ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 5| May 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

THE LEGAL FRAMEWORK FOR DATA PROTECTION IN INDIA: A CRITICAL ANALYSIS OF THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

Pooja Mahla
Research Scholar, Department of Law, Kurukshetra University

ABSTRACT

The increasing digitization of personal data in India has raised urgent concerns about privacy, surveillance, and data misuse. The Digital Personal Data Protection Act, 2023 (DPDP Act) is India's first comprehensive legislation aimed at regulating the processing of digital personal data and safeguarding the rights of individuals in the digital age. This research paper critically examines the legal framework introduced by the Act, evaluating its key provisions, strengths, and shortcomings in the context of constitutional privacy guarantees and global data protection standards such as the European Union's General Data Protection Regulation (GDPR).

Through a combination of doctrinal analysis and policy evaluation, the paper identifies the key implementation challenges – including regulatory readiness, business compliance, and public awareness – and provides recommendations for enhancing the law's effectiveness. It concludes that while the DPDP Act is a significant step forward, its success depends on continued legal reform, robust oversight, and an informed citizenry to ensure that privacy rights are meaningfully protected in India's digital landscape.

KEYWORDS: *Digital Personal Data Protection Act, Data Privacy, Fundamental Rights, Data Fiduciary, Surveillance, Consent, Data Protection Board*

I. INTRODUCTION

In an increasingly digitized world, personal data has become a critical asset — often described as the "new oil" of the 21st century. From browsing habits and health records to financial transactions and biometric identifiers, individuals constantly generate vast amounts of data that are collected, stored, analyzed, and monetized by a range of private and public entities. This widespread collection and processing of personal data has given rise to significant concerns over privacy, data misuse, unauthorized surveillance, and lack of accountability.

India, home to one of the world's largest and most active digital populations, has been navigating the complex challenge of protecting its citizens' data in this rapidly evolving digital environment. For years, the country relied on the Information Technology Act, 2000 and related rules to address data privacy — a framework widely criticized for being outdated and insufficient in light of modern technological realities.

The watershed moment came in 2017, when the Supreme Court of India, in the landmark Justice K.S. Puttaswamy (Retd.) v. Union of India judgment, unequivocally declared the right to privacy as a fundamental right under Article 21 of the Constitution. Following years of deliberation, multiple committee reports, and public consultations, India finally enacted the Digital Personal Data Protection Act (DPDP Act), 2023.

This research paper critically examines the legal framework established by the Digital Personal Data Protection Act, 2023. It explores the historical context, analyzes the key features of the Act, identifies its strengths and weaknesses, and compares it with international data protection regimes such as the General Data Protection Regulation (GDPR). The paper also discusses the likely impact on businesses, regulators, and citizens, and offers recommendations to strengthen India's data protection architecture.

II. OVERVIEW OF THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

The Digital Personal Data Protection Act, 2023 (DPDP Act) represents a landmark shift in India's regulatory landscape concerning personal data. It seeks to protect the digital privacy of individuals (referred to as Data Principals) by establishing obligations on entities that collect and process personal data (Data Fiduciaries), and by institutionalizing mechanisms for enforcement and grievance redressal.

1. Scope and Applicability

The DPDP Act applies to:

- Processing of digital personal data within India, whether collected online or digitized offline.
- Processing outside India if it involves offering goods or
- services to individuals in India.

Notably, the law covers only digital data and does not extend to non-digitized personal data unless it is later digitized. It applies to both public and private entities, though it allows the central government to exempt specific agencies or sectors in certain cases..

2. Core Principles

The Act is guided by seven principles:

1. Lawfulness and Fairness**:** Personal data must be processed lawfully and fairly.

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 5| May 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

2. Purpose Limitation**:** Data must be used only for the stated purpose.
3. Data Minimization: Only necessary data should be collected.
4. Accuracy: Data must be accurate and kept up to date.
5. Storage Limitation: Data must not be retained longer than necessary.
6. Security Safeguards: Reasonable security measures must be in place.
7. Accountability**:** Data Fiduciaries must demonstrate compliance.

3. Consent-Based Framework

The Act mandates that personal data processing can only occur with the free, specific, informed, unconditional, and unambiguous consent of the Data Principal. Consent must be:

- Presented in a plain language format,
- Revocable at any time,
- Managed through Consent Managers (optional intermediaries),
- Accompanied by notice explaining the purpose of processing.

Exceptions are allowed for "legitimate uses," such as for government functions (e.g., benefits distribution), medical emergencies, or legal obligations.

