DATA PRIVACY AND PROTECTION IN INDIA: ANALYSE THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

Shyam Jaiswal*

ABSTRACT

This article, which is based on a critical analysis of the Data Personal Data Protection Act (DPDP), has emerged as a new concern relating to how to regulate digital personal data and the protection of citizens' rights in the digital age. This act aims to provide an individual right to privacy to protect individuals as well as establish a legal framework for the lawful processing of data by government and private individuals or organisations. There is some core elements related to the applicability of this provision which examined such as the rights of data principals, obligations of data fiduciaries, consent requirements, penalties for breaches and grievance redressal mechanisms and also highlights concerns, broader state exemptions, absence of certain user rights, and the strong claims of compliance and concludes with recommendations for improved privacy protections and endorsement of transformation in India.

Keywords: Digital Personal Data, Data Protection, Data, Privacy.

INTRODUCTION

The swift adoption of digital technology in India has led to a significant legal issue of protecting personal data. The "K.S. Puttaswamy judgment" signifies the pivotal judgment by the Supreme Court of India in Justice K.S. Puttaswamy vs. Union of India, which recognised the right to privacy as a fundamental right protected by the Constitution[1]. Until 2023, there was no distinct data protection legislation in India, and personal data was only subject to the provisions of the Information Technology Act, 2000. Consequently, in 2018, the government formed a

*BA LLB, FIRST YEAR, BHARATI VIDYAPEETH, NEW LAW COLLEGE, PUNE.

[1] Supreme Court Observer" (*Supreme Court Observer*, July 16, 2025) https://www.scobserver.in/cases/puttaswamy-v-union-of-india-fundamental-right-to-privacy-case-background/ accessed 24 December 2025

specialised committee and put forth legislative proposals. The Digital Personal Data Protection Act, 2023, received passage from Parliament in August 2023 and received Presidential assent on 11 August 2023[2]. It is India's inaugural standalone law about digital personal data. (Earlier objectives - Personal Data Protection Bill – 2019 and a Bill in 2022 - were evolving as a result of the prior Supreme Court privacy decision in 2017, but did not become law.)

The purpose of this Act is to strike a balance between the right of privacy of individuals and the permissible use of data. The framework adopts a "SARAL" (Simple, Accessible, Rational and Actionable) approach, emphasising the use of plain language for compliance. The Act is informed by seven principles: consent and transparency, purpose limitation, data minimisation, accuracy, storage limitation, security safeguards, and accountability. Together, these principles structure the processing of the digital personal data of individuals residing in India. The Act further provides for the establishment of a Data Protection Board to enforce the required provisions while prescribing penalties for non-compliance.

The remainder of this article focuses on the DPDP Act in detail. We first set the stage with a description of its scope, definitions and core principles. Then, we outline the rights and duties conferred to Data Principals (individuals) and obligations imposed on Data Fiduciaries (the entity that determines how it will be used). After that, we discuss state powers and some of the exemptions built into the Act. We also illustrate enforcement mechanisms, penalties, and implementation mechanisms such as the Data Protection Board. Finally, we will assess the Act from perspectives of interests – citizens' rights, governance, the digital economy, and administrative feasibility – and stakeholders' priorities. The article concludes by suggesting approaches to overcoming the challenges posed by the DPDP Act to strengthen the data protection regime in India.

SCOPE AND FUNDAMENTAL PRINCIPLES

The DPDP Act particularly concerns personal data that is "digital" in nature and relevant to the territorial jurisdiction of India. "Personal data" is defined quite broadly as "any data that relates to an identifiable individual." The law covers all data that is collected or digitised in digital form. The territorial reach of the law is also broad: it applies to personal data when processing activity occurs in India, as well as processing activity that occurs outside of India related to the

[2] The Digital Personal Data Protection Bill, 2023," PRS Legislative Research, n.d., https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023. accessed 24 December 2025

provision of goods or services to individuals residing in India. Consequently, foreign companies that provide goods or services to users in India must comply.

The two main definitions in the Act are Data Principal, which is universal for all individuals to whom the data relates, with additional clarification for children and Persons with Disabilities, and Data Fiduciary, which is any entity, company, organisation, or person that determines how and why an individual's personal data is processed. Third-party vendors are paid processors that act on behalf of fiduciaries under a contract. There is also a provision for the government to designate a class of Data Fiduciaries as "Significant Data Fiduciaries" based on data volume, sensitivity, and level of impact on the individual's rights. Significant Data Fiduciaries carry greater obligations, such as appointing a Data Protection Officer, conducting audits and impact assessments, and so on.

