Naveen Shodh Sansar (An International Refereed / Peer Review Multidisciplinary Research Journal)
RNI No.- MPHIN/2013/60638, ISSN 2320-8767, E- ISSN 2394-3793, Scientific Journal Impact Factor (SJIF)- 8.054,
July to September 2025, E-Journal, Vol. I, Issue LI (51), ISO 9001:2015 - E2024049304 (QMS)

Digital Personal Data Protection Act, 2023: A Critical Examination Of India's New Data Privacy Framework

Dr. Narendra Singh Rana*

***Assistant Professor, Govt Law College, Gwalior (M.P.) INDIA**

Abstract: The Digital Personal Data Protection Act, 2023 (DPDP Act) represents India's first comprehensive legislation governing the processing of digital personal data, marking a transformative shift from the fragmented regime under the Information Technology Act, 2000. Enacted in August 2023. This research paper critically examines the DPDP Act's constitutional foundations, key provisions, enforcement mechanisms, and emerging challenges. Drawing upon the landmark Supreme Court judgment in *K.S. Puttaswamy v. Union of India* (2017), which recognized privacy as a fundamental right under Article 21, the paper analyzes the Act's alignment with constitutional mandates. Through detailed examination of the Data Protection Board of India's enforcement powers, the novel "negative list" approach to cross-border data transfers, and the amendment to the Right to Information Act, 2005, the paper identifies significant tensions between data protection and transparency. The study incorporates recent judicial developments, including the Madras High Court's ruling on the right to be forgotten in *Karthick Theodore v. Registrar General* (2024). The paper concludes with recommendations for harmonizing the DPDP framework with constitutional rights, strengthening the independence of the Data Protection Board, and addressing ambiguities regarding algorithmic decision-making and artificial intelligence.

Keywords: Digital Personal Data Protection Act, 2023, right to privacy, Data Protection Board of India, cross-border data transfer, right to be forgotten, Right to Information Act, K.S. Puttaswamy judgment, *Karthick Theodore* judgment, data fiduciary, data principal, consent manager.

Introduction - The digital transformation of India's economy and governance has generated unprecedented volumes of personal data, raising fundamental questions about privacy, consent, and state surveillance. For decades, India's data protection regime consisted of fragmented provisions under the Information Technology Act, 2000, particularly Section 43A and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. This framework proved inadequate to address the complexities of modern data processing, cross-border data flows, and the rights of individuals over their personal information.

The constitutional foundation for data protection in India was firmly established by the Supreme Court's nine-judge bench in *K.S. Puttaswamy v. Union of India* (2017), which unanimously held that the right to privacy is a fundamental right intrinsic to the right to life and personal liberty under Article 21 of the Constitution. The Court articulated a three-fold test for any law encroaching upon privacy: legality (existence of law), a legitimate state aim, and proportionality.

Responding to this constitutional imperative and the demands of a digital economy, Parliament enacted the Digital Personal Data Protection Act, 2023, which received Presidential assent on August 11, 2023. However, the Act remained largely inoperative until the notification of the Digital Personal Data Protection Rules, 2025 following an extensive consultation process that gathered 6,915 inputs from start-ups, MSMEs, civil society, and citizens across seven cities.

The DPDP framework introduces a comprehensive regulatory architecture governing the processing of digital personal data, establishing the rights of data principals (individuals whose data is processed), obligations of data fiduciaries (entities determining the purpose and means of processing), and the enforcement mechanism through the Data Protection Board of India.

This research paper examines the DPDP Act's provisions, enforcement mechanisms, and constitutional challenges through the lens of India's evolving privacy jurisprudence. It analyzes the Act's treatment of cross-border data transfers, the right to be forgotten, the impact on the Right to Information Act, and the emerging challenges posed by artificial intelligence and automated decision-making. The paper is structured as follows: Section 2 states the objectives; Section 3 reviews the constitutional and statutory framework; Section 4 presents landmark case

studies; Section 5 provides critical analysis; Section 6 offers recommendations; Section 7 concludes; and Section 8 lists references.

