JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Safeguarding Privacy in the Digital Age: A Critical Examination of India's Digital Personal Data Protection Act, 2023 and the Jurisprudential Milestones Leading to Its Enactment

Author : Ashwary Ghuley, Research Scholar, Government Law College,Rewa

Co-Author : Aayuushi Pandey,Research Scholar, Government Law College,Rewa

Abstract

The enactment of the Digital Personal Data Protection Act, 2023 (DPDP Act) marks a significant milestone in India's journey toward establishing a robust data protection regime. It seeks to balance the individual's right to privacy with the necessity of processing personal data for lawful purposes. This paper provides a critical analysis of the Act, its background, salient features, and its comparison with global counterparts like the GDPR. More importantly, it identifies key loopholes in the Act, such as government exemptions, lack of independent oversight, and limited rights of data principals. The paper concludes with suggested reforms to align the legislation more closely with constitutional mandates and international best practices.

Key-words: Data Protection,Digital Privacy,Data Fiduciaries,Fundamental Rights,Surveillance and Oversight

List of Abbreviations

Abbreviation	Full Form
DPDP Act	Digital Personal Data Protection Act, 2023
GDPR	General Data Protection Regulation
IT Act	Information Technology Act, 2000
SDF	Significant Data Fiduciary
DPB	Data Protection Board
PMO	Prime Minister's Office
EPFO	Employees' Provident Fund Organisation
CCI	Competition Commission of India
COPPA	Children's Online Privacy Protection Act
SCC	Supreme Court Cases

1. Introduction

The right to privacy was declared a fundamental right under Article 21 of the Indian Constitution in the landmark case of *Justice K.S. Puttaswamy v. Union of India* (2017) 10 SCC 1[1]. This necessitated the enactment of a comprehensive data protection legislation. The Digital Personal Data Protection Act, 2023, enacted on August 11, 2023, is the culmination of a prolonged legislative process, beginning with the Justice B.N. Srikrishna Committee Report in 2018.

This paper aims to critically examine the DPDP Act, analyze its strengths and weaknesses, and identify the legislative gaps it seeks to fill or fails to address. It also contrasts the Indian law with international benchmarks, especially the EU's General Data Protection Regulation (GDPR).[2]

2. Background and Evolution of Data Protection in India

India lacked a comprehensive data protection framework prior to 2023. Key developments in this domain include:

- **Information Technology Act, 2000**: Section 43A and Rules under Section 87(2)(ob) offered some protection for sensitive personal data.[3]
- **Puttaswamy Judgment (2017)**: Recognized privacy as a fundamental right.
- **Srikrishna Committee Report (2018)**: Recommended a draft Personal Data Protection Bill.[4]
- **Withdrawal of PDP Bill (2019)**: Cited the need for a more comprehensive and simpler framework.
- **DPDP Act, 2023**: Enacted to regulate digital personal data and ensure lawful processing.

3. Objectives of the DPDP Act, 2023

The DPDP Act aims to:

- Safeguard the right to privacy of individuals.
- Establish principles for lawful processing of personal data.
- Provide a framework for data fiduciaries and data principals.
- Establish the Data Protection Board of India.

[1] Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
[2] Digital Personal Data Protection Act, No. 22 of 2023, Acts of Parliament, 2023 (India).

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), 2016 O.J. (L 119) 1.

[4] Binoy Viswam v. Union of India, (2017) 7 S.C.C. 59 (India).

- Promote data protection compliance in both public and private sectors.

4. Key Definitions and Scope

- **Personal Data**: Any data about an individual who is identifiable by or in relation to such data (Section 2(t)).
- **Data Fiduciary**: Any person who determines the purpose and means of processing personal data (Section 2(i)).
- **Consent**: Freely given, specific, informed, unconditional and unambiguous indication of the data principal's agreement (Section 6).[5]
- **Significant Data Fiduciary (SDF)**: Entities processing large volumes of personal data and notified by the government.

The Act applies only to digital personal data, or data digitized subsequently (Section 3), excluding non-digital data and anonymized data.

5. Salient Features of the Act

5.1 Consent-Based Processing

Data processing is based on consent or legitimate uses (Section 7). Consent must be informed and revocable (Section 6).[6]

5.2 Duties of Data Fiduciaries

Fiduciaries must:

- Ensure accuracy, security, and accountability.
- Appoint a Data Protection Officer (for SDFs).
- Notify breaches and implement safeguards (Section 8).