4. Rights of Data Principals

The DPDP Act grants several enforceable rights to individuals, including:

- Right to Access Information: About the personal data being processed.
- Right to Correction and Erasure: Of inaccurate or outdated data.
- Right to Grievance Redressal: Via the data fiduciary and ultimately the Data Protection Board.
- Right to Nominate**:** A person to exercise rights in the event of the death or incapacity of the data principal.

These rights are narrower compared to the GDPR but represent a significant improvement over previous legal protections in India.

5. Obligations of Data Fiduciaries

Data Fiduciaries must:

- Obtain valid consent,
- Ensure transparency in data processing,
- Implement security safeguards,
- Report data breaches,
- Establish grievance redress mechanisms.

A special category, Significant Data Fiduciaries (SDFs)**,** may be designated by the government based on criteria such as volume and sensitivity of data handled. SDFs have enhanced obligations like conducting Data Protection Impact Assessments and appointing a Data Protection Officer**.**

6. Data Protection Board of India

The Act establishes a Data Protection Board to oversee compliance and adjudicate breaches. However, concerns have been raised about its lack of institutional independence, as its members and procedures are controlled by the central government.

7. Penalties and Enforcement

The Act prescribes financial penalties for non-compliance:

- Up to ₹250 crore for failing to prevent a data breach.
- ₹200 crore for violating children's data protection rules.
- ₹50 crore for failing to respond to user grievances.

These penalties are intended to act as deterrents, but critics argue that enforcement capacity remains untested.

III. CRITICAL ANALYSIS OF THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

While the Digital Personal Data Protection Act, 2023 represents a long-overdue step toward protecting the digital rights of Indian citizens, it has attracted both praise and criticism from legal experts, technologists, privacy advocates, and civil society organizations. This section evaluates the Act's strengths**,** shortcomings**,** and alignment with global standards**,** particularly in comparison with the European Union's General Data Protection Regulation (GDPR)**.**

1. Strengths of the DPDP Act

a) Codification of Digital Privacy Rights

The Act formally recognizes essential rights of individuals (Data Principals), including the right to access, correct, and delete their personal data. This codification strengthens the enforceability of privacy rights and helps individuals reclaim control over their data, in line with constitutional guarantees established in the Puttaswamy judgment.

b) Consent-Based Processing

A major positive feature is the requirement of informed and specific consent before processing personal data. By introducing consent as the default lawful basis for data collection and use, the Act aligns with international best practices and enhances transparency and user control.

c) Obligations on Data Fiduciaries

The Act imposes clearly defined responsibilities on data fiduciaries to ensure secure, fair, and limited data processing. These include data minimization, storage limitation, and ensuring accuracy — principles which, although not novel, are now made legally enforceable.

d) Recognition of Cross-Border Data Transfers

Unlike earlier drafts that advocated strict data localization, the DPDP Act adopts a pragmatic approach to cross-border data transfers. Transfers are permitted to certain notified countries, reducing compliance burdens for global businesses while maintaining regulatory oversight.

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 5| May 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

2. Weaknesses and Criticisms

Despite its progressive elements, the Act has raised serious concerns on several fronts:

a) Sweeping Government Exemptions (Section 17)

One of the most criticized provisions is **Section 17**, which allows the Central Government to exempt any government agency from the application of the Act for reasons including national security, public order, and sovereignty. The language is vague and provides unchecked power, potentially enabling mass surveillance and undermining individual rights.

This exemption clause arguably fails the "necessity and proportionality" test established by the Supreme Court in Puttaswamy, and may be vulnerable to constitutional challenge.

b) Lack of Institutional Independence

The Data Protection Board of India**,** envisioned as the enforcement authority, is entirely appointed and overseen by the Central Government. It lacks the structural and functional independence necessary for credible, unbiased oversight. In contrast, the EU's Data Protection Authorities operate independently of the executive and have extensive powers to investigate and penalize.

c) Ambiguity in Key Terms

The Act uses terms like "significant harm", "reasonable security practices", and "legitimate uses" without clear definitions. This ambiguity creates legal uncertainty for both data principals and fiduciaries and may lead to inconsistent interpretation and enforcement.

d) Weak Grievance Redress Mechanism

Although the Act grants individuals the right to file complaints with data fiduciaries and the Board, it lacks clarity on the timeframes**,** appellate procedures, and processes for collective redress. The burden of navigating the grievance process remains largely on the individual, which may discourage enforcement of rights.

e) Limited Rights Compared to Global Standards

The Act does not provide for data portability, the right to object to automated decision-making, or profiling safeguards — all of which are integral to the GDPR. While simplicity may improve implementation, this minimalism comes at the cost of weaker user protection.