Objectives Of The Study:

1. To examine the constitutional foundations of the right to privacy in India and their relationship to the Digital Personal Data Protection Act, 2023.
2. To analyze the key provisions of the DPDP Act and the DPDP Rules, 2025, including the definitions of data fiduciaries, data principals, and the obligations imposed on data processors.
3. To critically evaluate the enforcement mechanism established under the Act, particularly the composition, powers, and independence of the Data Protection Board of India.
4. To study the Act's approach to cross-border data transfers through the "negative list" regime and its implications for Indian businesses and global data flows.
5. To examine the interface between the DPDP Act and the Right to Information Act, 2005, particularly the amendment to Section 8(1)(j) of the RTI Act.
6. To analyze recent judicial pronouncements on the right to be forgotten and their interaction with the DPDP framework.
7. To identify gaps in the DPDP framework, particularly regarding artificial intelligence, algorithmic decision-making, and state surveillance.
8. To propose recommendations for strengthening the data protection regime in India while balancing privacy with transparency and innovation.

Constitutional And Statutory Framework

1. The Right to Privacy as a Fundamental Right- The recognition of privacy as a fundamental right under Article 21 represents a watershed moment in Indian constitutional jurisprudence. In *K.S. Puttaswamy v. Union of India* (2017), the Supreme Court overruled earlier precedents (*M.P. Sharma v. Satish Chandra* and *Kharak Singh*) and held that the right to privacy is intrinsic to the right to life and personal liberty-. The Court articulated that any law infringing upon privacy must satisfy the three-fold requirement of legality, necessity, and proportionality.

The judgment has profound implications for data protection legislation. Any law governing the collection, processing, and transfer of personal data must comply with these constitutional standards. The DPDP Act, 2023, is explicitly framed as a response to this constitutional mandate, providing the statutory framework for protecting digital personal data while enabling legitimate data processing for economic and social purposes-.

2. The Digital Personal Data Protection Act, 2023: Key Provisions

2.1. Scope and Applicability: The DPDP Act applies exclusively to digital personal data-personal data in digital form or in non-digital form subsequently digitized. This narrower scope distinguishes it from the GDPR, which applies to both digital and physical records. The Act has extraterritorial application, extending to processing of digital personal data outside India if such processing is in connection with offering goods or services to data principals in India.

The Act exempts individuals processing personal data for personal or domestic purposes, as well as processing for research, archiving, or statistical purposes carried out in the prescribed manner.

2.2. Key Definitions

Data Principal: The individual to whom personal data relates. For children, this includes their parent or lawful guardian; for persons with disabilities, their lawful guardian.

Data Fiduciary: Any person who, alone or with others, determines the purpose and means of processing personal data-3. This concept is borrowed from the GDPR.

Data Processor: Entities that process data on behalf of data fiduciaries. Data fiduciaries remain liable for the actions of data processors.

Significant Data Fiduciary (SDF): Categories of data fiduciaries that the Government may notify based on criteria including volume and sensitivity of personal data processed, risks to data principals' rights, impact on sovereignty and integrity of India, risk to electoral democracy, and security of state and public order. More stringent requirements apply to SDFs.

Consent Manager: A novel concept introduced by the Act—an independent entity distinct from data fiduciaries and data processors, entrusted with managing data subjects' consent. Consent Managers must register with the Data Protection Board and serve as the central interface through which individuals manage data permissions across multiple organizations.

2.3. Obligations of Data Fiduciaries: Data fiduciaries must comply with several obligations under the Act:

- **Notice and Consent**: Provide clear notice to data principals regarding the purpose of data processing and obtain consent.
- **Reasonable Security Safeguards**: Implement appropriate technical and organizational measures to protect personal data.
- **Breach Notification**: Intimate data breaches to the Data Protection Board and affected data principals.
- **Data Retention**: Retain personal data only as long as necessary for the specified purpose.
- **Data Protection Officer**: Appoint a Data Protection Officer or equivalent contact person.
- **Child Protection**: Obtain verifiable parental consent for processing children's data, except for essential services like healthcare.

