Page: 947-958 *URL: www.lijdlr.com*

LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

ISSN: 2583-7753

LawFoyer International Journal of Doctrinal Legal Research

[ISSN: 2583-7753]

Volume 3 | Issue 2

2025

DOI: https://doi.org/10.70183/lijdlr.2025.v03.78

THE REGULATORY CONUNDRUM: A MULTIDIMENSIONAL ANALYSIS OF THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023, AND ITS IMPLICATIONS FOR INDIAN STARTUPS

Parul Shukla[1]

I. ABSTRACT

The Digital Personal Data Protection Act, 2023 (DPDP Act), marks India's first comprehensive data protection legislation, reaffirming the constitutional right to privacy as upheld in K.S. Puttaswamy v. Union of India (2017). This paper employs a multidimensional analytical framework encompassing political, social, economic, technological, environmental, and legal (PSETEL) lenses to evaluate the Act's implications on India's startup ecosystem, particularly data-intensive sectors such as SaaS, health-tech, ed-tech, and fintech. Politically, while aligning with global benchmarks like the GDPR, the Act asserts digital sovereignty through the creation of the Data Protection Board of India, which wields enforcement and adjudicatory powers under Section 27, thus balancing innovation incentives under Section 17(1)(e) with concerns of potential executive overreach. Socially, the Act enhances data principal rights, including informed consent, correction, and erasure, expected to improve consumer trust, though requirements like verifiable parental consent (Section 9) may affect user acquisition strategies, especially in ed-tech sectors. Economically, compliance costs are projected to increase by 7–10% for early-stage startups due to obligations such as appointing Data Protection Officers and conducting Data Protection Impact Assessments, with non-compliance penalties extending up to Rs. 250 Crores under Schedule I. Technologically, the Act necessitates system-wide changes in data processing and architecture to meet principles of data minimization and purpose limitation, though its regulatory silence on AI and ML raises compliance ambiguities. Environmentally, data localization mandates could elevate energy demands through the expansion of domestic data centers, albeit offset partially by sustainable data minimization practices. Legally, the Act's extraterritorial scope (Section 3), mandatory

[1] Author is a final year law student at Law Centre II, University of Delhi.

 (ISSN: 2583-7753)

breach reporting (Section 8), and amendments to the RTI Act create regulatory uncertainties and increase administrative burdens, particularly for cross-border operations. Despite these challenges, the Act presents opportunities for startups to differentiate themselves through ethical data stewardship, thereby aligning with India's ambition of achieving a USD 1 trillion digital economy by 2030.

II. KEYWORDS

Consent Management, Cross Border Data Transfer, Data Localization, DPDP, Privacy, Regulation, Significant Data Fiduciaries, Startups

III. INTRODUCTION

The enactment of the Digital Personal Data Protection Act, 2023 (hereinafter referred to as 'DPDP Act') has been instrumental in enforcing privacy as a fundamental right post K.S. Puttaswamy judgment by the Hon'ble Supreme Court. It marks a pivotal shift in India's data governance landscape by introducing the nation's first comprehensive data protection legislation. The aim of DPDP Act is to strike a fine balance between individual privacy and corporate requirement of innovation and business.[2] The central to the debate is the fate of startups in India given their booming rise across the economic landscape. This is particularly relevant for startups in data intensive sectors like SaaS, heath-tech, ed-tech and fintech.

IV. METHODOLOGY

This paper adopts a multidimensional analytical framework based on the PESTEL (Political, Economic, Social, Technological, Environmental, and Legal) approach to examine the impact of the Digital Personal Data Protection Act, 2023, on India's startup ecosystem. Each dimension is used to dissect specific provisions of the Act in relation to the operational realities of data-intensive startups in sectors such as SaaS, health-tech, ed-tech, and fintech. The analysis is primarily doctrinal and qualitative in nature, relying on statutory interpretation, regulatory texts, comparative references to international frameworks like the GDPR, and secondary literature including policy

[2] The Digital Personal Data Protection Act, 2023, s 4(1).

papers, industry reports, and judicial pronouncements. Where relevant, the study incorporates sectoral data and compliance cost projections to offer grounded insights. This comprehensive methodology enables an integrated understanding of both normative goals and practical implications of the DPDP Act for emerging businesses in the Indian digital economy.

