DIGITAL PERSONAL DATA PROTECTION ACT, 2023: FIRST ATTEMPT INCONSISTENCIES AND CHALLENGES

Yash Vardhan Singh*

ABSTRACT

The Digital Personal Data Protection Act, 2023, marks India's first comprehensive legislative effort to regulate the processing of personal data in an increasingly digitised economy. Enacted in the backdrop of the Supreme Court's landmark decision in Justice K.S. Puttaswamy v. Union of India, which recognised the right to privacy as a fundamental right under Article 21 of the Constitution, the Act seeks to balance individual data protection rights with legitimate state and commercial interests. Alongside the Act, the Digital Personal Data Protection Rules, 2025, aim to operationalise its provisions and facilitate phased compliance. This paper critically analyses the statutory framework of the DPDP Act, 2023 and the accompanying Rules, identifying both progressive developments and significant legal inconsistencies. On the positive side, the Act introduces notable mechanisms such as the recognition of persons with disabilities as Data Principals, the institutionalisation of Consent Managers, and enhanced transparency obligations on Data Fiduciaries. These provisions reflect an attempt to adopt an inclusive and user-centric approach to data governance, distinguishing the Indian framework from several international models. However, the paper argues that these advancements are undermined by broad executive exemptions, ambiguous statutory terminology, and internal contradictions between the Act and the Rules. Provisions relating to Significant Data Fiduciaries, undefined standards such as "legitimate uses" and "reasonable security safeguards," and expansive state exemptions justified on grounds of sovereignty, security, and integrity raise serious concerns regarding surveillance, accountability, and erosion of consent. Further, inconsistencies in prescribed timelines for data retention and breach notification dilute enforcement efficacy and create uncertainty for both Data Principals and Data Fiduciaries. The paper concludes that while the DPDP Act, 2023, represents an essential step

*LLB, FIRST YEAR, CAMPUS LAW CENTRE, UNIVERSITY OF DELHI.

towards establishing a data protection regime in India, its effectiveness depends upon narrowly tailored exemptions, clearer definitions, and alignment between primary legislation and delegated rules. Without such reforms, the Act risks falling short of the constitutional promise of informational privacy affirmed by the judiciary.

Keywords: Digital Personal Data Protection Act, 2023, Article 21, K.S. Puttaswamy v. Union of India.

INTRODUCTION

The Digital Personal Data Protection Act, 2023 (hereinafter referred to as "the Act") is the first attempt at building a framework that aims to strike a balance between protecting the rights of citizens pertaining to their personal data while lawfully allowing companies to process it for certain uses.

The Digital Personal Data Protection Rules, 2025, are a comprehensive set of rules that guide the application and enforcement of the Act. The rules will be implemented in a phased manner to allow the companies to adopt them seamlessly. This paper argues that while the DPDP Act, 2023, marks a significant step towards data protection in India, its broad executive exemptions, undefined standards, and internal inconsistencies risk undermining constitutional privacy protections.

EVOLUTION AND BACKGROUND

In 2012, multiple petitions were filed before the Supreme Court challenging the norms for the compilation of demographic biometric data by the Government of India as a violation of the Right of Privacy of an individual. The case was led by the petition filed by Justice K. S. Puttaswamy.[1]

A nine-judge bench was constituted, which, while pronouncing the judgment, unanimously held that "the right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 of the Indian Constitution and as a part of the freedoms guaranteed by Part III of the Constitution."

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

The Supreme Court, by doing so, also overruled the precedent held in M. P. Sharma v. Satish Chandra, District Magistrate, Delhi, decided by an eight-judge bench,[2] and Kharak Singh v. State of Uttar Pradesh[3] observing in both cases that there was no express recognition of the Right of Privacy in the Indian Constitution.

