensive data protection legislation.

1.2 Research Problem

Despite the constitutional mandate established in *Puttaswamy*, the legislative journey towards comprehensive data protection in India was protracted and contentious. Multiple drafts of the Personal Data Protection Bill were introduced between 2019 and 2022, each facing criticism from stakeholders for various shortcomings including excessive state powers, inadequate safeguards, and compliance burdens. The Digital Personal Data Protection Act, 2023, enacted on 11 August 2023 and brought into force with the notification of the DPDP Rules on 13 November 2025, represents the culmination of this legislative process.

However, the DPDP Act has been subject to intense scholarly and public scrutiny. Critics argue that while the Act ostensibly codifies the right to informational privacy, it contains structural and normative deficiencies that undermine its effectiveness. Key concerns include: (i) legislative minimalism that delegates critical policy decisions to executive rule-making; (ii) expansive exemptions for the State under Section 17 on grounds of national security, public order, and sovereignty without adequate judicial oversight; (iii) the dilution of consent through broad "legitimate uses" exceptions; (iv) the absence of key data principal rights such as data portability; and (v) the lack of robust safeguards against automated decision-making and AI-driven surveillance.

This paper addresses the following research questions:

1. How does the DPDP Act 2023 operationalise the constitutional right to privacy established in *Puttaswamy*?
2. What are the key rights and obligations created under the Act, and how do they compare to global standards such as the EU GDPR?
3. What are the critical deficiencies in the Act's design, particularly regarding state exemptions and executive discretion?
4. What legislative reforms are necessary to strengthen the Act's alignment with constitutional principles and international best practices?

1.3 Objectives of the Study

The primary objectives of this study are:

1. To provide a comprehensive, chapter-wise analysis of the DPDP Act 2023, explaining its structural framework and key provisions.
2. To critically evaluate the rights of data principals and the obligations of data fiduciaries under the Act.
3. To examine the institutional architecture of the Data Protection Board of India and its adjudicatory powers.
4. To identify and analyse the Act's deficiencies, including state exemptions, legislative minimalism, and the absence of key rights.
5. To compare the DPDP Act with the EU GDPR and other global data protection frameworks.

6. To analyse the *Puttaswamy* judgment and its impact on the DPDP Act's constitutional validity.

7. To propose recommendations for legislative reform to enhance the Act's effectiveness and constitutional compliance.

1.4 Research Methodology

This study employs a **doctrinal legal research methodology**, relying primarily on primary sources including:

- The text of the Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023) and the DPDP Rules, 2025.
- Judicial precedents, particularly *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017) 10 SCC 1.
- Legislative history including parliamentary debates and committee reports on earlier PDP Bill drafts.

Secondary sources include:

- Academic journal articles, law review commentaries, and scholarly books on data protection and privacy law.
- Reports from civil society organisations, think tanks, and industry bodies.
- Comparative analysis of the EU GDPR and other international data protection frameworks.]

The research adopts a **critical-analytical approach**, evaluating the DPDP Act against constitutional principles established in *Puttaswamy*, international best practices, and practical implementation challenges.

1.5 Scope and Limitations

Scope: This study focuses exclusively on the Digital Personal Data Protection Act, 2023, and its accompanying Rules notified in 2025. It examines the Act's provisions chapter-wise, with particular emphasis on the rights-duties framework, state exemptions, and institutional design. The analysis is situated within the broader constitutional jurisprudence of privacy in India, with *Puttaswamy* serving as the foundational reference point.

Limitations:

1. The DPDP Rules, 2025 were notified only in November 2025, and their practical implementation is still in early stages. Empirical data on enforcement outcomes, penalty imposition, and compliance challenges is therefore limited.

2. This study does not cover sector-specific regulations (e.g., RBI guidelines for banks, IRDAI rules for insurers) that may impose additional data protection obligations.

3. The analysis is confined to the statutory text and judicial precedents available as of September 2026; subsequent judicial interpretations or constitutional challenges to the Act are beyond the scope of this paper.

4. Cross-border data transfer provisions under Section 16 are analysed at a high level; detailed examination of restricted country notifications is beyond scope.

CHAPTER II: HISTORICAL EVOLUTION OF DATA PROTECTION IN INDIA

2.1 Pre-2017: The Information Technology Act, 2000 Regime

Before the enactment of the DPDP Act 2023, India's data protection framework was anchored in the Information Technology Act, 2000 (IT Act), particularly Section 43A, and the SPDI Rules, 2011.

Section 43A of the IT Act provided:

"Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security

practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

Key Features of the Pre-DPDP Regime:

Feature	Description
Scope	Applied only to "body corporates" (not individuals or government entities)
Definition of Sensitive Personal Data	Included passwords, financial information, health conditions, sexual orientation, biometric information, etc. (Rule 3, SPDI Rules)
Obligation	Implement "reasonable security practices and procedures" (certified to IS/ISO/IEC 27001 or equivalent)
Remedy	Compensation for wrongful loss/gain caused by negligence; no upper ceiling on damages
Enforcement	Adjudicated by officers appointed under Section 46 of the IT Act; appeals to Cyber Appellate Tribunal (now TDSAT)
Consent	Required for collection of sensitive personal data; purpose limitation and disclosure restrictions under Rules 4-6

Critical Deficiencies:

1. **Limited Scope:** Section 43A applied only to body corporates, excluding government agencies and individuals.
2. **No Comprehensive Rights:** Individuals had no statutory rights to access, correct, erase, or port their data.
3. **No Independent Regulator:** Enforcement was through adjudicating officers, not an independent data protection authority.
4. **Narrow Definition:** Only "sensitive personal data" was covered; ordinary personal data was largely unprotected.
5. **Weak Enforcement:** Compensation claims were civil in nature; no deterrent penalties or criminal sanctions.

The DPDP Act 2023 explicitly repeals Section 43A of the IT Act, superseding the SPDI Rules, 2011. However, the old regime remains in force during the phased implementation period of the DPDP Act.

2.2 The Puttaswamy Judgment (2017): A Constitutional Turning Point

Case Citation: *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1; AIR 2017 SC 4161

Facts: The case arose from a constitutional challenge to the Aadhaar biometric identification scheme, which required residents of India to provide biometric and demographic data for authentication in accessing government subsidies and services. Petitioners argued that mandatory Aadhaar enrollment violated the fundamental right to privacy.

Issues: The nine-judge Constitution Bench was constituted specifically to determine whether the right to privacy is a fundamental right under the Constitution of India. The Court was not tasked with deciding the validity of Aadhaar itself (that was addressed in a subsequent 2018 judgment).

Judgment (24 August 2017): In a unanimous 547-page judgment comprising six concurring opinions, the Court held:

1. **Privacy is a Fundamental Right:** The right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21, and as part of the freedoms guaranteed by Part III of the Constitution (Articles 14, 19, and 21).

2. **Overruling Precedents:** The Court overruled *M.P. Sharma v. Satish Chandra* (1954) and *Kharak Singh v. State of Uttar Pradesh* (1962), which had held that privacy is not a fundamental right.

3. **Informational Privacy:** The judgment explicitly recognised "informational privacy" as an essential facet of the right to privacy in the digital age, protecting individuals' control over their personal data.

4. **Three-Prong Proportionality Test:** Any state action that restricts privacy must satisfy a three-fold test:

    - **Legality:** The restriction must be based on a valid law.
    - **Legitimate State Aim:** The law must pursue a legitimate state interest (e.g., national security, public order).
    - **Proportionality:** The means adopted must be proportionate to the objective sought to be achieved.

5. **Natural and Inalienable Right:** Privacy is a natural, inherent, and inalienable right that protects individuals from arbitrary interference by the State and private entities, ensuring freedom in personal choices, bodily integrity, and informational control.

Impact on Data Protection Jurisprudence:
The *Puttaswamy* judgment imposed a constitutional obligation on the State to enact comprehensive data protection legislation. Justice Chandrachud, writing for the majority, observed:

"Informational privacy is a facet of the right to privacy. The dangers to privacy in an age of information can originate not only from the state but from non-state actors as well. We commend to the Union Government the need to examine and put into place a robust regime for data protection.

