CONSENT, CONTROL, AND COMPLIANCE: ASSESSING INDIA'S DIGITAL PERSONAL DATA PROTECTION LAWS

Shivani, Research Scholar, Desh Bhagat University, Mandi Gobindgarh

Dr. Arti, Assistant Professor, University School of law, Desh Bhagat University, Mandi Gobindgarh

Dr. Avon Kumar Vaid, Principal, Amritsar Law College

ABSTRACT

The Digital Personal Data Protection Act, 2023 (DPDP Act) is a watershed moment in the changing legal environment of India for digital regulation. Passed in response to heightened alarm about data privacy and the Supreme Court's historic ruling in Justice K.S. Puttaswamy v. Union of India (2017), the Act seeks to reconcile the right to privacy with economic and administrative concerns. This research paper critically discusses the DPDP Act conceptually in terms of consent, control, and compliance. It probes into the character of data principal rights, fiduciary duties, and institutional enforcement mechanisms. Comparative analysis with the GDPR and CCPA has been provided to place India's data protection law within the global context. The report highlights critical challenges and provides policy suggestions to enhance the implementation and efficacy of the Act.

Keywords: Digital Personal Data Protection, Consent, Data Privacy, India, Data Fiduciary, Compliance, GDPR, Surveillance, User Rights, Data Governance

1. Introduction

The digital era has revolutionized personal data collection, processing, and commodification, bringing forth serious issues with privacy, security, and accountability. In India, a fast-expanding digital populace, extensive use of digital public infrastructure and spread of data-driven services have amplified the demand for a strong personal data protection law. The Supreme Court's 2017 ruling in Justice K.S. Puttaswamy v. Union of India recognized the right to privacy as a constitutional right under Article 21 of the Constitution, galvanizing attempts at a legislative regime for data protection.

India's first bespoke law on personal data protection, the Digital Personal Data Protection Act, 2023, is analyzed in this paper. The DPDP Act is critically assessed on three pillars of analysis: consent (the extent to which individuals can grant data processing freely and meaningfully), control (the level of autonomy individuals may exercise over their data), and compliance (the extent to which the law facilitates enforcement and accountability). These are the dimensions that are paramount in analyzing the strengths and weaknesses of the Act in India's democratic, economic, and technologically evolving context.

2. Evolution of Data Protection in India

India's path towards an integrated data protection regime mirrors the nation's larger move towards becoming a digitally enabled nation. At the very beginning, personal data protection was dealt with in an ad hoc fashion in the form of sparse provisions under the Information Technology Act, 2000, specifically Sections 43A and 72A, which concerned compensation for negligence and punishment for breach of confidentiality, respectively. These provisions remained unclear, unenforceable, and failed to establish privacy as a constitutional right.

Legal momentum for a stronger data protection regime grew with the Supreme Court's historic ruling in Justice K.S. Puttaswamy v. Union of India (2017), which recognized privacy as a fundamental right under Article 21. Sensing the void in India's data governance framework, the government formed the Justice B.N. Srikrishna Committee, which in 2018 released a full report and draft Personal Data Protection Bill. This paper underscored the importance of protecting autonomy, providing informational self-determination, and placing accountability frameworks—frameworks borrowed from constitutional ideals as well as best practices internationally.

Thereafter, several drafts of the Personal Data Protection Bill were tabled in Parliament in 2019 and 2021. These drafts raised considerable controversy relating to government exemptions, data localization, and regulatory autonomy. Following criticism and setbacks, the previous bills were withdrawn in 2022.

The culmination of all these efforts has been the enactment of the Digital Personal Data Protection Act, 2023, India's first specific data protection law. In contrast to the European Union's GDPR, constructed from several decades of privacy jurisprudence and institutional capacity, India's DPDP Act comes into being in the context of an emerging digital economy, where state capacity, infrastructure, and digital literacy are still uneven. The Act is therefore molded by the imperative of ensuring economic innovation, state supervision, and basic rights in an increasingly dynamic digital environment.

