International Journal of Law, Policy and Social Review
www.lawjournals.net
Online ISSN: 2664-6838
Received: 19-02-2026, Accepted: 20-03-2026, Published: 06-04-2026
Volume 8, Issue 2, 2026, Page No. 10-15

A critical legal analysis of the digital personal data protection Act, 2023

Ramkumar V
SRM School of Law, SRM University, Kattankulathur, Tamil Nadu, India

Abstract
The Digital Personal Data Protection Act, 2023 (DPDP Act) represents India's definitive legislative response to the constitutional imperative established in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) [1], which enshrined privacy as a fundamental right under Article 21 [2]. The Act marks a paradigm shift from the fragmented and outdated IT regime to a comprehensive framework governing digital personal data [3]. Its legal philosophy is rooted in a "consent-based" architecture, balanced against "legitimate uses" that serve state and economic interests [4]. While it grants individuals enforceable rights as Data Principals and imposes statutory obligations on Data Fiduciaries, its ultimate success will be judged by the operationalization of its quasi-judicial enforcement mechanism and its resilience against state overreach [5]. The Act's true significance lies not merely in its codification of rights, but in its attempt to navigate the precarious balance between individual autonomy, national security imperatives, and the demands of a burgeoning digital economy [6].

Keywords: Digital Data Protection, Right to Privacy, Consent-based Framework, Data Governance

Introduction

The journey towards the DPDP Act began from a position of legal insufficiency. Prior to its enactment, India's data protection landscape was governed by a fragmented and ill-equipped regime: the Information Technology Act, 2000 (IT Act) [7], and its subordinate legislation, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules) [8]. This framework was fundamentally inadequate for the digital age. It defined "sensitive personal data" narrowly, provided no statutory rights to individuals, imposed minimal obligations on entities, and lacked an independent oversight mechanism [9]. The rapid proliferation of digital services, coupled with the rise of surveillance capitalism and an alarming increase in data breaches, exposed the deep vulnerabilities of Indian citizens in the digital ecosystem [10].

The legislative journey was catalyzed by the Supreme Court's 2017 judgment in Puttaswamy, which unequivocally declared that informational privacy is an intrinsic facet of the right to life and liberty [11]. This constitutional mandate necessitated a robust statutory framework. The subsequent formation of the Committee of Experts under Justice B.N. Srikrishna led to the draft Personal Data Protection Bill, 2018—a comprehensive, GDPR-influenced piece of legislation [12]. However, this bill underwent extensive scrutiny by a Joint Parliamentary Committee, which proposed over 80 amendments, leading to its withdrawal in 2022 [13]. The government then introduced a streamlined, leaner version—the DPDP Act, 2023—which was passed by both houses of Parliament and received presidential assent in August 2023 [14]. This legislative journey reflects a deliberate policy shift from a principle-heavy, rights-centric model towards a more business-friendly, state-flexible framework [15].

Justification for dpdp ACT

The necessity of the DPDP Act can be justified on four critical grounds:

- **Constitutional Fulfilment:** The Puttaswamy judgment created a legal vacuum. Without a dedicated data protection law, the fundamental right to privacy was left without a statutory enforcement mechanism, making it an abstract constitutional promise rather than a practical reality [16]. The Act provides the statutory architecture to give effect to this fundamental right [17].

- **Countering Big Tech Data Dominance:** The asymmetry of power between individual citizens and large technology firms (Data Fiduciaries) had become untenable [18]. Entities like Meta, Google, and Amazon operated under a self-regulated framework, often exploiting opaque consent mechanisms and user data for unanticipated purposes [19]. The Act introduces a fiduciary duty, legally compelling these entities to act in the interest of Data Principals [20].

- **Mitigating Cyber Threats and Data Breaches:** The absence of mandatory breach notification and significant penalties for security failures left organizations with insufficient incentives to invest in robust security infrastructure [21]. The Act's stringent penalty regime (up to ₹250 crore for breach-related failures) serves as a powerful economic deterrent, compelling a culture of security by design [22].

