INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

THE "MISUSE" NARRATIVE VS. SUBSTANTIVE JUSTICE: DECONSTRUCTING SECTION 498A

AUTHORED BY - SACHI
Ll.M (Constitutional Law)
Amity Law School Lucknow, Amity University Uttar Pradesh Lucknow Campus

CO-AUTHOR - DR RAJEEV KUMAR SINGH
Professor Of Law
Amity Law School Lucknow, Amity University Uttar Pradesh Lucknow Campus

ABSTRACT

This research paper critically evaluates India's transition from the fragmented Information Technology Act, 2000, to the comprehensive Digital Personal Data Protection Act, 2023 (DPDP Act), a legislative evolution catalysed by the Supreme Court's recognition of privacy as a fundamental right in Puttaswamy. The study analyses the Act's core statutory mechanisms, including its rigid consent architecture, the fiduciary obligations imposed on data processors, and the innovative introduction of "Consent Managers" to bolster India's Digital Public Infrastructure.

However, the analysis reveals significant constitutional tensions. It argues that the broad state exemptions under Section 17 fail the Supreme Court's proportionality test, prioritizing executive discretion over informational privacy. Furthermore, the paper highlights a "transparency-privacy paradox" where amendments to the Right to Information Act subordinate democratic accountability to data protection. Finally, the research scrutinizes the Data Protection Board of India (DPBI), identifying severe "federal friction" and an "enforcement deficit" caused by centralizing regulatory power in an executive-controlled body. The paper concludes that while the DPDP Act modernizes digital governance, it requires legislative amendments ensuring decentralization and judicial oversight to fully align with constitutional mandates.

Key Words: DPDP Act 2023, Puttaswamy Judgment, Data Fiduciaries, Consent Managers, Data Protection Board of India (DPBI)

ISSN: 2582-6433

Introduction

The transition of India's data protection regime from a fragmented, sector-specific patchwork of subsidiary rules to a comprehensive, constitutionally grounded statutory framework represents one of the most profound legal evolutions in the nation's contemporary digital history. For decades, the governance of personal data in India operated within a legislative vacuum, relying heavily on piecemeal provisions embedded in broader information technology statutes that were ill-equipped to address the complexities of a rapidly digitising economy and the vast expansion of India's Digital Public Infrastructure (DPI). The foundational shift occurred with the judicial recognition of privacy as a fundamental right, which acted as a constitutional catalyst for the drafting, intense negotiation, and subsequent enactment of the Digital Personal Data Protection Act, 2023 (DPDP Act).

This chapter shifts the dissertation's focus toward a rigorous statutory and constitutional analysis of this new legislative framework. Section 4.1 traces the historical evolution of data protection laws in India, mapping the turbulent trajectory from the Information Technology Act, 2000, through various contentious draft bills, to the final operationalisation of the DPDP Act and its corresponding 2025 Rules. Section 4.2 dissects the key statutory provisions of the Act, critically evaluating the newly established consent architecture, the statutorily defined duties of data fiduciaries, the novel introduction of Consent Managers within the digital governance ecosystem, and the Act's alignment with constitutional mandates. This includes an assessment of the DPDP Act against the stringent proportionality test established by the Supreme Court, with a specific focus on the broad exemptions granted to state instrumentalities and the resulting structural clash with the Right to Information Act, 2005. Finally, Section 4.3 evaluates the institutional mechanisms established by the Act, scrutinising the composition, powers, and independence of the Data Protection Board of India (DPBI), and uncovering the profound federal implications of centralising data enforcement in a constitutionally decentralised state.

Evolution Of Data Protection Laws: From The IT Act 2000 To The DPDP Act 2023

To understand the architecture of the DPDP Act, it is imperative to trace the historical and jurisprudential evolution of data governance in India. The journey reflects a complex negotiation between the state's desire to foster a booming digital economy, the imperative of

ISSN: 2582-6433

national security, and the necessity of safeguarding individual civil liberties.