V. POLITICAL APPROACH

From a political standpoint, the enactment can be termed as an ambitious attempt to align the policy framework with the global standards particularly the General Data Protection Regulation (GDPR) by the European Union. However, this alignment has also ensured assertion of our sovereignty in the policy digital space.[3] Through its nuanced provisions, the DPDP Act empowers the Union Government to constitute a Data Protection Board of India to oversee the compliance. The board has wide powers to define exemptions, impose penalties and restrict cross border data transfers.[4] For the Indian Startup ecosystem this creates a situation of a double edged sword with section 17(1)(e) easing the compliance burden and fostering innovation[5] while on the other hand, the discretionary power of the board raises critical questions of state surveillance given that in the backdrop of the Information Technology Act, 2000, interception are legally permissible for state bodies.[6] From the political forefront, startups may face political pressure to align with the priorities of the state in sectors such as health tech where data localization could complicate the startup relations with international partners.[7]

An additional political concern arises regarding the institutional independence of the Data Protection Board of India. Although envisaged as an adjudicatory and enforcement body under the DPDP Act, its autonomy is undermined by structural

[3] Sonali Srivastava, 'India: Decrypting Critical Concepts under India's Digital Personal Data Protection Act, 2023 and Comparison with GDPR and PIPL' (2024) International Journal of Law and Technology https://www.ijlt.in accessed 10 July 2025.
[4] The Digital Personal Data Protection Act, 2023, s 18.
[5] The Digital Personal Data Protection Act, 2023, s 17(1)(e).
[6] The Information Technology Act, 2000, s 69.
[7] FIG Paper (No. 40 – Data Law Series 6), 'Draft Digital Personal Data Protection Rules, 2025 - Key Implications for Financial Services Sector' (Cyril Amarchand Mangaldas, 14 January 2025) https://corporate.cyrilamarchandblogs.com accessed 10 July 2025.

vulnerabilities. Notably, the Central Government retains significant discretion over key aspects of the Board's constitution, including appointments, service conditions, and removal procedures of its Chairperson and Members. The prescribed two-year tenure, as opposed to a longer fixed term commonly seen in independent regulatory bodies, risks incentivizing short-term compliance with executive preferences rather than long-term institutional integrity. Such executive control compromises the Board's ability to function impartially, especially when adjudicating disputes involving government departments or politically sensitive sectors such as health-tech or fintech. For startups, this raises serious apprehensions about regulatory capture and the lack of a neutral forum to address grievances, thereby chilling innovation and investment in sectors heavily reliant on trust in institutional fairness and due process.

VI. SOCIAL APPROACH

From a social viewpoint, the DPDP Act has reinforced privacy as a fundamental right under Article 21 of our constitution.[8] The provisions of the act foster trust of the masses in the digital services. For instance, right to correction, right to erasure, informed consent, grievance redressal, these data principal rights can drive the next wave of digital innovation while balancing the public trust.[9] This can be looked as an opportunity for the early startups to establish their consumer trust through transparent data practices. However, it has potentially unaddressed challenges in place. Section 9 of the DPDP Act, which essentially mandates verifiable parental consent and prohibits targeted advertising for minors, pose challenges for startups relying heavily on user profiling like ed-tech and consumer tech.[10] The act not only creates a burden on the fiduciaries but also upon the principal's by mandating authentic and genuine data which essentially undermines the social goal of protecting the vulnerable populations.[11]

[8] Justice K.S. Puttaswamy (Retd.) v Union of India (2017) 10 SCC 1.
[9] The Digital Personal Data Protection Act, 2023, ss 5, 6.
[10] The Digital Personal Data Protection Act, 2023, s 9.
[11] The Digital Personal Data Protection Act, 2023, s 11.