- **Economic Imperative for Trust:** For India to achieve its vision of a $1 trillion digital economy, establishing a trusted data governance framework is paramount [23]. Foreign investment and the expansion of domestic digital enterprises are contingent on a predictable and protective legal environment [24]. The Act aims to create this trust, positioning India as a responsible jurisdiction for data processing [25].

Structure & key provisions

- **Definitions:** The Act establishes a clear dyadic relationship. The Data Principal is the individual, granted a suite of rights [26]. The Data Fiduciary is the

entity that determines the purpose and means of processing, bearing the primary compliance burden [27]. Consent is defined as a "clear, affirmative, informed, and freely given" action, moving beyond implied consent [28]. Significant Data Fiduciaries (SDFs) are a designated subclass subject to heightened accountability, including Data Protection Officer (DPO) appointments and Data Protection Impact Assessments (DPIAs), signaling a risk-based regulatory approach [29].

- **Rights of Individuals:** The Act provides a set of enforceable rights: the right to access information about processing; the right to correction and erasure; the right to grievance redressal; and the right to nominate a representative [30]. However, unlike the GDPR [31], it does not explicitly grant a "right to data portability" or a "right to restriction of processing" [32].

- **Duties of Individuals:** A notable feature is the imposition of duties on Data Principals, such as providing authentic information and refraining from frivolous complaints [33]. This reflects a policy of reciprocal responsibility but introduces a potential avenue for Data Fiduciaries to deny service based on alleged non-compliance by the Principal [34].

- **Obligations of Data Fiduciaries:** Core obligations include: providing a clear notice at the time of consent; implementing reasonable security safeguards; reporting data breaches to the Board and affected Principals; and mandatory deletion of data once the purpose is served [35]. The Act does not prescribe specific security standards, leaving them to be

The DPBI is the adjudicatory body [37]. It is designed defined by rules or best practices, which introduces regulatory uncertainty [36].

- **Data Protection Board of India (DPBI):** to function as a "digital office," aiming for efficiency [38]. However, its composition (members appointed by the central government) and its role as both investigator and adjudicator raise concerns about its operational independence, distinguishing it from the "Data Protection Authority" envisioned in earlier drafts which was to be a multi-member independent statutory body [39].

- **Penalties and Enforcement:** The Act adopts a civil penalty regime with high monetary penalties listed in its Schedule [40]. This is a significant shift from the criminal liability under the IT Act for cyber contraventions, prioritizing a compliance-oriented deterrent over criminal prosecution [41].

- **Cross-Border Data Transfer:** The Act abandons the strict data localization requirements of the 2019 Bill [42]. It adopts a "whitelisting" approach, where the central government will notify countries to which data cannot be transferred [43]. This flexibility is a boon for global businesses but leaves a critical policy gap until the list is notified [44].

Comparative Analysis: DPDP ACT, 2023 (India) vs GDPR (EU) vs UK Data protection ACT, 2018

Consent Standards

DPDP Act, 2023 (India)

Consent must be clear, affirmative, informed, and freely given, with withdrawal as easy as giving consent [45].

→ Substantially aligned with GDPR principles.

GDPR (EU):

Consent must be freely given, specific, informed, and unambiguous.

→ Pre-ticked boxes are strictly prohibited [46].

UK Data Protection Act, 2018:

→ Substantially mirrors GDPR consent requirements [47].

Data Subject Rights

DPDP Act, 2023 (India)

Provides rights to access, correction, erasure, grievance redressal, and nomination [48].

→ Does not explicitly include rights such as data portability and restriction [49].

GDPR (EU):

Provides comprehensive rights including:

Access, rectification, erasure, restriction, portability, and objection [50].

UK Data Protection Act, 2018:

→ Incorporates all GDPR rights with certain national security carve-outs [51].

Government Exemptions

DPDP Act, 2023 (India):

Grants broad exemptions to state agencies on grounds of sovereignty, public order, and security [52].

→ No requirement of judicial review.

GDPR (EU):

Allows state restrictions only under strict proportionality and subject to independent oversight [53].

