THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023: A SIMPLIFIED LEGAL ANALYSIS

Prasanna Pramod Vaidya*

ABSTRACT

In the contemporary digital ecosystem, personal data has emerged as a critical asset, necessitating robust legal protection to safeguard individual privacy and prevent misuse. The Digital Personal Data Protection Act, 2023, represents India's first comprehensive legislation dedicated to regulating the processing of digital personal data. This article provides an analytical and exam-oriented overview of the Act, tracing the evolution of data protection in India from the Information Technology Act, 2000, to the recognition of privacy as a fundamental right in Justice K.S. Puttaswamy v Union of India. It examines the key features of the Act, including consent-based processing, rights of data principals, obligations of data fiduciaries, and the role of the Data Protection Board. The article further evaluates the strengths of the framework while critically addressing its limitations, such as broad state exemptions and enforcement challenges, thereby offering a balanced understanding of India's emerging data protection regime.

Keywords: Data Privacy, DPDP Act 2023, Informational Privacy, Data Protection Law, Digital Rights.

INTRODUCTION

In the contemporary digital age, personal data has become one of the most valuable resources. Everyday activities such as online shopping, social media usage, digital payments, e-governance services, and mobile applications involve the constant sharing of personal information. While digitalisation has increased efficiency and accessibility, it has also exposed individuals to serious risks such as data misuse, identity theft, profiling, and surveillance. These

*BA LLB, FIRST YEAR, DES SHRI NAVALMAL FIRODIYA LAW COLLEGE, PUNE.

concerns made it necessary for India to adopt a comprehensive legal framework for data protection.

The Digital Personal Data Protection Act, 2023 (hereinafter referred to as the DPDP Act) represents India's first comprehensive law dedicated exclusively to the protection of personal data in digital form. The Act seeks to balance the right to privacy of individuals with the legitimate needs of the State and private entities to process personal data for lawful purposes. This article aims to provide a simplified and exam-oriented legal analysis of the DPDP Act, explaining its background, key provisions, rights and duties, and major criticisms in clear and accessible language.

MEANING AND IMPORTANCE OF DATA PRIVACY

Data privacy refers to the right of individuals to control the collection, use, storage, and disclosure of their personal information. Personal data includes any data by which an individual can be identified, such as name, address, phone number, Aadhaar number, email ID, biometric data, financial details, and online identifiers.

In the absence of adequate legal safeguards, personal data can be misused for commercial exploitation, discrimination, surveillance, and cybercrime. Data privacy laws are therefore essential to protect individual autonomy, dignity, and informational self-determination. In India, the recognition of privacy as a fundamental right has further strengthened the need for statutory data protection.

THE EVOLUTION OF DATA PROTECTION IN INDIA

The evolution of data protection in India has been gradual, moving from a fragmented statutory approach to a comprehensive rights-based framework. The Information Technology Act 2000 was the first legislation to incidentally address data protection, particularly through section 43A, which imposed liability on body corporates for failure to protect sensitive personal data, though its primary focus remained cybercrime and e-commerce rather than privacy protection.[1]

To operationalise section 43A, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 were introduced, defining sensitive personal data and mandating consent, privacy policies, and reasonable security

[1] Information Technology Act 2000, s 43A.

practices; however, their applicability was limited to private entities and excluded the State, resulting in weak enforcement.[2]

A constitutional shift occurred with Justice K.S. Puttaswamy (Retd.) v Union of India, where a nine-judge bench of the Supreme Court of India unanimously recognised the right to privacy as a fundamental right under Article 21, emphasising informational privacy and the necessity of a comprehensive data protection law.[3]

This landmark judgment directly influenced legislative reform, culminating in the enactment of the Digital Personal Data Protection Act 2023, which establishes a dedicated framework for personal data protection based on consent, defines the roles of data fiduciaries and data principals, grants enforceable rights to individuals, and introduces significant penalties for non-compliance, thereby marking a decisive shift towards a modern data protection regime in India.[4]

KEY FEATURES OF THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

The Digital Personal Data Protection Act, 2023 (DPDP Act) represents a landmark development in India's data protection jurisprudence by providing a unified statutory framework governing the processing of digital personal data. The Act applies to personal data processed within India, where such data is collected in digital form or collected offline and subsequently digitised, thereby covering most contemporary data practices. In addition, the Act has extra-territorial applicability where personal data is processed outside India in connection with the offering of goods or services to individuals within India, reflecting the global and borderless nature of digital data flows. However, the Act carves out specific exclusions, including personal data processed for personal or domestic purposes and personal data that has been made publicly available either by the data principal or under a legal obligation. A defining feature of the Act is its strong emphasis on consent-based processing of personal data. Consent must be free, specific, informed, unconditional, and unambiguous, and must be signified through a clear affirmative action. To ensure transparency, data fiduciaries are required to provide a clear and accessible notice detailing the purpose of processing, the categories of personal data involved, and the rights available to data principals. The Act also recognises the

