

Manuscript ID:
TIJCMBLIR-2025-020627

Volume: 2

Issue: 6

Month: December

Year: 2025

E-ISSN: 3065-9191

Submitted: 17 Nov. 2025

Revised: 28 Nov. 2025

Accepted: 16 Dec. 2025

Published: 31 Dec. 2025

Address for correspondence:

Lokanath Patra
Assistant Professor, Ganjam Law
College, Berhampur & Research
Scholar, PG Dept. of Law,
Berhampur University
Email:
lokanath_aisect@rediffmail.com

DOI: 10.5281/zenodo.19061328

DOI Link:

<https://doi.org/10.5281/zenodo.19061328>



Creative Commons (CC BY-NC-SA 4.0):

This is an open access journal, and articles are distributed under the terms of the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International Public License, which allows others to remix, tweak, and build upon the work noncommercially, as long as appropriate credit is given and the new creations are licensed under the identical terms.

Data Protection, Trust, and Sustainability in Digital Commerce: A Legal Analysis of India's Digital Personal Data Protection Act, 2023

Lokanath Patra

Assistant Professor, Ganjam Law Collge, Berhampur & Research Scholar, PG Dept. of Law, Berhampur University

Abstract

The rapid expansion of digital commerce and e-business platforms in India has altered market structures, customer behavior, and corporate strategies. This swift digitization has concurrently heightened apprehensions over personal data exploitation, monitoring, algorithmic profiling, and the deterioration of customer trust. The Digital Personal Data Protection Act, 2023 (DPDP Act) is India's first complete set of laws that govern how personal data is used in digital settings. This paper examines the DPDP Act, 2023 about the governance of digital commerce, emphasizing privacy protection, regulatory accountability, and sustainable digital business practices. This study utilizes a doctrinal and analytical research methodology to rigorously evaluate major components of the DPDP Act, encompassing consent management, data fiduciary responsibilities, cross-border data transfers, grievance resolution mechanisms, and penalties for non-compliance. The document contextualizes these regulations within the practical frameworks of e-commerce platforms, fintech services, digital marketplaces, and AI-driven business models. Comparative analyses of worldwide data protection regulations, especially the EU GDPR, are utilized to assess the sufficiency and shortcomings of India's developing data protection framework. The study concludes that although the DPDP Act enhances consumer rights and establishes accountability within digital commerce ecosystems, persistent structural and enforcement issues exist, especially with platform asymmetry, informed consent, and regulatory capacity. The paper contends that the effective execution of the DPDP Act can substantially improve consumer confidence, ethical data utilization, and the enduring viability of digital commerce in India. The article concludes by asserting that strong data protection is not only a legal obligation but also a fundamental component for inclusive, resilient, and sustainable digital economic development.

Keywords: Digital Commerce; E-Business; Digital Personal Data Protection Act, 2023; Data Privacy; Consumer Trust; Sustainable Digital Economy

Introduction

India has become one of the fastest-growing digital economies globally, propelled by fast improvements in information and communication technology, extensive internet access, and the widespread adoption of smartphones and digital payment systems. Digital commerce and e-business platforms have revolutionized conventional market frameworks by facilitating effortless online transactions, algorithmic personalization, immediate customer interaction, and international trade. Industries such as e-commerce, fintech, health-tech, and ed-tech increasingly depend on personal data as a fundamental economic asset to improve efficiency, competitiveness, and innovation (World Economic Forum, 2021). In this data-driven world people often call personal data the new oil of the digital economy. In contrast to conventional economic resources, personal data is fundamentally associated with individual dignity, autonomy, and privacy. The comprehensive accumulation, analysis, and commercialization of personal data by digital platforms have engendered significant apprehensions about surveillance capitalism, profiling, data breaches, and the deterioration of customer confidence. Recurring occurrences of large data breaches and unauthorized data dissemination have underscored the dangers intrinsic to digital ecosystems (Solove, 2021).

Before the Digital Personal Data Protection Act, 2023 went into effect, India's data protection system was not well-organized. The Information Technology Act, 2000, and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, were the main laws that governed it. These methods did not provide enough protection and were not strong enough to deal with modern issues like analytics driven by artificial intelligence, behavioral advertising, automated decision-making, and data flows between countries.