5.3 Rights of Data Principals

Includes the right to:

- Access information (Section 11),

[5] Karmanya Singh Sareen v. Union of India, W.P. (C) No. 7663 of 2016, High Court of Delhi (India).
[6] Information Technology Act, No. 21 of 2000, Acts of Parliament, 2000 (India).

- Correction and erasure (Section 12),
- Grievance redressal (Section 13),
- Nominate representatives (Section 14).

5.4 Exemptions (Section 17)

The Central Government can exempt any data fiduciary from application of the Act in the interest of sovereignty, public order, etc.[7]

5.5 Establishment of the Data Protection Board (DPB)

The DPB will inquire into data breaches and impose penalties. However, it is not an independent constitutional authority and functions more like a quasi-judicial body under executive control.

6. Loopholes and Criticisms

6.1 Government Overreach and Exemptions

Section 17 empowers the government to exempt its agencies from most obligations, effectively undermining the core purpose of privacy protection. This raises constitutional concerns under *Puttaswamy* which held that restrictions on privacy must meet the test of necessity and proportionality.[8]

6.2 Lack of Data Localization Mandate

Unlike the earlier PDP Bill, the DPDP Act does not mandate data localization. Cross-border transfer is permitted to countries notified by the central government (Section 16), leaving room for arbitrary decision-making and potential risks to national security.

6.3 Absence of Independent Regulator

The Data Protection Board is appointed and controlled by the executive (Section 19), compromising its independence. In contrast, the GDPR provides for truly independent supervisory authorities under Article 51.

6.4 Limited Data Principal Rights

The Act does not recognize several rights present in GDPR such as:

[7] Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501–6506 (2021).
[8] Srikrishna Committee Report on Data Protection, Ministry of Electronics and Information Technology, Government of India (2018).

- Right to data portability,
- Right to be forgotten (explicitly),
- Right to object to processing,
- Right against automated profiling.

6.5 Vague and Broad Definitions

Terms like "public order," "legitimate use," and "fair and reasonable" processing are vague and subject to broad interpretation, leading to potential misuse.[9]

6.6 No Provisions on Children's Data

The Act does not impose strict obligations for processing data of children, apart from prohibiting tracking and targeted advertising (Section 9(6))—which is less rigorous than international standards like the Children's Online Privacy Protection Act (COPPA) in the U.S.[10]

6.7 Lack of Strong Penalty Regime

Although the Act prescribes penalties up to ₹250 crore (Schedule), actual enforcement mechanisms and deterrents remain unclear and dependent on the discretionary power of the Board.[11]

7. Comparative Analysis: DPDP Act vs GDPR

Feature	DPDP Act, 2023	GDPR
Scope	Digital personal data only	All personal data
Consent	Must be informed and clear	Freely given, specific, informed, unambiguous
Data Localization	No requirement	Transfer restricted under adequacy decision or safeguards
Regulator	Data Protection Board (executive-led)	Independent Supervisory Authority
Rights	Limited (no data portability, profiling objection)	Comprehensive data subject rights
Penalties	₹10,000 to ₹250 crore	Up to €20 million or 4% of global turnover
Government Exemptions	Broad under Section 17	Limited exemptions under Article 23

[9] Gautam Bhatia, Privacy: A Constitutional History and a Political Right (2019).
[10] Apar Gupta, Digital Rights and Indian Democracy, J. Const. L. (India), 2022.
[11] Arun Sukumar, India's Data Protection Law: A Glass Half Empty, The Hindu (Aug. 15, 2023), https://www.thehindu.com

8. Legislative Gaps Addressed by the DPDP Act

Despite its limitations, the Act fills several legislative voids:

- Establishes a framework for lawful digital data processing.
- Mandates consent mechanisms and grievance redressal.
- Recognizes basic rights of data principals.
- Imposes obligations on private data fiduciaries.
- Provides a quasi-regulatory enforcement mechanism.[12]

9. Major Case Studies Leading to the Enactment of the DPDP Act

Several high-profile data breaches and legal battles laid the foundation for a dedicated data protection law in India. These incidents underscored the urgency of data protection and helped galvanize public and legislative action.

9.1 Justice K.S. Puttaswamy v. Union of India (2017)

This landmark case recognized the right to privacy as a fundamental right under Article 21 of the Constitution. The judgment emphasized the need for a robust data protection framework and acted as a catalyst for the government to initiate legislative action.