The Pre-Puttaswamy Era: Sectoral Fragmentation and the IT Act 2000

The genesis of digital governance in India can be traced to the Information Technology Act, 2000 (IT Act), the country's first major cyber legislation, which was primarily aimed at providing legal recognition for e-commerce and electronic governance and at mitigating cybercrime.[1] However, in its original formulation, the IT Act lacked robust mechanisms to protect personal data, focusing instead on penalising unauthorised access and data theft. It was not until a major legislative amendment in 2008 that Sections 43A and 72A were inserted, introducing the concept of corporate liability for negligence in implementing reasonable security practices, specifically concerning a narrowly defined category of "sensitive personal data".[2]

This provision was subsequently operationalised through the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules).[3] The SPDI Rules established a rudimentary baseline for privacy in India by mandating privacy policies, basic consent mechanisms, and the appointment of grievance officers for corporate entities that handle sensitive data, such as financial information, medical records, and biometrics.[4]

Nevertheless, this framework was fundamentally inadequate for a rapidly scaling digital economy. It was severely restricted in scope, applying only to body corporates and leaving government data processing entirely unregulated.[5] Furthermore, its enforcement mechanisms were exceptionally weak: it lacked a dedicated regulatory authority, relied on under-equipped adjudicatory officers, and required individuals to prove actual, quantifiable damages to claim compensation for data breaches.[6] Collection and handling of non-sensitive personal data remained largely unregulated, creating a permissive environment that prioritised rapid technological deployment over informational privacy.[7]

The Constitutional Catalyst: The Puttaswamy Judgment

The trajectory of Indian data policy was irrevocably altered on August 24, 2017, when a nine-judge constitution bench of the Supreme Court of India delivered its unanimous, landmark verdict in *Justice K.S. Puttaswamy (Retd.) v. Union of India*.[8] The Court unequivocally recognised the right to privacy as an intrinsic and fundamental component of the right to life

ISSN: 2582-6433

and personal liberty guaranteed under Article 21. It is deeply entrenched within the broader freedoms protected by Part III of the Constitution of India.[9]

The judgment dismantled the archaic, property-based "places-or-things" conception of privacy that had dominated earlier constitutional interpretations, placing individual dignity, decisional autonomy, and informational self-determination at the very heart of constitutional jurisprudence.[10] The Court acknowledged that, in the digital age, personal data is an extension of the self, and that its unauthorised extraction or manipulation constitutes a direct violation of human dignity.[11]

Crucially, the Supreme Court noted that while the right to privacy is fundamental, it is not absolute. To balance individual rights against legitimate state interests, the Court established a rigorous standard of review and formulated a multi-pronged proportionality test. Any state interference with privacy must satisfy the following criteria:

1. **Legality:** The restriction must be explicitly sanctioned by a valid, codified law.
2. **Legitimate Aim:** The law must pursue a legitimate state interest (e.g., national security, distribution of public welfare, or crime prevention).
3. **Proportionality (Necessity and Narrow Tailoring):** There must be a rational nexus between the objective and the means adopted, and the state must utilise the least intrusive measure available to achieve its goal.
4. **Procedural Safeguards:** The law must incorporate robust procedural safeguards to prevent executive abuse.[12]

By affirming privacy as a fundamental right and explicitly calling for a "carefully structured regime" for data protection, the Supreme Court created an unavoidable constitutional imperative for the Indian government to enact comprehensive legislation, shifting the national discourse from mere corporate compliance to the protection of fundamental human rights.[13]

Enactment and Phased Operationalisation of the DPDP Act 2023

The protracted legislative process culminated in the passage of the Digital Personal Data Protection Act, 2023 (DPDP Act) by both Houses of Parliament and its assent by the President on August 11, 2023.[14] Operating as an "umbrella" framework, the DPDP Act outlines a high-level, principle-based governance structure, leaving the vast majority of substantive operational and procedural details to delegated legislation.[15]

ISSN: 2582-6433

The transition from the obsolete IT Act regime to the new DPDP framework is defined by a phased implementation timeline, which was formally clarified with the notification of the Digital Personal Data Protection Rules on November 14, 2025.[16] The 2025 Rules completely repeal the 2011 SPDI Rules and establish a staggered, multi-year rollout strategy to afford organisations sufficient time to design compliance systems.[17]

The staggered implementation timeline is structured as follows:

- **Immediate Implementation (November 2025):** Rules governing the establishment, composition, and operational procedures of the Data Protection Board of India (DPBI) came into effect immediately, initiating the regulatory enforcement architecture.[18]
- **12-Month Horizon (November 2026):** Provisions concerning the registration, operational standards, and technical onboarding of Consent Managers are scheduled for enforcement.
- **18-Month Horizon (May 13, 2027):** The core compliance obligations, including the deployment of verifiable consent mechanisms, reasonable security safeguards, strict breach notification protocols, the facilitation of data principal rights, and the operational duties of Significant Data Fiduciaries, will become strictly enforceable.