UK Data Protection Act, 2018:

Provides exemptions for national security, but subject to oversight by the Investigatory Powers Commissioner [54].

Data Localization & Cross-Border Transfers

DPDP Act, 2023 (India):

→ No mandatory data localization [55].

→ Uses a negative list (whitelist approach) for cross-border transfers.

GDPR (EU):

Transfers allowed only with safeguards such as Standard Contractual Clauses (SCCs) or *Binding Corporate Rules (BCRs)* [56].

UK Data Protection Act, 2018:

→ Follows GDPR framework post-Brexit (EU adequacy recognized) [57].

Regulatory Authority

DPDP Act, 2023 (India):

→ Regulated by the *Data Protection Board of India (DPBI)* [58].

→ Not fully independent; members appointed and removed by the government.

→ Functions primarily as an adjudicatory body.

GDPR (EU):

→ Governed by European Data Protection Board (EDPB) and national authorities.
→ Fully independent with investigative, corrective, and punitive powers [59].
UK Data Protection Act, 2018:
→ Enforced by the Information Commissioner's Office (ICO).
→ Independent authority with strong enforcement powers [60].

Enforcement Strength
DPDP Act, 2023 (India):
→ Provides high monetary penalties (up to ₹250 crore) [61].
→ Purely civil enforcement regime.
→ No criminal liability for fiduciaries.
GDPR (EU):
→ Provides highest tier penalties (up to €20 million or 4% of global turnover) [62].
→ Includes criminal liability in certain cases.
UK Data Protection Act, 2018:
→ Enforcement framework substantially similar to GDPR [63]

Conclusion
The DPDP Act, 2023 represents a "GDPR-lite" framework. While it adopts the core architecture of consent and data rights, it significantly dilutes protections in two key areas: Lack of independence of the regulatory authority, Broad government exemptions Overall, it reflects a policy shift toward flexibility and ease of doing business, unlike the strict, rights-based approach of GDPR [64].

Identify loopholes / Weaknesses
1. Unbridled Government Exemptions (Section 17) [65]: This is the most significant constitutional vulnerability. The government can exempt any agency from the Act's provisions for reasons including "sovereignty," "public order," and "friendly relations with foreign states." The power is absolute, with no requirement for proportionality, no judicial review, and no parliamentary oversight. This creates a "privacy black hole" where state surveillance can operate with zero accountability, potentially undermining the very fundamental right the Act purports to protect [66].

2. Weak Institutional Independence: The DPBI is not an independent statutory authority but a body appointed by and removable by the central government [67]. Its members serve at the "pleasure of the government." This erodes its credibility as an impartial adjudicator, particularly in matters involving state entities [68].

3. Absence of Data Localization Clarity: While flexibility is an advantage, the Act's silence on data localization leaves a significant policy gap [69]. It defers a critical national security and economic sovereignty decision to executive rule-making, creating business uncertainty [70].

4. Disproportionate Compliance Burden on MSMEs: While the Act does not create a separate class for MSMEs, the costs of implementing security safeguards, consent mechanisms, and grievance redressal systems can be prohibitive for small businesses, potentially stifling innovation [71].

5. Lack of Algorithmic Accountability: The Act is data-focused, not algorithm-focused. It does not address the risks of automated decision-making, profiling, or AI-driven harms [72]. A decision based on a flawed algorithm that causes significant harm to a Data Principal may not be directly actionable under this Act [73].

Research findings & GAP analysis
A gap analysis reveals a critical disconnect between the law on paper and its potential efficacy in practice:

- **Institutional Capacity Gap:** The DPBI is envisioned as a digital-first, lean body. However, given the scale of India's digital population and the volume of potential grievances, the Board is likely to be severely under-resourced [74]. Without a robust internal mechanism, it risks becoming a bottleneck, leading to adjudicatory delays that undermine the right to grievance redressal [75].

- **Digital Literacy Gap:** The Act's entire framework is predicated on the Data Principal's ability to give informed consent and exercise their rights [76]. India faces a significant digital literacy challenge [77]. Without massive investment in public awareness, the rights conferred by the Act will remain inaccessible to a vast majority of its citizens, rendering them theoretical [78].

