WWJMRD 2025; 11(05): 20-22
www.wwjmrd.com
International Journal
Peer Reviewed Journal
Refereed Journal
Indexed Journal
Impact Factor SJIF 2017: 5.182 2018: 5.51, (ISI) 2020-2021: 1.361
E-ISSN: 2454-6615

Sittender Kour
Assistant Professor
Shamsher Bahadur Saxena College of Law, Rohtak, India.

Data Protection in India: Legal Framework, Challenges, and the Road Ahead

Sittender Kour

Abstract
The growth of India's digital economy is contributing to massive data collection across different industries which poses significant risks concerning privacy and data misuse. The Supreme Court of India's landmark ruling acknowledged privacy to be a fundamental right, leading to the requirement of effective legislation concerning data protection. The DPDPA, or Digital Personal Data Protection Act of 2023, (Hereinafter, DPDPA, 2023), marks an important milestone in Indian law due to the regulations it seeks to impose on the processing of data. In particular, it attempts to safeguard the rights of users while also enforcing responsibility on data controllers or fiduciaries. This research attempts to detail the trajectory of evolution of data protection legislation in India, evaluate the key provisions and scope of the DPDPA, and measure it against other international legislations, specifically the European Union's General Data Protection Regulation (Herein after GDPR). In addition, it has identified the absence of autonomy in the control and independence of data subjects, secondary data use for global cross-border flows, and data subject's rights. After analyzing the contexts of data subject rights, these research findings emphasize the need to adopt best international practices and establish domestic policies to resolve under-regulation and over-regulation dilemmas. It is concluded that while the DPDPA represents a proactive step, without institutional changes and alignment with other international standards to strategic policies these reforms will not achieve effective data governance.

Keywords: Data Protection, Legal Framework, Digital Economy, DPDPA

Introduction
The digitization of services in India has made an individual's data a highly valuable commodity. Individuals generate and share tremendous amounts of data through numerous public and private services such as Aadhaar registration, online banking, and even maintaining digital health records. While there are exponential benefits to the digital world, there is still a sinister risk of personal data being misused, accessed without authorization, or surveilled. The landmark verdict pronounced by the Indian Supreme Court in Justice K.S. Puttaswamy v. Union of India (2017) has set the stage by considering privacy a fundamental right under Article 21, thereby necessitating comprehensive legislation to protect data on constitutional grounds.

The Information Technology Act of 2000 and its rules, along with other Indian policies, had been insufficient to address all issues. But in a recent move demonstrating the need to strengthen international standing, the government has formally initiated a framework for Indian data protection through the DPDPA, 2023, which now becomes the benchmark legislation. This paper books the journey of legal milestones concerning data protection in the country, assess features of the new law, examines overlaps with cross-border data privacy standards, and describes barriers to enforcement.

Background and Evolution of Data Protection Laws
Before 2023, India's data governance was guided by loose and incoherent frameworks, chiefly under Section 43A IT Act, 2000 and the Sensitive Personal Data Rules, 2011. These provisions were limited to corporate bodies and did not place stringent obligations on governmental units or offer effective rights to individuals.

Correspondence:
Sittender Kour
Assistant Professor
Shamsher Bahadur Saxena College of Law, Rohtak, India

The 2017 Puttaswamy judgment served as the turning point which made it necessary for lawmakers to take some action. Follow up, the Justice B. N. Srikrishna committee was set up to design a framework for data protection. Its report and draft Personal Data Protection Bill published in 2018 paved way for what is now the DPDPA, 2023.

Digital Personal Data Protection Act, 2023

This act has recently come into force and it tries to create an all-encompassing structure that helps safeguard the privacy of the people while simultaneously promoting innovation in the digital space. It has a two-pronged jurisdiction which includes the processing of personal data collected through digital means within the territory of India as well as applies to foreign entities who deal with Indian users by offering goods or services. This means that even companies outside of India, but who interact with Indian residents will need comply with the data protection regulations in India.