This observation directly catalysed the drafting of the Personal Data Protection Bill, 2019, and ultimately the DPDP Act, 2023. The DPDP Act's preamble explicitly references the *Puttaswamy* judgment, stating its purpose is to provide for processing of digital personal data "in a manner that recognises both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes.

2.3 Legislative Journey: From PDP Bill 2019 to DPDP Act 2023

The legislative process leading to the DPDP Act 2023 spanned nearly six years and involved multiple drafts, each subject to intense stakeholder consultation and criticism.

Timeline:

Year	Milestone	Key Features/Criticism
2017	*Puttaswamy* Judgment (August2017)	Constitutional recognition of privacy; mandate for data protection law
2018	Srikrishna Committee Report (July 2018)	Draft Personal Data Protection Bill, 2018; proposed comprehensive rights, independent regulator (DPA)
2019	PDP Bill 2019 introduced in Lok Sabha (December 2019)	Referred to Joint Parliamentary Committee (JPC); included data localisation, significant data fiduciaries, consent manager framework
2021	JPC Report submitted (December 2021)	91 recommendations; proposed amendments on data localisation, government exemptions, non-personal data regulation

Year	Milestone	Key Features/Criticism
2022	PDP Bill 2022 withdrawn (August 2022)	Government cited "comprehensive changes"; new draft promised
2022	Draft DPDP Bill 2022 released (November 2022)	Simplified framework; reduced compliance burden; expanded government exemptions; no non-personal data regulation
2023	DPDP Act 2023 enacted (11 August 2023)	Presidential assent; 44 sections, 9 chapters; penalties up to ₹250 crore
2025	DPDP Rules 2025 notified (13 November 2025)	Operationalised the Act; phased implementation over 12-18 months

Key Changes from PDP Bill 2019 to DPDP Act 2023:

1. **Simplified Framework:** The DPDP Act adopted a "principles-based" rather than prescriptive approach, focusing on core obligations rather than detailed compliance requirements.

2. **Reduced Compliance Burden:** Eliminated requirements for data localisation (replaced with cross-border transfer restrictions under Section 16), reduced obligations for small data fiduciaries.

3. **Expanded Government Exemptions:** Section 17 of the DPDP Act grants broad exemptions to the State for national security, public order, and other grounds—criticised as excessive and lacking judicial oversight.

4. **No Non-Personal Data Regulation:** Unlike the PDP Bill 2019 and JPC recommendations, the DPDP Act governs only "digital personal data," excluding non-personal and anonymised data.

5. **Weakened Regulator:** The Data Protection Board of India (DPBI) is an adjudicatory body, not an independent regulator with rule-making powers; significant policy decisions are reserved for the Central Government.

CHAPTER III: THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023: STRUCTURAL OVERVIEW

3.1 Chapter-wise Breakdown of the Act

The DPDP Act, 2023 comprises **44 sections** organised into **9 chapters** (some sources cite 8 or 10 chapters depending on whether the Schedule is counted). The Act received Presidential assent on 11 August 2023 and was published as Act No. 22 of 2023.

Chapter-wise Structure:

Chapter	Sections	Title	Key Provisions
Chapter I	1-3	Preliminary	Short title, commencement, definitions (Section 2), application of Act (Section 3)
Chapter II	4-10	Obligations of Data Fiduciary	Grounds for processing (Section 4), notice (Section 5), consent (Section 6), legitimate uses (Section 7), general obligations (Section 8), children's data (Section 9), significant data fiduciary obligations (Section 10)
Chapter III	11-15	Rights and Duties of Data Principal	Right to information (Section 11), correction and erasure (Section 12), grievance redressal (Section 13), nomination (Section 14), duties of data principal (Section 15)

Chapter	Sections	Title	Key Provisions
Chapter IV	16	Transfer of Personal Data Outside India	Restrictions on cross-border data transfers to notified countries/territories
Chapter V	17	Exemptions	Exemptions for government instrumentalities on national security, public order, and other grounds
Chapter VI	18-23	Data Protection Board of India	Establishment, composition, powers, functions, adjudication process
Chapter VII	24-28	Appeals	Appeals from Board orders to Telecom Disputes Settlement and Appellate Tribunal (TDSAT)
Chapter VIII	29-32	Miscellaneous	Offences by companies, compounding of offences, protection of action taken in good faith, power to make rules
Chapter IX	33-44	Penalties and Adjudication	Penalties (Section 33), schedule of penalties, adjudication process, directions by Board (Section 34)
Schedule	—	Penalties	Graded penalty structure: ₹10,000 to ₹250 crore per violation

Note: Some sources group Sections 33-44 as part of Chapter VIII (Penalties and Adjudication), while others separate penalties (Section 33) and miscellaneous provisions (Sections 29-32) into distinct chapters. The official Gazette text organises the Act into 9 chapters plus a Schedule.

3.2 Key Definitions and Scope of Application

Section 2: Definitions

The Act defines key terms that shape its scope and application:

Term	Definition	Section
Personal Data	Any data about an individual who is identifiable by or in relation to such data.	2(t)
Digital Personal Data	Personal data in digital form (the Act applies only to digital data, not physical records).	2(i)
Data Principal	The individual to whom the personal data relates (includes parents/guardians for children).	2(j)
Data Fiduciary	Any person (including the State, companies, individuals) who alone or in conjunction with others determines the purpose and means of processing personal data.	2(k)
Data Processor	Any person who processes personal data on behalf of a data fiduciary.	2(l)
Processing	Any operation performed on personal data, including collection, storage, use, disclosure, erasure, etc.	2(v)
Consent	Free, specific, informed, unconditional, and unambiguous indication of the data principal's wishes, expressed through a clear affirmative action.	2(h)
Significant Data Fiduciary (SDF)	A data fiduciary notified by the Central Government based on volume, sensitivity, risk, and other factors; subject to additional obligations.	2(x)

Term	Definition	Section
Data Protection Board of India (DPBI)	The adjudicatory body established under Section 18 to enforce the Act.	2(m)

Section 3: Application of Act

The DPDP Act applies to the processing of digital personal data:

1. **Within India:** Where data is collected in digital or non-digital form and subsequently digitised.
2. **Outside India:** If processing is related to offering goods/services to data principals within India, or profiling of data principals within India.

Exclusions: The Act does not apply to:

- Personal data processed by individuals for purely personal or domestic purposes.
- Personal data made publicly available by the data principal or under a legal obligation.
- Non-personal data (anonymised or aggregated data).

Key Principles Embedded in the Act:

1. **Consent as the Cornerstone:** Personal data may be processed only for lawful purposes with the free, specific, informed, and unambiguous consent of the data principal (Sections 4-6).
2. **Purpose Limitation:** Data can only be processed for the purpose for which consent was given or for legitimate uses under Section 7.
3. **Data Minimisation:** Only data necessary for the specified purpose should be collected.
4. **Storage Limitation:** Data should not be retained beyond the period necessary for the stated purpose.
5. **Security Safeguards:** Data fiduciaries must implement reasonable security measures to prevent data breaches (Section 8(5)).
6. **Accountability:** Data fiduciaries are accountable for compliance and must maintain records, report breaches, and cooperate with the Board.

CHAPTER IV: RIGHTS OF DATA PRINCIPALS AND OBLIGATIONS OF DATA FIDUCIARIES

4.1 Rights of Data Principals (Sections 11-15)

The DPDP Act grants data principals (individuals) four core rights, enforceable against data fiduciaries. These rights are codified in Chapter III (Sections 11-15) and operationalised through Rule 14 of the DPDP Rules, 2025.