- **Surveillance Oversight Gap:** The exemption for state agencies is not just a loophole; it is a gaping oversight [79]. There is no provision in the Act for an independent oversight mechanism for government surveillance, akin to the UK's Investigatory Powers Commissioner [80]. This leaves the state's vast surveillance apparatus unchecked, creating a systemic risk of abuse [81].

- **Cross-Border Enforcement Gap:** The Act has no mechanism for cooperation with foreign data protection authorities [82]. If a foreign Data Fiduciary violates the rights of an Indian Data Principal, the DPBI has limited power to enforce its orders extraterritorially, creating a significant accountability gap [83].

What additional criteria should be added (law reform)
To strengthen the Act and align it with global best practices, the following reforms are essential:

- **Establish an Independent Data Protection Authority:** The DPBI must be reconstituted as a multi-member body with statutory independence [84]. Appointments should be made by a collegium system (involving the Chief Justice of India or a high court judge), and removal should be for proven misconduct, not at the government's pleasure [85].

- **Codify a Proportionality Principle for Government Exemptions:** Section 17 must be amended to include a proportionality requirement [86]. Government exemptions should be subject to judicial review and require parliamentary oversight. A specialized bench to handle national security-related privacy matters could be established [87].

- **Adopt a "Hybrid" Data Localization Model:** Instead of a blanket rule, mandate the localization of critical personal data (e.g., health, financial) while allowing

non-critical data to flow freely [88]. This balances economic interests with strategic sovereignty [89].

- **Incorporate Algorithmic Transparency and AI Governance:** Introduce provisions requiring Data Fiduciaries undertaking automated decision-making to provide meaningful information about the logic involved, and grant Data Principals the right to request human intervention [90]. This is critical for AI regulation [91].

- **Strengthen Child Data Protection:** While the Act has provisions, they lack specificity [92]. It should mandate privacy-by-design standards for platforms used by children and prohibit the creation of detailed profiles for targeted advertising, with active enforcement against non-compliance [93].

Legal & policy recommendations

1. **Enforceable Amendments:** The foremost recommendation is to immediately amend Section 17 to insert a "necessity and proportionality" clause [94]. A sunset clause should be attached to exemptions for specific state agencies, requiring them to periodically justify their exempt status [95].

2. **Judicial Safeguards:** The Act should explicitly provide for a statutory appeal against DPBI orders to a High Court, not just the appellate tribunal, to ensure a constitutional safety valve, especially in cases involving government exemptions [96].

3. **Parliamentary Oversight Mechanism:** A Joint Parliamentary Committee on Data Protection should be established to annually review the operation of the Act, particularly the use of government exemptions, and table a report in Parliament [97].

4. **Strengthen Compliance Audits:** For Significant Data Fiduciaries, the Act should mandate that the DPO be a person of high professional standing with guaranteed tenure and cannot be penalized by the fiduciary for discharging their statutory duties [98]. Audit reports should be shared with the DPBI [99].

5. **Corporate Accountability:** Introduce personal liability for the senior management of a Data Fiduciary for wilful non-compliance or for directing a strategy that systematically violates the Act [100]. The current regime of only corporate penalties is insufficient to ensure accountability at the highest levels [101].

Conclusion

The Digital Personal Data Protection Act, 2023, is an evolving and, in many ways, a foundationally imperfect piece of legislation [102]. It is a necessary and significant first step, replacing a legal void with a structured framework [103]. However, its current form reflects a strategic choice by the state to prioritize its own informational interests and economic flexibility over the creation of a robust, independent, and rights-centric privacy regime [104].

It is not a sufficient privacy law for a maturing democracy [105]. The Act's "weak spots"—the broad government exemptions, the lack of an independent regulator, and the absence of algorithmic accountability—represent not just gaps but potential sources of constitutional friction [106]. The law, as it stands, favours the state and big business by creating a regime that is more about managing compliance than guaranteeing fundamental rights [107].

