UNPACKING DPDP ACT 2023: ACHIEVEMENTS, APPLICATION, CRITICISM AND QUEST FOR BALANCED DATA PRIVACY

Ariba Khan & Safdar Imam, Department of Law, Aligarh Muslim University.

ABSTRACT

The paramount importance of a comprehensive legislature in the contemporary world, where everything revolves around the internet, and everything is digitalized, cannot be overlooked. Individual's personal data and privacy have to be respected, which is provided under Article 21 of the Indian Constitution and the case of Justice K. S. Puttaswamy, which directly catalysed India's data privacy evolution. Several steps have been taken to overcome the problem of data corruptions. The General Data Protection Regulations of the European Union is considered the global benchmark for data privacy and security. One such step has given India its Digital personal data protection Act of 2023. It has addressed the gaps which were highlighted in the case of K. S. Puttaswamy. It governs the processing of digital personal data and allows lawful data use with its application extending to both online and offline digitised data. It enforces strict consent security and data handling. The Act is the first Act where she/her has been used unlike the usual he/him pronouns. The DPDP Act provides penalties of upto 250 crore rupees, enhancing its enforcement. Prior to it, the Information Technology Act,2000 governed the same area, with Section 43A requiring reasonable security practices for sensitive data and cyber offences such as data breaches and intermediaries liabilities. This paper conducts a structured and comparative analysis of the main parts of the act, including its background, application, and criticism. A core focus of this study is the comprehensive analysis of DPDP and the European General Data Protection Regulation,2018.

Introduction

The Information Technology Act 2000 has been the only legislative act which has penalised the offences of cybercrimes, which include data theft and hacking, providing a comprehensive framework. But in the contemporary world, where everything is dependent online, the protection Personal data is of the utmost importance. The case of K. S. Puttaswamy[1] has emphasised the fundamental right to privacy as guaranteed by Article 21 of the Indian Constitution. It was then that the legislature realised that a framework to address such issues was needed. A committee under Justice B. N. Srikrishna was set up in 2018, and after a series of recommendations, the Digital Protection Data Privacy Act,2023, was introduced. Some of the provisions of the Act came into force in 2025, and the rest are yet to be implemented. The Act has been framed with a SARAL approach, i. e. , simple, accessible, rational and Actionable approach.

The Act mainly concerns consent, security and data handling, with the Board having the authority to impose up to rupees 250 crores of penalty in case of violation of the Act. The Act provides the details of what data is to be collected, for what purpose it is collected and mechanisms of complaint if any party faces violations.

The Data Protection Board, as set up under section 18, Functions as a fully digital institution, enabling citizens to file and track complaints online and any appeal against such a decision will lie in the Appellate department, TDSAT[2]. The members of the board are appointed by the central government, emphasising the eligibility criteria mentioned under the provisions of the act.

Background of the Digital Personal Data Protection Act, 2023

The history of the Digital Personal Data Protection Act, 2023, can be traced back to the Personal Data Protection Bill, 2019[3]. The committee that was set up under Justice B. N. Srikrishna prepared a draft version of the Personal Data Protection Bill. It was modified several

[1] *Justice K. S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
[2] Press Information Bureau, *Government Notifies DPDP Rules to Empower Citizens and Protect Privacy*, Press Release ID 2190014 (Ministry of Electronics & IT, Government of India, 14 Nov. 2025), https://www. pib. gov. in/PressReleasePage. aspx?PRID=2190014. pib
[3] Digital Personal Data Protection Act, 2023, Wikipedia, last modified 6 August 2023, available at: https://en. wikipedia. org/wiki/Digital_Personal_Data_Protection_Act,_2023 (accessed 26 January 2026).

times in the parliament, and public recommendations were also reviewed. It aimed at the protection of the privacy of individual data and provided for extensive provisions around the collection of consent, assessment of datasets, data flows and transfer of personal data, including third countries. But the revised version of the bill was criticised by Justice B. N. Srikrishna himself, who said that it would turn India into an "Orwellian State", as the Government could anytime access the personal information on the grounds of public interests. But the bill was withdrawn in 2022 as the reason provided was the need for a simpler and more focused framework[4]. Afterwards, the DPDP Act 2023 was enacted to provide a comprehensive framework for both individuals to protect their data and the lawful use of such data. On 11 August 2023, the bill was passed by both houses of the parliament and subsequently received the presidential assent. The act came into force on 13 November 2025, with some of the provisions having an 18-month phased compliance period, which will come into force in 2027. It creates a legal framework for managing the digital data, accountability and purpose limitations.