Table: Data Principal Rights under DPDP Act 2023

Right	Section	Description	Key Features
Right to Access Information	Section 11	Data principal can obtain from the data fiduciary: (a) summary of personal data being processed; (b) processing activities undertaken; (c) identities of all other data fiduciaries/processors with whom data was shared, along with description of data shared.	- Applies only to data fiduciaries to whom consent was previously given - Must be provided in accessible format - No fee can be charged

Right	Section	Description	Key Features
Right to Correction and Erasure	Section 12	Data principal can request: (a) correction of inaccurate data; (b) completion of incomplete data; (c) updating of outdated data; (d) erasure of data no longer necessary for the stated purpose.	- Data fiduciary must respond within prescribed time - If correction affects third parties, they must be notified - Erasure subject to legal retention obligations
Right to Grievance Redressal	Section 13	Every data fiduciary must establish and publish a readily available grievance redressal mechanism. Data principal can escalate to the Data Protection Board if unsatisfied.	- First layer: Data fiduciary/consent manager - Must respond within prescribed timeline - Escalation to Board after exhaustion
Right to Nomination	Section 14	Data principal can nominate another individual to exercise their rights under the Act in case of death or incapacity.	- Nominee can exercise all rights (access, correction, erasure, grievance) - Must be designated in prescribed manner
Right to Withdraw Consent	Section 6(4)	Data principal can withdraw consent at any time; withdrawal must be as easy as giving consent.	- Consequences of withdrawal must be explained at time of consent - Withdrawal does not affect lawfulness of prior processing

Duties of Data Principals (Section 15):
The Act also imposes duties on data principals:

1. **Compliance with Laws:** Do not impersonate others or provide false information while exercising rights.
2. **Genuine Grievances:** Do not file frivolous or vexatious complaints.
3. **Penalty for Breach:** Up to ₹10,000 for violating duties (e.g., filing false complaints).

Critical Analysis of Data Principal Rights:

1. **Limited Scope of Access and Correction:** Rights under Sections 11 and 12 apply only to data fiduciaries to whom consent was previously given. This excludes processing under "legitimate uses" (Section 7) where consent is not required, significantly narrowing the practical utility of these rights.
2. **No Data Portability:** Unlike the EU GDPR (Article 20), the DPDP Act does not grant data principals the right to data portability—the ability to receive their data in a structured, machine-readable format and transmit it to another fiduciary. This limits user control and competition.
3. **No Right to Object to Automated Decision-Making:** The Act lacks safeguards against profiling and automated decision-making, which are critical in the age of AI and algorithmic governance.

4. **Grievance Redressal Mechanism:** While Section 13 mandates grievance redressal, the Rules do not specify detailed timelines or standards, leaving room for inconsistent implementation.

4.2 Obligations of Data Fiduciaries (Sections 4-10)

Data fiduciaries bear the primary compliance burden under the DPDP Act. Chapter II (Sections 4-10) outlines their obligations:

Table: Data Fiduciary Obligations under DPDP Act 2023

Obligation	Section	Description	Key Requirements
Grounds for Processing	Section 4	Personal data may be processed only for lawful purposes: (a) with consent; or (b) under "legitimate uses" (Section 7).	- Consent must be free, specific, informed, unambiguous - Legitimate uses include state functions, employment, medical emergencies, etc.
Notice	Section 5	Before or at the time of collecting personal data, data fiduciary must give a clear, itemised notice in English or any Eighth Schedule language.	- Description of data being collected - Purpose of processing - Rights of data principal (access, correction, grievance, nomination) - How to withdraw consent, exercise rights, complain to Board
Consent	Section 6	Consent must be free, specific, informed, unconditional, unambiguous, and expressed through clear affirmative action.	- Must be capable of being withdrawn as easily as given - Consent manager framework for managing consent - Burden of proof on fiduciary to demonstrate valid consent
Legitimate Uses	Section 7	Processing without consent is permitted for specified purposes: (a) state functions under law; (b) employment-related purposes; (c) medical emergencies; (d) legal claims; (e) publicly available data; (f) prevention/detection of crimes.	- Criticised as overly broad, diluting consent requirement - No requirement for necessity or proportionality assessment
General Obligations	Section 8	Data fiduciary must: (a) ensure accuracy of data; (b) implement reasonable security safeguards; (c) notify breach to Board and affected individuals; (d) erase data when purpose is fulfilled; (e) comply with codes of practice.	- Security safeguards under Section 8(5): penalty up to ₹250 crore for failure - Breach notification under Section 8(6): penalty up to ₹200 crore
Children's Data	Section 9	Special protections for data of children (under 18 years): (a) no processing that may cause harm; (b) no tracking, behavioural monitoring, or targeted advertising; (c) verifiable parental consent required.	- Penalty up to ₹200 crore for violations - Applies to all data fiduciaries, not just SDFs

Obligation	Section	Description	Key Requirements
Significant Data Fiduciary (SDF) Obligations	Section 10	SDFs (notified by government) must: (a) appoint data protection officer (DPO); (b) conduct data protection impact assessments (DPIA); (c) periodic audits; (d) additional security measures.	- Criteria for SDF notification: volume, sensitivity, risk, systemic impact - Penalty up to ₹150 crore for non-compliance

Key Compliance Requirements for Data Fiduciaries:

1. **Appoint Consent Managers:** Entities managing consent on behalf of data principals must be registered as consent managers.

2. **Implement Consent Mechanisms:** Systems for obtaining, managing, and withdrawing consent must be user-friendly and accessible.

3. **Breach Notification:** Report personal data breaches to the Data Protection Board within 72 hours of discovery, detailing nature, extent, consequences, and mitigation steps.

4. **Data Retention:** Retain personal data only for the period necessary to fulfil the stated purpose; notify data principal 48 hours before erasure.

5. **Record-Keeping:** Maintain records of processing activities, consent logs, and breach reports for inspection by the Board.

4.3 Special Provisions: Children's Data and Significant Data Fiduciaries

Children's Data (Section 9):[
The DPDP Act provides enhanced protections for children (defined as individuals under 18 years):

- **Prohibited Processing:** No processing that may cause harm to the child, including tracking, behavioural monitoring, or targeted advertising.
- **Parental Consent:** Verifiable parental consent is required before processing children's data.
- **Penalty:** Violations attract penalties up to ₹200 crore.

Critical Analysis:

1. **Age Definition:** The Act defines "child" as under 18, aligning with the Protection of Children from Sexual Offences (POCSO) Act, 2012, but creating compliance challenges for platforms serving teenagers (e.g., social media, edtech).

2. **Parental Consent Mechanism:** The Rules do not specify detailed procedures for verifiable parental consent, leaving ambiguity for platforms.

3. **Behavioural Monitoring Ban:** The prohibition on tracking and behavioural monitoring is progressive but may conflict with legitimate educational or safety-related monitoring by schools/parents.

Significant Data Fiduciaries (SDFs) (Section 10):
The Central Government may notify certain data fiduciaries as "Significant Data Fiduciaries" based on:

- Volume and sensitivity of personal data processed
- Risk to the rights of data principals
- Potential impact on the sovereignty and integrity of India
- Electoral democracy and public order considerations

Additional Obligations for SDFs:

1. **Appoint Data Protection Officer (DPO):** A senior official responsible for compliance.
2. **Data Protection Impact Assessment (DPIA):** Assess risks before high-risk processing.
3. **Periodic Audits:** Independent audits of data protection practices.
4. **Enhanced Security Measures:** Additional technical and organisational safeguards.

Penalty: Non-compliance with SDF obligations attracts penalties up to ₹150 crore.

Critical Analysis:

1. **Government Discretion:** The criteria for SDF notification are broad and discretionary, raising concerns about arbitrary classification.
2. **Compliance Burden:** SDF obligations may disproportionately impact startups and SMEs if thresholds are not calibrated carefully.
3. **No Appeal Mechanism:** The Act does not provide a clear mechanism for challenging SDF notification.

CHAPTER V: INSTITUTIONAL FRAMEWORK: THE DATA PROTECTION BOARD OF INDIA

5.1 Composition, Powers, and Functions

Establishment (Section 18):
The DPDP Act establishes the **Data Protection Board of India (DPBI)** as the primary adjudicatory body for enforcing the Act. The Board is a digital-first, online mechanism designed for faster resolution of complaints and penalties.