3. Consent: The Legal Basis for Processing Personal Data

Consent is an established norm in data protection systems around the world, and the Digital Personal Data Protection Act, 2023 (DPDP Act) makes it the key legal ground for processing digital personal data. Under the Act, consent is made free, informed, specific, unambiguous, and affirmative, following international best practices like those of the General Data Protection Regulation (GDPR). The data fiduciaries are required to obtain consent in understandable and simple terms, available in English or any of the 22 scheduled Indian languages, thus increasing readability for India's diverse populace. Additionally, the Act affirms the right to withdraw consent at any time, further emphasizing individual autonomy.

In spite of all these protections, the efficacy of consent is diluted considerably by Section 7 of the Act, which brings into play a wide range of exemptions under the umbrella of "legitimate uses." These provisions permit data to be processed without express consent in a range of situations including government service delivery, law enforcement, employment-related issues, and public emergencies. While such exemptions are proper in narrowly circumscribed situations, their open-ended and vague drafting invites abuse. The statute lacks advance notice to persons in a large number of such situations, and it also fails to include independent scrutiny, e.g., parliamentary or judicial review.

This "deemed consent" notion whereby people are assumed to have given consent by implication of context weakened the original notion of consent as an act of willing and

affirmative agreement. This puts the data principal out of balance with the data fiduciary, especially when the state is acting as processor. Without strong procedural protections, these exemptions may result in mission creep wherein personal information ends up being applied for uses orders of magnitude beyond the original purpose, thus negating the constitutional privacy right acknowledged by the Supreme Court.

4. Control: Rights and Empowerment of Data Principals

The Digital Personal Data Protection Act, 2023 aims to empower individuals, or data principals, by bestowing a package of rights intended to enhance their control over personal data. These rights encompass the right to know how their data is processed, the right to seek correction or deletion of irrelevant or wrong information, and the right to file a complaint and access grievance redressal mechanisms. Significantly, the Act also permits individuals to appoint a representative to exercise these rights in case of the death or incapacitation of the data principal, a progressive provision that aims to satisfy digital legacy and post-mortem rights concerns.

These rights are the core of individual control, though the Act significantly excludes a number of key safeguards found in international data protection systems. For example, the Act does not include the right to data portability, which would enable users to move their data to other service providers and thereby increase competition and choice for the user. Likewise, the Act does not include the right to object to profiling or automated decision-making, which becomes more important with algorithmic government and targeted advertising.

Another serious limitation is the Act's inability to categorize data according to sensitivity. While the GDPR provides extra protection to sensitive categories of data like biometric, health, and finance data, the DPDP Act addresses all personal data in the same manner. The lack of a tiered or risk-based framework weakens safeguards for data types that are more privacy-threatening and dignity-threatening if handled improperly.

In addition, inadequate digital literacy and public awareness in India pose practical barriers to exercising data rights meaningfully. Without ongoing education efforts and available rights-enforcement mechanisms, the rights afforded by the Act could prove more symbolic than substantive, especially for vulnerable or digitally underserved groups.

5. Compliance: Obligations and Enforcement Mechanisms

The Digital Personal Data Protection Act, 2023 provides a systematic compliance regime that imposes a variety of obligations on data fiduciaries processing personal data. These duties are intended to guarantee proper handling of data and involve essential principles like purpose limitation—guaranteeing that data will only be used for the specified purposes for which it was amassed—and data minimization, which restricts the amassing of personal data to what is absolutely necessary. Fiduciaries must also put in place technical and organizational means of protection to guarantee data security from unwarranted access or data breaches.

However, if any breach of data occurs, the fiduciaries have to notify both the Data Protection Board of India and the concerned data principals. For those entities categorized as SDFs: the volume and sensitivity of data processed-there are more stringent compliance demands, such as the appointment of a DPO and periodic DPIAs.

The Indian Data Protection Board is the central enforcing authority under the Act. Nevertheless, the absence of statutory independence raises serious issues. The DPB's composition and operations are under executive control, as members are appointed and supervised by the central government. This arrangement differs from international best practices, such as the European Data Protection Board (EDPB) under the GDPR, ensuring independence from political interference and institutional bias.

Though the Act imposes monetary sanctions of up to ₹250 crore for non-compliance or data breach, they are mostly at the discretion of the regulators and the lack of criminal sanctions could potentially weaken their deterrent impact. Further, the powers of the government to exempt its own agencies from compliance in exceptional situations create regulatory asymmetry, thus jeopardizing the universality and equity of the enforcement regime.