9.2 Aadhaar Controversy and *Binoy Viswam v. Union of India*

The linking of Aadhaar with various services including bank accounts and mobile numbers raised concerns about state surveillance. In *Binoy Viswam v. Union of India*, [13]the Supreme Court upheld the constitutional validity of Aadhaar but imposed strict usage limitations. This demonstrated the legal vacuum in personal data protection.

9.3 Cambridge Analytica-Facebook Scandal (2018)

The global scandal involving the unauthorized harvesting of personal data of millions of Facebook users, including Indian users, led to heightened awareness of the need for data privacy. It pushed the Indian government to expedite data protection legislation.

[12] Internet Freedom Foundation, DPDP Act: An Analysis (2023), https://internetfreedom.in
[13] Competition Comm'n of India, Case No. 01 of 2021 (WhatsApp Privacy Policy Case).

9.4 Paytm Data Sharing Allegations

In 2018, Paytm was accused of sharing user data with the Prime Minister's Office (PMO). Though denied, the controversy sparked fears of misuse of data by private players with governmental links, urging legal safeguards.

9.5 Truecaller Data Scraping Incident

Truecaller was reported to be collecting user data beyond what was necessary and sharing it with advertisers, leading to massive privacy concerns and multiple complaints to regulators. The incident underlined the lack of consent-based frameworks in existing laws.

9.6 Pegasus Spyware Controversy (2021)

The use of Pegasus spyware to monitor journalists, activists, and politicians without consent showcased the vulnerability of digital data and the absence of redressal under Indian law. The Supreme Court's order for a committee probe further underscored the need for statutory protections.

9.7 Health Data Breaches During COVID-19

The pandemic revealed lapses in the handling of sensitive health data by both private apps and government agencies. Several states were found to be publishing health records and quarantine details online, violating privacy norms.

9.8 WhatsApp Privacy Policy Update (2021)

WhatsApp's new privacy policy, which allowed sharing of user data with parent company Facebook, triggered widespread backlash and a suo motu case by the Competition Commission of India (CCI). It demonstrated the need for clearer rules on data processing and consent.

9.9 Data Breaches in Public Sector Banks

Multiple reports emerged between 2019–2021 of large-scale data leaks from banks, insurance firms, and even the EPFO. The lack of consequences for these breaches highlighted the absence of a legal deterrent.[14]

9.10 Delhi High Court in *Karmanya Singh Sareen v. Union of India*

The court questioned the validity of WhatsApp's data-sharing practices, stressing the absence of statutory regulation. The judgment called for an urgent legislative response.

These cases created public momentum and provided judicial and political impetus for the enactment of a comprehensive data protection law.[15]

[14] Facebook-Cambridge Analytica Scandal, BBC News (Mar. 19, 2018), https://www.bbc.com/news/technology-43465968.
[15] Paytm Data Leak Allegations, India Today (May 23, 2018), https://www.indiatoday.in.

10. Suggested Reforms

10.1 Strengthen Oversight Mechanisms

Make the Data Protection Board a constitutionally protected and independent body, like the Election Commission or Comptroller and Auditor General.

10.2 Narrow Government Exemptions

Section 17 must be revised to require parliamentary oversight and judicial scrutiny for granting exemptions.

10.3 Broaden Data Principal Rights

Incorporate rights to data portability, right to object, right to be forgotten, and protection from automated decision-making.

10.4 Improve Definitions

Clarify and narrow terms like "legitimate use," "public order," and "fair and reasonable."

10.5 Introduce Data Localization Norms

Mandate that critical personal data be stored and processed in India, with exceptions governed by international adequacy frameworks.

10.6 Child Data Protection

Introduce stricter norms for children's data akin to COPPA or GDPR's Article 8.[16]

10.7 Penalty Enforcement Framework

Develop a transparent mechanism to assess penalties, including factors like harm caused, repetitive violations, and fiduciary size.[17]

CONCLUSION

The DPDP Act, 2023 represents a necessary legislative step toward data privacy in the digital era. However, its success hinges on effective implementation, clarity in interpretation, and future reforms to plug existing loopholes. The Act currently leans in favor of state discretion over individual privacy and lacks the robust protections offered by international laws like the GDPR. Moving forward, stakeholder engagement, judicial guidance, and periodic legislative review will be essential to make India's data protection regime truly privacy-centric and rights-based.[18]

[16] Truecaller Data Scraping Controversy, The Quint (Jan. 2019), https://www.thequint.com.
[17] Supreme Court of India, Order Regarding Pegasus Spyware Case, W.P. (Crl.) No. 314 of 2021.
[18] Medianama, Report on Health Data and Privacy During COVID-19 (2020), https://www.medianama.com