Digital Privacy in the Age of Data Economy: A Comparative Analysis of India's Digital Personal Data Protection Act, 2023 and Global Frameworks

Dr. Ravinder Kumar

Associate Professor of Law, Sri Sukhmani College of Law, Dera Bassi(Punjab)

Abstract

The rapid digitisation of economies and societies has made personal data one of the most valuable commodities of the 21st century. India's enactment of the Digital Personal Data Protection Act, 2023 (DPDP Act) marks a watershed moment in the country's legal history, establishing for the first time a comprehensive statutory framework for the protection of personal data. This paper undertakes a comparative analysis of the DPDP Act, 2023 against the European Union's General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and China's Personal Information Protection Law (PIPL), examining structural similarities, critical differences, and significant gaps. The paper further interrogates the constitutional underpinnings of the right to privacy in India, the adequacy of the consent mechanism, the scope of exemptions granted to the State, the independence of the proposed Data Protection Board, and the implications of the Act for cross-border data flows. It concludes with recommendations for strengthening India's data protection regime to meet the demands of an increasingly surveillance-prone digital landscape.

Keywords: Digital Personal Data Protection Act 2023, Right to Privacy, Data Protection Law, GDPR (General Data Protection Regulation), Cyber Law India

1. Introduction

We live in an era where data is described, with increasing accuracy, as the "new oil." Every digital transaction — a Google search, an e-commerce purchase, a UPI payment, a health consultation on a telemedicine platform — generates data trails that are harvested, processed, monetised, and in

many cases, weaponised. The individual whose data is being processed often has little awareness of, and even less control over, what happens to their personal information.

For the world's most populous democracy, the stakes are extraordinarily high. India has over 900 million internet users, a thriving fintech sector, one of the world's largest biometric databases in Aadhaar, and a rapidly expanding digital public infrastructure. Yet, until 2023, India operated without any dedicated data protection legislation, leaving citizens legally exposed and the regulatory environment uncertain for businesses.

The journey toward a data protection law in India was neither short nor smooth. It began with the landmark Supreme Court judgment in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017), wherein a nine-judge bench unanimously held that the right to privacy is a fundamental right under Article 21 of the Constitution. This judgment created a constitutional imperative for Parliament to enact data protection legislation. The B.N. Srikrishna Committee submitted a draft Personal Data Protection Bill in 2018. A revised version was introduced in Parliament in 2019, only to be withdrawn in 2022 amid widespread criticism. Finally, the Digital Personal Data Protection Act, 2023 received Presidential assent on 11 August 2023.

This paper situates the DPDP Act within the broader global context of data protection law, comparing it with three major international frameworks: the EU's GDPR (considered the gold standard), the CCPA (representing a market-driven American approach), and China's PIPL (representing a State-centric model). Through this comparative lens, the paper evaluates the strengths and weaknesses of India's approach and charts a path forward.

2. Constitutional Foundation: Privacy as a Fundamental Right

Before examining the DPDP Act on its own terms, it is essential to understand its constitutional anchor. The *Puttaswamy* judgment (2017) was transformative. Overruling earlier decisions in *M.P. Sharma v. Satish Chandra* (1954) and *Kharak Singh v. State of U.P.* (1962), the Supreme Court held that privacy is intrinsic to life and liberty under Article 21. Justice D.Y. Chandrachud, in his concurring opinion, explicitly stated that informational privacy — the right of individuals to control personal data — is a component of the fundamental right to privacy.

This constitutional grounding distinguishes India from the United States, where there is no explicit constitutional right to privacy in the data context, and from China, where State interests are constitutionally supreme. It places India closer to the European model, where Article 8 of the EU Charter of Fundamental Rights recognises data protection as a standalone fundamental right.

However, a critical constitutional tension runs through the DPDP Act. Article 21 rights can only be curtailed by a procedure established by law that is fair, just, and reasonable. The DPDP Act contains sweeping exemptions for government agencies — allowing the State to exempt itself from virtually all obligations of the Act in the interest of national security, sovereignty, public order, and the maintenance of friendly relations with foreign states. Critics argue these exemptions are so broad as to be constitutionally suspect, because they replicate the very surveillance architecture that *Puttaswamy* sought to constrain.

3. Key Provisions of the DPDP Act, 2023

3.1 Scope and Applicability

The Act applies to the processing of digital personal data within India, as well as to processing outside India if it involves offering goods or services to data principals within India. "Personal data" is defined as any data about an individual who is identifiable by or in relation to such data. The Act notably does not cover non-digital personal data, a significant limitation given the ongoing digitisation of physical records.