 (ISSN: 2583-7753)

Section 9 of the DPDP Act, which mandates verifiable parental consent for processing the personal data of children, introduces complex operational challenges for startups, particularly in ed-tech, gaming, and social media sectors that cater to users below 18 years. Unlike jurisdictions such as the United States under COPPA, which defines a child as under 13, the DPDP Act sets the bar at 18 years, thereby widening the compliance net. Implementing verifiable consent mechanisms, such as OTP-based validation through government ID, biometric authentication, or manual document verification, would significantly increase friction in user onboarding and raise concerns around privacy-invasive methods that paradoxically conflict with the Act's own data minimization goals. For resource-constrained startups, the technological and financial costs of developing secure age-gating systems and ensuring real-time verification of parental identity are substantial. Moreover, the absence of standardised verification protocols or regulatory guidance adds uncertainty, exposing startups to inadvertent non-compliance and penal consequences. As a result, startups may be deterred from engaging younger demographics altogether, leading to under-inclusivity in digital services designed for education, healthcare, or social development, thus undermining the broader social goals of digital inclusion and empowerment.

VII. ECONOMIC APPROACH

DPDP Act introduces a significant burden in the form of compliance costs on the fund short startups from the economic standpoint. The act mandates the fiduciaries to conduct Data Protection Impact Assessment (DPIA) and appoint DPOs for significant data fiduciaries.[12] These regulations are coupled with hefty potential penalties that goes up to Rs. 250 Crores for non-compliance. Early stage startups which are short on financial resources may face critical conditions and the ecosystem might be negatively impacted.[13] These early stage startups are usually operating on high initial year burns which magnifies the crisis. Fintech startups rely heavily on sensitive financial data but post enactment of DPDP Act, they are bound in invest a big percentage on encryption,

[12] The Digital Personal Data Protection Act, 2023, ss 8(5), 10.
[13] The Digital Personal Data Protection Act, 2023, s 33.

access controls and data breach reporting mechanisms which at the end of the day alleviates the compliance and operational costs.[14] On the reverse side, the DPDP Act focusses on data minimization and purpose limitation which can potentially foster innovation and efficiency in privacy centric conditions.[15] The India e Conomy Report 2023 puts out the ambitious goal of USD 1 Trillion Digital Indian Economy by 2030. This underscores the economic incentive for startups to adapt to the changing regulatory landscape.[16]

To contextualize the economic burden imposed by the DPDP Act, it is pertinent to compare its penalty framework with international standards, particularly the European Union's General Data Protection Regulation (GDPR). Under the GDPR, non-compliance can attract fines of up to €20 million or 4% of a company's global annual turnover, whichever is higher. The DPDP Act, while setting an upper penalty cap of Rs. 250 Crores (~€27 million), does not tie the fine quantum to the turnover of the violating entity. This fixed-cap model can disproportionately impact startups with limited capital reserves as compared to established corporations, potentially deterring small-scale innovation. Moreover, unlike the GDPR, which allows for some discretion based on intent, harm, and mitigation efforts, the DPDP Act remains vague on the gradation criteria for penalty imposition, thereby increasing financial uncertainty for fledgling ventures. The absence of a tiered or proportional penalty structure, especially for first-time or inadvertent breaches, may result in over-compliance or operational hesitancy among startups, hampering risk-taking and experimentation that are intrinsic to early-stage growth. Thus, while the penalty regime under the DPDP Act is arguably less severe in absolute monetary terms than the GDPR, its inflexible structure may pose a more acute threat to startup sustainability in the Indian context.

[14] 'India's DPDP Act: Impact on Tech Companies' (Law.asia, 18 April 2024) https://law.asia accessed 10 July 2025.
[15] 'Data Privacy Compliance: Indian Startups Adapt to DPDP Act 2023' (Arohana Legal, 22 January 2025 https://arohanalegal.com accessed 10 July 2025.
[16] 'India e-Conomy Report 2023' (Bain & Company, 2023) 78, 79.

 (ISSN: 2583-7753)

VIII. TECHNOLOGICAL APPROACH

On the technological forefront, the DPDP Act compels the startups to overhaul their data architectures in order to be in consonance with principles like purpose limitation, data minimization and storage limitation.[17] This can be a new wave of technological innovation in India where startups are tasked with the challenge of redesigning data collection touchpoints, consent management techniques, accommodating data erasure and modification requests. This is a potentially driver of FDI investments in the software and technology sectors of India.[18] For instance, SaaS startups may need to adopt interoperable technologies in order to be able to manage user consent.[19] However, on the flip side the DPDP Act is silent on the latest entrant in the market, i.e., the AI. AI and Machine Learning (ML) are raising significant and daunting questions. Startups which are actively utilizing AI and ML services for data analytics may face regulatory oversight and scrutiny due to privacy concerns.[20] Sensitive data being utilized to train AI/ML remains vulnerable. This is coupled with the exemption of publicly available data from the scope of DPDP. This could potentially undermine user privacy.[21] This concern has been reiterated time and again by the Reserve Bank of India.[22]