Composition (Section 19):
The Board consists of:

- **Chairperson:** A person with legal expertise and experience in data protection, technology, or related fields.
- **Members:** Up to 6 members with expertise in law, technology, data governance, and related domains.
- **Appointment:** By the Central Government on the recommendation of a selection committee.
- **Term:** 3 years, renewable once.

Powers and Functions (Sections 20-23):

1. **Adjudication of Complaints:** Hear complaints from data principals regarding violations of their rights (Sections 11-14).
2. **Penalty Imposition:** Impose penalties under Section 33 and the Schedule for violations by data fiduciaries.
3. **Breach Investigation:** Investigate personal data breaches and direct remedial measures.
4. **Dispute Resolution:** Resolve disputes between data fiduciaries and data principals, including consent managers.
5. **Directions:** Issue directions to data fiduciaries to comply with the Act (Section 34).
6. **Suo Motu Action:** Initiate proceedings on its own motion based on information received.

Procedural Features:

- **Digital-First:** All proceedings are conducted online through a dedicated portal.]
- **Time-Bound:** The Board must dispose of complaints within a prescribed timeline (Rules to specify).
- **Natural Justice:** Data fiduciaries have the right to be heard before penalties are imposed.

Critical Analysis:

1. **Adjudicatory Body, Not Independent Regulator:** Unlike the EU GDPR's Data Protection Authorities (DPAs), the DPBI is primarily an adjudicatory body, not an independent regulator with rule-making, standard-setting, or advisory powers. Significant policy decisions (e.g., SDF notification, cross-border transfer restrictions) are reserved for the Central Government.

2. **Government Control:** The Board's members are appointed by the Central Government, raising concerns about independence and autonomy.

3. **Limited Rule-Making Powers:** The Board cannot issue regulations or guidelines; it can only adjudicate complaints and impose penalties.

4. **Resource Constraints:** The effectiveness of the Board depends on adequate staffing, technical infrastructure, and expertise, which are not guaranteed under the Act.**5.2 Adjudication and Penalty Mechanism**

Section 33: Penalties
The DPDP Act prescribes a graded penalty structure based on the severity of the violation. The Schedule to the Act specifies maximum penalties for different categories of breaches:

Table: Penalty Schedule under DPDP Act 2023

Violation	Section	Maximum Penalty
Failure to take reasonable security safeguards (resulting in data breach)	Section 8(5)	₹250 crore (~USD 30 million)
Failure to notify breach to Board or affected data principals	Section 8(6)	₹200 crore
Violation of children's data obligations	Section 9	₹200 crore
Breach of SDF additional obligations	Section 10	₹150 crore
Breach of consent, notice, or any other provision of Act/Rules	Sections 4-7, 11-14, etc.	₹50 crore
Failure to comply with Board directions	Section 34	₹250 crore
Data principal breaching duties (e.g., false complaints)	Section 15	₹10,000

Adjudication Process (Sections 21-23, 33):

1. **Complaint Filing:** Data principals or any person can file complaints with the Board.
2. **Preliminary Inquiry:** Board conducts initial assessment to determine if a prima facie case exists.
3. **Notice to Respondent:** Data fiduciary is given notice and opportunity to respond.
4. **Hearing:** Virtual hearing conducted; parties can present evidence and arguments.
5. **Adjudication Order:** Board issues order with findings and penalty (if any).

6. **Penalty Calculation:** Board considers factors such as:
    - Nature, gravity, and duration of the breach
    - Volume of data affected
    - Whether breach was intentional or negligent
    - Actions taken to mitigate harm
    - Previous compliance history
    - Economic impact on the fiduciary
7. **Appeal:** Orders can be appealed to the Telecom Disputes Settlement and Appellate Tribunal (TDSAT) within 60 days.

Key Features of Penalty Regime:

1. **Per-Contravention Basis:** Penalties are imposed per violation; multiple contraventions attract multiple penalties.
2. **Board Discretion:** The Board can reduce or increase penalties by up to twice the base amount under Section 33(3), potentially reaching ₹500 crore for severe breaches.
3. **No Criminal Liability:** The Act does not impose criminal sanctions; penalties are civil in nature.
4. **Compounding of Offences:** Certain offences can be compounded (settled) before prosecution under Section 30.

Critical Analysis:

1. **Deterrent Penalties:** The ₹250 crore maximum penalty is among the highest globally, comparable to GDPR's 4% of global turnover. This creates a strong deterrent for large corporations.
2. **Discretionary Nature:** The Board's wide discretion in calculating penalties (including the ability to double the base amount) may lead to inconsistency and unpredictability.
3. **No Private Right of Action:** Unlike some jurisdictions, the DPDP Act does not grant data principals a direct right to claim compensation for damages; they must rely on the Board's adjudication.
4. **Enforcement Capacity:** The Board's ability to enforce penalties, especially against large tech companies, depends on adequate resources and governmental support.

CHAPTER VI: CRITICAL ANALYSIS: STRENGTHS AND DEFICIENCIES

6.1 Progressive Features of the DPDP Act

Despite its shortcomings, the DPDP Act 2023 introduces several progressive features that align India's data protection regime with global standards:

1. **Constitutional Foundation:** The Act explicitly operationalises the fundamental right to privacy recognised in *Puttaswamy*, providing a statutory framework for informational privacy.
2. **Consent-Centric Framework:** Consent is established as the primary lawful basis for processing, with detailed requirements for free, specific, informed, and unambiguous consent. The consent manager framework enables individuals to manage consent across multiple fiduciaries.
3. **Comprehensive Rights:** The Act grants data principals enforceable rights to access, correct, erase, and seek grievance redressal, empowering individuals to control their data.

4. **Stringent Penalties:** The graded penalty structure with maximum fines up to ₹250 crore creates a strong deterrent for non-compliance, particularly for large corporations.

5. **Children's Protections:** Enhanced safeguards for children's data, including bans on tracking, behavioural monitoring, and targeted advertising, are progressive and align with global best practices.

6. **Digital-First Enforcement:** The online, time-bound adjudication mechanism of the Data Protection Board is designed for efficiency and accessibility.

7. **Principles-Based Approach:** The Act focuses on core principles (purpose limitation, data minimisation, security safeguards) rather than prescriptive rules, allowing flexibility for innovation.

8. **Cross-Border Transfer Framework:** Section 16 enables the government to restrict data transfers to specific countries, balancing openness with sovereignty concerns.

6.2 Legislative Minimalism and Executive Discretion

A major criticism of the DPDP Act is its **legislative minimalism**—the tendency to delegate critical policy decisions to executive rule-making rather than embedding them in the statute.

Examples of Legislative Minimalism:

1. **Vague Definitions:** Key terms like "reasonable security safeguards" (Section 8(5)), "legitimate uses" (Section 7), and "harm to children" (Section 9) are not defined in the Act, leaving them to be specified through Rules or government notifications.

2. **Delegated Powers:** The Central Government retains broad powers to:
   - Notify Significant Data Fiduciaries (Section 10)
   - Restrict cross-border data transfers to specific countries (Section 16)
   - Grant exemptions to government instrumentalities (Section 17)
   - Make rules on procedural matters (Section 36)

3. **Absence of Safeguards:** The Act does not specify detailed procedures for consent managers, data portability (if introduced later), or algorithmic accountability, deferring these to future Rules.

Implications:

1. **Executive Overreach:** Excessive delegation concentrates power in the executive, undermining legislative scrutiny and democratic accountability.

2. **Regulatory Uncertainty:** Businesses face uncertainty until Rules are notified, delaying compliance planning.

3. **Judicial Challenges:** Vague provisions may be subject to constitutional challenges on grounds of arbitrariness (Article 14) and excessive delegation.

Scholarly Critique:
Akshita Singh (2026) notes: "The DPDP Act's legislative minimalism reflects a deliberate choice to prioritise flexibility over certainty, but at the cost of undermining the rule of law and enabling executive discretion.

6.3 State Exemptions and Surveillance Concerns (Section 17)

Section 17: Exemptions
The most contentious provision of the DPDP Act is Section 17, which grants broad exemptions to government instrumentalities from the Act's obligations.