6. Comparative Analysis: India's DPDP vs. Global Frameworks

India's answer to the global trend towards data governance centered around rights has been the Digital Personal Data Protection Act, 2023 (DPDP). Although it has taken cues from well-established global legislation like the European Union's General Data Protection Regulation (GDPR) and California's Consumer Privacy Act (CCPA), inherent differences in terms of ambit, enforcement, and empowerment of users show serious lacunae in the Indian landscape.

Aspect	DPDP (India)	GDPR (EU)	CCPA (California)
Legal Basis	Consent + Legitimate Uses	Consent + Legitimate Interest	Opt-out-based system
Sensitive Data Definition	Not defined	Defined and specially protected	Limited recognition
Individual Rights	Access, correction, erasure	Full spectrum including portability, objection	Limited compared to GDPR
Regulator	Data Protection Board (executive-controlled)	Independent Supervisory Authorities	California Privacy Protection Agency (CPPA)
Penalties	Up to ₹250 crore	Up to €20M or 4% of global turnover	Up to $7,500 per violation

India's DPDP Act complies with international standards in its consent-first regime, focus on data fiduciary duties, and codification of rights for users. It differs notably from the GDPR in several aspects, though. For example, the failure to define sensitive personal data leaves no room for risk-based safeguards for high-risk data categories like biometrics or health data. The GDPR's wide-ranging body of user rights, such as the right to data portability and right of objection against automated decision-making, are not reflected in the Indian legislation.

Regulatory autonomy is another point of contention. Although the GDPR requires independent supervisory authorities, India's Data Protection Board is still under executive control, hence casting doubt on its neutrality. Unlike the CCPA, the DPDP has better affirmative consent provisions but no meaningful opt-out rights for profiling or selling of data.

Overall, although the DPDP Act is broad progress, it needs to undergo necessary and constructive criticism in order to compete with the depth, balance, and enforceability of

advanced data protection legislations in other jurisdictions.

7. Implementation Challenges

The successful implementation of the Digital Personal Data Protection Act, 2023 depends on the overcoming of various structural, institutional, and societal challenges. These challenges, if left undeterred, could prejudice the law's aims and its acceptance by all the interested stakeholders.

• Institutional Design

The Indian Data Protection Board (DPB) under the Act is not institutionally independent. Appointed and controlled by the central government, it could be questioned regarding its impartiality in deciding cases against state agencies. Lacking structural autonomy, the Board might find it challenging to generate public confidence and have unbiased application.

A very significant part of India's population remains legally and digitally unaware, especially in rural and semi-urban regions. Without mass, multilingual campaigns to inform people about their rights and responsibilities according to the Act, legal provisions are likely to remain ineffective on the ground.

• Regulatory Conflicts and Jurisdictional Ambiguity

India's regulatory framework has several sector-specific entities like Reserve Bank of India (RBI), Telecom Regulatory Authority of India (TRAI), and IRDAI. It is not very clear how the DPDP Act will interface with these regulators, and this can result in jurisdictional conflicts and conflicting enforcement.

• SME Compliance Burden

Startups and small players might struggle to comply with the DPDP Act's legal, technical, and administrative requirements. In the absence of proper support mechanisms, the compliance burden could dampen innovation and discourage smaller players from adopting privacy-oriented practices.

• State Surveillance and Judicial Oversight

The Act does not address government surveillance and practices of data interception. It makes

no provision for judicial or independent oversight over state access to personal data, leaving a glaring gap in privacy protection with a strong risk of constitutional violation.

8. Recommendations

To enhance the efficacy, transparency, and inclusivity of the Digital Personal Data Protection (DPDP) Act, 2023, the following recommendations are put forth:

1. Create an Independent Regulator

- Reconstitute the Data Protection Board of India (DPB) as a statutorily autonomous institution.
- Provide transparent appointment procedures and appoint members with law, technology, and civil liberties expertise.
- Provide financial and functional autonomy to boost credibility and curtail political interference.

2. Curtail the Scope of Deemed Consent

- Well define the terms of "legitimate use" exemptions under Section 7.
- Provide procedural safeguards like independent monitoring, documentation requirements, and time-bound usage for non-consensual processing of non-personal data.
- Mandate accountability mechanisms for public and private parties.