IX. ENVIRONMENTAL APPROACH

The DPDP Act may also have environmental ramifications, albeit indirect. Data localization mandate would potentially drive the demand for domestic data centres.[23] These data centres are high energy consuming units which can potentially put strain on the energy resources of the country. Startups, especially in cloud based services may face governmental and public pressure to adopt sustainable practices which may

---

[17] The Digital Personal Data Protection Act, 2023, s 6.
[18] Draft Digital Personal Data Protection Rules, 2025, r 4.
[19] 'Impact of India's Data Protection on Business and Policy' (Law.asia, 25 March 2025) https://law.asia accessed 10 July 2025.
[20] 'India: Regulators Must Balance Growth and Innovation with User Protection' (Global Competition Review, 17 May 2024) https://globalcompetitionreview.com accessed 10 July 2025.
[21] 'GDPR v India's DPDPA: Key Differences and Compliance Implications' (Legal500, 1 March https://www.legal500.com accessed 10 July 2025.
[22] Reserve Bank of India, 'Storage of Payment System Data' (RBI/2017-18/153, 6 April 2018).
[23] The Digital Personal Data Protection Act, 2023, s 16(1).

be financially unviable, creating a difficult conundrum for the early stage startups.[24] This has to be read in consonance with Article 48 A of the Constitution of India. However on the flip side, the act also lays stress on data minimization requirements which can potentially lower the carbon footprint of the digital operations.[25]

X. LEGAL APPROACH

The enactment introduces a daunting regulatory landscape for the vulnerable early stage startups which even has legal ramifications. It is pertinent to note that the act has extraterritorial applicability which essentially covers data processing beyond Indian territory.[26] This is a legal nightmare for startups engaged in cross border data flows as the act empowers the board to restrict such flow. This creates uncertainties in the International partnerships, especially the Tech Transfer Agreements.[27] The act lays down the requirement of mandatory reporting of all data breach events to the board. This can be overwhelming for early stage startups creating an administrative impediment.[28] The DPDP Act has also sought to amend Section 8(1)(j) of the RTI Act which essentially removes the 'larger public interest' test for withholding personal data. This is particularly challenging for startups heavily reliant upon public data for innovation.[29] The absence of a specific 'Right to be Forgotten' limits the act's alignment with the GDPR which exposes Indian startups to the risk of International Regulatory Penalties.[30]

XI. CONCLUSION

The Digital Personal Data Protection Act, 2023, while imposing a challenging regulatory framework, presents a transformative opportunity for startups to develop trust-centric business models and contribute to a sustainable digital economy. The Act

---

[24] Constitution of India, art 48A.
[25] 'Environment (Protection) Act, 1986' cited in 'Directive Principles of State Policy' (Drishti IAS, 23 January 2025) https://www.drishtiias.com accessed 10 July 2025.
[26] The Digital Personal Data Protection Act, 2023, s 3.
[27] Draft Digital Personal Data Protection Rules, 2025, r 13.
[28] The Digital Personal Data Protection Act, 2023, s 8(6).
[29] The Digital Personal Data Protection Act, 2023, s 44(3).
[30] 'Information Privacy Rights in India: A Study of the Digital Personal Data Protection Act, 2023' (IntechOpen, 2024) https://www.intechopen.com accessed 10 July 2025.

 (ISSN: 2583-7753)

reflects India's ambition to balance the imperatives of privacy, innovation, and economic growth in an increasingly data-driven ecosystem. However, the multidimensional analysis highlights that without calibrated implementation, the compliance burden may disproportionately affect early-stage startups, potentially stifling innovation. Therefore, the way forward requires coordinated efforts from both policymakers and startup entrepreneurs.

From a political perspective, policymakers should ensure the institutional independence of the Data Protection Board of India by extending fixed tenure, providing operational autonomy, and introducing transparent appointment procedures. This would foster investor and industry confidence while preventing regulatory capture. For startups, proactive engagement with regulatory sandboxes and industry forums can mitigate political risks and enhance compliance readiness.