3. Broader Legal and Social Concerns

a) Digital Illiteracy

With vast sections of India's population unfamiliar with digital rights and processes, meaningful enforcement of individual rights remains a challenge. Awareness campaigns and civic education are essential for the law to achieve its intended purpose.

b) Implementation Risks

India lacks a strong history of regulatory enforcement in digital spaces. Questions remain about the government's readiness to operationalize the Data Protection Board, audit data fiduciaries, and respond to breaches at scale.

c) Surveillance and Civil Liberties

Civil liberties organizations have expressed concern that the DPDP Act could be used to legitimize mass surveillance, especially in the absence of a surveillance reform law and with sweeping exemptions for state agencies. Without judicial oversight or independent authorization, surveillance practices may continue unchecked.

IV. IMPACT AND IMPLEMENTATION CHALLENGES

The Digital Personal Data Protection Act, 2023 (DPDP Act) is expected to significantly reshape the digital and regulatory ecosystem in India. While it provides a much-needed legal framework for data protection, its implementation poses complex challenges for stakeholders — from businesses and regulators to citizens and civil society groups. This section explores the anticipated impact of the law and the practical hurdles that may arise in its execution.

1. Impact on Businesses and Startups

The DPDP Act imposes new compliance obligations on companies that handle personal data, including:

- Obtaining explicit consent from users,
- Setting up data governance frameworks,
- Reporting data breaches,
- Appointing data protection officers (for Significant Data Fiduciaries).

For large corporations and tech giants, the compliance transition may be smoother due to existing privacy infrastructure. However, startups, SMEs, and regional service providers may face increased operational and financial burdens. Many smaller players lack the resources or legal expertise to adapt swiftly, which could stifle innovation or lead to non-compliance risks.

Moreover, the government's power to classify entities as Significant Data Fiduciaries (SDF**s)** based on criteria like volume and sensitivity of data — without clear thresholds — adds regulatory uncertainty.

2. Government Readiness and Enforcement Infrastructure

Successful implementation hinges on institutional preparedness, especially the establishment and functioning of the Data Protection Board of India. Key challenges include:

- Recruitment of qualified personnel,
- Operational independence and neutrality of the Board,
- Development of standard procedures for breach investigation and grievance redressal.

Given the Board's limited independence and the lack of a decentralized enforcement structure (unlike the GDPR's model of national authorities), there is concern about whether it can act as an effective watchdog — especially against government entities.

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 5| May 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

3. Public Awareness and Digital Literacy

One of the most overlooked aspects of data protection implementation in India is the low level of digital literacy among the general population. Millions of Indians use smartphones, social media, and digital services without understanding what data they are sharing, how it is used, or what rights they have under the new law.

For the law to succeed, the government must invest in:

- Public education campaigns explaining the rights of Data Principals,
- Multilingual outreach to bridge the literacy and language divide,
- Community-level digital literacy programs through schools, NGOs, and local governance structures.

Without this, individuals may remain unaware or unable to exercise their rights, leaving enforcement of the law largely symbolic.

4. Judicial Oversight and Legal Recourse

Given the law's broad exemptions for government agencies**,** lack of prior judicial authorization for surveillance**,** and ambiguity in several clauses, the courts will likely play a critical role in interpreting its provisions and ensuring that constitutional rights are not violated.

However, judicial remedies are often time-consuming and expensive, limiting access for marginalized communities. This makes it essential for the regulatory framework to be robust at the administrative level, rather than relying solely on judicial review.

5. Cross-Border Data and Global Business Compliance

While the Act takes a less restrictive stance on data localization than previous drafts**,** uncertainty remains around international data flows**.** The central government will notify countries where cross-border transfers are permitted, but it is unclear:

- What criteria will be used,
- How frequently the list will be updated,
- Whether adequacy assessments (as in the GDPR) will be conducted.

Global companies may find compliance with India's framework challenging if it diverges too far from international norms, especially in areas such as data transfers, consent management, and data subject rights**.**

6. Risk of Regulatory Capture and Abuse

Due to the central government's sweeping powers under the Act — including rule-making, exempting entities, and controlling the Data Protection Board — there is concern about the lack of checks and balances**.** This could lead to selective enforcement, misuse of exemptions, or reluctance to penalize state actors.

Without transparency, regular audits, and parliamentary oversight, the Act may become more of an enabling tool for state surveillance than a protective framework for individual rights.