[2] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.
[3] *Justice K.S. Puttaswamy (Retd.) v Union of India* (2017) 10 SCC 1.
[4] Digital Personal Data Protection Act 2023.

right of data principals to withdraw consent at any time, subject to the consequences of such withdrawal being communicated in advance. At the same time, the DPDP Act balances individual autonomy with administrative efficiency by recognising certain "legitimate uses" where consent is not required, such as compliance with law, performance of State functions, or provision of benefits and services. This approach seeks to harmonise privacy protection with governance and public interest considerations.

Another significant feature of the DPDP Act is the articulation of enforceable rights of data principals alongside clearly defined duties of data fiduciaries, thereby embedding accountability into the data processing ecosystem. Data principals are granted the right to obtain information about the personal data processed by a data fiduciary, including the nature of data processed and the purpose for which it is used. They also possess the right to correction, completion, updating, and erasure of personal data that is inaccurate, misleading, or no longer necessary for the stated purpose. The right to withdraw consent and the right to grievance redressal further strengthen individual control over personal data and provide procedural safeguards against misuse. Complementing these rights are the duties imposed on data fiduciaries, who are required to process personal data lawfully, fairly, and only for specified and legitimate purposes. Data fiduciaries must ensure the accuracy and completeness of personal data, implement reasonable security safeguards to prevent data breaches, and erase personal data once the purpose of processing has been fulfilled, unless retention is required under law. The Act also introduces the category of Significant Data Fiduciaries, identified based on factors such as volume and sensitivity of data processed and risk to the rights of individuals. Such fiduciaries are subject to additional obligations, including the appointment of a Data Protection Officer, conducting data protection impact assessments, and undertaking periodic audits. These enhanced duties reflect a risk-based regulatory approach aimed at mitigating harms arising from large-scale data processing.

The DPDP Act places special emphasis on the protection of children's personal data, recognising their heightened vulnerability in digital environments. A child is defined as an individual below the age of eighteen years, and processing of a child's personal data requires verifiable consent of a parent or lawful guardian. The Act expressly prohibits tracking, behavioural monitoring, and targeted advertising directed at children, thereby prioritising their welfare over commercial interests. In addition to substantive obligations, the Act establishes a comprehensive framework for penalties and enforcement to ensure compliance. The Data

Protection Board of India is designated as the primary enforcement authority, empowered to inquire into instances of non-compliance, impose monetary penalties, and direct remedial measures. Penalties under the Act are civil in nature and may extend to substantial amounts depending on the nature, gravity, and duration of the breach, particularly in cases involving failure to implement reasonable security safeguards or violations relating to children's data. The penalty-based enforcement mechanism seeks to create deterrence while avoiding excessive criminalisation. Overall, the Digital Personal Data Protection Act, 2023, marks a decisive transition from fragmented and limited data protection norms to a comprehensive, consent-driven, and accountability-oriented regulatory regime, aligning constitutional privacy values with the practical realities of India's rapidly expanding digital economy.

RIGHTS OF INDIVIDUALS UNDER THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

Under the Digital Personal Data Protection Act, 2023 (DPDP Act), individuals whose personal data is processed are referred to as Data Principals. The Act recognises several statutory rights to ensure informational self-determination, transparency, and accountability in data processing.

Right to Information about Personal Data: A data principal has the right to obtain information from a data fiduciary regarding the processing of their personal data. This includes details of the personal data being processed, the purpose of such processing, and the identities of data fiduciaries or processors with whom the data has been shared. This right enhances transparency and allows individuals to understand how their data is being used.

Right to Correction and Erasure: The Act grants data principals the right to seek correction, completion, updating, and erasure of their personal data. If personal data is inaccurate, incomplete, misleading, or no longer necessary for the purpose for which it was collected, the data fiduciary is required to rectify or delete such data. This right ensures data accuracy and prevents continued misuse or unnecessary retention of personal information.