Text of Section 17(1):

"The provisions of this Act shall not apply to the processing of personal data by or under the authority of any instrumentality of the State, as may be notified by the Central Government, in the interests of:
(a) sovereignty and integrity of India;
(b) security of the State;
(c) friendly relations with foreign States;
(d) public order;
(e) preventing incitement to the commission of any cognisable offence.

Additional Exemptions (Section 17(2)):
The Central Government may also exempt itself from obligations under the Act when processing data furnished by notified instrumentalities.

Critical Concerns:

1. **Overbreadth:** The grounds for exemption—sovereignty, security, public order—are broad and ill-defined, potentially covering a wide range of government activities.

2. **No Judicial Oversight:** The Act does not require written, reasoned orders or judicial review for exemptions, enabling arbitrary use.

3. **Surveillance Enabling:** Critics argue that Section 17 creates a "carve-out" for law enforcement and intelligence agencies, enabling mass surveillance without accountability.

4. **Conflict with Puttaswamy:** The exemptions may violate the proportionality test established in *Puttaswamy*, as they lack necessity and proportionality safeguards.

5. **Chilling Effect:** Broad exemptions may deter individuals from exercising their rights, fearing government surveillance.

Recent Judicial Developments:
In a 2025 challenge to Section 17, the Supreme Court reportedly read down the provision, holding that exemptions must be based on **written, reasoned orders** and are subject to **judicial review**. However, the full text of this judgment is not yet publicly available as of September 2026.

Comparative Perspective:

- **EU GDPR:** Article 23 allows member states to restrict data protection rights for national security, but such restrictions must be "necessary and proportionate" and subject to judicial oversight.

- **US:** No comprehensive federal data protection law; sector-specific exemptions for law enforcement (e.g., FISA for surveillance).

- **South Africa (POPIA):** Section 7 allows exemptions for national security but requires ministerial approval and parliamentary oversight.

Recommendations:

1. **Narrow Exemptions:** Limit exemptions to specific, narrowly-defined purposes (e.g., counter-terrorism, not general "public order").

2. **Judicial Oversight:** Require prior judicial approval or post-facto review by an independent body.

3. **Transparency:** Mandate annual reports on the number and nature of exemptions invoked.

4. **Sunset Clause:** Exemptions should expire after a fixed period unless renewed.

6.4 Dilution of Consent through "Legitimate Uses"

Section 7: Certain Legitimate Uses
The Act permits processing without consent for specified "legitimate uses," including:

- State functions under law
- Employment-related purposes
- Medical emergencies
- Legal claims
- Publicly available data
- Prevention/detection of crimes

Critical Concerns:

1. **Overbreadth:** The categories are broad and may be interpreted expansively, undermining the consent requirement.
2. **No Necessity Test:** Unlike the GDPR's "legitimate interests" ground (Article 6(1)(f)), Section 7 does not require a necessity or proportionality assessment.
3. **Employment Exception:** The employment exemption may enable employers to process employee data without consent, raising privacy concerns.
4. **Publicly Available Data:** The exemption for publicly available data may enable scraping and profiling without consent.

Scholarly Critique:
A 2026 study notes: "The 'legitimate uses' exception creates a significant loophole, allowing data fiduciaries to bypass consent for a wide range of processing activities, diluting the Act's core principle of individual autonomy.

Recommendations:

1. **Narrow Interpretation:** Courts and the Board should interpret "legitimate uses" narrowly, requiring necessity and proportionality.
2. **Legislative Amendment:** Amend Section 7 to include a necessity test and exclude sensitive categories (e.g., health, biometric data).
3. **Guidance:** The Board should issue guidelines clarifying the scope of each legitimate use category.

6.5 Absence of Data Portability and Other Rights

Missing Rights Compared to GDPR:
The DPDP Act omits several rights present in the EU GDPR, limiting individual control over data:

Right	GDPR (Article)	DPDP Act	Implication
Data Portability	Article 20	Not included	Individuals cannot transfer data between fiduciaries, limiting competition and user control.
Right to Object	Article 21	Not included	No right to object to processing based on legitimate interests or direct marketing.

Right	GDPR (Article)	DPDP Act	Implication
Automated Decision-Making	Article 22	Not included	No safeguards against profiling or algorithmic decision-making.
Restriction of Processing	Article 18	Not included	Individuals cannot request temporary suspension of processing.
Prior Consultation	Article 36	Not included	No requirement for high-risk processing to consult regulator beforehand.

Critical Analysis:
The absence of these rights reflects the Act's "minimalist" approach but undermines its alignment with global best practices. Data portability, in particular, is critical for fostering competition and enabling individuals to switch service providers easily.

Recommendations:

1. **Introduce Data Portability:** Amend the Act to include a right to data portability, aligned with GDPR Article 20.
2. **Safeguards for Automated Decision-Making:** Introduce provisions requiring transparency, human oversight, and the right to contest algorithmic decisions.
3. **Right to Object:** Grant individuals the right to object to processing for direct marketing or based on legitimate interests.

CHAPTER VII: COMPARATIVE PERSPECTIVE: DPDP ACT VIS-À-VIS GDPR AND GLOBAL STANDARDS

7.1 Comparison with EU General Data Protection Regulation

The EU GDPR (Regulation 2016/679) is the global benchmark for data protection laws. Comparing the DPDP Act with the GDPR reveals both alignments and gaps:

Table: DPDP Act 2023 vs. EU GDPR

Feature	DPDP Act 2023	EU GDPR	Analysis
Scope	Digital personal data only; applies to processing in India or targeting Indians.	All personal data (digital + physical); extraterritorial application to entities targeting EU residents.	GDPR has broader scope; DPDP excludes non-digital data.
Lawful Basis	Consent (primary) + "legitimate uses" (Section 7).	Six lawful bases: consent, contract, legal obligation, vital interests, public task, legitimate interests.	GDPR offers more flexibility; DPDP's "legitimate uses" are narrower but less defined.
Consent	Free, specific, informed, unambiguous, affirmative action.	Same standards; explicit consent for sensitive data.	Aligned; both require high standards for consent.

Feature	DPDP Act 2023	EU GDPR	Analysis
Data Principal Rights	Access, correction, erasure, grievance, nomination.	Access, rectification, erasure, restriction, portability, object, no automated decision-making.	GDPR grants more rights (portability, object, restriction).
Data Fiduciary Obligations	Notice, consent, security, breach notification, children's protections.	Same + DPIA, DPO, records of processing, privacy by design.	GDPR has more comprehensive obligations (e.g., privacy by design).
Regulator	Data Protection Board (adjudicatory body).	Independent Data Protection Authorities (DPAs) with rule-making, advisory, enforcement powers.	GDPR regulators are more independent and empowered.
Penalties	Up to ₹250 crore (~USD 30M) per violation.	Up to €20M or 4% of global turnover, whichever is higher.	Comparable deterrent effect; GDPR's turnover-based penalty may be higher for large firms.
Cross-Border Transfers	Government can restrict transfers to specific countries (Section 16).	Adequacy decisions, standard contractual clauses, binding corporate rules.	GDPR has more structured mechanisms; DPDP relies on government notifications.
State Exemptions	Broad exemptions for national security, public order (Section 17).	Limited exemptions for national security, subject to necessity and proportionality (Article 23).	GDPR exemptions are narrower and more safeguarded.
Children's Data	Under 18; parental consent required; no tracking/targeted ads.	Under 16 (member states can lower to 13); parental consent for information society services.	DPDP has stronger protections (ban on tracking/ads).

Key Takeaways:

1. **Alignment on Core Principles:** Both frameworks emphasise consent, purpose limitation, data minimisation, and security safeguards.
2. **Gaps in Rights:** The DPDP Act lacks key rights (portability, object, restriction) present in the GDPR.
3. **Weaker Regulator:** The DPBI is less independent and empowered than EU DPAs.
4. **Broader State Exemptions:** Section 17 of the DPDP Act is more expansive and less safeguarded than GDPR Article 23.

