# SHORTCOMINGS OF THE DPDP ACT

## Shortcomings of The DPDP Act

**AUTHOR'S NAME : Aritra Dutta**

**INSTITUTION - Jindal Global Law School**

In August 2023, the Indian Parliament enacted the Digital Personal Data Protection Act, 2023.[1] This groundbreaking legislation marks India's first comprehensive law addressing personal data protection across various sectors. It comes as a result of extensive discussions spanning over five years[2], reflecting a significant development in India's data privacy landscape.

Amidst India's urgent need for a Data Protection Act, driven by rampant cyber-attacks, limited accountability for personal data, and frequent cyber frauds, the introduction of the Digital Personal Data Protection Act 2023 (DPDP) has been met with disappointment. The Act, coming after a prolonged anticipation, not only leaves many of its clauses open to public interpretation but also raises significant concerns, which include deficiencies such as falling short of addressing the critical issues it was expected to tackle in the evolving digital landscape.

Firstly, the Act does not prescribe a definite timeline for the report of breaches. While the European counterpart, the General Data Protection Regulation (GDPR) prescribes the mandated timeline of 72 hours for reporting data breaches[3], the DPDP Act within Rule 8(6) does not prescribe a time limit for the reporting ofbreaches, which presents an opportunity for data fiduciaries to delay the reporting of such breaches in order to evade penalty, which will undoubtedly impact the Right to Privacy of Data Principals.

Secondly, another shortcoming of the Data Protection Act is the lack of security auditing mandates. A security audit is crucial for detecting and addressing data security flaws, and it is done for the purposes of testing whether a company has the capability of securing sensitive data. When such audits are not performed, the gaps and lapses that are present within in a company's data protection framework are revealed. This is akin to letting companies self-

[1]The Digital Personal Data Protection Act, 2023 (No. 22 of 2023), Gazette of India, August 11, 2023
[2]Justice K.S. Puttaswamy and Anr. v. Union of India and Ors. (10 SCC 1, Supreme Court of India, 2017)
[3]Article 33 GDPR 2018

regulate their tax compliance without audits. Considering the law's enactment in 2023, it's surprising that it doesn't mandate regular third-party security audits for sensitive sectors like healthcare and fintech, unlike countries such as the USA, Singapore, UAE, and Oman. The Act only mentions government-recommended audits for certain cases involving national safety or public order.

Looking further into the legislation, Rule 37[1][b] and 37[2] of the act enable the central government to restrict public access to any content recommended by the board after consulting the relevant data fiduciary. This provision allows the government to remove content, even if it's critical of the government, without the involvement of neutral third parties like courts. This raises concerns about the potential for censorship, as the central government holds the power to determine the accessibility of information to the public. For example, if a Comptroller and Auditor General (CAG) report uncovers corruption in a government department over a public welfare project, the central government could potentially direct various media outlets, including newspapers, television channels, YouTube, Instagram, and other social media platforms, to stop disseminating such news, with the threat of penalties for non-compliance. This illustrates a scenario where the government could exert control over the flow of information.

Another problem that may be highlighted is the fact that despite the inclusion of "personal" in its title, the bill defines personal data rather vaguely as *"any data about an individual who is identifiable by or in relation to such data*."[4] This broad and somewhat nebulous definition leaves room for interpretation. It's unclear whether various types of data like images, audio, metadata, analytics, and video transcripts are covered under this definition of personal data. Furthermore, the bill does not clearly distinguish between sensitive, confidential, Personally Identifiable Information (PII), and public data, nor does it establish distinct governance rules for these categories. This ambiguity in the bill could lead to loopholes, particularly during data breaches, where organizations might argue that the compromised data does not constitute personal data. It also diminishes the significance of breaches involving non-personal data, such as corporate assets or copyrighted material.

The most alarming issue with the Act is the extensive data access granted to the government. Under section 17[2][a], the government can request any data for national sovereignty and integrity, but it's unclear if such requests must be recorded and made public. Rule 36 also

[4]S.2(t) The Digital Personal Data Protection Act, 2023

permits the government to demand any data without stating its intent, lacking transparency. These provisions raise concerns about surveillance and targeting opposition. The Act also lacks provisions for penalties related to spreading fake news and regulations for data storage and transmission, leaving gaps in the anticipated privacy framework.

In conclusion, the Digital Personal Data Protection Act, 2023, represents a pivotal step in India's journey towards data privacy regulation. However, compared to the GDPR, which addresses similar concerns with more definitive and stringent measures, the DPDP Act exhibits several critical shortcomings. These include ambiguities in definitions, lack of mandatory security audits, potential for government censorship, and excessive government access to data without adequate transparency or checks. This contrast underscores that India's privacy laws still have a considerable distance to cover to provide robust data protection akin to global standards like the GDPR. This journey is essential for safeguarding individual privacy rights and fostering a trust-based digital environment.