Legislative Milestone	**Key Features and Strategic Shifts**
IT Act 2000 & SPDI Rules 2011	Governed only "sensitive" personal data. Applied solely to body corporates; completely exempted state entities. Weak enforcement relying on proven financial damages.
Puttaswamy Judgment (2017)	The Supreme Court recognised privacy as a fundamental right under Article 21. Established the strict necessity and proportionality test for data processing.
Draft PDP Bill (2018 & 2019)	Modelled on GDPR. Proposed an independent Data Protection Authority. Included rights to data portability and erasure. Introduced controversial state exemptions in 2019.
JPC Report (2021)	Expanded scope to include non-personal data. Recommended treating social media platforms as publishers. Resulted in the withdrawal of the 2019 Bill due to overcomplexity.

ISSN: 2582-6433

DPDP Act (2023) & Rules (2025)	Applies to all digital personal data. Consent-centric. Replaces the independent DPA with a centrally controlled adjudicatory Board. Drops data portability. Establishes phased implementation culminating in May 2027.

1.2 Key Statutory Provisions and Constitutional Alignment

The DPDP Act 2023 completely restructures the legal relationship between the individual and the entity collecting their data. The Act deliberately eschews traditional European terminology (Data Subject and Data Controller), opting instead for "Data Principal" and "Data Fiduciary".[19] This lexical choice is deeply significant; it embeds a legal and moral fiduciary duty of trust, care, and absolute accountability into the heart of India's digital economy. The Act applies exclusively to personal data in digital form, or data collected offline and subsequently digitised, expressly excluding non-personal data and personal data that has been made publicly available by the data principal themselves or through a legal obligation.

The Consent Architecture and "Legitimate Uses"

At the core of the DPDP Act is a highly regulated consent architecture. The processing of personal data relies on two primary lawful bases: explicit consent and "certain legitimate uses".[20] The Act mandates that consent must be free, specific, informed, unconditional, and unambiguous, as evidenced by a clear affirmative act by the Data Principal. Unlike earlier frameworks, the DPDPA strictly prohibits "bundled consent," requiring data fiduciaries to present users with granular choices, allowing them to consent to or decline specific data-processing purposes independently. This consent must be preceded or accompanied by an itemised privacy notice in English and in all 22 languages listed in the Eighth Schedule to the Constitution of India, ensuring linguistic accessibility for the diverse populace.

In a sharp departure from the European GDPR model, which recognises six distinct lawful bases for processing (including "legitimate interests" and "contractual necessity"), the Indian framework is rigidly binary.[21] It replaces the broad and highly flexible concept of legitimate interests with a narrowly defined statutory list of "legitimate uses". Under Section 7, fiduciaries may process data without explicit consent only in specific, pre-defined scenarios. These include instances where data is voluntarily provided by the principal for a specific purpose, for the state's provision of subsidies and benefits, during medical and public order emergencies, or for

ISSN: 2582-6433

specific employment purposes.

The absence of "contractual necessity" as a standalone legal basis requires significant operational restructuring for multinational corporations operating in India. Businesses that globally rely on contractual necessity to process user data for service delivery must now re-engineer their user interfaces and legal agreements to rely almost exclusively on explicit, withdrawable consent mechanisms.[22]

Significant Data Fiduciaries (SDFs) and Vulnerable Populations

To balance the regulatory burden on small enterprises with the need to check monopolistic technological power, the Act empowers the Central Government to classify certain large or high-risk entities as Significant Data Fiduciaries (SDFs). This classification is a dynamic metric based on the volume and sensitivity of the data processed, the potential risk posed to the rights of Data Principals, the risk to electoral democracy, and the potential impact on India's sovereignty and public order.[23]

SDFs face enhanced governance obligations designed to ensure algorithmic accountability and systemic resilience. These obligations include the mandatory appointment of a resident Data Protection Officer (DPO), the engagement of an independent data auditor to assess compliance, and the requirement to conduct periodic Data Protection Impact Assessments (DPIAs) to mitigate risks before launching new processing activities. By segregating fiduciaries by risk profile, the legislation seeks to foster a startup-friendly environment while placing the greatest compliance obligations on entities capable of causing mass societal harm.

