DATA PRIVACY IN INDIA: A CRITICAL ANALYSIS OF THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

Drashti Mehta, KES' Shri Jayantilal H. Patel Law College, Mumbai

Ami Bhandari, KES' Shri Jayantilal H. Patel Law College, Mumbai

ABSTRACT

The Explosive growth of digital technologies has increased concerns surrounding the protection of personal data in India. The Digital Personal Data Protection Act, 2023 represents a notable legislative initiative aimed at regulating the collection, processing, and storage of personal data within a structured legal framework. This paper examines the principal features of the Act, including its consent-oriented approach, the rights granted to individuals, and the obligations enforced on data fiduciaries. It further analyses the extent to which the Act fulfils the constitutional requirement of safeguarding privacy, as recognised in judicial precedent. While the legislation introduces significant mechanisms aligned with international data-protection standards, it also raises concerns relating to state exclusions, enforcement capacity, and practical implementation challenges. The paper concludes that although the Act marks meaningful progress, further refinement and effective enforcement are necessary to ensure strong data protection in India.

Keywords: Data Privacy, Digital Personal Data Protection Act, 2023, Informational Privacy, Data Protection Law, Fundamental Right to Privacy

INTRODUCTION

The globalization of digital technologies into everyday life has resulted in an unprecedented production and circulation of personal data. In India, this transformation has escalated concerns regarding the misuse of sensitive information, including financial details, identity records, and digital tracking patterns . As digital participation continues to expand, the risks associated with data breaches, identity theft, and unauthorized surveillance have become more evident.

The recognition of privacy as a fundamental right by the Supreme Court in Justice K. S. Puttaswamy v. Union of India marked a turning point in India's constitutional framework. The judgment highlighted the necessity of protecting informational privacy and the State's obligation to establish a comprehensive data protection regime. Prior to this development, the legal framework governing data protection remained fragmented and insufficient to address emerging technological challenges.

In response, the enactment of the Digital Personal Data Protection Act, 2023 seeks to provide a systematic approach in regulating personal data throughout India . The legislation introduces clearly defined roles, including Data Principals and Data Fiduciaries, and establishes a system of rights and duties designed to enhance accountability in data processing. At the same time, it attempts to balance individual privacy with broader considerations such as governance and economic development.

This paper adopts a doctrinal method to analyse the key provisions of the Act and evaluate its effectiveness in protecting the right to privacy. It further examines whether the current framework adequately addresses the challenges posed by growing data dependence on both public and private sectors.

KEY PROVISIONS OF THE ACT

Consent–Based Data Processing

The Digital Personal Data Protection Act, 2023 adopts a consent-governed model as the basic foundation for lawful data processing. Under this framework, personal data can be processed only when a clear and lawful purpose exists, and either valid consent has been acquired or the processing falls within specified authorised uses.

For consent to be legally valid, it must fulfill certain qualitative standards. It should be given voluntarily and must be explicit, informed, and clearly communicated through an affirmative action. This obligation ensures that individuals are not unwittingly subjected to data processing practices. The Act also deters practices that weaken genuine consent, such as pre-set options or vague authorisations.

An important feature of the framework is the highlighting on transparency. Data Fiduciaries are required to provide accessible and intelligible notices outlining the purpose of data collection and the rights available to individuals. Without such disclosure, consent cannot be regarded as meaningful.

Additionally, individuals retain ongoing control over their data through the right to cancel their consent. The Act mandates that this process should be simple and equivalent to the method used for granting consent. Once consent is withdrawn, the entity must stop processing, unless retention is justified under legal or regulatory requirements.

Rights of Data Principals

The Digital Personal Data Protection Act, 2023 grants individuals a set of enforceable rights designed to enhance their control over personal data. These rights enable individuals to seek information regarding how their data is being processed, including details about the nature, purpose, and entities involved in such processing.

In addition to the right to access information, individuals are entitled to request correction of inaccurate or incomplete data, as well as the erasure of data that is no longer necessary for the purpose for which it was collected. These provisions aim to ensure both accuracy and relevance in data handling practices.

The Act also introduces the concept of nomination, allowing individuals to designate another person to exercise their rights in the event of death or incapacity. This provision reflects an effort to extend data protection beyond the lifetime or capacity of the individual.

Furthermore, a structured grievance redressal mechanism is provided, enabling individuals to raise complaints against data fiduciaries. However, the Act also imposes certain responsibilities on individuals, such as refraining from filing false or frivolous complaints or misrepresenting identity. This reflects an attempt to balance individual empowerment with accountability.

Obligations of Data Fiduciaries

Under the Digital Personal Data Protection Act, 2023, entities responsible for determining the purpose and means of processing personal data are subject to specific obligations intended to ensure responsible data governance.

A key requirement is the maintenance of data accuracy and completeness, particularly where such data is likely to be used for decision-making affecting individuals. This obligation is essential to prevent harm arising from incorrect or outdated information.