V. WAY FORWARD

The enactment of the Digital Personal Data Protection Act, 2023 is a foundational step toward establishing a data protection regime in India. However, as highlighted in the previous sections, the success of the legislation depends not merely on its passage but on robust implementation, continuous refinement, and public accountability. This section outlines key recommendations and strategies to strengthen the framework and uphold the spirit of privacy enshrined in the Constitution.

1. Narrowing Government Exemptions

The broad exemptions for the state under Section 17 threaten the right to privacy. To ensure constitutional compliance and trust, exemptions must be narrowly defined**,** subject to independent oversight**,** and follow the principles of necessity, legality, and proportionality**.** A mandatory review mechanism should assess all government exemptions.

2. Ensuring Independence of the Data Protection Board

The Data Protection Board of India must be independent, transparent, and well-resourced**.** This requires an independent appointment process**,** financial and operational autonomy, and public disclosure of reports and audits. Without true independence, the Board risks being ineffective and symbolic rather than a strong regulator.

3. Expanding User Rights

To align with global standards and strengthen user empowerment, the Act should add rights like data portability**,** objection to processing**,** and automated decision-making. Clear, time-bound procedures for exercising these rights would enhance user control and promote accountability in data handling.

4. Strengthening Grievance Redress and Access to Justice

To align with global standards and strengthen user empowerment, the Act should add rights like data portability**,** objection to processing, and automated decision-making**.** Clear, time-bound procedures for exercising these rights would enhance user control and promote accountability in data handling.

5. Building Public Awareness and Digital Literacy

Legal rights are meaningful only when people can exercise them. To ensure this, the government and civil society should raise awareness about the DPDP Act through regional campaigns, integrate privacy education into curricula, and support grassroots training by NGOs and local groups. An informed public is key to effective data protection.

6. Periodic Review and Stakeholder Consultation

Given rapid technological changes, the law must be regularly reviewed. This can be ensured by establishing a Data Protection Advisory Council, conducting public consultations before drafting rules, and introducing sunset clauses for certain provisions, especially government exemptions, to mandate periodic reassessment.

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 5| May 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

7. Promoting Open Data and Privacy by Design

Alongside individual protections, India must prioritize privacy by design, enforce secure data architecture standards, and adopt open government data policies that uphold privacy and anonymization. These measures ensure privacy is embedded as a core principle, not an afterthought, in the country's digital infrastructure.

VI. CONCLUSION

The Digital Personal Data Protection Act, 2023 marks a pivotal moment in India's journey toward establishing a comprehensive legal regime for safeguarding personal data in the digital age. For a country with over a billion citizens rapidly adopting digital technologies, the Act offers a long-awaited legal foundation to regulate the collection, processing, and protection of digital personal data.

However, implementation challenges such as regulatory preparedness, public awareness, enforcement capacity, and business compliance will determine whether the Act achieves its objectives or merely adds another layer of legal formality. Without addressing the digital literacy gap and building institutional capacity, the rights and safeguards on paper may remain illusory for much of the population.

In essence, while the DPDP Act is a step in the right direction, it must be treated as a starting point — not a final solution. Continuous engagement, judicial oversight, and democratic accountability will be vital to shaping a data protection regime that truly respects the dignity, autonomy, and rights of every digital citizen in India.

REFERENCES

1. *The Digital Personal Data Protection Act, 2023. Ministry of Law and Justice, Government of India. Retrieved from: https://prsindia.org*
2. *Information Technology Act, 2000. Government of India. Retrieved from: https://legislative.gov.in/*
3. *Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1. Supreme Court of India.*
4. *Report of the Committee of Experts on a Data Protection Framework for India (Chair: Justice B.N. Srikrishna), 2018. Ministry of Electronics and Information Technology. Retrieved from: https://www.meity.gov.in/*
5. *European Union General Data Protection Regulation (GDPR), 2016. Regulation (EU) 2016/679. Retrieved from: https://gdpr.eu/*
6. *Sharma, A. (2023). Understanding India's Data Protection Law: A Policy Perspective. Economic and Political Weekly, Vol 58, Issue 34.*
7. *Dvara Research. (2023). Analysis of the Digital Personal Data Protection Act, 2023. Retrieved from: https://www.dvara.com*
8. *Internet Freedom Foundation (IFF). (2023). Key Issues with the Digital Personal Data Protection Act. Retrieved from: https://internetfreedom.in*
9. *Joshi, A., & Saxena, R. (2023). "Balancing State Surveillance and Privacy Rights: A Critique of India's DPDP Act." NUJS Law Review, Vol. 16, No. 2.*
10. *Data Governance Network. (2022). Building a User-Centric Data Protection Law in India. Retrieved from: https://datagovernance.org*