The Act also introduces stringent, bright-line rules for the processing of children's data. Any processing of data belonging to individuals under the age of 18 requires verifiable parental consent. The Act categorically prohibits Data Fiduciaries from processing children's data in any manner that causes detrimental effects to their well-being, and strictly bans tracking, behavioural monitoring, and targeted advertising directed at minors.[24] However, the government retains the authority to exempt specific fiduciaries from these restrictions if the processing is deemed "verifiably safe," thereby allowing educational technology platforms to operate while restricting predatory advertising networks.

ISSN: 2582-6433

The Innovation of Consent Managers and Digital Public Infrastructure (DPI)

Perhaps the most globally unique and structurally ambitious feature of the DPDP Act is the statutory creation and regulation of "Consent Managers".[25] Defined as specialised entities registered with the DPBI, Consent Managers provide interoperable digital platforms that serve as a single point of contact, enabling individuals to grant, review, manage, and withdraw consent across multiple data fiduciaries simultaneously.

This framework is not merely a compliance tool; it is a structural pillar of India's rapidly expanding Digital Public Infrastructure (DPI). Systems like the Unified Payments Interface (UPI), the Account Aggregator framework in banking, and the Ayushman Bharat Digital Health Mission rely entirely on high-velocity, secure, and seamless data flows between public and private entities. The DPDP Act, through its Consent Manager architecture, provides the legal scaffolding for the broader Data Empowerment and Protection Architecture (DEPA). This moves India away from the Western model of monopolistic corporate data silos toward a decentralised, user-centric data governance model. In this ecosystem, citizens use Consent Managers to manage their digital footprints actively, thereby enabling access to microcredit, healthcare, and state subsidies with unprecedented speed and granular control.

The Transparency-Privacy Paradox: Structural Clash with the RTI Act 2005

A secondary, yet equally consequential, constitutional clash engineered by the DPDP Act is its direct and regressive impact on India's robust transparency framework. Section 44(3) of the DPDP Act amends Section 8(1)(j) of the Right to Information (RTI) Act, 2005, fundamentally disrupting the delicate democratic equilibrium between the Right to Know (derived from Article 19(1)(a) regarding freedom of speech and expression) and the Right to Privacy (protected under Article 21).[26]

Before this amendment, Section 8(1)(j) of the RTI Act provided a highly nuanced, qualified exemption for personal information. It prohibited the disclosure of personal data that had no relationship to any public activity, or which would cause unwarranted invasion of privacy, *unless* the Public Information Officer determined that the "larger public interest justifies the disclosure". This public interest override served as a crucial safety valve for democratic accountability, ensuring that privacy could not be weaponised as a shield for bureaucratic

ISSN: 2582-6433

corruption, maladministration, or the concealment of illicit assets by public servants.

This absolute exemption creates a severe "chilling effect" on investigative journalism, whistleblower protections, and public interest litigation. It allows a state bureaucracy historically inclined toward opacity to legally withhold data concerning public officials' assets, educational qualifications, the disbursement of state funds, and the identities of beneficiaries of government subsidies, entirely under the guise of data protection. Legal scholars and civil rights advocates characterise this amendment as a "hierarchy inversion," in which a statutory privacy restriction is maliciously used to subordinate a fundamental constitutional democratic right, thereby eroding the participatory democracy the RTI Act sought to build.

Sectoral Harmonisation and Legal Precedence (Section 38)

The interplay between the DPDP Act and India's existing sectoral regulations introduces further structural complexity into the legislative framework. Section 38 of the DPDP Act stipulates that its provisions shall be "in addition to, and not in derogation of" other laws currently in force. However, it explicitly includes a primacy clause stating that in the event of a direct conflict between the DPDP Act and any other law, the DPDP Act shall prevail to the extent of such conflict.

This primacy clause creates significant compliance friction for entities already heavily regulated by bodies such as the Reserve Bank of India (RBI), the Securities and Exchange Board of India (SEBI), the Insurance Regulatory and Development Authority of India (IRDAI), and the Telecom Regulatory Authority of India (TRAI).[27] For instance, older RBI regulations, KYC directives, and the Payment and Settlement Systems Act, 2007, historically allowed for the "implied consent" or "deemed consent" of customers for certain data disclosures required for financial processing.