Right to Withdraw Consent: Since the DPDP Act is fundamentally based on consent, data principals have the right to withdraw their consent at any time. Upon withdrawal, the data fiduciary must cease processing the personal data, unless such processing is permitted under legitimate uses provided by the Act. The ease of withdrawal must be comparable to the ease with which consent was given, reinforcing individual autonomy.

Right to Grievance Redressal: The Act provides data principals with the right to access effective grievance redressal mechanisms. Data fiduciaries are required to establish procedures for addressing complaints relating to personal data processing. If a data principal is dissatisfied with the response, they may escalate the matter to the Data Protection Board of India. This right ensures enforcement and accountability.

Right to Nominate: A unique feature of the DPDP Act is the right to nominate another individual who may exercise the data principal's rights in the event of death or incapacity. This provision reflects a rights-based and humane approach, ensuring continuity of data protection even when the data principal is unable to act.

CRITICISMS AND CHALLENGES OF THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

Despite being a significant step towards recognising informational privacy, the Digital Personal Data Protection Act, 2023 (DPDP Act) has attracted considerable criticism on substantive, institutional, and practical grounds. One major criticism relates to the broad exemptions granted to the State. The Act allows the government to exempt any of its agencies from the application of the law on grounds such as sovereignty, public order, or security of the State. These exemptions are phrased in wide and discretionary terms, raising concerns about potential misuse and dilution of the fundamental right to privacy. Critics argue that such sweeping powers undermine the proportionality standard laid down in constitutional jurisprudence and may result in excessive surveillance without adequate safeguards or judicial oversight.

Another important criticism concerns the limited independence of the enforcement mechanism. The Data Protection Board of India, which is entrusted with enforcement, is constituted and controlled by the executive, with no clear guarantees of institutional independence comparable to constitutional or quasi-judicial bodies. The absence of strong structural safeguards may weaken impartial adjudication, especially in cases involving State entities. Further, the DPDP Act adopts a penalty-only enforcement model, excluding compensation to affected individuals for harm suffered due to data breaches. This shift from a rights-remedial framework to a compliance-focused regime has been criticised for prioritising regulatory efficiency over individual justice. For data principals, the lack of a direct statutory right to compensation limits meaningful remedies in cases of serious data misuse.

The Act also faces criticism for its narrow scope of applicability, as it applies only to digital personal data. Personal data processed in non-digital form that is never digitised remains outside its purview, creating regulatory gaps in sectors where manual record-keeping is still prevalent. Additionally, the absence of a distinction between personal data and sensitive personal data has been questioned, as it subjects all categories of personal data to a uniform compliance framework. This may dilute protection for highly sensitive information such as health or biometric data, which arguably requires enhanced safeguards.

From a rights perspective, concerns have been raised about the limited set of rights available to data principals. The DPDP Act does not recognise certain internationally accepted data protection rights, such as the right to data portability and the right to object to processing. This places India's framework at a comparatively lower standard than comprehensive regimes like the GDPR. Moreover, the emphasis on consent as the primary ground for processing may be problematic in practice, as individuals often lack real bargaining power or understanding in digital ecosystems, making consent more formal than meaningful.

Practical implementation also presents serious challenges. Compliance obligations may impose a significant burden on small businesses and startups, which may lack the technical and financial capacity to meet security, consent, and grievance redressal requirements. At the same time, enforcement effectiveness depends heavily on delegated legislation and executive rule-making, leading to uncertainty until subordinate rules are fully operationalised. The lack of clarity on cross-border data transfers and evolving technological practices, such as artificial intelligence, further complicates implementation.

CONCLUSION

In conclusion, the Digital Personal Data Protection Act, 2023, marks a significant milestone in India's journey toward a robust and rights-based data protection regime. By formally recognising the importance of informational privacy in an increasingly digital society, the Act seeks to balance individual rights with the legitimate needs of the State and businesses in the digital economy. Its emphasis on consent-based processing, accountability of data fiduciaries, and protection of children's data reflects a clear legislative intent to foster trust in digital governance and online transactions. However, the effectiveness of the DPDP Act will depend not only on its legal framework but also on widespread public awareness. Citizens must be educated about their rights and remedies, while organisations must be sensitised to their

compliance obligations to ensure meaningful implementation. Looking ahead, as technologies such as artificial intelligence, big data analytics, and cross-border data flows continue to evolve, India's data protection framework will need to remain adaptive and responsive. The DPDP Act should therefore be viewed as a foundational step, with future amendments, judicial interpretation, and regulatory guidance shaping the long-term future of data privacy in India.