3.2 Consent Framework

The DPDP Act adopts a consent-based model as its foundational principle. A data fiduciary (equivalent to a "data controller" under GDPR) must obtain free, specific, informed, unconditional, and unambiguous consent from the data principal (the individual) before processing their personal data. Consent must be given through a clear affirmative action. The data principal has the right to withdraw consent at any time, and withdrawal must be as easy as giving consent.

Importantly, the Act also recognises "legitimate uses" — analogous to legitimate interests under GDPR — where consent is not required. These include processing for employment-related

purposes, compliance with legal obligations, medical emergencies, and processing by the State for provision of benefits and services.

3.3 Rights of Data Principals

The Act confers several rights on individuals: the right to access information about their personal data being processed; the right to correction and erasure of inaccurate or incomplete data; the right to grievance redressal; and the right to nominate another individual to exercise these rights in case of death or incapacity. Conspicuously absent is an explicit right to data portability and a right to object to processing — rights that exist under GDPR.

3.4 Obligations of Data Fiduciaries

Data fiduciaries must implement appropriate technical and organisational measures to ensure compliance, appoint a Data Protection Officer (for Significant Data Fiduciaries), conduct Data Protection Impact Assessments, and notify the Data Protection Board and affected data principals in the event of a data breach.

3.5 Data Protection Board of India

The Act establishes a Data Protection Board as the regulatory and adjudicatory body. The Board has the power to investigate breaches, issue directions, and impose penalties of up to ₹250 crore per instance of non-compliance and up to ₹10,000 crore for systemic failures. However, the Board is constituted by the Central Government, and its Chairperson and members are appointed by the Government — raising serious concerns about its independence.

3.6 Cross-Border Data Transfers

The Act adopts a whitelist approach to cross-border data transfers. Personal data may be transferred to countries or territories notified by the Central Government. This is a departure from India's earlier draft bills which proposed data localisation requirements. The whitelist approach provides flexibility but raises questions about the adequacy assessment process and whether it will be sufficiently rigorous.

4. Comparative Analysis

4.1 The EU's General Data Protection Regulation (GDPR)

The GDPR, which came into force in May 2018, is widely regarded as the most comprehensive and influential data protection regime in the world. It has directly or indirectly shaped legislation in over 130 countries, including the DPDP Act.

Similarities: Both frameworks require freely given, specific, informed, and unambiguous consent. Both confer rights of access, correction, and erasure. Both require notification of data breaches. Both impose obligations on data processors and controllers/fiduciaries.

Critical Differences: The GDPR recognises six lawful bases for processing (consent, contract, legal obligation, vital interests, public task, and legitimate interests), providing greater flexibility and clarity for businesses. The DPDP Act's "legitimate uses" framework is narrower and less precisely defined. The GDPR has a comprehensive right to data portability and an explicit right to object to processing, both of which are absent from the DPDP Act. The GDPR established the European Data Protection Board — a fully independent multi-country supervisory authority. In contrast, the DPDP Act's Data Protection Board, appointed entirely by the Central Government and operating as a digital office without physical hearings, raises independence concerns. GDPR penalties are calibrated as a percentage of global annual turnover (up to 4% or €20 million, whichever is higher), making them proportionate and genuinely deterrent for large corporations. DPDP Act's fixed penalties, while substantial in absolute terms, may be inadequate for global tech giants. Perhaps most fundamentally, the GDPR does not permit Member States to grant blanket exemptions to government agencies. State processing of personal data is subject to the same standards of necessity and proportionality. The DPDP Act's near-absolute government exemption has no parallel in the GDPR framework.

4.2 California Consumer Privacy Act (CCPA) / CPRA

The CCPA (2018), as amended by the California Privacy Rights Act (CPRA, 2020), represents the most significant data privacy legislation in the United States. The US federal system means there is no single national privacy law, making California's framework particularly influential.

Similarities: Both laws require transparency about data collection and use. Both provide opt-out rights for the sale of personal data. Both impose obligations on businesses regarding breach notification.