The Act embraces fundamental data protection principles. This means that organizations will have to obtain explicit consent from individuals before they can process their data for the stated processing purposes, request only data that is definitely needed (minimization), ensure the data is accurate and up to date, retain only as much data as is actually necessary for storage limitation purposes, put in place appropriately secure safeguards for the data, and be held accountable by the data fiduciaries for being non-compliant with relevant laws. In addition, the fiduciary must also be transparent: they must provide easy, stand-alone notices that are clear about what data is being collected, what data is being collected, and why, and they must obtain free consent, informed consent, and updateable consent. The government's press release describes this as a *"consent and transparency"* emphasis. Overall, the Act aims to foster trust by making rules clear and enforceable while enabling innovation within these guardrails.

RIGHTS OF DATA PRINCIPALS

Right to Information (Access): A Data Principal has the right to obtain a summary from a fiduciary of what her personal data is being processed and what processing they are doing. The Data Principal may also ask for the identities of all other parties (fiduciaries or processors) that were given access to that data and the nature of the data that was shared. (However, if the data was shared with an authorised governmental authority, then a fiduciary may not provide disclosure of that sharing.)[3]

[3] Taxmann, "Rights of Data Principals under the DPDP Act 2023" https://www.taxmann.com/post/blog/rights-of-data-principals-under-the-dpdp-act accessed 24 December 2025

Right to Correction and Erasure: If the Data Principal had previously consented to processing, the Data Principal has the right to ask a fiduciary to correct, complete, or erase her personal data. A fiduciary is required to correct any inaccuracies and any misleading data as soon as possible, and must update incomplete data. Further, if the individual requests deletion (erasure) of her data, the fiduciary must erase it unless the data is being retained for that original collection or if it is required by law.[4]

Right to Grievance Redressal: Every fiduciary or consent manager must establish a grievance redressal mechanism for affected Data Principals. The individual can lodge complaints of any violation of her rights, as well as the fiduciary's obligations. The fiduciary (or consent manager) shall reply within a certain timeframe (as defined by rules). The Data Principal must exhaust this internal remedy before any appeal to the Board or Tribunal for relief.[5]

Right to Nominate: A Data Principal can nominate another individual to exercise her rights. If the Data Principal dies or becomes incapacitated, the nominee will stand in the place of the Data Principal for purposes of exercising rights under the Act.

It is another section that deals with the Data Principal Duties (Section 15). In this section, there are some rules related to the breach of a duty, such as not filing false/frivolous complaints; this breach of a duty is redressable by penalty (up to ₹ 10,000).

OBLIGATIONS OF DATA FIDUCIARIES

Consent and Purpose Limitation: The fundamental principle of data minimisation is embodied in section 6 of the DPDP Act. There is a need for consent for operating digital personal data, which must be free, specified, explicated, unconditional and unambiguous with a clear affirmative action. This consent is processing of personal data only for the specified purpose.

Security Safeguards: Data fiduciaries must implement reasonable security measures - technical, organisational, and procedural - to protect against unauthorised access to, disclosure of, or destruction of data. Examples of security measures may include encryption, access

[4] Advocate Prashant Mali, "SECTION 12 | INTERPRETATION" https://www.dpdpa.com/dpdpa2023/chapter-3/section12.html> accessed 24 December 2025

[5] S&R Associates, "Navigating Data Minimization Requirements under India's DPDP Act" (*S&R Associates*, February 6, 2025) https://www.snrlaw.in/navigating-data-minimization-requirements-under-indias-dpdp-act/> accessed 24 December 2025

controls, regular vulnerability testing or assessments, and incident response procedures. The standard required will reflect industry standards, but the specifics will be provided through rules issued by the Data Protection Board.

Breach Notification: In the case of breach of a data, there are some mechanisms through which redresses the breach such as Data Fiduciaries must be immediately notify Data Principals Without Delay with particulars on their notification obligations and steps for mitigation of known harm to Data Principals and must also notify Board with an initial account and then the next 72 hours a detailed description of the same. This duty of care holds the Data Fiduciary accountable and prevents future Data Principals and/or risk of harm through the Data Fiduciary's obligation to notify and explain.[6]

Data Minimisation and Retention: Under Section 8(7) (b) of the DPDPA, a data fiduciary must ensure that its processor deletes any personal data shared for processing unless retention is required by law. This principle prevents data accumulation and associated exploitation risks. This is a framework to foster transparent and smooth regulations in the obligation of data fiduciaries.[7]

HOW IT CONNECTS WITH REAL-LIFE SITUATIONS

Withdrawal of Consent in Practice: The DPDP Act has a provision that a data Principal has the right to withdraw consent at any time, and the mechanism for withdrawal must be as easy and flexible as the mechanism for giving consent. For instance, a user subscribes to an online platform and agrees to all terms and conditions. Later, if the user faces the problem of breach of conditions, whatever is given in the conditions. They can withdraw consent immediately. It has an advanced version of the mechanism to show the red flags and protect the processing of the data.