7.2 Lessons from Other Jurisdictions

United States:

- No comprehensive federal data protection law; sector-specific regulations (HIPAA for health, GLBA for finance, COPPA for children).
- State laws (e.g., California Consumer Privacy Act, CCPA) grant rights similar to GDPR (access, deletion, opt-out).
- **Lesson:** Sector-specific approach may be easier to implement but creates fragmentation; comprehensive law (like DPDP) is preferable for uniformity.

South Africa (POPIA):

- Protection of Personal Information Act, 2013 (POPIA) aligns closely with GDPR.
- Independent regulator (Information Regulator) with enforcement powers.
- **Lesson:** Independent regulator is critical for effective enforcement; DPBI should be strengthened.

Brazil (LGPD):

- Lei Geral de Proteção de Dados (2018) is GDPR-inspired.
- National Data Protection Authority (ANPD) has rule-making and enforcement powers.
- **Lesson:** Comprehensive law with strong regulator is effective; India can emulate LGPD's balanced approach.

Singapore (PDPA):

- Personal Data Protection Act, 2012 focuses on consent and accountability.
- No comprehensive rights (e.g., no data portability).
- **Lesson:** Singapore's pragmatic, business-friendly approach may have influenced DPDP's minimalist design; but India's constitutional context requires stronger rights.

CHAPTER VIII: CASE LAW ANALYSIS: JUSTICE K.S. PUTTASWAMY (RETD.) V. UNION OF INDIA

8.1 Facts and Issues

Case Citation: *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1; AIR 2017 SC 4161

Facts:

- Petitioners challenged the constitutional validity of the Aadhaar biometric identification scheme, which required residents to provide biometric (fingerprints, iris scans) and demographic data for authentication.
- Aadhaar was mandatory for accessing government subsidies, services, and benefits under various schemes.
- Petitioners argued that mandatory enrollment violated the fundamental right to privacy, as it involved collection and storage of sensitive biometric data without adequate safeguards.

Issues Before the Nine-Judge Bench:

1. Whether the right to privacy is a fundamental right under the Constitution of India.
2. Whether earlier precedents (*M.P. Sharma*, 1954; *Kharak Singh*, 1962) holding that privacy is not a fundamental right should be overruled.
3. What is the scope and content of the right to privacy, particularly in the digital age?

Note: The Court did not decide the validity of Aadhaar itself; that was addressed in a subsequent 2018 judgment (*Puttaswamy II*).

8.2 Judgment and Reasoning

Unanimous Holding (24 August 2017):
The nine-judge Constitution Bench unanimously held:

1. **Privacy is a Fundamental Right:**
   - The right to privacy is protected under Article 21 (right to life and personal liberty) and is an intrinsic part of the freedoms guaranteed by Part III of the Constitution (Articles 14, 19, 21).
   - Privacy is a natural, inherent, and inalienable right that protects individuals from arbitrary interference by the State and private entities.
2. **Overruling Precedents:**
   - *M.P. Sharma v. Satish Chandra* (1954) and *Kharak Singh v. State of Uttar Pradesh* (1962) were overruled to the extent they held that privacy is not a fundamental right.
3. **Informational Privacy:**
   - The Court explicitly recognised "informational privacy" as an essential facet of the right to privacy in the digital age.
   - Individuals have a right to control the collection, storage, and use of their personal data by the State and private entities.
4. **Three-Prong Proportionality Test:**
   - Any state action that restricts privacy must satisfy:
     - **Legality:** Based on a valid law.
     - **Legitimate State Aim:** Pursues a legitimate state interest (e.g., national security, public order).
     - **Proportionality:** Means adopted are proportionate to the objective.
5. **Dignity and Autonomy:**
   - Privacy is essential for human dignity, autonomy, and the ability to make personal choices without state interference.

Key Observations:

- **Justice Chandrachud (for the majority):** "Informational privacy is a facet of the right to privacy. The dangers to privacy in an age of information can originate not only from the state but from non-state actors as well. We commend to the Union Government the need to examine and put into place a robust regime for data protection.
- **Justice Chandrachud:** "Privacy is the constitutional core of human dignity. It protects the inner sphere of the individual from intrusive state action.

8.3 Impact on DPDP Act 2023

Constitutional Foundation:
The *Puttaswamy* judgment is the constitutional bedrock of the DPDP Act 2023. The Act's preamble explicitly references the judgment, stating its purpose is to operationalise the right to informational privacy.

Key Impacts:

1. **Mandate for Legislation:** *Puttaswamy* imposed a constitutional obligation on the State to enact comprehensive data protection legislation, catalysing the drafting of the PDP Bill 2019 and ultimately the DPDP Act 2023.
2. **Proportionality Test for State Actions:** The three-prong proportionality test established in *Puttaswamy* is the benchmark for evaluating the constitutional validity of the DPDP Act's provisions, particularly Section 17 exemptions.

- Critics argue that Section 17 fails the proportionality test because it lacks necessity and proportionality safeguards.
- The Supreme Court's 2025 reading down of Section 17 (requiring written, reasoned orders) reflects the application of *Puttaswamy* principles.

3. **Informational Privacy as a Fundamental Right:** The DPDP Act codifies the right to informational privacy by granting data principals rights over their personal data (access, correction, erasure).

4. **Balance with State Interests:** While *Puttaswamy* recognises privacy as fundamental, it also acknowledges that the right is not absolute and can be restricted for legitimate state aims. The DPDP Act attempts to balance individual rights with state interests (e.g., national security exemptions under Section 17), though critics argue the balance is skewed.

5. **Judicial Scrutiny:** Future constitutional challenges to the DPDP Act will be evaluated against *Puttaswamy* standards, particularly the proportionality test.

Ongoing Constitutional Challenges:
As of 2026, several petitions challenging the constitutional validity of Section 17 exemptions and other provisions are pending before the Supreme Court. The outcomes of these challenges will shape the Act's future interpretation and implementation.

CHAPTER IX: CONCLUSION AND RECOMMENDATIONS

9.1 Summary of Findings

This paper has provided a comprehensive, chapter-wise analysis of the Digital Personal Data Protection Act, 2023, situating it within the broader constitutional jurisprudence of privacy in India. Key findings include:

1. **Constitutional Alignment:** The DPDP Act operationalises the fundamental right to informational privacy recognised in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017), fulfilling the constitutional mandate for comprehensive data protection legislation.

2. **Progressive Features:** The Act introduces a consent-centric framework, comprehensive data principal rights, stringent penalties (up to ₹250 crore), enhanced children's protections, and a digital-first enforcement mechanism.

3. **Structural Deficiencies:** The Act suffers from legislative minimalism, excessive executive discretion, expansive state exemptions under Section 17, dilution of consent through "legitimate uses," and the absence of key rights (data portability, right to object, safeguards against automated decision-making).

4. **Institutional Weaknesses:** The Data Protection Board of India is an adjudicatory body, not an independent regulator with rule-making powers, limiting its effectiveness.

5. **Comparative Gaps:** Compared to the EU GDPR, the DPDP Act lacks comprehensive rights, has a weaker regulator, and grants broader state exemptions.

6. **Surveillance Concerns:** Section 17 exemptions enable state surveillance without adequate judicial oversight, potentially violating the proportionality test established in *Puttaswamy*.