Critical Differences: The CCPA is fundamentally an opt-out regime — it allows businesses to collect and process data by default, giving consumers the right to opt out of the sale of their data. The DPDP Act, by contrast, is an opt-in regime requiring affirmative consent, which is more protective. The CCPA grants an explicit right to know what categories of personal information are collected, a right to delete, a right to opt-out of sale, and a right to non-discrimination for exercising privacy rights. The DPDP Act does not explicitly provide a right against discriminatory treatment. The CCPA has a private right of action for data breaches, allowing individual consumers to sue companies directly. The DPDP Act provides no such private right of action — individuals can only approach the Data Protection Board. This significantly limits individuals' ability to seek direct legal remedies.

4.3 China's Personal Information Protection Law (PIPL)

China enacted the PIPL in 2021, making it one of the most recent major data protection laws. It is heavily influenced by the GDPR in structure but reflects China's distinctly State-centric political economy.

Similarities: Both the PIPL and DPDP Act require consent as a primary basis for processing. Both regulate cross-border data transfers. Both impose obligations on data handlers and provide individuals with rights of access, correction, and deletion.

Critical Differences: The PIPL contains elaborate provisions for cross-border data transfers, requiring security assessments by the Cyberspace Administration of China for significant data exports and certification by approved institutions for others. The DPDP Act's whitelist approach is simpler but less rigorous. Interestingly, China's PIPL actually provides stronger protections against certain forms of commercial data processing — particularly algorithmic profiling and automated decision-making — than the DPDP Act, which is largely silent on these issues. Both laws, however, share a fundamental structural flaw: expansive carve-outs for State agencies. In China, government processing of personal data is effectively unregulated. In India, the DPDP Act's

exemptions for the Union Government are similarly sweeping, drawing criticism that the legislation protects citizens from corporations but not from the State.

5. Critical Gaps and Concerns in the DPDP Act

5.1 Overbroad Government Exemptions

Section 17(2) of the DPDP Act empowers the Central Government to exempt any instrumentality of the State from the application of the Act's provisions in the interest of national security, sovereignty, public order, and other grounds. These grounds are virtually unlimited in scope and are not subject to judicial review in any meaningful way. This stands in stark contrast to the *Puttaswamy* judgment's requirement that any restriction on the right to privacy must satisfy the three-part test of legality, legitimate aim, and proportionality. Legal scholars have argued convincingly that Section 17(2) is constitutionally vulnerable and may not survive judicial scrutiny.

5.2 Absence of Data Localisation

Earlier versions of India's data protection bill proposed significant data localisation requirements, particularly for sensitive and critical personal data, requiring storage of such data on servers within Indian territory. The DPDP Act completely abandons this approach in favour of a government-notified whitelist. While data localisation has its own costs and complexities, the complete removal of localisation requirements — reportedly following lobbying pressure from US technology companies — has raised concerns about India's strategic data sovereignty.

5.3 No Protection for Non-Digital Data

The DPDP Act explicitly applies only to digital personal data. This means that personal data in physical form — medical records, financial documents, paper-based government records — falls entirely outside its scope. In a country where vast amounts of sensitive personal information continue to exist in non-digital formats, this is a significant gap.

5.4 Children's Data Protection

The Act defines a child as any person under the age of 18 and prohibits the processing of children's data without verifiable parental consent. It also prohibits tracking, behavioural monitoring, and targeted advertising directed at children. These are welcome provisions. However, the Act provides no mechanism for age verification beyond what data fiduciaries may self-implement, and the practical enforcement of these provisions in a country of India's scale remains deeply uncertain.

5.5 Independence of the Data Protection Board

A data protection authority's credibility depends entirely on its independence from the government it is meant to hold accountable. The DPDP Act's Data Protection Board is appointed by the Central Government, its members serve terms determined by the Government, and it operates as a "digital office" — processing complaints digitally without physical hearings. The absence of structural guarantees of independence is a fundamental weakness. By comparison, EU Data Protection Authorities operate under strict independence requirements mandated by GDPR Article 52, and their decisions are subject to independent judicial review.

5.6 No Right to Data Portability

The right to data portability — the right to receive one's personal data in a structured, machine-readable format and to transfer it to another service provider — is a key competitive tool that promotes consumer choice and market competition in digital services. Its absence from the DPDP Act is a notable gap, particularly given India's ambition to build competitive digital markets.

6. Cross-Border Data Flows and Digital Sovereignty

The question of cross-border data flows sits at the intersection of privacy law, trade law, and geopolitics. The DPDP Act's whitelist approach — allowing transfers to countries notified by the Central Government — gives the government significant discretionary power. The criteria for inclusion in or exclusion from the whitelist are not specified in the Act itself, leaving them to be determined by subordinate legislation.