Because the DPDP Act strictly invalidates implied consent, requiring unambiguous affirmative action or reliance on narrowly defined statutory legitimate uses, regulated financial and telecommunications entities face overlapping and sometimes contradictory compliance burdens. Conflicts also arise regarding data retention periods. At the same time, the DPDP Act mandates data minimisation and erasure once the purpose is served, financial regulators often require the indefinite or prolonged retention of transactional data for anti-money laundering (AML) and forensic purposes. Resolving these conflicts will require deep inter-regulatory

ISSN: 2582-6433

coordination to ensure that the DPDP Act's strict privacy standards do not destabilise the operational realities, forensic requirements, and systemic stability of India's financial and telecommunications ecosystems.

1.3 Institutional Roles: The Data Protection Board of India and Federal Implications

A robust data protection regime relies entirely on the efficacy, independence, and capacity of its enforcement authority. To operationalise and enforce this new regulatory paradigm, the DPDP Act establishes the Data Protection Board of India (DPBI).[28] However, the institutional design, composition, and jurisdictional scope of the DPBI deviate significantly from global best practices and raise critical questions about regulatory independence and the balance of federal power in India.

Composition, Powers, and Regulatory Restraint of the DPBI

Unlike the structurally independent, highly proactive Data Protection Authorities (DPAs) envisioned in the 2018 Srikrishna Committee draft, or the powerful Supervisory Authorities established under the European GDPR, the DPBI is conceived not as an autonomous policymaker but as a strictly reactive, quasi-judicial adjudicatory body. The DPDP Act explicitly denies the DPBI any autonomous rule-making, standard-setting, or legislative powers; all regulatory and policy-making authority remains exclusively centralised within the Union Government (specifically, the Ministry of Electronics and Information Technology).

Furthermore, Section 27(3) of the Act grants the Union government the unprecedented power to issue binding directions to the DPBI and, critically, to direct the Board to "modify, suspend, or cancel" its own binding directions upon an executive reference. This executive override mechanism fatally undermines the Board's ability to act as an impartial, independent arbiter, particularly when it must adjudicate massive privacy violations or data breaches committed by central state agencies.

Federal Implications: The Centralisation of Data Governance

The establishment of a single, highly centralised Data Protection Board based in New Delhi introduces severe federal friction within India's constitutional structure. India operates as a quasi-federal republic in which state governments exercise significant, constitutionally

ISSN: 2582-6433

protected legislative and executive powers. Crucially, state governments and regional authorities are major processors of personal data, managing vast, localised databases related to public health care (Entry 6 of the State List), law and order, land records, municipal education, and the distribution of regional welfare subsidies.

Despite the inherently decentralised nature of public data collection and administration, the DPDP Act centralises all enforcement, adjudication, and regulatory oversight exclusively at the Union level. The Act defines the "State" broadly under Article 12 of the Constitution, encompassing central ministries, state-level government departments, local panchayats, and state public sector undertakings. Consequently, state utilities (e.g., regional power distribution companies) and state health departments are granted the same broad exemptions from consent and storage limitations as central intelligence agencies.[29]

However, the regulatory authority over these state entities, the power to define exemptions, restrict cross-border data flows, classify Significant Data Fiduciaries, and appoint the adjudicatory body that will penalise state departments rests entirely with the Central Government. This concentration of power creates a profound constitutional imbalance. A data breach involving a municipal hospital database in Kerala or a state welfare registry in Tamil Nadu will be adjudicated by a central board, fully controlled by the Union government in New Delhi. This dynamic threatens to generate immense mistrust and intergovernmental turf wars, as state authorities find their digital administrative practices subject to punitive oversight by a Union-controlled executive body without any state-level representation.

The "Enforcement Deficit" and the Case for Decentralisation

Beyond political federalism, the centralised architecture of the DPDP Act creates a massive functional "enforcement deficit".[30] A single national board is tasked with overseeing the digital footprints of over 800 million internet users and regulating an estimated 600 million data-processing entities across a vast geographical and linguistic landscape. This immense scope risks creating an enforcement bottleneck akin to the GDPR's early struggles, in which the centralised authority will inevitably be forced to prioritise scrutinising high-profile Significant Data Fiduciaries (SDFs) and multinational tech conglomerates, while a massive "long tail" of smaller, regional data fiduciaries remains effectively under-regulated.