2.4. Rights of Data Principals: The Act grants data principals several rights over their personal data:

1. Right to obtain confirmation of processing
2. Right to access personal data

3. Right to correction and erasure
4. Right to grievance redressal
5. Right to nominate a representative in case of death or incapacity

2.5. Penalties and Enforcement: The Act provides for substantial penalties for non-compliance:

Violation	Maximum Penalty
Failure to take reasonable security safeguards	Rs250 crore
Failure to notify breach to Data Protection Board	Rs 200 crore
Failure to notify affected data principals	Rs 200 crore
Non-compliance with SDF obligations	Rs150 crore
Other violations	Rs.50 crore

The Data Protection Board of India, headquartered in the National Capital Region and comprising four members, functions as a fully digital adjudicatory authority with powers to investigate breaches, issue directions, and impose penalties-. Appeals against Board decisions lie to the Telecom Disputes Settlement and Appellate Tribunal (TDSAT).

3. Cross-Border Data Transfers: The "Negative List" Approach: One of the most significant features of the DPDP framework is its approach to cross-border data transfers. Unlike the GDPR's "adequacy" or "whitelist" mechanism, India has adopted a **"negative list" system**.

Section 16 of the DPDP Act provides that a data fiduciary may transfer personal data outside India **except where the Central Government restricts such transfer**. The Government may restrict transfers to specific countries, territories, classes of data fiduciaries, or specific sectors.

This approach offers considerable flexibility for Indian businesses and multinational companies operating global, cloud-centric infrastructures. However, it also introduces uncertainty, as companies cannot predict when the Government may impose restrictions based on geopolitical considerations, national security concerns, or sector-specific sensitivities.

4. Interface with the Right to Information Act, 2005: Section 44(3) of the DPDP Act amended Section 8(1)(j) of the RTI Act, 2005-24. The amendment created a **blanket exemption** for "personal information" from disclosure under the RTI Act. Previously, Section 8(1)(j) exempted personal information only if it had no relationship to public activity or if disclosure would amount to unwarranted invasion of privacy, with a public interest override. The DPDP Act removed this nuanced balancing test, replacing it with a blanket prohibition.

This amendment has been challenged before the Supreme Court in *Venkatesh Nayak v. Union of India* and connected petitions, with petitioners arguing that it disproportionately curtails the right to information by creating a blanket exemption for personal information. Senior Advocate Vrinda Grover submitted that the amendment "fundamentally altered the balance previously maintained under the RTI Act by removing the safeguards that permitted disclosure of personal information where public interest outweighed privacy concerns".

Senior Advocate Prashant Bhushan argued that while both privacy and the right to information are fundamental rights, the RTI Act had struck a careful balance by protecting only such personal information that had no nexus with public activity or public interest. The DPDP Act, he contended, disrupted that balance by replacing the nuanced exemption with a blanket prohibition.

The Supreme Court, hearing the matter on August 7, 2026, observed that both the DPDP Act and the RTI Act are central legislations and there is a need to harmonize them. Justice Joymalya Bagchi remarked: "The earlier law (Right to Information Act, 2005) gave certain access with conditions. Here (2023 Act), there is an en bloc embargo. Is this latter law repugnant to earlier law? This has to be looked into with extreme circumspection".

Landmark Case Studies

Case Study 1: K.S. Puttaswamy v. Union of India (2017) - The Constitutional Foundation

Background: Justice K.S. Puttaswamy (Retd.) challenged the constitutional validity of the Aadhaar scheme, arguing that the collection and use of biometric and demographic data violated the right to privacy.

Judgment: A nine-judge bench of the Supreme Court unanimously held that the right to privacy is a fundamental right intrinsic to the right to life and personal liberty under Article 21. The Court overruled earlier judgments in *M.P. Sharma v. Satish Chandra* (1954) and *Kharak Singh v. State of Uttar Pradesh* (1963) which had held that privacy was not a fundamental right.