After the landmark judgment of the Justice Puttaswamy Case, a committee was set up under the Chairmanship of Justice B. N. Srikrishna in August 2017, which submitted its report in July 2018 titled "A Free and Fair Digital Economy" along with a Draft of the Data Protection Bill.[4] The report suggested a robust data protection framework for India. It recommended classifying personal data, establishing fiduciary obligations for data processors, mandatory data localization and other measures it deemed fit for the evolving needs and rights of a digital population in the coming years.[5]

A revised draft of the Bill was released by the Ministry of Electronics and Information Technology, headed by Ashwini Vaishnaw, on November 18, 2022, titled the Digital Personal Data Protection Bill, 2022.

The Bill was passed by both houses of the Parliament and received the assent of the President on August 11, 2023 and matured into the Digital Personal Data Protection Act, 2023 and subsequently, to bridge the gap between generic provisions and effective enforcement of those provisions.[6]

WELCOME STEPS

While the Digital Personal Data Protection Act, 2023, has its own shortcomings, some of the provisions incorporated within the Act are welcome steps that address the needs of an evolving and progressive society. These steps are purposefully meant to widen the ambit of the application and enforcement of the Act in India. Such steps include:

Inclusivity About PwD Citizens: Section 2(j) defines Data Principal as the individual to whom the personal data relates, and where such individual is—

[2] *M P Sharma v Satish Chandra, District Magistrate, Delhi [1954] SCR 1077 (SC)*
[3] *Kharak Singh v State of Uttar Pradesh [1964] 1 SCR 332 (SC)*
[4] https://elplaw.in/wp-content/uploads/2023/09/ELP-Discussion-Paper-Justice-BN-Srikrishna-Committee-Data-Protection-2.pdf
[5] https://prsindia.org/policy/report-summaries/free-and-fair-digital-economy
[6] Aiman J. Chishti, 'President Gives Assent to Digital Personal Data Protection Act, 2023' (LiveLaw, 12 August 2023) www.livelaw.in accessed on 26 December 2025

i. a child, includes the parents or lawful guardian of such a child;

ii. a person with disability, includes her lawful guardian, acting on her behalf;

It is commendable that the Act includes persons with Disabilities as regular Data Principals, something that is not present even in the model legislation of the European Union called the "General Data Protection Regulation" (GDPR). Similar laws made in New Zealand, Canada and Japan also do not take into account the disabled citizens as a Data Subject (similar in definition to Data Principal).[7]

Consent Manager: The Act necessitates the creation of a Consent Manager, defined in Section 2(g) as a person registered with the Board, who acts as a single point of contact to enable a Data Principal to give, manage, review and withdraw her consent through an accessible, transparent and interoperable platform. Part A of the First Schedule of the Digital Personal Data Protection Rules, 2025, lays down the conditions required to be fulfilled by a company to be qualified to apply for appointment as a Consent Manager. Rule 4 underlines that the Board, on being satisfied of the qualification of a company, appoint them as a Consent Manager as well as suspends and cancels the registration if the Board deems it fit in the interests of the Data Principals.

Transparency in Resolving Queries: Rule 9 mandates every Data Fiduciary to prominently publish the business contact information of the person responsible for dealing with and resolving the queries of the Data Principals with respect to the processing of data. Where such Data Fiduciary is a Significant Data Fiduciary, it mandates the publication of the business contact information of a Data Protection Officer who shall adhere to the duties specified in sub-section (2) of Section 10 of the Act.

THE IRREGULARITIES AND INCONSISTENCIES

While no legislation can be perfect from the get-go, the Act also has its own share of shortcomings and inconsistencies that give the impression of certain aspects being a lacklustre attempt, while also raising questions about the Act being a Draconian provision meant to benefit the Government at the expense of the valuable data of the citizens. It cannot be

[7] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation) art 4 https://eur-lex.europa.eu accessed 19 December 2025

emphasised enough that Data is the new Oil, meaning that it is one of the most valuable assets in this day and age.[8]

Significant Data Fiduciary: The Seventh Schedule of the DPDP Rules, 2025, enables the Government to create a Significant Data Fiduciary under the authority of an officer of the Central Government. As per Rule 23, the Government may ask any intermediary or Data Fiduciary to furnish any information to them. Sub-section (2) states that disclosure of such information to the Government will not be made to the Data Principal. These provisions pose a grave threat towards decreased transparency and increased surveillance as they essentially allow the Government to furnish and process the Data of Data Principals without their consent.