Implementing state-level Data Protection Boards would effectively bridge the "Missing

ISSN: 2582-6433

Middle" in India's data governance architecture.[31] Regional bodies would be intimately familiar with local administrative contexts, regional business practices, and vernacular languages, making them better positioned to oversee local business compliance and state government data processing. Most importantly, it would provide ordinary citizens with geographically and linguistically accessible forums for rapid grievance redressal, rather than forcing a rural citizen to navigate a centralised tribunal in the capital. Under this proposed, mature federal framework, the central DPBI would transition to act as an appellate, standard-setting, and coordinating authority functioning similarly to the European Data Protection Board (EDPB), resolving interstate disputes and ensuring a uniform interpretation of data protection jurisprudence across state lines, while fully respecting the constitutional distribution of federal power.[32]

Conclusion

The Digital Personal Data Protection Act, 2023, transitions India from a fragmented, obsolete regulatory landscape into a modernised, statutory data governance regime. By shifting from the outdated IT Act to a framework explicitly centred on fiduciary accountability, robust penalty structures, and the highly innovative deployment of Consent Managers, the legislation makes significant strides toward securing digital transactions and supporting the expansion of India’s Digital Public Infrastructure.

However, deep statutory analysis reveals that the Act’s current formulation structurally privileges state power and corporate operational efficiency over the fundamental right to informational privacy. The broad, unchecked exemptions granted to state instrumentalities under Section 17 bypass the vital necessity and procedural safeguard prongs of the *Puttaswamy* proportionality test, leaving citizens vulnerable to unchecked surveillance. Simultaneously, the absolute barring of personal data disclosures under the amended RTI Act creates a severe transparency-privacy paradox, weaponising data protection to shield the state from democratic accountability. Finally, the institutional design of the Data Protection Board of India, characterised by centralised Union control, a lack of autonomous rule-making power, executive override clauses, and an absence of state-level enforcement infrastructure, threatens to create an insurmountable enforcement deficit that strains India's federal equilibrium. For the DPDP Act to fully fulfil the constitutional mandate of Article 21, subsequent legislative amendments must decentralise enforcement to the states, integrate stringent judicial oversight into state data exemptions, and definitively restore the public interest equilibrium within India's broader transparency and digital governance laws.

ISSN: 2582-6433

BIBLIOGRAPHY

Constitutional and Statutory Law

- **The Constitution of India**, specifically Part III (Fundamental Rights), Article 19(1)(a) (Freedom of Speech), Article 21 (Right to Life and Personal Liberty), and the Eighth Schedule.
- **The Digital Personal Data Protection Act, 2023**.
- **The Digital Personal Data Protection Rules, 2025**.
- **The Information Technology Act, 2000**, including Sections 43A and 72A.
- **The Right to Information Act, 2005**, including Section 8(1)(j).
- **The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011** (SPDI Rules).
- **The Payment and Settlement Systems Act, 2007**.
- **The Consumer Protection Act**.

Judicial Precedent

- ***Justice K.S. Puttaswamy (Retd.) v. Union of India***, (2017) (The "Right to Privacy" Judgment).

Committee Reports and Draft Legislation

- Committee of Experts under the Chairmanship of Justice B.N. Srikrishna (2018), Report and Draft Bill.
- The Personal Data Protection Bill, 2018.
- The Personal Data Protection Bill, 2019.
- Report of the Joint Parliamentary Committee (JPC) on the Personal Data Protection Bill (2021).
- The Digital Personal Data Protection Bill, 2022.

International Instruments

- General Data Protection Regulation (GDPR) (European Union).

Digital Frameworks

- Data Empowerment and Protection Architecture (DEPA).

ISSN: 2582-6433

- Unified Payments Interface (UPI).
- Ayushman Bharat Digital Health Mission.

