INTERNATIONAL JOURNAL OF LEGAL STUDIES AND SOCIAL SCIENCES [IJLSSS]

ISSN: 2584-1513 (Online)

Volume 3 | Issue 4 [2025] | Page 59 – 63

INDIA'S DATA PROTECTION LAW IS HERE. BUT DOES IT REALLY PROTECT PRIVACY?

- Shourya Parihar[1]

ABSTRACT

The Digital Personal Data Protection Act, 2023 is India's first serious attempt at regulating personal data use and harmonization with global privacy norms. Although the Act brings forward progressive concepts like consent-based data processing, sanctions for non-compliance, and the creation of a regulatory body, it is also plagued with a number of structural and institutional weaknesses. This article examines the loopholes in the law like poor enforcement, loose cross-border data transfer provisions, and the disproportionate executive dominance over the Data Protection Board. It critiques the Act on the basis of constitutional standards enunciated in seminal judgments like Puttaswamy and Union of India v. R. Gandhi. The article then compares India's framework against international standards such as GDPR and suggests that unless regulatory autonomy and transparency increase, India's data protection regime could be an illusion of privacy instead of an assurance of privacy.

India's Digital Personal Data Protection Act vows protections, but is it merely a regulatory floss over unchecked state power?

INTRODUCTION

Aligning Indian regulatory framework with worldwide data protection standards, the Digital Personal Data Protection Act (DPDP) is a major turning point. The Digital Personal Data Protection Act is first ever law that safeguards privacy of individuals by protecting their personal data. It ensures individual privacy and holds data fiduciaries accountable in digital economy, violating the rules could result in hefty fines, data breaches, and harm to a company's reputation, hence eroding consumer trust and business growth.

Digital Personal Data Protection Act was passed by Indian Parliament and notified in the official gazette on 11 August 2023. It was necessary as there were rising threats posed by data breaches

[1] 4th year law student at Vivekanand Institute of Professional Studies (Affiliated under Guru Gobind Singh Indraprastha University)

and cross- border data transfers. The Act promotes data safety of Individuals while also promoting "Digital India" and global data trade compliance.

It not only safeguards privacy rights of individuals but also hold companies accountable for any kind of data breach. Companies that want to present themselves as responsible data stewards, the DPDP ultimately poses both a challenge and an opportunity. Companies have to invest in data security measures and promote openness.

Companies will have to reform their data management systems, acquire new technologies and compliance with procedures mentioned in DPDP act to avoid sanctions and hefty fines. It would not only help companies and business to reduce risk but also increase consumer trust which would help them in building their reputation in the market.

EVOLUTION OF DATA PROTECTION ACT

As the digital economy grows, companies increasingly rely on data, so data protection laws are crucial for privacy and safe business practices. In the modern age, data is the new oil as it is a key driver of commerce, communication and governance. The evolution of data protection law helps us understanding this as moving from scattered privacy norms to enacting comprehensive data protection schemes, the legal landscape has significantly evolved from fragmented norms to formal regulation.

In pre digital era we can trace the idea of privacy and data protection under the common law which had provision of "right to be let alone". In India privacy was traditionally inserted in Constitutional doctrine of Article 21 which talks about right to life and personal liberty. In Justice K.S.Puttaswamy And Anr. v. Union Of India And Ors.,2017 (10 SCC 1) the Supreme Court held right to privacy as a fundamental right, paving the need for DPDP Act.

During 1970s due to concerns regarding government database lead to first data protection laws in 1980s OECD Guidelines on the Protection of Privacy and Transborder flows of Personal Data which lead to EU Data Protection Directive (1995) that laid the foundation of General Data Protection Regulation (GDPR) which was first act regarding data protection.

The European Union's General Data Protection Regulation (GDPR) in 2018 was a first of its kind, imposing tough data security and privacy standards. GDPR affects not just EU companies but also non-EU companies handling EU citizen's data. It lays down principles such as **data minimization**, **purpose limitation** and **accountability** and changes the way companies process data.

