The Indian Journal for Research in Law and Management

Open Access Law Journal–Copyright©2025

Editor-in-Chief–Dr. Muktai Deb Chavan;Publisher– Alden Vas; ISSN: 2583-9896

PRIVACY IN THE DIGITAL AGE: INDIA'S DATA PROTECTION LAW AND THE ILLUSION OF CONTROL

Riya Maurya

A NEW LAW FOR A NEW AGE?

After years of legal guidance and public debate, India, in 2023, passed the Digital Personal Data Protection Act, 2023[1]. The Act claims to develop a rights-based digital framework for the management of personal data and protecting individual autonomy in cyberspace.

Despite being described as India's version of the European Union's GDPR[2], the Act is largely symbolic rather than substantive when examined closely. It has the form of consent, rights, and accountability; however, when constructed, it raises concerns of executive overreach, poor enforcement and limited user empowerment.

THE DPDP FRAMEWORK: SUMMARY OVERVIEW

The Act provides fundamental principles that will be familiar from global data protection frameworks:

• **Consent-based processing** - Data must only be collected and processed with valid consent that is free, informed, specific, and unambiguous.[3]

[1] Digital Personal Data Protection Act, No. 22 of 2023, Acts of Parliament, 2023 (India).

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 Apr. 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), 2016 O.J. (L 119) 1.

[3] Digital Personal Data Protection Act § 6, No. 22 of 2023, Acts of Parliament, 2023 (India).

• **Obligations on fiduciaries** - Those processing personal data must comply with purpose limitation, data minimization, security safeguards, and erasure obligations.[4]

• **User rights** - Individuals (who are referred to as "Data Principals") are given the right to access their data, correct it, and seek redressal.[5]

• **Regulatory board** - A Data Protection Board of India (DPBI) is endowed with the power to arbitrate disputes and impose penalties.[6]

• **Cross-border transfers** – Transfers of personal data to nations specified by the Central Government (presumably approved under the Data Protection Act) are allowed with no strict requirement to localize.[7]

While these represent improvements, the architecture for implementation still exposes significant gaps.

CONSENT: A THEORETICAL RIGHT?

While the Act professes informed consent, in reality, consent is rarely meaningful. Most users, particularly in low-literate and surveilled environments, cannot make informed choices when selecting digital options. Additionally, the Act also permits "deemed consent" - where a user's data can be processed without consent simply for reasons which may include state service delivery, employment, or public interest[8]. As a result, consent is reduced to a formal checkbox, rather than a substantive means for user autonomy.

THE SURVEILLANCE LOOPHOLE

Section 17 of the DPDP Act permits the Central Government to exempt any of its departments/public agencies from complying altogether with the provisions of the Act generally on the grounds of national security, sovereignty, or public order, or where any other applicable

[4] *Id*. §§ 7–8.
[5] *Id*. §§ 11–13.
[6] *Id*. § 18.
[7] *Id*. § 16.
[8] *Id*. § 7.

law allows[9]. These exemptions mean that state surveillance actions are unregulated by the DPDP Act, thus undermining the privacy protections it is supposed to provide.

These exemptions are a direct affront to the necessity and proportionality test in Puttaswamy[10], which requires any limitation on privacy ("the right to informational privacy") to be legal, necessary in a democratic society, and proportional. To consider the adequacy of DPDP Act, it is useful to critically assess it in relation to other data protection regimes across the globe.

A COMPARATIVE NARRATIVE

When viewed alongside the EU's GDPR, the DPDP Act seems to have limited scope and ambition. The GDPR incorporates both digital and non-digital personal information, incorporates foundational individual rights such as data portability, the right to object to profiling, and the right to be forgotten[11], and contains independent regulatory authorities with substantial powers of investigatory and enforcement.

The DPDP Act only applies to data processed digitally, has omitted significant rights implementing e.g. data portability and algorithmic transparency, and has relegated regulatory discretion under the executive branch of government. While the penalties may enact substantial financial consequences (up to ₹ 250 crore), it is entirely at the discretion of a board that does not have any independence guarantees in place.

Consequently, while India's law imitates the form of international frameworks it does not deliver on the function.

A WEAK REGULATOR

Compared to the GDPR's independent supervisory authorities[12], the DPBI is not statutorily autonomous. Its members are appointed by and are accountable to the Central Government. The DPBI possesses no independent investigatory powers, and operates as an administrative tribunal rather than a proactive enforcement agency[13]. This diminishes the efficacy of the enforcement of

[9] *Id*. § 17.
[10] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).
[11] Regulation (EU) 2016/679, arts. 17, 20–22.
[12] *Id*. art. 51.
[13] Digital Personal Data Protection Act §§ 18–21, No. 22 of 2023, Acts of Parliament, 2023 (India).

data protection standards, especially in the public sector and where large corporations are involved.

LOOKING AHEAD

For Individuals:

While the law outlines a core set of rights, challenges of public knowledge and digital literacy arise. The concept of meaningful consent is largely pie in the sky in rural or impoverished contexts, unless there is clear, well-resourced ground education as an ally.

For Businesses:

Companies and organizations that will collect large amounts of consumer data should expect to adopt new privacy policies, consent options, and mechanisms for grievance redressal. However, the lack of clarity in enabling subordinate rules may hinder compliance entirely or worse, drive some degree of form over substance.

For Civil Society and Judiciary:

As the law is put to the test of implementation, and with constitutional challenges as a fact of life, there is a very real likelihood that these exemptions will invite constitutional scrutiny, and it is not likely these exemptions will survive judicial scrutiny or review unless the exemptions are drawn narrowly and strictly, as well as adhere to the tests of necessity and proportionality.

Already, privacy rights activists and academics have invoked Parliamentary accountability, independent scrutiny, and reform of the surveillance law as complements to this Act that are needed.

CONCLUSION

The DPDP Act marks a vital milestone in India's journey toward data protection; however, it is far from being the final step. Symbolically, it signals the recognition of privacy, but it stands on shaky ground regarding institutional protections, regulatory independence, and genuine user control.

The very nature of privacy must be viewed as a non-negotiable right that is protected by independent institutions from public or private actors' encroachments, in this day and age when data has become currency and the eye of surveillance is omnipresent.

As Puttaswamy reiterated, privacy is essential to dignity, freedom, and autonomy. The real test of the DPDP Act will be whether these principles are protected by rights that can be enforced, or whether it merely offers rhetorical acknowledgment without substantive protection.