[1] Information Technology Act, 2000 (Act 21 of 2000); Raktima Roy & Gabriela Zanfir-Fortuna, "The Digital Personal Data Protection Act of India, Explained", *Future of Privacy Forum* (2023).
[2] Information Technology Act, 2000 (Act 21 of 2000); Digital Personal Data Protection Act, 2023 (Act 22 of 2023); "DPDP Act vs IT Act", *Taxmann* (2024).
[3] Digital Personal Data Protection Act, 2023 (Act 22 of 2023); Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
[4] Digital Personal Data Protection Act, 2023 (Act 22 of 2023); Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011; "India's Digital Personal Data Protection Act 2023 vs the GDPR", *Latham & Watkins* (2023).
[5] Abdullah Zubair Motiwala, "A Jurisprudential Analysis of the DPDP Rules 2025 and the Evolution of Data Privacy Laws in India", *SSRN* 4 (2025); Lisa P. Lukose, "Data Protection in Light of the Digital Personal Data Protection Act, 2023", *ResearchGate* (2025); Suyash Rai, "Data Protection in India", *Carnegie Endowment for International Peace* (2023).
[6] Lisa P. Lukose, "Data Protection in Light of the Digital Personal Data Protection Act, 2023", *ResearchGate* (2025); Nandini Sinha, "Right to Privacy and Data Protection Act: An Analytical Study", 4 *Indian Journal of Integrated Research in Law* 1005 (2024).
[7] Abdullah Zubair Motiwala, "A Jurisprudential Analysis of the DPDP Rules 2025 and the Evolution of Data Privacy Laws in India", *SSRN* 4 (2025).
[8] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1; Vrinda Bhandari et al., "An Analysis of Puttaswamy: The Supreme Court's Privacy Verdict", *IndraStra Global* 3 (2017); "Judicial Interpretation and Data Rights in India: From Puttaswamy to the DPDP Act 2023", *Indian Journal of Integrated Research in Law* 1894 (2025).
[9] Vrinda Bhandari et al., "An Analysis of Puttaswamy: The Supreme Court's Privacy Verdict", *IndraStra Global* 3 (2017); "Judicial Interpretation and Data Rights in India: From Puttaswamy to the DPDP Act 2023", *Indian Journal of Integrated Research in Law* 1894 (2025); Teesha and Shankar Srivastava, "Data Anonymisation, The Right to Explanation, and The Architecture of Accountability Under the Digital Personal Data Protection Act", *HILSR Law Review* 102 (2025).
[10] Gautam Bhatia, "State Surveillance and the Right to Privacy in India", 26 *National Law School of India Review* 127 (2014); "The Transparency–Privacy Paradox in India: A Critical Examination of the Digital Personal Data Protection Act 2023", *Indian Journal of Integrated Research in Law* 976 (2025); Nidhi Jha and Rudraksh Lakra, "Publicly Available Data in the DPDP Act 2023", *SSRN* 18 (2024).
[11] "Judicial Interpretation and Data Rights in India: From Puttaswamy to the DPDP Act 2023", *Indian Journal of Integrated Research in Law* 1894 (2025); *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1, at 501.
[12] Vrinda Bhandari et al., "An Analysis of Puttaswamy: The Supreme Court's Privacy Verdict", *IndraStra Global* 3 (2017), at 4; *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1, at 504.
[13] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1; Teesha and Shankar Srivastava, "Data Anonymisation, The Right to Explanation, and The Architecture of Accountability Under the Digital Personal Data Protection Act", *HILSR Law Review* 102 (2025), at 105; Raktima Roy & Gabriela Zanfir-Fortuna, "The Digital Personal Data Protection Act of India, Explained", *Future of Privacy Forum* (2023).
[14] Digital Personal Data Protection Act, 2023 (Act 22 of 2023); Raktima Roy & Gabriela Zanfir-Fortuna, "The Digital Personal Data Protection Act of India, Explained", *Future of Privacy Forum* (2023).
[15] Abdullah Zubair Motiwala, "A Jurisprudential Analysis of the DPDP Rules 2025 and the Evolution of Data Privacy Laws in India", *SSRN* 4 (2025), at 10; Section 38, Digital Personal Data Protection Act, 2023; Nandini Sinha, "Right to Privacy and Data Protection Act: An Analytical Study", 4 *Indian Journal of Integrated Research in Law* 1005 (2024), at 1007.
[16] Draft Digital Personal Data Protection Rules, 2025; Draft Digital Personal Data Protection Rules, 2025, Rule 4.
[17] Digital Personal Data Protection Act, 2023 (Act 22 of 2023); Draft Digital Personal Data Protection Rules, 2025; "DPDP Act vs IT Act", *Taxmann* (2024), at 6.
[18] Draft Digital Personal Data Protection Rules, 2025; Abdullah Zubair Motiwala, "A Jurisprudential Analysis of the DPDP Rules 2025 and the Evolution of Data Privacy Laws in India", *SSRN* 4 (2025), at 12; Teesha and Shankar Srivastava, "Data Anonymisation, The Right to Explanation, and The Architecture of Accountability Under the

ISSN: 2582-6433

Digital Personal Data Protection Act", *HILSR Law Review* 102 (2025), at 103.