For the DPDP Act to truly honor the Puttaswamy judgment and protect India's digital future, it must be seen as a living document subject to continuous critical scrutiny and reform [108]. The judiciary will play a pivotal role in reading down the overbroad government exemptions and in ensuring that the fundamental right to privacy is not rendered a mere legislative formality [109]. The true test will be in the implementation of the Rules and in the decisions of the DPBI [110]. India stands at a crossroads: it can either settle for a system that grants privacy as a state-controlled privilege or fight for an architecture that treats it as an inviolable, constitutionally-protected right [111]. The DPDP Act, as it stands, provides the foundation for the former but, with the proposed amendments and judicial vigilance, it could yet be built into the latter [112].

References

1. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
2. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
3. Constitution of India, art. 21.
4. The Digital Personal Data Protection Act, 2023, No. 22 of 2023, § 2(a) (India).
5. Id. at § 4.
6. Id. at Ch. V (establishing the Data Protection Board of India).
7. Ministry of Electronics & Information Technology, Press Release: Cabinet Approves Digital Personal Data Protection Bill 2023, July 5, 2023.
8. Information Technology Act, 2000, No. 21 of 2000 (India).
9. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, G.S.R. 313(E) (Apr. 11, 2011).
10. See Malavika Raghavan, The SPDI Rules: A Toothless Tiger, The Centre for Internet & Society (Mar. 23, 2015).
11. National Crime Records Bureau, Annual Report on Cyber Crimes in India 2022, Ministry of Home Affairs (2023).
12. Puttaswamy, (2017) 10 SCC 1, ¶ 328.
13. Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians, Ministry of Electronics & Information Technology (July 27, 2018).
14. Joint Committee on the Personal Data Protection Bill, 2019, Report of the Joint Committee on the Personal Data Protection Bill, 2019, Lok Sabha Secretariat (Dec. 16, 2021).
15. The Digital Personal Data Protection Act, 2023, Passed by both Houses of Parliament, Aug. 9-10, 2023.
16. See Anirudh Rastogi, The Shift from a Rights-Based to a Consent-Based Model, The Economic Laws Practice, ELP Blog (Aug. 12, 2023).
17. Puttaswamy, (2017) 10 SCC 1, ¶ 426 (Chandrachud, J., concurring).