Applicability of the Act

As the Act provides for the protection of personal data and its lawful use, certain aspects related to it need to be clear, which includes the obligations and duties of data fiduciaries and data processors.

The data fiduciaries are the entities or individuals who ensure lawful processing, obtain explicit consent, maintain data accuracy and security and notify of breaches, for instance, banks, e-commerce platforms. Data processors are the ones who handle personal data on behalf of a data fiduciary, following its instructions.

The act under section 11 provides the right to access information about personal data, where data The principal can request access to personal data and who has access to it, section 12 right to correction and erasure of personal data if data is inaccurate or incomplete, right to grievance redressal under section 13, where the concerns about the data handling can be raised, and the right to Nominate under section 14, where the other person can exercise certain rights on your

[4] Evolution of Digital Personal Data Protection Law in India, Manupatra Academy, (2025) (PDF), available at: https://www. manupatracademy. com/assets/pdf/legalpost/evolution-of-digital-personal-data-protection-law-in-india. pdf, last accessed on 26 January 2026.

behalf[5].

Further, the act also includes provisions for withdrawing consent and objecting to how your data is being used. These rights give a sense of control, transparency and accountability on data processing.

Data Protection Board

Deriving its authority from Part V, section 18 of the Act, the data protection board is the adjudicatory body that addresses the grievances registered by the users[6]. The authority has the jurisdiction of imposing up to rupees 250 crore rupees on the violation of any sections of the act, which makes an effective implementation. Any appeal against the decision of the board lies with the appellate tribunal, TDSAT.

Section 19 comprises the composition of the board, which includes the Chairperson and such members as the government notifies, and they are appointed by the central government. They hold the office for a term of two years and are eligible for re-appointment. The eligibility of the chairperson and the member has been provided under the section 19 (3) which says that they should be a person of ability, integrity and standing who possesses special knowledge or practical experience in the fields of data governance, administration or implementation of laws related to social or consumer protection, dispute resolution, information and communication technology, digital economy, regulation or techno-regulation or in any other field which in the opinion of the central government maybe useful to the board and at least one among them shall be an expert in the field of law.[7]

Digital Privacy Data Protection Act and General Data Protection Regulation

The GDPR is the European Union's data protection framework. Both Digital Privacy Data Protection and General Data Protection Regulations work for the same cause, yet there are some differences which have to be understood. The similarities of both acts include the emphasis on consent, the rights of individuals to access and obtain data information and the

[5] Taxmann, 'Rights of Data Principals under the DPDP Act 2023' (Taxmann, 4 May 2025) <https://www. taxmann. com/post/blog/rights-of-data-principals-under-the-dpdp-act> accessed 26 January 2026.
[6] ibid.
[7] The Digital Personal Data Protection Act, 2023, No. 22 of 2023, § [section number] (India).

obligation of careful data handling.

● The differences between them are that the GDPR protects the data of European residents worldwide, but the DPDP focuses on the personal data only in India.

● The DPDP Act does not use the complex classification as that used in GDPR[8].

● The GDPR covers any data, whether offline, but the Indian DPDP Act only covers data that is digitalised.

● GDPR mandates detailed notices for all data collection regardless of the basis, whereas the DPDP Act requires notice only when relying on consent.

● Where GDPR uses a risk-based approach, i. e. , notifying the authority if risky and individuals when high risk is involved, but the DPDP Act mandates reporting of all breaches to the data protection board.

● The GDPR regulates exports outside the European Union with standard clauses, whereas the DPDP lets the government restrict transfers to specific countries.

● The fines imposed under GDPR are up to euro 20 million or 4% global turnover, but the DPDP Act allows the board to impose fines limited to rupees 250 crores.