The Informed consent and consent-based principle remains a main tenet of the Act. Processing Data is not allowed if the person in question, called the "Data Principal," in this case does not provide explicit, verifiable, and specific consent of their choice. Such requests must be accompanied with adequate notice of the particular intention under which the data will be processed. This kind of assumption is being made to try to improve the situation around honesty which actually proves that trust in the internet rests on disclosures that are real and on the ground participation.

Following global benchmarks, the law prescribes a range of rights to Data Principals. These contain the right to information access concerning how their data is used, the right to amend personal information or demand its deletion, and the right to lodge complaints in cases where there is suspected wrongdoing with the data. Furthermore, the Act introduces new provisions that permit a person to designate another individual to exercise these rights, in case of their incapacity or demise which guarantees control of personal information even after death.

To improve responsibility, the legislation imposes several obligations on 'Data Fiduciaries,' the specified term for the data collection and processing services. Such obligations include implementing appropriate security measures to prevent data breaches, timely notification of users about any breaches, and retaining the data only for as long as it remains relevant to the stated purpose. This principle of relevance inhibits the perpetuation and collection of data and promotes minimizing data retention.

Furthermore, the Law differentiates another subcategory of Data Fiduciaries—'Significant Data Fiduciaries'—who hold greater volumes of more sensitive personal data or whose operations are likely to present a heightened risk to individual rights. These entities are subject to more stringent compliance mandates such as additional mandated audits, appointment of Data Protection Officers, and advanced evaluations of risks posed by the data processing, evaluating the impact of the data processing. This compliance stratification system ensures that the actors in the data ecosystem do not impose disproportionate risks with layers of redundant compliance requirements.

Comparison with International Data Protection Regimes

India's DPDPA, 2023 complies with major guidelines such as the GDPR, but still differs in critical areas. One of the principal differences is the scope of jurisdiction. India's enactment is restricted to personal data processed in automated systems only, unlike GDPR which applies to both manual and automated systems. Another divergence relates to enforcement mechanisms.

Also, with regard to rights granted to individuals, the provisions of the GDPR are wider as it incorporates the rights of data portability as well as automated decision making and profiling objection. Such safeguards are absent in Indian law which narrows the scope of individual control over personal data. The regime of exemptions also reflects differing philosophies; the GDPR has a constraining view adopting an approach where exemptions only apply in narrowly defined circumstances, while the Indian Act gives a permissive view with broad scope to exclude a range of subjects, including public bodies, from compliance. Also, with cross-border data transfer, European regulation is very protective of data leaving the EU where it prescribes stringent safeguards and conditions for the data to be transferred outside the EU. There is no such framework provided by India and leaves it to future government notifications which creates uncertainty.

Major Concerns and Challenges

Despite its significance, the DPDP Act has raised several concerns:

Exemptions for Government Agencies

The Act permits the central government to exempt any agency for reasons such as national security (Section 17), without requiring judicial oversight. This could lead to unchecked surveillance.

Regulatory Independence

The Data Protection Board lacks institutional independence, as appointments and rules governing its functioning are controlled by the central government, raising questions about impartiality.

Lack of Key Rights

Unlike the GDPR, the Act does not provide the **right to data portability**, nor does it sufficiently address **automated decision-making** or profiling.

Conclusion

With the adoption of the DPDPA, 2023, India now has a sophisticated legal framework concerning digitized data. The Act establishes user rights and systematizes the processes of collection and processing of data. Nevertheless, the Act's implementation features some shortcomings, such as unrestrained governmental control, limited independence of the regulatory l board, and the lack of fundamental protective measures.

For robust privacy protection, India must strive to evolve the data protection regime by integrating transparency, accountability, and citizen engagement. Strengthening the institutional framework, narrowing the scope of broad exclusions, and aligning with international data governance standards would be essential steps in India's journey toward effective data governance.

References

1. Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1
2. Digital Personal Data Protection Act, 2023
3. Information Technology Act, 2000, Section 43A
4. General Data Protection Regulation (EU) 2016/679
5. Justice B.N. Srikrishna Committee Report (2018)
6. Amber Sinha, Protecting Privacy in India's Digital Future, 2020
7. Chinmayi Arun, "Privacy and Surveillance in India," IJLT Vol. 15 (2019)