Sovereignty, Security and Integrity: The Act is filled with ambiguous and uncertain terms that raise concerns about transparency and accountability. Values that you expect from a democratic and answerable government are hidden away under the garb of terms like "sovereignty, security and integrity".

Sub-section (2) of Section 17 of the Act exempts the State from any liability under the provisions of this Act if the State, or any instrumentality stemming from it, processes personal data in the interests of Sovereignty, Security and Integrity. Part A of the Fourth Schedule, laid down in DPDPR, 2025, fails to define "educational institutions" that can act as Data Fiduciaries under the Act. Without emphasis, the protection of children from any misuse of their data and targeted advertisements is of paramount importance. Some other terms, such as "legitimate uses", as per Section 4(1)(b) and "reasonable security safeguards", as per Section 8(5), are also either left undefined or have ambiguities within the given definitions.

Time Delays: The Rules lay down specified time periods under which certain acts have to be carried out. These include erasure of personal data, notification of breach of personal data to the Data Principal and the Government Board, etc. As per Rule 7, in case of personal data breach, the government board has to be notified within 72 hours with set headlines including the cause and potential consequences of such breach to the Data Principal. However, the intimation of such a breach to the Data Principal doesn't have to be carried out under a specified time limit. The term used in the Rule is "without delay", which, again, leads to subjectivity, derides transparency and decreases effectiveness in enforcement.

[8] Nayan Chandra Mishra, 'Sequestering Digital Autonomy: How New Data Protection Act Affects Digital Accessibility'(LiveLaw, 27 September 2023) www.livelaw.in accessed 25 December 2025

As per Rule 8, the personal data of a Data Principal has to be kept for a minimum time period of One Year before it is deleted by any Data Fiduciary. This has two problems:

It is in direct conflict with sub-section 7 of Section 8 of the Act, which states that any data being used by an intermediary or a Data Fiduciary has to be deleted when the purpose of that data is not being served, or the Data Principal has withdrawn their consent.

Companies that process huge amounts of data may not be able to take reasonable safeguards to protect it, as it may be under-prioritised and sidelined for not being in active use.

CONCLUSION

The Digital Personal Data Protection Act, 2023 and Digital Personal Data Protection Rules, 2025 are the first established legislative frameworks that are based on the idea of personal data protection in today's digital society. However, there are some impediments to its effective enforcement, which might render the judiciary burdened to widen the ambit of the Act and incorporate the rightful beneficiaries while deciding matters related to it.[9] If the legislature, by way of amendments or delegated legislation, corrects the flaws of the Act, it can lead to bolstering and establishing the Act as one of the key legislations to arrive in modern times.

Beyond legislative reform, the long-term success of India's data protection framework will inevitably depend on judicial interpretation and institutional independence. Given the breadth of delegated powers and exemptions available to the executive under the current regime, courts will play a crucial role in subjecting state action to standards of proportionality, necessity, and reasonableness as laid down in *Puttaswamy*.

Simultaneously, the effective functioning of the Data Protection Board must be ensured through transparency and insulation from executive influence. A rights-centric enforcement approach, rather than a compliance-driven or surveillance-oriented model, is essential to preserve public trust. Only through sustained judicial oversight and accountable governance can the DPDP Act evolve into a meaningful safeguard of informational privacy in India's digital future.

[9] Chandan Sha, 'Data Protection in India – From M.P. Sharma case to the DPDP Act, 2023' (JusCorpus Blogs, 27 December 2025) www.juscorpus.com accessed 29 December 2025