Consent and Practical Applications: Section 6 of the DPDP Act mandates that data shall be processed only after obtaining free, specific, informed, unconditional, and unambiguous consent of the data Principle.[8] For instance, when a person downloads any apps, it asks to share

[6] Shubhi, "Digital Personal Data Protection Rules, 2025 Explained | SCC Times" (*SCC Times*, November 14, 2025) https://www.scconline.com/blog/post/2025/11/14/meity-notified-digital-personal-data-protection-rules-2025/

[7] "How Data Fiduciaries Should Engage Processors for Effective Compliance" *The New York Times and the Washington Post* (September 29, 2025) https://www.ey.com/en_in/insights/technology/how-data-fiduciaries-should-engage-processors-for-effective-compliance> accessed 24 December 2025

[8] Parliament, "THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023" (2023)

personal details, such as name, mobile number, address, and location. It has a provision under the DPDP Act; the app cannot collect or use that data unless the user agrees to it. If they share any personal data with a third party without consent, it would be a clear violation of the Act.

Data Breach and Financial Fraud: Data fiduciaries must ensure a proper mechanism for security safeguards and prevent personal data breaches. If it finds any data breach, it notifies the Data Protection Board "within a reasonable time'' followed by detailed reporting within 72 hours.

For instance, if a person's account is hacked and account holder details are leaked, in consequence of those unauthorised transactions, the bank would be responsible under the DPDP Act. It is the responsibility of the bank to notify the customer so that they can take reasonable steps, such as blocking cards or changing passwords.

KEY CHALLENGES ASSOCIATED WITH DPDP

Government Exemption and Surveillance Risks: In this Act, there are some exemptions granted to the government by the law for data operating in the interest of sovereignty and public order; it reflects the concern related to unregulated systems and casts doubt on the privacy violations.

For instance, from this issue, there has arisen the controversy that it is going contrary to the judgment of KS Puttaswamy on the fundamental right to privacy.

Non-dependence of Regulatory System: Despite the well-structured organisation of the Data Protection Board formed by the government, there are still concerns, such as a lack of transparency, full autonomy, and pre-decided enforcement, which can prove to be a barrier for public trust in data regulation.[9]

For instance, with an unequal power-sharing mechanism, such as appointments and administrative frameworks directly controlled by the executive, the board may not get opportunities to perform their role as a full liberal institution, which is crucial for surveillance on transparency.

https://prsindia.org/files/bills_acts/bills_parliament/2023/Digital_Personal_Data_Protection_Act,_2023.pdf accessed 24 December 2025

[9] (*Drishti IAS*) https://www.drishtiias.com/daily-updates/daily-news-editorials/towards-a-robust-digital-data-protection-regime-in-india> accessed 24 December 2025

Technological Gaps and New Digital Era: In modern times, emerging advanced technologies, such as blockchain, AI, big data, and IoT, are being developed. These are governed by decentralised mechanism systems, which is a rising concern related to regulatory gaps and legal uncertainties.

For instance, the most controversial term is "deepfake, which means the deliberate use of such forms of manipulation can lead to many outcomes, including the manipulation of public opinion, the destruction of an individual's reputation, or, as in some cases, crimes.

In the case of deepfakes in India, the actress Rashmika Mandaana, whose video clips had gone viral on social media, had her image negatively affected through the use of a forged video recording. In this case, we can see how society is misleading, creating rumours, and inculcating misinformation in the right person through hoax images, videos and audio clips. This algorithm is making unreal things real by using machine learning technology (AI).[10]

Lack of Public Awareness and Digital Literacy: After the 20th century, new users who lack digital literacy are particularly susceptible to phishing, online fraud, and false information, as are the elderly and those from low-income backgrounds. Lack of information about safe digital activities results in identity theft and financial losses, which are frequently ignored out of fear or ignorance of reporting procedures.