18. Id.
19. See Shoshana Zuboff, The Age of Surveillance Capitalism (2019).
20. See European Commission, Antitrust: Commission Fines Google €2.42 Billion for Abusing Dominance as Search Engine by Giving Illegal Advantage to Own Comparison Shopping Service, Press Release (June 27, 2017).
21. DPDP Act, § 2(i) (defining Data Fiduciary).
22. See Centre for Internet and Society, A Study of Data Breaches in India (2021).
23. DPDP Act, Schedule (providing for penalties).
24. Ministry of Electronics & Information Technology, India's Trillion Dollar Digital Opportunity, (Feb. 2019).
25. See World Bank, Digital India: Unlocking the Trillion Dollar Opportunity, (2019).
26. Supra note 6.
27. DPDP Act, § 2(j).
28. Id. at § 2(i).
29. Id. at § 2(e).
30. Id. at § 2(p).
31. Id. at §§ 11-15.
32. Supra note 30.
33. Supra note 30.
34. DPDP Act, § 15.
35. Id. at § 15(a).
36. Id. at §§ 8-9.
37. Id. at § 8(5).
38. Id. at § 18.
39. Id. at § 20.
40. Compare Personal Data Protection Bill, 2019, cl. 49 (establishing the Data Protection Authority of India as an independent statutory body), with DPDP Act, §§ 18-36 (establishing the DPBI as a government-appointed body).
41. DPDP Act, Schedule.
42. Compare Information Technology Act, 2000, § 43A (compensation for negligence), with DPDP Act, Schedule.
43. Compare Personal Data Protection Bill, 2019, cl. 33 (mandating data localization for critical personal data), with DPDP Act, § 16.
44. DPDP Act, § 16.
45. Id.
46. Id. at § 2(e).
47. GDPR, art. 4(11), art. 7.
48. Data Protection Act 2018, c. 12, § 2 (UK).
49. DPDP Act, §§ 11-15.
50. Id.
51. GDPR, arts. 15-22.
52. UK Data Protection Act 2018, §§ 2, 3.
53. DPDP Act, § 17.
54. GDPR, art. 23.
55. Investigatory Powers Act 2016, c. 25, pt. 7 (UK); see also UK Data Protection Act 2018, pt. 6.
56. DPDP Act, § 16.
57. GDPR, art. 45 (adequacy decisions); art. 46 (appropriate safeguards, including Standard Contractual Clauses and Binding Corporate Rules).
58. UK Data Protection Act 2018, pt. 3, ch. 5.
59. DPDP Act, § 18.
60. GDPR, arts. 68-76.
61. UK Data Protection Act 2018, pt. 6.
62. DPDP Act, Schedule.
63. GDPR, art. 83.
64. UK Data Protection Act 2018, pt. 6, ch. 4.
65. Supra note 15.
66. DPDP Act, § 17.
67. See Veranda Bhandari, The DPDP Act's Exemption Clause: A Threat to Privacy, The Indian Express, Aug. 22, 2023.
68. DPDP Act, § 18.
69. See Apar Gupta, The Need for an Independent Regulator, The Economic Times, Sept. 10, 2023.
70. Supra note 42.
71. Id.
72. See Federation of Indian Chambers of Commerce & Industry, Report on the Impact of DPDP Act on MSMEs (Jan. 2024).
73. See European Union, Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), COM/2021/206 final.
74. DPDP Act, § 8(1)(a) (purpose limitation) could be interpreted to restrict algorithmic processing, but there is no specific provision.
75. Supra note 38.
76. Id.
77. DPDP Act, § 4 (consent requirement).
78. National Sample Survey Office, Household Social Consumption on Education in India, Ministry of Statistics and Programme Implementation (2023).
79. See Nikhil Nair, Digital Literacy: The Missing Link in India's Data Protection Law, The Wire, Dec. 5, 2023.
80. Supra note 65.
81. Supra note 54.
82. See K. S. Puttaswamy, Concurring Opinion, (2017) 10 SCC 1, ¶ 104 (highlighting the need for oversight of state surveillance).
83. DPDP Act, Ch. V.
84. Id.
85. Supra note 39.
86. See Report of the Committee of Experts (Srikrishna Committee), supra note 12, at 178-180.
87. Supra note 65.
88. See Constitutional Court of South Africa, South African Police Service v. Public Servants Association, 2023 (2) SA 405 (CC) (demonstrating judicial review of surveillance powers).
89. See Personal Data Protection Bill, 2019, cl. 33(3).
90. Id.
91. Ministry supra Electronics & Information Technology, Press Release: Cabinet Approves Digital Personal Data Protection Bill 2023, July 5, 2023.
92. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
93. See UK Age Appropriate Design Code, The Age Appropriate Design Code, Information Commissioner's Office (2020).
94. The Digital Personal Dnotea Protection Act, 2023, No.22 of 2023, § 2(n) (India).
95. Id.
96. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
97. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

98. See Malavika Raghavan, The SPDI Rules: Toothless Tiger, The Centre for Internet & Society (Mar. ons, 2015).
99. § 4.
100. Constitution on individuals in some contexts); UK Data Protection Act 2018, § 149 (offences by corporate offences by corporate bodies: liability of directors, art. 21.
101. Supra note 40.
102. Supra note 15.
103. The Digital Personal DIda Protection Act, 2023, No22 of 2023, § 2(I) (India).
104. Supra note 65.
105. Id.
106. Supra note 66, 68, 73.
107. [107] Supra note 64.
108. Constitution to be privacy is a constitutional value to be protected by evolving law, art. 21.
109. Id.
110. Hc). Data Protection Rules, 2025, Draft for Public Consultation, Ministry of Electronics le Ul. V (establishing the & Information Board Digital India).
111. Supra note 65.
112. Id.