9.2 Recommendations for Legislative Reform

To strengthen the DPDP Act's alignment with constitutional principles and international best practices, the following amendments are recommended:

1. **Narrow State Exemptions (Section 17):**
   - Limit exemptions to specific, narrowly-defined purposes (e.g., counter-terrorism, not general "public order").
   - Require written, reasoned orders for each exemption.
   - Introduce judicial oversight (prior approval or post-facto review).
   - Mandate annual transparency reports on exemptions invoked.
2. **Strengthen Data Principal Rights:**
   - Introduce a right to data portability (aligned with GDPR Article 20).
   - Grant a right to object to processing for direct marketing or based on legitimate interests.
   - Add safeguards against automated decision-making and profiling (right to human review, explanation).
3. **Enhance Regulator Independence:**
   - Transform the Data Protection Board into an independent regulator with rule-making, standard-setting, and advisory powers (similar to EU DPAs).
   - Ensure transparent, merit-based appointments to the Board.
   - Provide adequate resources and technical expertise.
4. **Clarify "Legitimate Uses" (Section 7):**
   - Introduce a necessity and proportionality test for each legitimate use category.
   - Exclude sensitive data (health, biometric, financial) from legitimate use exemptions.
   - Issue Board guidelines clarifying the scope of each category.
5. **Introduce Privacy by Design:**
   - Mandate data fiduciaries to implement privacy by design and default (as under GDPR Article 25).
   - Require Data Protection Impact Assessments (DPIAs) for high-risk processing, not just for SDFs.
6. **Strengthen Breach Notification:**
   - Specify detailed timelines and formats for breach notification in the Act (not just Rules).
   - Require notification to affected individuals within 72 hours, not just to the Board.
7. **Introduce Private Right of Action:**
   - Allow data principals to claim compensation for damages in civil courts, in addition to Board adjudication.
8. **Sunset Clause for Exemptions:**
   - All exemptions under Section 17 should expire after 2 years unless renewed by Parliament (not just the executive).

9.3 Future Research Directions

1. **Empirical Studies:** Research on the practical implementation of the DPDP Act, including compliance challenges faced by businesses, enforcement outcomes of the Data Protection Board, and the impact on data breaches.

2. **Sector-Specific Analysis:** Examination of how the DPDP Act interacts with sector-specific regulations (e.g., RBI guidelines for banks, IRDAI rules for insurers, health data under the Digital Information Security in Healthcare Act).

3. **Cross-Border Data Flows:** Analysis of the impact of Section 16 restrictions on international trade, cloud computing, and digital services.

4. **AI and Algorithmic Accountability:** Research on the need for additional safeguards against AI-driven profiling, automated decision-making, and predictive policing in light of the DPDP Act's gaps.

5. **Constitutional Challenges:** Monitoring ongoing and future constitutional challenges to the DPDP Act, particularly regarding Section 17 exemptions and the proportionality test under *Puttaswamy*.

6. **Comparative Studies:** In-depth comparison of the DPDP Act with emerging data protection laws in the Global South (e.g., Brazil's LGPD, South Africa's POPIA, Kenya's Data Protection Act).

LIST OF ABBREVIATIONS

Abbreviation	Full Form
Aadhaar	Unique Identification Authority of India (UIDAI) biometric identification system
ANPD	Autoridade Nacional de Proteção de Dados (Brazil's National Data Protection Authority)
CCPA	California Consumer Privacy Act (USA)
CERT-In	Indian Computer Emergency Response Team
CCTNS	Crime and Criminal Tracking Network & Systems
DPBI	Data Protection Board of India
DPA	Data Protection Authority
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DPDP Act	Digital Personal Data Protection Act, 2023
DPDP Rules	Digital Personal Data Protection Rules, 2025
EU	European Union
GDPR	General Data Protection Regulation (EU Regulation 2016/679)
HIPAA	Health Insurance Portability and Accountability Act (USA)
IRDAI	Insurance Regulatory and Development Authority of India

Abbreviation	Full Form
IS/ISO/IEC 27001	International Standard for Information Security Management Systems
IT Act	Information Technology Act, 2000
JPC	Joint Parliamentary Committee
LGPD	Lei Geral de Proteção de Dados (Brazil's General Data Protection Law)
MeitY	Ministry of Electronics and Information Technology, Government of India
PDP Bill	Personal Data Protection Bill (2019/2022 drafts)
PIB	Press Information Bureau, Government of India
POCSO	Protection of Children from Sexual Offences Act, 2012
POPIA	Protection of Personal Information Act, 2013 (South Africa)
RBI	Reserve Bank of India
SCC	Supreme Court Cases (law reporter)
SDF	Significant Data Fiduciary
SPDI Rules	Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011
TDSAT	Telecom Disputes Settlement and Appellate Tribunal
UIDAI	Unique Identification Authority of India
USA	United States of America

BIBLIOGRAPHY

Primary Sources

Legislation:

1. The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023), Gazette of India, Part II, Section 1, 11 August 2023.

2. The Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), Gazette of India, 13 November 2025.

3. The Information Technology Act, 2000 (Act No. 21 of 2000), as amended.

4. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, S.O. 2363(E), Gazette of India, 13 April 2011.

Case Law:

5. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1; AIR 2017 SC 4161 (Supreme Court of India, Nine-Judge Constitution Bench, 24 August 2017).

6. *M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300 (Supreme Court of India, Eight-Judge Bench, 1954).

7. *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295 (Supreme Court of India, 1962).

8. *Justice K.S. Puttaswamy (Retd.) v. Union of India (Aadhaar Validity)*, (2018) 1 SCC 1 (Supreme Court of India, Five-Judge Constitution Bench, 26 September 2018).

Secondary Sources

Books:

9. Chandrachud, D.Y., *The Nature and Scope of the Right to Privacy in India*, Oxford University Press, 2018.

10. Basu, D.D., *Shorter Constitution of India*, 6th ed., LexisNexis, 2020.

11. Chander, A., *The Digital Constitution: Data Protection and Privacy in the Age of AI*, Cambridge University Press, 2022.

Journal Articles:

12. Singh, Akshita, "Constitutional Status of Data Protection in India: A Critical Analysis of the Digital Personal Data Protection Act, 2023", *Indian Journal of Law and Legal Research*, Vol. 8, Issue 2, 2026, pp. 45-67.

13. Kumar, R., & Sharma, P., "Privacy after Puttaswamy: Constitutional Boundaries of State Data Collection under the Digital Personal Data Protection Act, 2023", *Journal of Privacy Law*, Vol. 12, Issue 3, 2026, pp. 89-112.

14. Gupta, S., "The Constitutional Enigma of India's Digital Personal Data Protection Act, 2023", *International Journal of Law, Management and Humanities*, Vol. 9, Issue 4, 2026, pp. 234-256.

15. Reddy, M., "Predictive Policing, AI Surveillance, and Privacy in India: A Critical Legal Analysis of the DPDP Act, 2023", *Zenodo*, 2025.

16. Verma, A., "Data Protection and Privacy in India: From IT Act 2000 to DPDP Act 2023", *Legal Vichar*, June 2026.

17. Choudhary, S., "DPDP Act 2023: A Comparative Analysis with EU GDPR", *Journal of Cyber Law and Policy*, Vol. 5, Issue 1, 2026, pp. 12-34.

Reports:

18. Justice B.N. Srikrishna Committee, *Report of the Committee of Experts on a Data Protection Framework for India*, Ministry of Electronics and Information Technology, July 2018.

19. Joint Parliamentary Committee on the Personal Data Protection Bill, 2019, *Report of the Joint Parliamentary Committee*, Lok Sabha, December 2021.

20. Internet Freedom Foundation, *Analysis of the Digital Personal Data Protection Act, 2023*, New Delhi, August 2023.

21. Centre for Internet and Society, *Submission on the Draft Digital Personal Data Protection Rules, 2025*, Bangalore, February 2025.

Online Resources:

22. Press Information Bureau, "DPDP Rules, 2025 Notified", PIB, 14 November 2025.

23. Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act, 2023", MeitY Website, 2023.

24. India Code, "The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023)", Legislative Department, Ministry of Law and Justice, 2023.

25. CADP, "DPDP Act & Rules Full Text — Interactive Legal Reference", cadp.in, 2026.

26. dComply, "DPDP Act 2023 — All 44 Sections Indexed by Chapter", dpdpa.dcomply.in, 2026.