How to Cite this Article:

Patra, L. (2025). Data Protection, Trust, and Sustainability in Digital Commerce: A Legal Analysis of India's Digital Personal Data Protection Act, 2023. *The International Journal of Commerce Management and Business Law in International Research*, 2(6), 132–135. <https://doi.org/10.5281/zenodo.19061328>

The Supreme Court of India's important decision in Justice K.S. Puttaswamy v. Union of India (2017) confirmed that privacy is a basic right under Article 21 of the Constitution. This made it clear that we need a strong data protection system right away (Justice K.S. Puttaswamy (Retd.) v. Union of India, 2017).

Given this constitutional and economic framework, the Digital Personal Data Protection Act, 2023, serves as a vital legislative measure designed to reconcile individual privacy rights with the legitimate requirements of digital commerce, innovation, and government. The Act aims to create a trust-oriented digital environment that fosters sustainable economic development while protecting personal information.

Objectives and Research Methodology

This study aims to critically analyze the Digital Personal Data Protection Act, 2023 concerning digital commerce and e-business operations in India. The study aims to evaluate whether the Act adequately reconciles the safeguarding of individual privacy with the commercial demands of data-driven business models.

The study's particular aims encompass:

- To analyze the legislative structure and fundamental tenets of the DPDP Act, 2023.
- To examine the rights of data principals and the responsibility placed upon data fiduciaries.
- To assess the influence of the Act on consumer trust and the sustainability of digital commerce.
- To evaluate compliance obstacles encountered by e-commerce and finance platforms.
- To evaluate India's data protection framework against international benchmarks, namely the EU's GDPR.

The research utilizes a doctrinal and analytical methodology. The DPDP Act of 2023, constitutional law, and policy papers are all examples of primary materials. Secondary sources encompass scholarly publications, industrial analyses, and expert critiques. A comparative methodology is employed to situate India's framework within the global data protection landscape.

The Digital Personal Data Protection Act, 2023's legal framework

The Digital Personal Data Protection Act, 2023 is the first law in India that only deals with the protection of digital personal data. It replaces the fragmented regulatory framework created by the IT Act, 2000, and reflects India's constitutional commitment to privacy as an inherent right (Government of India, 2023).

1. What it covers and who it applies to

The Act regulates the processing of digital personal data in India and applies to extraterritorial processing when products or services are offered to individuals in India. This extraterritorial scope illustrates the unbounded character of internet commerce and connects India with international regulatory standards (India Briefing, 2023).

2. Fundamental Legal Principles

The Act establishes essential legal classifications including data principal, data fiduciary, data processor, and consent manager (India Briefing, 2023). Digital commerce platforms, fintech firms, and online marketplaces are designated as data fiduciaries, thus assuming primary responsibility for lawful and transparent data processing.

3. Fundamental Principles of Data Processing

The DPDP Act is based on principles of lawful processing, informed consent, purpose limitation, data minimization, retention limitation, and adequate security measures. These principles directly govern commercial techniques such as targeted advertising, behavioral profiling, and data analytics, prevalent in digital commerce.

4. Rights of Data Principals

The Act confers persons with enforceable rights such as access, correction, erasure, withdrawal of consent, and grievance redressal. These rights rectify the power disparity between consumers and major digital platforms, augmenting transparency and accountability (Srikrishna, 2018).

5. Duties and Implementation

Data fiduciaries must establish privacy notices, consent management systems, grievance redressal methods, and cybersecurity protections. The Data Protection Board of India have enforcement authority, encompassing investigation and the application of financial penalties. This accountability-oriented structure enhances regulatory supervision in digital marketplaces.