This contrasts with the GDPR's adequacy decision framework, which requires the European Commission to make a formal determination that a third country offers an "essentially equivalent" level of data protection. India has been seeking an adequacy decision from the EU — the DPDP Act's passage is a necessary but not sufficient step toward that goal. EU adequacy assessments will scrutinise the independence of India's Data Protection Board and the scope of government exemptions, both of which remain problematic.

The geopolitical dimensions cannot be ignored. The US, EU, and China each seek to shape global data governance in their own image — what scholars call "regulatory imperialism" or "data nationalism." India's DPDP Act, by abandoning localisation requirements and adopting a flexible whitelist, has arguably positioned itself more in alignment with US preferences than with the EU's rights-based model or China's sovereignty-first model. Whether this serves India's long-term strategic interests is a matter of ongoing debate.

7. Recommendations

Based on the foregoing comparative analysis, this paper makes the following recommendations for strengthening India's data protection framework:

First, Section 17(2)'s blanket government exemption must be narrowed. Any State exemption should be subject to a proportionality test, time limits, parliamentary oversight, and judicial review. This would bring the Act in line with the constitutional mandate of *Puttaswamy*.

Second, the independence of the Data Protection Board must be structurally guaranteed. Appointments should involve a collegium-style process with representation from the judiciary, civil society, and technical experts, not the Central Government alone.

Third, the Act should be amended to include a right to data portability and an explicit right to object to certain categories of processing, particularly automated decision-making and profiling.

Fourth, a private right of action for data breaches should be introduced, allowing individuals to seek direct legal redress without being exclusively dependent on the Board's machinery.

Fifth, the whitelist criteria for cross-border data transfers should be legislatively defined and subject to parliamentary scrutiny, not left entirely to executive discretion.

Sixth, the Act's scope should be expanded in a phased manner to cover non-digital personal data, particularly in health, finance, and government service delivery contexts.

8. Conclusion

The Digital Personal Data Protection Act, 2023 is a significant milestone in India's legal history. It signals India's arrival as a data governance jurisdiction, creates a statutory framework where none existed, and establishes rights and obligations that were previously entirely absent. For the millions of Indian citizens whose personal data is processed daily by state and private actors, the Act represents meaningful, if imperfect, progress.

However, measured against the standards set by the GDPR, and evaluated against the constitutional promise of *Puttaswamy*, the Act falls short in several critical respects. The government exemption is constitutionally suspect and practically dangerous in a surveillance-conscious age. The Data Protection Board lacks the structural independence necessary to function as a credible regulator. The absence of key rights — portability, right to object, private right of action — weakens the individual's legal position relative to powerful data fiduciaries. And the Act's silence on automated decision-making and algorithmic profiling is a serious omission in an age of AI-driven data processing.

The DPDP Act is best understood not as a completed edifice but as a foundation — one that requires significant further construction. The true test of India's data protection framework will lie in the quality of the subordinate legislation and rules that will flesh out the Act's skeletal provisions, the independence and effectiveness of the Data Protection Board once constituted, and the willingness of courts to enforce the fundamental right to privacy against State as well as private infringements. India has taken the first step. The harder work lies ahead.

References

1. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (Supreme Court of India)
2. Digital Personal Data Protection Act, 2023 (No. 22 of 2023), Ministry of Law and Justice, Government of India
3. General Data Protection Regulation (EU) 2016/679, Official Journal of the European Union
4. California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100–1798.199 (2018), as amended by CPRA (2020)
5. Personal Information Protection Law of the People's Republic of China (2021)
6. B.N. Srikrishna Committee Report, "A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians" (2018), Ministry of Electronics and Information Technology
7. Raman Jit Singh Chima, "India's DPDP Act: An Assessment," Access Now Policy Brief (2023)
8. Graham Greenleaf, "Asian Data Privacy Laws: Trade and Human Rights Perspectives," Oxford University Press (2014)
9. Paul M. Schwartz & Karl-Nikolaus Peifer, "Transatlantic Data Privacy Law," Georgetown Law Journal, Vol. 106 (2017)
10. Usha Ramanathan, "A Unique Identity Bill," Economic and Political Weekly, Vol. 45, No. 30 (2010)
11. European Data Protection Board, "Guidelines on the Concept of Personal Data" (2022)
12. Vrinda Bhandari & Renuka Sane, "Towards a Privacy Framework for India in the Age of the Internet," NIPFP Working Paper (2018)