Significance for Data Protection: The judgment established the constitutional foundation for comprehensive data protection legislation in India-. The Court articulated that any law encroaching upon privacy must satisfy the three-fold test of legality, legitimate state aim, and proportionality. The DPDP Act, 2023, is explicitly framed as a response to this constitutional mandate, providing the statutory framework contemplated by the Court.

Legal Analysis: The *Puttaswamy* judgment represents a paradigm shift in Indian constitutional law. By recognizing privacy as a fundamental right, the Court imposed constitutional constraints on both state and private actors processing personal data. The DPDP Act must be interpreted and applied in light of these constitutional standards. Any provision that disproportionately infringes upon privacy or fails to provide adequate safeguards may be vulnerable to constitutional challenge.

Case Study 2: Karthick Theodore v. Registrar General, Madras High Court (2024) - The Right to be Forgotten

Background: Mr. Karthick Theodore filed a writ petition seeking redaction of his name and personal details from a

publicly accessible judgment dated April 30, 2014, in which he was acquitted of charges under Sections 417 and 376 of the Indian Penal Code, 1860. He argued that the continued availability of the judgment online was causing significant harm to his personal and professional life, including the denial of a visa application.

Judgment: The Madras High Court made a significant ruling examining the 'right to be forgotten'/'right to be remembered well' vis-à-vis the right to privacy under Article 21 and under the DPDP Act, 2023. The Court also examined the applicability of the DPDP Act on courts in India, emphasizing the need for courts to maintain a fine balance between aggregation of data required to perform their functions and protection of personal data so collected.

Appeal to Supreme Court: Ikanoon Software Development Private Limited appealed the judgment before the Supreme Court, which passed a stay order on the Madras High Court's directions. The Supreme Court clubbed the appeal with another matter, *Alka Malhotra v. Union of India*, dealing with a similar issue.

Legal Analysis: The case raises fundamental questions about the interaction between the right to privacy, the right to be forgotten, and the principle of open justice. While courts must ensure transparency and public access to judgments, individuals acquitted of charges have a legitimate interest in not being perpetually stigmatized by online availability of court records. The DPDP Act does not explicitly address the right to be forgotten, creating uncertainty about its application to judicial proceedings.

Critical Analysis

1. Constitutional Alignment and Challenges: The DPDP Act is framed as a response to the constitutional mandate established in *Puttaswamy*, providing the statutory framework for protecting digital personal data-. However, several provisions raise constitutional concerns:

The RTI Amendment (Section 44(3)): The blanket exemption for personal information under the RTI Act may disproportionately infringe upon the right to information, which is essential for democratic accountability. The Supreme Court's observations in *Venkatesh Nayak* suggest that the Court is concerned about whether the DPDP Act's approach "works to repeal earlier transparency legislations".

State Surveillance (Sections 7(c) and 17(2)(a)): These provisions give unchecked powers to the state to direct data fiduciaries to undertake personal data processing of Indian citizens in a legal vacuum. The Act further empowers the Centre with unfettered discretion to bypass the DPDP Act and Rules on principles such as lawful processing, fairness, transparency, informed consent, purpose limitation, and data minimization. This raises serious concerns about arbitrary state surveillance without adequate safeguards.

Independence of the Data Protection Board: The Data Protection Board of India, while empowered to impose penalties up to Rs 250 crore-, may lack the independence necessary for impartial adjudication. The absence of judicial oversight and the Board's composition raise concerns about its ability to function as a check on state power.

2. The "Negative List" Approach to Cross-Border Data Transfers: India's adoption of a "negative list" system for cross-border data transfers represents a significant departure from global norms. While this approach offers flexibility for Indian businesses and multinational companies, it introduces uncertainty because companies cannot predict when the Government may impose restrictions.

The absence of mechanisms such as adequacy assessments, standard contractual clauses, binding corporate rules, or onward transfer controls may create compliance challenges for businesses operating in multiple jurisdictions. The executive-led, policy-driven regime-39 may lack the predictability and legal certainty that businesses require for long-term planning.