Data Protection, Consumer Trust, and Sustainability in Digital Commerce

Trust is the foundation of internet commerce. In contrast to physical marketplaces, digital transactions encompass imperceptible mechanisms of data acquisition, algorithmic determinations, and the dissemination of data to third parties. Consumers frequently lack transparency regarding the utilization of their data, heightening susceptibility to exploitation and misuse (World Economic Forum, 2021). The DPDP Act is essential for establishing trust by legally requiring transparency, consent, and responsibility. When customers are confident that their personal data will be handled equitably and securely, their propensity to participate in digital transactions rises. Consequently, trust operates not only as a social benefit but also as an economic facilitator (PwC India, 2024). From a sustainability standpoint, trust-centric data governance fosters enduring stability in the digital marketplace. Platforms that neglect privacy face brand harm, regulatory penalties, and consumer disengagement. In contrast, privacy-respecting platforms are more likely to acquire client loyalty, adhere to regulatory standards, and foster sustainable growth. The DPDP Act reinterprets data protection as a device for market stabilization rather than a governmental encumbrance. It promotes ethical innovation and appropriate data utilization, which are crucial for the stability of digital commerce ecosystems.

How the DPDP Act affects e-commerce and fintech platforms

E-commerce and banking platforms are two of the digital economy's most data-heavy businesses. These businesses consistently handle sensitive personal and financial information to facilitate payments, credit evaluations, fraud mitigation, and customized services.

1. Compliance and Operational Difficulties

Adherence to the DPDP Act necessitates substantial organizational and technological modifications. Platforms must build consent management systems, redesign user interfaces to guarantee informed consent, monitor data inventories, and execute breach response protocols. These duties incur compliance expenses, especially for small and medium firms (PwC India, 2024).

2. Concerns Specific to FinTech

Fintech platforms encounter distinct obstacles stemming from real-time transaction processing and regulatory intersections with financial industry standards. Transaction-specific consent mandates may impact fluid payment experiences. Achieving equilibrium between consumer protection and operational efficiency necessitates tailored regulatory guidelines for each sector.

3. Competitive and Market Consequences

From a commercial standpoint, adherence to the DPDP Act can serve as a competitive differentiation. Platforms exhibiting robust privacy governance may cultivate consumer trust and achieve a competitive market advantage. Conversely, non-compliance may lead to sanctions, reputational damage, and diminished consumer trust.

Enforcement Mechanism, Exemptions, and Governance Challenges under the Data Protection and Digital Privacy Act, 2023

Robust enforcement is essential for the efficacy of any data protection framework. The DPDP Act creates an enforcement framework focused on responsibility and deterrence, while also highlighting governance issues.

1. The Data Protection Board of India

The Act says that the Data Protection Board of India (DPBI) will be the main body that makes decisions. The Board is authorized to investigate infractions, give directives, and levy financial penalties. This establishes specific regulatory supervision and enhances accountability for digital commerce platforms (Government of India, 2023). Nonetheless, apprehensions persist over the Board's institutional autonomy, as its makeup and operations are influenced by executive oversight. This may impact regulatory neutrality in comparison to the independent supervisory authority of the GDPR (Kuner, 2020).

2. Penalties and Deterrence

The Act implements an enforcement model based on civil penalties. Significant penalties promote adherence and internalize the expenses associated with privacy infringements. The lack of criminal responsibility may hinder deterrence in instances of intentional or recurrent misbehavior.

3. Exemptions and Trust Deficit

The Act provides extensive exemptions to the State based on considerations such as national security and good order. Although exclusions are not intrinsically unlawful, their extensive scope and absence of control may erode public trust. In digital commerce ecosystems connected to state-affiliated digital infrastructure, such exemptions pose substantial issues related to proportionality and accountability (Justice K.S. Puttaswamy (Retd.) v. Union of India, 2017).

4. Challenges in Capacity and Governance

Effective enforcement necessitates technical proficiency, institutional capability, and procedural transparency. In the absence of sufficient resources and transparency, enforcement is likely to be reactive instead of proactive.

Comparative Analysis and Global Coordination

In a globalized digital economy, national data protection legislation must conform to international norms to enable cross-border commerce and data transfer.

1. Alignment with International Standards

The DPDP Act integrates fundamental elements seen in international frameworks like the GDPR, encompassing consent, purpose limitation, and accountability. This convergence bolsters India's credibility in global digital commerce (European Union, 2016).