Many countries were influenced by this due to which they introduced similar regulation acts. Some of which are California's CCPA gives consumers the right to access and own their data and Brazil's LGPD copies GDPR's tough requirements. These regulations point towards an international trend towards more robust privacy laws where companies would be liable for huge financial and reputational penalties if they fail to comply. GDPR fines are up to **€20 million** or **4% of annual turnover**, so companies are putting compliance on top of their priority list.

OVERVIEW OF THE DPDP ACT, 2023

FRAMEWORKS AND ACTORS

The Digital Personal Protection Data Act is India's first attempt to frame a comprehensive legislation to govern the processing of digital personal data. It is enacted after years of passing multiple drafts. This Act aims to balance between data privacy of individuals and facilitating lawful use of data for innovation, governance and economic growth. DPDP Act introduced a framework based on two principal actors which is data principal and data fiduciaries, data principal is data that relates to individuals and data fiduciaries that is entities that determine meaning and purpose of such data. The Act mandates that any type of data that is collected or processed should be preceded by notice and consent.

KEY PROVISIONS

Section 5 requires that data fiduciaries must provide clear notice in plain language to outline the purpose of data processing. DPDP **Section 7** allows processing of data without consent under the "**doctrine of legitimate use**" if the data that is collected is for medical emergencies, employment related etc, but weak oversight could lead to corporate loopholes threatening Adhar data. DPDP aims to protect individual privacy rights while promoting India's digital economy. **Section 6** of DPDP Act,2023 regulates cross-border data transfers in which transfer of data is permitted through cross-border unless restriction by government notification but it lacks GDPR standard contractual clauses risking leaks like the 2024 Star Health breach. **Section 8** ensures consent withdrawal, while **Section 11-13** mandates purpose limited processing and audits. This act also involves penalties in result of data breach or due to non-compliance of rules under **Section 33** which allows financial penalties upto ₹250 crores.

ENFORCEMENT MECHANISM

Chapter V of the act establishes **Data Protection Board of India** which is responsible for monitoring data, adjudicating breaches and enforcing penalties. Power and composition of the

board is in the hands of government as they are required to appoint Chairperson of the board which again could be misused by the Central Government for its own benefit.

CHALLENGES IN ENFORCEMENT AND IMPLEMENTATION

INSTITUTIONAL FLAWS

Although as India's first all-encompassing data protection law, the Digital Personal Data Protection Act, 2023 is promising, it has significant institutional and structural flaws that undermine its efficiency. Number one among them is the absence of an autonomous watchdog agency. The Data Protection Board of India, as the key adjudicatory and enforcement agency created under Chapter V of the Act, is controlled by the Central Government. The executive holds complete power to appoint members, their term of office, and the framing of the Board's working procedures, which is raising serious issues about its independence. It goes against recognized constitutional norms as in Union of India v. R. Gandhi (2010) 11 SCC 1, where the Supreme Court emphasized the need for adjudicatory institutions to have their independence.

CROSS- BORDER RISKS

Section 6 ambiguous cross-border provisions do not keep up with GDPR's protection, as the CJEU in Data Protection Commissioner v. Facebook Ireland Ltd. & Schrems struck down EU-US transfers for insufficient safeguards. India's 206,000 incidents in 2024 highlight the imperative of strong frameworks.

PRACTICAL HURDLES

Additionally, **Section 40** of the Act authorizes the Central Government to make rules on significant issues such as the definition of "Significant Data Fiduciaries," international data transfer standards, and Board procedures without explicit legislative direction. Such over-delegation contravenes the constitutional prohibition against delegating fundamental legislative powers, as in In Re: Delhi Laws Act AIR (1951) SC 332 and Devans Modern Breweries (2004) 5 SCC 558. Finally, the redressal mechanism for grievances is ambiguous, without enforceable timelines or process guarantees for data principals, and especially prejudicing vulnerable users.

CONCLUSION

Digital Personal Data Protection Act, 2023 is a long awaited but a perfect step towards codifying privacy protection in India. While it looks promising, it has notable structural limitations include limited rights framework and lack of institutional independence which undermine its capabilities.

It is necessary to uphold the spirit for Puttaswamy judgment and meet global standards for that future reforms must be made that would help the act to align with constitutional principles and regulatory autonomy. It must avoid replicating historical patterns of unaccountable governance in digital age.