3. The Right to be Forgotten: An Unresolved Issue: The DPDP Act does not explicitly address the right to be forgotten, despite the Madras High Court's examination of this issue in *Karthick Theodore*. The Supreme Court's stay on the Madras High Court's directions indicates that this issue remains unresolved.

The tension between the right to be forgotten and the principle of open justice is particularly acute in the context of judicial proceedings. While individuals acquitted of charges have a legitimate interest in not being perpetually stigmatized, courts must ensure transparency and public access to judgments. The DPDP Act's silence on this issue creates uncertainty for both courts and individuals.

4. Artificial Intelligence and Algorithmic Decision-Making: The DPDP Act does not explicitly cover AI automated decision-making or algorithmic transparency. No cryptographic provenance standard for AI outputs exists in any DPDP Act provision, DPDP Rules instrument, or Data Protection Board guidance document.

This gap is significant given the increasing use of AI in welfare, credit, and health diagnostic systems. As one analysis notes, the first enforcement ruling against an AI-driven system will be challenged before TDSAT on the absence of a technical standard against which compliance was measured. The structural gap between the Board's enforcement authority and the technical standards required to make that authority legally sustainable represents a significant challenge for the DPDP framework.

5. Phased Implementation and Compliance Challenges: The phased implementation of the DPDP Act, while intended to reduce friction, creates compliance challenges for businesses. The core compliance obligations will apply after eighteen months, but businesses must begin preparing well in advance to meet the requirements.

The transition from the previous regime under the IT Act to the DPDP framework requires significant adjustments in legal, technical, and operational processes. The continued applicability of the SPDI Rules, 2011 for eighteen

months provides a bridge but also creates the potential for confusion regarding which regime applies.

Suggestions And Recommendations

1. Harmonizing the DPDP Act with the RTI Act: The blanket exemption for personal information under Section 8(1)(j) of the RTI Act should be reconsidered. A more nuanced approach, similar to the previous provision that balanced privacy with public interest, would better serve India's democratic framework. The Supreme Court's observation in *Venkatesh Nayak* that both the DPDP Act and the RTI Act need to be harmonized should guide legislative and judicial interpretation.

Recommendation: Amend Section 44(3) of the DPDP Act to restore the public interest override in Section 8(1)(j) of the RTI Act, allowing disclosure of personal information where public interest outweighs privacy concerns.

2. Strengthening the Independence of the Data Protection Board: The Data Protection Board of India should be provided with greater independence from executive control. The current composition, with members appointed by the Central Government, may not provide adequate safeguards against arbitrary exercise of authority.

Recommendation: Establish a selection committee comprising the Chief Justice of India or a nominee, the Chairperson of the Law Commission, and the Union Law Minister to appoint Board members. Provide security of tenure and adequate safeguards against removal except for proven misbehavior or incapacity.

3. Addressing State Surveillance Concerns: Sections 7(c) and 17(2)(a) of the DPDP Act, which give unchecked powers to the state to direct data fiduciaries to process personal data, should be amended to provide adequate safeguards against arbitrary surveillance.

Recommendation: Require judicial authorization for state directions to data fiduciaries, except in cases of imminent threat to national security. Provide for oversight mechanisms, including parliamentary scrutiny of state surveillance activities.

4. Clarifying the Right to be Forgotten: The DPDP Act should explicitly address the right to be forgotten, particularly in the context of judicial proceedings and public records.

Recommendation: Amend the DPDP Act to include provisions on the right to be forgotten, balancing individual privacy with the principle of open justice and public interest in access to information. Provide for a mechanism for individuals to request redaction of personal information from publicly accessible records, with appropriate safeguards.

5. Addressing Artificial Intelligence and Algorithmic Decision-Making: The DPDP Act should be amended to address AI automated decision-making and algorithmic transparency.

Recommendation: Include provisions requiring transparency in algorithmic decision-making, the right to human review of automated decisions, and technical standards for AI systems processing personal data. Establish a framework for cryptographic provenance of AI outputs.