From a social perspective, policymakers should issue standardized guidelines for verifiable parental consent and age-gating mechanisms to avoid inconsistent and privacy-invasive practices. This would reduce operational burdens on startups in ed-tech, gaming, and youth-focused sectors. Entrepreneurs, in turn, should adopt user-friendly consent management frameworks and leverage privacy-enhancing technologies to cultivate consumer trust and expand user acquisition responsibly.

From an economic standpoint, the government could explore phased compliance timelines, tiered penalties, or turnover-based fine structures for first-time and small-scale violators, thereby aligning the regulatory regime with startup realities. Access to financial incentives, tax rebates, or subsidized cybersecurity infrastructure for early-stage ventures could further ease the economic pressure. Startup founders should, meanwhile, integrate privacy-by-design principles into their products early on to reduce long-term compliance costs and attract privacy-conscious investors.

From a technological perspective, policymakers should issue clarifications on the application of the DPDP Act to AI and machine learning systems, including the use of anonymized or publicly available data. Sector-specific best practice guidelines on data anonymization, secure APIs, and interoperable consent tools can drive responsible innovation. Startups should invest in modular and scalable data architecture that

incorporates consent management, breach detection, and data minimization from inception, thereby turning regulatory compliance into a market differentiator.

From an environmental perspective, the anticipated growth of domestic data centers necessitates policies promoting green data infrastructure, energy-efficient cooling technologies, and renewable energy incentives for digital operations. Startups can preemptively align with these goals by adopting sustainable data retention policies, cloud-based scalable solutions, and leveraging carbon-neutral hosting services, thereby strengthening both environmental stewardship and brand reputation.

From a legal perspective, policymakers should provide detailed compliance toolkits, safe-harbor provisions for good-faith reporting of breaches, and model contractual clauses for cross-border data transfers. Harmonization with international standards such as GDPR would reduce legal uncertainty for globally integrated startups. Entrepreneurs should invest in early legal due diligence, implement robust data protection policies, and explore cross-border legal risk mitigation strategies, including local partnerships and contractual safeguards.

In essence, the DPDP Act is a double-edged sword for India's startup ecosystem: it imposes immediate compliance costs but unlocks long-term opportunities for responsible and trust-based growth. A collaborative approach, where regulators ensure clarity, proportionality, and support for emerging businesses, and startups embrace privacy-centric innovation—will be crucial in achieving India's vision of a $1 trillion digital economy by 2030 while safeguarding the fundamental right to privacy.

XII. BIBLIOGRAPHY

A. Legislation and Government Documents

i. Digital Personal Data Protection Act 2023 (India)

ii. Information Technology Act 2000 (India)

iii. Right to Information Act 2005 (India)

iv. Constitution of India 1950

v. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 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] OJ L119/1

vi. Children's Online Privacy Protection Act 1998 (US)

vii. Google, Bain & Company and Temasek, *India e-Conomy Report 2023* (2023)

viii. Reserve Bank of India, *Annual Report 2022–23* (May 2023)

B. Case Law

i. *Justice K S Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1

C. Reports and White Papers

i. Committee of Experts under the Chairmanship of Justice B N Srikrishna, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (Government of India 2018)

ii. Dvara Research, *Understanding the DPDP Act, 2023: A Regulatory Commentary* (2023)

iii. Internet Freedom Foundation, *Analysis of the Digital Personal Data Protection Act, 2023* (2023)

iv. NITI Aayog, *National Strategy for Artificial Intelligence* (2018)

v. OECD, *Data-Driven Innovation: Big Data for Growth and Well-Being* (OECD Publishing 2015)

vi. World Economic Forum, *Personal Data: The Emergence of a New Asset Class* (2011)

D. Books

1. Daniel J Solove, *Understanding Privacy* (Harvard University Press 2008)

2. Graham Greenleaf, *Asian Data Privacy Laws: Trade and Human Rights Perspectives* (OUP 2014)

E. Online Sources

1. Ministry of Electronics and Information Technology (MeitY), 'Official Website' https://www.meity.gov.in accessed 28 July 2025
2. European Commission, 'Data Protection' https://ec.europa.eu/info/law/law-topic/data-protection accessed 28 July 2025