Data Fiduciaries are also required to implement appropriate technical and organisational safeguards to protect personal data from unauthorized access, disclosure, or loss. These safeguards play a crucial role in mitigating the risks associated with data breaches in an increasingly digital environment.

In the event of a breach, the Act mandates prompt notification to both the regulatory authority and affected individuals. This requirement promotes transparency and allows individuals to take necessary precautions to minimise potential harm.

The principle of storage limitation is also incorporated, requiring entities to retain personal data only for as long as necessary to fulfil the specified purpose. However, certain exemptions—particularly those applicable to government entities—raise concerns regarding unequal standards of accountability within the framework.

Penalties for Violations

The Digital Personal Data Protection Act, 2023 establishes a penalty-based enforcement mechanism aimed at ensuring adherence to its provisions. The Act prescribes substantial financial penalties for various categories of non-compliance, thereby creating a strong deterrent against negligent or unlawful data practices.

For instance, failure to implement adequate security safeguards or to prevent data breaches may result in significant monetary penalties. Similarly, violations relating to the processing of children's data attract stringent consequences, reflecting the heightened need for protection in such cases.

These penalties are imposed by the Data Protection Board of India following an inquiry process, which is intended to ensure procedural fairness. While the magnitude of penalties demonstrates regulatory seriousness, their effectiveness ultimately depends on consistent and impartial enforcement.

At the same time, the Act provides certain exemptions to the State in relation to data processing. While these may be justified on grounds such as national security or public interest, their broad scope raises questions regarding the balance between regulatory enforcement and governmental discretion.

CRITICAL ANALYSIS

Strengths:

One of the notable strengths of the Digital Personal Data Protection Act, 2023 lies in its effort to create a unified legal framework for data protection in India. Prior to its enactment, the regulatory landscape was fragmented, leading to inconsistencies and gaps in enforcement. The Act addresses this issue by introducing a structured regime that aligns with global developments in data protection law.

The emphasis on consent as a central principle reflects a shift towards recognising individual autonomy in data-related decisions. By requiring that consent be informed and clearly

expressed, the Act attempts to ensure that individuals retain meaningful control over their personal information.

Another important strength is the introduction of significant financial penalties for non-compliance. These penalties serve as a deterrent and encourage organisations to adopt stronger data protection practices. The establishment of a dedicated regulatory body further contributes to institutional accountability.

Limitations:

Despite its strengths, the Act raises several concerns. A primary issue relates to the scope of exemptions granted to the State. The broad discretionary powers available to government authorities may undermine the objective of protecting privacy, particularly in the absence of

stringent safeguards or oversight mechanisms.

Enforcement also presents a challenge. The effectiveness of the framework depends heavily on the capacity and independence of the regulatory authority. Without adequate resources and autonomy, there is a risk that enforcement may be inconsistent or insufficient to address violations.

Additionally, the practical implementation of the consent framework may be limited by low levels of digital literacy. Many individuals may not fully understand the implications of consenting to data processing, especially when privacy notices are complex or inaccessible. This creates a gap between the legal framework and its real-world effectiveness.

CONCLUSION

The Digital Personal Data Protection Act, 2023 represents a significant development in India's approach to data governance. By establishing a comprehensive framework for the regulation of personal data, the Act seeks to address longstanding gaps in the legal system and respond to the challenges posed by rapid digitalisation.

In light of the recognition of privacy as a fundamental right in Justice K. S. Puttaswamy v. Union of India, the Act reinforces the importance of safeguarding individual autonomy in the digital age. However, its success will depend not only on the strength of its provisions but also on the effectiveness of its implementation.

Key concerns, including broad state exemptions, enforcement limitations, and lack of public awareness, highlight the need for continued refinement of the framework. Addressing these issues will be essential to ensure that the objectives of the legislation are fully realised.

Ultimately, the Act must strike a careful balance between enabling technological and economic advancement and protecting the fundamental right to privacy. Achieving this balance will determine the long-term effectiveness of India's data protection regime.

REFERENCE

[1]Kashyap, Pradip. (2024). DIGITAL PERSONAL DATA PROTECTION ACT, 2023: A new light into the data protection and privacy law in India.

[2]*Justice K. S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

[3]https://www.taxmann.com/post/blog/lawful-processing-and-consent-under-dpdp-act?amp

[4]https://www.dpdpa.com/dpdpa2023/chapter-2/section4.html?utm_source=perplexity

[5]https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023?utm_source=perplexity

[6]https://ksandk.com/data-protection-and-data-privacy/consent-under-dpdp-act-2023-compliance-strategies/?utm_source=perplexity

[7]https://www.nishithdesai.com/research-and-articles/hotline/technology-law-analysis/indias-digital-personal-data-protection-act-2023-history-in-the-making-10703

[8]https://eprajournals.com/IJMR/article/16128/abstract

[9]https://www.tscld.com/does-the-dpdpa-2023-strengthen-the-right-to-privacy-in-india-a-constitutional-perspective?utm_source=perplexity