6. Strengthening Cross-Border Data Transfer Provisions: While the "negative list" approach offers flexibility, the absence of mechanisms such as standard contractual clauses or binding corporate rules creates uncertainty for businesses.

Recommendation: Develop model contractual clauses for cross-border data transfers, provide guidance on the criteria for restricting transfers to specific countries, and establish a mechanism for businesses to seek prior approval for cross-border transfers.

7. Enhancing Compliance Support for Businesses: The phased implementation of the DPDP Act requires businesses to make significant adjustments. The Government should provide adequate support to facilitate compliance.

Recommendation: Issue detailed guidance on compliance requirements, establish a helpdesk for businesses, and provide a transition period for small and medium enterprises to meet compliance obligations.

8. Strengthening Data Principal Rights: While the Act grants data principals several rights, enforcement mechanisms for these rights remain unclear.

Recommendation: Establish a mechanism for data principals to file complaints directly with the Data Protection Board, provide for class action suits for data breaches, and ensure adequate compensation for violations.

Conclusion: The Digital Personal Data Protection Act, 2023, represents a transformative step in India's legal framework, establishing the first comprehensive legislation governing the processing of digital personal data. Building upon the constitutional foundation laid by the Supreme Court in *K.S. Puttaswamy v. Union of India* (2017), which recognized privacy as a fundamental right under Article 21, the DPDP Act provides the statutory framework for protecting digital personal data while enabling legitimate data processing for economic and social purposes.

The Act's approach to cross-border data transfers through a "negative list" regime offers flexibility but introduces uncertainty. The absence of mechanisms such as adequacy assessments, standard contractual clauses, or binding corporate rules may create compliance challenges for businesses operating in multiple jurisdictions.

The right to be forgotten remains an unresolved issue, with the Supreme Court staying the Madras High Court's ruling in *Karthick Theodore* that examined this right. The DPDP Act's silence on this issue creates uncertainty for both courts and individuals.

Perhaps most significantly, the DPDP Act does not explicitly address AI automated decision-making or algorithmic transparency. The absence of technical standards for AI systems processing personal data represents a critical gap that will need to be addressed as AI becomes increasingly integrated into welfare, credit,

and health diagnostic systems.

The DPDP framework represents a significant achievement in India's legal development, establishing a comprehensive data protection regime that aligns with constitutional mandates. However, its success will depend on how these challenges are addressed through judicial interpretation, legislative amendments, and regulatory guidance. The Supreme Court's ongoing examination of the DPDP Act's provisions, including the RTI amendments and state surveillance concerns, will be crucial in shaping the future of data protection in India.

References:-

1. Constitution of India, 1950 Articles 19, 21.
2. Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023).
4. Information Technology Act, 2000 (Act No. 21 of 2000) – Section 43A.
5. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
6. Right to Information Act, 2005 (Act No. 22 of 2005) – Section 8(1)(j).
7. *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1-.
8. *Karthick Theodore v. Registrar General, Madras High Court*, Madurai Bench (2024).
9. *Ikanoon Software Development Private Limited v. Karthick Theodore*, Supreme Court (Stay Order).
10. *Alka Malhotra v. Union of India*, Supreme Court (Pending).
12. *Central Public Information Officer, Supreme Court of India v. Subhash Chandra Agarwal*, (2020) 5 SCC 481-21.
17. Bhandari, A. (2024). "India's Digital Personal Data Protection Act: A Comparative Analysis with the GDPR." *Journal of Indian Law & Technology*, Vol. 19.
18. Chandrachud, D.Y. (2018). "The Right to Privacy and the Constitution." *Supreme Court Cases Journal*, Vol. 10.
20. Jain, M.P. (2023). *Indian Constitutional Law*. 8th ed. LexisNexis.
21. Narrain, S. (2017). "The Puttaswamy Judgment: A New Chapter in Indian Constitutional Law." *Economic and Political Weekly*, Vol. 52(34).
22. Law Commission of India. (2012). *Report No. 228 – Need for a Data Protection Regime in India*.
26. Press Council of India. (2023). *Norms of Journalistic Conduct*.

****