27. Vels University, "Privacy vs. Government Surveillance", ir.vistas.ac.in, 2026.

28. TCSA, "DPDP Data Principal Rights (Sec 11-15)", tcsa.in, 2026.

29. TCSA, "DPDP Data Fiduciary Obligations (Sec 4-10)", tcsa.in, 2026.

30. Unified Chambers, "DPDP Compliance India", unifiedchambers.com, 2026.

31. CheckDPDP, "What is a Data Fiduciary under India's DPDP Act", checkdpdp.in, 2026.

32. Consiva, "Data Principal Rights Under the DPDP Act 2023", consiva.ai, 2026.

33. Motadata, "DPDPA Compliance: Requirements, Penalties & Checklist", motadata.com, 2026.

34. dComply, "DPDP Penalty Schedule", dpdpa.dcomply.in, 2026.

35. ComplyDP, "DPDP Act Section 33 and the Penalty Schedule Explained", complydp.com, 2026.

36. Lawful Legal, "The Supreme Court on the Digital Personal Data Protection Act, 2023", lawfullegal.in, 2025.

37. Record of Law, "Justice K.S. Puttaswamy (Retd.) v. Union of India (2017)", recordoflaw.in, 2026.

38. Valkya, "Puttaswamy, (2017) 10 SCC 1: Right to Privacy", valkya.org, 2026.

39. The Law Cademy, "Right to Privacy Case: Puttaswamy v. Union of India", thelawcademy.in, 2026.

40. RTI Wiki, "Justice K S Puttaswamy v. Union of India (2017)", righttoinformation.wiki, 2026.

41. Oquilia, "K.S. Puttaswamy v Union of India (2017): How Nine Judges Made Privacy a Fundamental Right", oquilia.com, 2026.

42. UnderstandUPSC, "Justice K.S. Puttaswamy (Retd.) v. Union of India (2017)", understandupsc.com, 2025.

43. Lexful Legal, "Justice K.S. Puttaswamy v Union of India (Right to Privacy)", lexfullegal.com, 2025.

44. World Law Digest, "Information Technology Act Section 43A", worldlawdigest.com, 2025.

45. LawMock, "Compensation for Failure to Protect Data (Section 43A)", lawmock.com, 2026.

46. GetNyay, "IT Act 2000: Sections 66, 66D, 67, 72A Explained", getnyay.in, 2026.

47. LawZone, "Information Technology Act, 2000: Complete Bare Act", lawzone.in, 2026.

48. ConsentOS, "DPDP Act vs IT Act 2000: Does It Override Section 43A?", consentos.in, 2026.

49. Matters.ai, "DPDP Act 2023: India's Digital Personal Data Protection Law Explained", matters.ai, 2026.

50. KS&K, "DPDPA 2023: Digital Personal Data Protection Act Guide", ksandk.com, 2026.

51. Vajiram & Ravi, "DPDP Act 2023, DPDP Rules 2025, Objectives, Provisions", vajiramandravi.com, 2025.

52. Public and Policy, "The Digital Personal Data Protection Act, 2023", publicandpolicy.com, 2026.

53. LinkedIn, "An Analysis of India's Digital Personal Data Protection (DPDP) Act, 2023", linkedin.com, 2025.

54. IJSR, "A Constitutional Analysis of India's Digital Personal Data Protection Act, 2023", ijsr.net, 2026.

55. EasyDP, "DPDP Act Summary: The Whole Law in Plain English (2026)", easydp.in, 2026.

56. DPDPActs, "Digital Personal Data Protection Act 2023 India", dpdpacts.com, 2026.

57. DPDPA.com, "DPDPA 2023 to DPDP Rules 2025 – Complete Section-wise Mapping", dpdpa.com, 2026.

58. Incorpx, "DPDP Act 2023 Compliance Guide for Indian Businesses", incorpx.io, 2026.

59. DPDPRules.org, "Your DPDP rights, explained in plain language", dpdprules.org, 2026.

60. Beacon Filing, "DPDP Act 2023 (India): Rules, Consent & Penalties", beaconfiling.com, 2026.

61. iPleaders, "DPDP Rules 2025: Operational Compliance Guide 2026", blog.ipleaders.in, 2026.

62. Vratex, "DPDP Act Penalties: Fines Up to Rs 250 Crore", vratex.com, 2026.

63. CheckDPDP, "DPDP penalties decoded — what ₹250 crore really means and who pays", checkdpdp.in, 2026.

64. HLC, "India's Digital Personal Data Protection Act 2023 brought into force", hlc.com, 2025.

65. SaralPrivacy, "Digital Personal Data Protection Act, 2023", saralprivacy.com, 2026.

66. LawOnTips, "Digital Personal Data Protection Act, 2023 (DPDP) - Complete Bare Act", lawontips.com, 2026.

67. Aizzentec, "DPDP Act 2023 Full Text: Sections, Rules and Schedules", aizzentec.com, 2026.

68. AramGRC, "DPDP Act PDF: Download the Act (2023) & Rules 2025", aramgrc.com, 2026.

69. InnnLegal, "DPDP Act - PDF download!", innnlegal.com, 2026.

70. MYITManager, "DPDP Act 2023 Glossary: Key Terms Explained", myitmanager.in, 2026.

71. CourtKutchehry, "Justice K.S. Puttaswamy (Retd.) v. Union of India", courtkutchehry.com, 2025.

72. Scribd, "Puttaswamy Case: Privacy as a Right", scribd.com, 2026.

73. Scribd, "DPDP", scribd.com, 2026.

74. Zenodo, "Predictive Policing, AI Surveillance, and Privacy in India", zenodo.org, 2025.

75. IJLLR, "A Critical Analysis Of The Digital Personal Data Protection Act, 2023", ijllr.com, 2026.

76. JournalsPress, "Privacy after Puttaswamy: Constitutional Boundaries of State Data Collection under the Digital Personal Data Protection Act, 2023", journalspress.com, 2026.

77. RTI Wiki, "DPDP Act 2023 Complete Guide for Citizens and Business", righttoinformation.wiki, 2026.

78. IJLMH, "The Constitutional Enigma of India's Digital Personal Data Protection Act", ijlmh.com, 2026.

Unpublished Materials

79. Class Lectures on Constitutional Law and Cyber Law, [Your College/University], 2025-2026.

80. Seminar Notes on "Data Protection and Privacy in India", [Your College/University], March 2026.

ANNEXURE: FULL TEXT REFERENCE: DPDP ACT 2023 (SECTION-WISE)

For ease of reference, the following table provides a section-wise index of the DPDP Act, 2023:

Section	Title	Chapter
1	Short title and commencement	I
2	Definitions	I
3	Application of Act	I
4	Grounds for processing personal data	II
5	Notice	II
6	Consent	II
7	Certain legitimate uses	II
8	General obligations of Data Fiduciary	II
9	Processing of personal data of children	II
10	Additional obligations of Significant Data Fiduciary	II
11	Right to information about personal data	III
12	Right to correction and erasure of personal data	III
13	Right to grievance redressal	III
14	Right to nomination	III
15	Duties of Data Principal	III
16	Transfer of personal data outside India	IV
17	Exemptions	V
18	Establishment of Data Protection Board of India	VI
19	Composition of Board	VI
20	Powers and functions of Board	VI
21	Adjudication of complaints	VI
22	Appeal from orders of Board	VII
23	Procedure for appeal	VII
24	Offences by companies	VIII
25	Compounding of offences	VIII

Section	Title	Chapter
26	Protection of action taken in good faith	VIII
27	Power to make rules	VIII
28	Power to remove difficulties	VIII
29	Repeal and savings	VIII
30	Act to have overriding effect	VIII
31	Amendments to other laws	VIII
32	Power to make transitional provisions	VIII
33	Penalties	IX
34	Directions by Board	IX
35	Adjudicating officer	IX
36	Inquiry by adjudicating officer	IX
37	Factors to be considered while imposing penalty	IX
38	Publication of orders	IX
39	Recovery of penalty	IX
40	Appeal against penalty order	IX
41	Offences to be cognizable and non-bailable	IX
42	Jurisdiction of courts	IX
43	Act not to apply in certain cases	IX
44	Power to make rules for implementation	IX
Schedule	Penalties	—

Note: Section numbers 22-44 are indicative based on available sources; the official Gazette text should be consulted for exact numbering.