For instance, lack of public awareness and digital literacy in India are significant challenges, principally caused by infrastructure deficiencies, socioeconomic disparities, and a sharp urban-rural divide. Just 38% of Indian households are thought to be digitally literate; in rural areas, this percentage is only 25%, whereas in urban areas, it is 61%.

WAY FORWARD FOR STRENGTHENING INDIA'S DATA PROTECTION MECHANISM

Narrow State Exemptions: To promote trust, the legislation could provide greater clarity or limitations around exemptions. An example in this space would be to make it a requirement for judicial (warrant) oversight of the processing of certain security-related data, paperwork on the conditions and appropriateness of state notifications, and the requirement for periodic reviews

[10] Academike, "Illusions of Identity: Legislative Challenges Revolving around Deepfake Technology" (*Academike*, August 6, 2025) https://www.lawctopus.com/academike/illusions-of-identity-legislative-challenges-revolving-around-deepfake-technology/> accessed 24 December 2025

of notifications and exemptions. Introducing accountability measures on how government agencies utilise their exceptions (data audits, for example) would ensure that state practices encourage privacy norms.[11]

Expanding Data Principal Rights: Introducing explicit data portability rights and improved erasure provisions would support user agency. For example, a citizen would be able to request that their material be made accessible in a machine-readable format for use with an alternative service provider, and forget previous profiles or accounts with other service providers within the digital ecosystem. While consent remains an important element of individuals' agency, these supplementary conditions represent global best practices in data protection/privacy regimes and provide a stimulus for citizens.

Enhanced Oversight of the DPB: In order to protect the independence of the Board, there could be an appointment model involving committee input from multiple stakeholders, or allow parliamentary input. Extending terms for Board members beyond two years (or prohibiting the immediate reappointment of Board members) would be an additional supportive measure in protecting Board members from political pressure. A transparent process for establishing selection criteria would be beneficial, for example, and reporting publicly on-Board members and Board functions and processes would lend legitimacy to the Board.

Minimise for Small Entities: Although registered persons are not subject to a general registration requirement under the Act, small business owners may find it expensive to comply with the Act's requirements. The government could create model agreement clauses or industry codes of practice to assist in compliance for micro, small and medium enterprises. Governments could create subsidised training programs or create a single-point-of-contact advisory portal to assist smaller firms in implementing 'privacy-by-design' requirements without too many burdens.

Public Outreach and Education: For people to invoke the new right, there must be a public outreach. Government or civil society should undertake campaigns sophisticated enough to articulate the consent notices, grievance mechanisms and privacy tools available to individuals. Education of citizens about engaging in secure digital practices (ex. strong passwords,

[11] "The Digital Personal Data Protection Act, 2023: A Legal Analysis in Light of Global Data Protection Standards" (Department of Law, Utkal University, Bhubaneswar, Odisha, India, 2025) journal-article https://www.lawjournals.org/assets/archives/2025/vol11issue3/11064.pdf?utm_source> accessed 24 December 2025

identifying phishing) supplements the legal rights available. Consumer literacy programs developed in indigenous languages and platforms for real-time feedback could assist with making the law accessible.

Continuous Review and Adjustment: The law has a requirement for review from time to time to keep pace with changes in technology and circumstances. Parliament may want to include a statutory review of data protection from time to time (following the review bodies established in the financial sector). The data protection review could research emergent circumstances (ex, Artificial Intelligence and ethical variations of AI, biometric identification, etc.) and recommend changes and improvements to the legal framework to ensure that the law stays relevant, sustainable and imperative.

CONCLUSION

The Digital Personal Data Protection Act, 2023, is a landmark development in the legal landscape in India. For the first time in India, citizens will have a dedicated set of rights and vehicles to protect their digital personal data, while entities will possess a clear set of obligations and penalties. The Act's SARAL and citizen-first philosophy is designed to streamline compliance and empower the data principal. At the same time, its extensive exceptions for state action and certain actions of the users highlight the peculiarities of governance in an Indian context. From a citizen viewpoint, the Act is a positive move towards establishing privacy as a recognised right, though countervailing gaps (such as no portability) and state exemptions lessen the impact. From a data governance perspective, India has adopted a collaborative technique wherein the Act provides a regulatory framework while accounting for economic and other interests. The digital economy now works under a framework of laws, which should create enhanced trust, although they impose new compliance requirements on businesses. From an administrative perspective, the phased implementation, rule-making process and Data Protection Board collectively establish a framework for enforcement, but will depend on capacity and clarity as we move forward.