2. Deviation from the GDPR

Notwithstanding similarities, discrepancies persist. The GDPR grants expanded rights, enhanced safeguards against profiling, and autonomous supervisory bodies. The DPDP Act has a somewhat moderate rights-based framework, mirroring India's developmental objectives.

3. International Data Transfers

The DPDP Act allows cross-border data transfers contingent upon government notification. This flexibility facilitates digital trade, but administrative discretion creates uncertainty. Explicit requirements would improve predictability for global platforms.

4. India's Role in Global Data Governance

India's data protection regime makes it a new leader in the Global South. Following global best practices all the time will be very important for long-lasting trust and compatibility.

Final Thoughts and Suggestions

The Digital Personal Data Protection Act, 2023 is a big step forward for India's digital rules. As digital commerce becomes integral to economic growth, data governance is increasingly recognized not just as a legal need but also as a crucial factor in establishing trust, legitimacy, and sustainability. This article has demonstrated that the DPDP Act seeks to harmonize technological advancement, economic efficiency, governmental interests, and fundamental rights. The Act establishes the right to privacy recognized in Justice K.S. Puttaswamy v. Union of India by transforming abstract concepts into actionable legal rights and obligations. From a

commercial perspective, it redefines data protection as a facilitator of trust and enduring market stability. Sustainable digital commerce cannot prosper in an atmosphere of ambiguity, insecurity, and consumer skepticism.

But structural limits still exist. If not fixed, the Act's ability to build trust could be hurt by a lot of government exclusions, worries about the Data Protection Board's independence, and a partial departure from worldwide best practices.

Suggestions

- To improve the Data Protection Board of India's independence and technical skills, appointment processes and operational autonomy must be clear.
- Secondly, official exclusions must be meticulously designed and submitted to proportionality assessments and independent scrutiny to maintain public confidence.
- Third, sector-specific compliance regulations for e-commerce and fintech platforms should be established to reconcile innovation with consumer protection.
- Fourth, prioritization of consumer awareness and digital literacy programs is essential for the efficient exercise of data principle rights.
- India should seek to align progressively with emerging global data protection standards to enhance cross-border digital trade and regulatory interoperability.

Final Assessment

The DPDP Act, 2023 should be regarded not only as a compliance act but as a fundamental element of India's digital constitutionalism and economic governance. The success of this initiative hinges on efficient execution, reliable enforcement, and iterative improvement. A rights-oriented, trust-centric data governance framework is essential for maintaining an inclusive, competitive, and sustainable digital commerce ecosystem in India over the long term.

Acknowledgment

The author expresses sincere gratitude to all those who directly or indirectly contributed to the successful completion of this research work. Special thanks are extended to colleagues, reviewers, and academic mentors for their valuable guidance, constructive suggestions, and continuous encouragement throughout the study.

Financial support and sponsorship

Nil.

Conflicts of interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

References

1. European Union. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation). Official Journal of the European Union, L119, 1-88.
2. Government of India. (2011). Information Technology (Reasonable Security Practices and

Procedures and Sensitive Personal Data or Information) Rules, 2011. Ministry of Electronics and Information Technology.

3. Government of India. (2023). Digital Personal Data Protection Act, 2023. Ministry of Law and Justice.
4. India Briefing. (2023). India's Digital Personal Data Protection (DPDP) Act, 2023. Retrieved from <https://www.india-briefing.com/news/indias-digital-personal-data-protection-act-2023-key-provisions-29021.html>
5. Justice K.S. Puttaswamy (Retd.) v. Union of India, 10 SCC 1 (2017).
6. Kuner, C. B. (2020). The EU General Data Protection Regulation (GDPR): A commentary. Oxford University Press.
7. PwC India. (2024). Digital Personal Data Protection Act, 2023: Compliance readiness and impact on Indian enterprises. PricewaterhouseCoopers Pvt. Ltd.
8. Solove, D. J. (2021). Understanding privacy (2nd ed.). Harvard University Press.
9. Srikrishna, B. N. (2018). A free and fair digital economy: Protecting privacy, empowering Indians. Government of India.
10. World Economic Forum. (2021). Data protection and privacy in the digital economy: A global perspective. WEF.