[19] Draft Digital Personal Data Protection Rules, 2025; Teesha and Shankar Srivastava, "Data Anonymisation, The Right to Explanation, and The Architecture of Accountability Under the Digital Personal Data Protection Act", *HILSR Law Review* 102 (2025), at 103; "The Transparency–Privacy Paradox in India: A Critical Examination of the Digital Personal Data Protection Act 2023", *Indian Journal of Integrated Research in Law* 976 (2025), at 977.

[20] Abdullah Zubair Motiwala, "A Jurisprudential Analysis of the DPDP Rules 2025 and the Evolution of Data Privacy Laws in India", *SSRN* 4 (2025), at 10; Nandini Sinha, "Right to Privacy and Data Protection Act: An Analytical Study", 4 *Indian Journal of Integrated Research in Law* 1005 (2024), at 1007; Draft Digital Personal Data Protection Rules, 2025.

[21] Vrinda Bhandari et al., "An Analysis of Puttaswamy: The Supreme Court's Privacy Verdict", *IndraStra Global* 3 (2017), at 4; "The Transparency–Privacy Paradox in India: A Critical Examination of the Digital Personal Data Protection Act 2023", *Indian Journal of Integrated Research in Law* 976 (2025), at 978; "Business Requirements Document for Consent Management System", *Ministry of Electronics and Information Technology* (2025), at 5.

[22] "India's Digital Personal Data Protection Act 2023 vs the GDPR", *Latham & Watkins* (2023), at 3; "DPDP Act vs IT Act", *Taxmann* (2024), at 5.

[23] Raktima Roy & Gabriela Zanfir-Fortuna, "The Digital Personal Data Protection Act of India, Explained", *Future of Privacy Forum* (2023); Abdullah Zubair Motiwala, "A Jurisprudential Analysis of the DPDP Rules 2025 and the Evolution of Data Privacy Laws in India", *SSRN* 4 (2025), at 10-12.

[24] Nandini Sinha, "Right to Privacy and Data Protection Act: An Analytical Study", 4 *Indian Journal of Integrated Research in Law* 1005 (2024), at 1007; Section 8, Digital Personal Data Protection Act, 2023; Section 17, Digital Personal Data Protection Act, 2023.

[25] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1; Abdullah Zubair Motiwala, "A Jurisprudential Analysis of the DPDP Rules 2025 and the Evolution of Data Privacy Laws in India", *SSRN* 4 (2025), at 10; Aditya Sushant Jain, "Decoding consent managers under the Digital Personal Data Protection Act, 2023", 7 *Journal of Data Protection & Privacy* 406 (2025).

[26] "Analysis: Reconciling DPDP Act and RTI Act", *Taxmann* (2024); "The Transparency–Privacy Paradox in India: A Critical Examination of the Digital Personal Data Protection Act 2023", *Indian Journal of Integrated Research in Law* 976 (2025), at 988.

[27] "Need for syncing sectoral regulations with data protection law", *Cyril Amarchand Mangaldas Blog* (2024), at 2; Section 38, Digital Personal Data Protection Act, 2023.

[28] Information Technology Act, 2000 (Act 21 of 2000); Draft Digital Personal Data Protection Rules, 2025; Section 18, Digital Personal Data Protection Act, 2023.

[29] Suyash Rai, "Data Protection in India", *Carnegie Endowment for International Peace* (2023).

[30] Abhijith Balakrishnan, "Enforcement Gaps in India's DPDP Act and the Case for Decentralized Data Protection Boards", *Express Computer* (2026).

[31] "The Missing Middle: Bridging the Gap Between State Exemptions and Citizen Autonomy under the Digital Personal Data Protection Act, 2023", *Jus Scriptum* (2023), at 4; Abhijith Balakrishnan, "Enforcement Gaps in India's DPDP Act and the Case for Decentralized Data Protection Boards", *Express Computer* (2026).

[32] Abhijith Balakrishnan, "Enforcement Gaps in India's DPDP Act and the Case for Decentralized Data Protection Boards", *Express Computer* (2026).