● The GDPR uses strict adequacy and safeguards on data transfers, but the DPDP Act allows the Government to access the data on grounds of security.

Conflict with other laws

The DPDP Act supplements other laws, such as the Information Technology Act,2000, rather than replacing them and filling the gap where other sectoral laws are silent. DPDP operates via section 3(b)'s non obstante clause, which specifies "notwithstanding anything in any other law" asserting primacy over general statutes while deferring the special laws which reflect "lex specialis generalibus derogat". It further addresses the issue of inconsistency with other laws under section 38(2), stating that its provisions prevail over any other framework. This section

[8] Rachit Bahl, Rohan Bagai & Archana Iyer, *Indian Data Protection Law versus GDPR – A Comparison*, AZB PARTNERS (Aug. 18, 2023),
https://www. azbpartners. com/bank/indian-data-protection-law-versus-gdpr-a-comparison/

overrides prior IT Act section 81, ensuring DPDP leads on personal data protection matters. It supersedes the IT Act's limited sensitive personal data focus, extending to all digital personal data.

Criticism

Though the act has come into force to address the issues of privacy, it is majorly criticized for its exemption that gives the right to the government to access the information, which does not go hand in hand with the judgement of Justice K. S. Puttaswamy. Other areas which are criticised are that it enables surveillance and lacks robust safeguards. Representing India's first data privacy law, it fails to address the key areas, as in the General Data Protection Regulation of Europe.

1. The critics have questioned its reliance on consent for data processing as being ineffective given power imbalances and lack of opt-out defaults, which risks exploitation by Big Tech.

2. The state has been given unrestricted access to personal data on the grounds of sovereignty and security under section 17 without oversight, which is seen as enabling mass surveillance.

3. The digital protection board is also being criticised as it is set up by the government and given the authority to impose fines up to 250 crore rupees, which is insufficient for deterrence against global giants.

4. Unlike the GDPR or many global laws, the Act allows the transfer of data to countries which the central government specifies.

The above-mentioned criticism highlights the main defects of the act that require review.

Conclusion

The Digital Personal Data Protection Act, 2023, marks a pivotal step in India's evolving digital governance landscape, building on the foundations of the Information Technology Act, 2000, and the landmark K. S. Puttaswamy judgment. By establishing a SARAL framework centred on consent, purpose limitation, data security, and individual rights—such as access, correction, erasure, and grievance redressal under Sections 11-14—the Act empowers citizens while imposing clear obligations on data fiduciaries and processors. The fully digital Data Protection

Board, empowered under Section 18 to levy penalties up to ₹250 crores, promises efficient enforcement, with appeals routed through TDSAT for accountability.

Tracing its roots from the Srikrishna Committee's 2019 Bill to its enactment on August 11, 2023, and partial enforcement from November 13, 2025, the DPDPA prioritises simplicity over the expansive, criticised iterations that risked an "Orwellian" overreach. It aligns partially with global standards like the EU's GDPR—sharing emphases on consent and individual rights—but diverges meaningfully: narrower territorial scope to digital personal data in India, mandatory breach reporting without risk tiers, government-restricted cross-border transfers, and capped fines that pale in comparison to GDPR's 4% global turnover penalties.

Yet, the Act is not without flaws. Its non-obstante clause under Section 3(b) asserts primacy over conflicting laws like the IT Act, filling critical gaps, but exemptions for government access under Section 17(1)—framed vaguely around sovereignty and security—undermines privacy guarantees, echoing Puttaswamy's proportionality test. Critics decry the Board's government-appointed composition (Section 19), potential surveillance enablement, consent-heavy reliance amid power imbalances, and inadequate deterrence for tech giants, contrasting GDPR's robust safeguards.

Ultimately, while the DPDPA bridges India's data privacy void, its success hinges on implementation, phased compliance by 2027, and reforms addressing surveillance risks and oversight deficits. As digital dependency surges, refining the Act through stakeholder input and Judicial scrutiny will ensure it truly balances innovation, security, and fundamental rights in a data-driven democracy.