3. Add Additional Rights to Data Principals

- Add the right to data portability, which allows users to take their data from one platform to another.
- Establish the right to object to profiling and automated decision-making, particularly in employment and credit contexts.
- Provide algorithmic transparency to ensure fairness and avoid discriminatory treatment.

4. Embrace Tiered Data Classification

- Establish and govern sensitive personal data (e.g., biometric, financial, and health data).
- Enforce tighter requirements and insist on clear consent for its processing.
- Promote a risk-based compliance regime.

5. Enact Surveillance Legislation

- Pass distinct legislation to govern state surveillance.
- Insist on judicial approval, transparency reporting, and independent state access audits of personal data.

6. Implement Public Awareness Campaigns

- Educate people in digital literacy and make citizens aware of their data rights via multilingual outreach.
- Collaborate with NGOs and local institutions for grassroots outreach.

7. Facilitate Compliance for SMEs

- Offer standardized compliance templates, training schemes, and financial rewards to simplify the regulatory load.
- Create a legal and technical inquiry support desk.

9. Conclusion

The Digital Personal Data Protection Act, 2023 is a turning point in India's digital governance development by providing a detailed legal regime for protecting personal data. It enshrines fundamental principles of consent, purpose limitation, and data minimization, as well as bestowing rights on individuals to access, rectify, and delete data. The establishment of the Data Protection Board of India also reflects the shift towards institutionalized enforcement, albeit with issues regarding independence and accountability.

Yet, despite its aspirations, the Act has its limitations. Excessive government use exemptions, an unimaginative lack of robust safeguards for surveillance, and a failure to include key rights like data portability and algorithmic transparency show gaps that could undermine its impact. Implementation difficulties such as low digital literacy levels, risks of regulatory overlaps, and compliance costs on small businesses complicate the way forward as well.

In order to make the DPDP Act reach its full potential, future amendments and policy measures need to center on increasing institutional autonomy, bolstering individual rights, and inculcating democratic protections in data governance. As India becomes a leading digital nation, it will be essential to strike a balance between economic growth and constitutional principles like privacy, accountability, and inclusion in order to create a robust and rights-based digital environment.

REFERENCES

1. Ministry of Electronics and Information Technology (Meity) (2023). The Digital Personal Data Protection Act, 2023. Government of India. https://www.meity.gov.in/data-protection-framework

2. PRS Legislative Research. (2023). The Digital Personal Data Protection Bill, 2023 – Summary and Analysis. https://prsindia.org/billtrack/the-digital-personal-data-protection-bill-2023

3. Internet Freedom Foundation (IFF). (2023). IFF's Legal Analysis of the DPDP Act, 2023. https://internetfreedom.in

4. Centre for Internet and Society (CIS). (2023). Preliminary Comments on the DPDP Bill, 2023. https://cis-india.org/internet-governance

5. NITI Aayog. (2023). Data Empowerment and Protection Architecture (DEPA): Policy Framework. https://www.niti.gov.in

6. Supreme Court of India. (2017). Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors., (2017) 10 SCC 1.

7. Srikrishna Committee Report. (2018). Report of the Committee of Experts on Data Protection. Ministry of Electronics and IT. https://www.meity.gov.in

8. National Law School of India University (NLSIU). (2024). Critical Perspectives on India's Data Protection Law. NLSIU Law Review, 36(1), 45–78.

9. Vidhi Centre for Legal Policy. (2023). DPDP Bill, 2023: An Assessment of Legal and Institutional Challenges. https://vidhilegalpolicy.in

10. Live Law. (2023). Explained: The Digital Personal Data Protection Act, 2023. https://www.livelaw.in

11. Bar and Bench. (2023). India's DPDP Act: Key Provisions and Legal Commentary. https://www.barandbench.com

12. Observer Research Foundation (ORF). (2023). Data Protection in India: Navigating the DPDP Act. https://www.orfonline.org

13. Indian Journal of Law and Technology. (2024). Algorithmic Profiling and Indian Data Law: A Missing Link? 20(2), 112–135.

14. Software Freedom Law Centre (SFLC.in). (2023). The DPDP Act and Government Exemptions: A Civil Liberties View. https://sflc.in

15. National Law University, Delhi (NLU-D). (2024). Compliance and Accountability Under the DPDP Act: A Regulatory Analysis. NLU Delhi Policy Brief Series.