



The Indian Journal for Research in Law and Management

Open Access LawJournal–Copyright©2026

Editor-in-Chief–Dr. Muktai Deb Chavan; Publisher– Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

PRIVACY VS. TRANSPARENCY

EXAMINING THE DPDP ACT & RTI CONFLICT IN INDIA

-MAHIMA SINGH

ABSTRACT

This Article, examines the constitutional and legal friction between individual data privacy rights and administrative transparency in India. The central theme focuses on the clash between the **Digital Personal Data Protection (DPDP) Act, 2023** and the **Right to Information (RTI) Act, 2005**. By amending Section 8(1)(j) of the RTI Act via Section 44 of the DPDP Act, the statutory "public interest" override is effectively removed. This establishes a blanket ban shielding personal data held by public authorities, which risks concealing critical public spending records, official appointments, corruption investigations, and welfare beneficiary lists from citizen audit. Beyond state transparency, the paper also evaluates corporate data harvesting by Big Tech platforms (such as Meta and Google), AI model training, and dark consent patterns, while outlining actionable governance measures under the DPDP Act—including the **Data Protection Board of India (DPBI)**, **Data Protection Officers (DPOs)**, and enhanced consent frameworks.

INDEX

No.	CONTENT	PAGES
	Abstract & Index	1-2
1.	Origins of the Doctrine & Existing Literature • <i>Timeline of Drafting Act</i> • <i>Penalties & Punishment</i> • <i>Government Measures & Enforcement</i>	3-6
2.	Doctrinal Breakdown & Federal Aftermath • <i>Issue</i> • <i>Evaluation</i> • <i>Impact</i>	6-9
3.	Actionable Reforms: Strategic Alternatives & Justifications • <i>Data Protection Board</i> • <i>Appointment of Data Protection Officer</i> • <i>Authorized Consent</i> • <i>End to End Encryption</i> • <i>Grievance Redressal Cell</i>	10-11
4.	Conclusion	12

ORIGIN OF THE DOCTRINES & EXISTING LITERATURE

"**Data**" refers to both online and offline systems of information, concepts, or instructions formalized for processing, storage, or management via automated, electronic, or digital technologies as "**Digital Data**" utilized systematically to compile, analyze, and maintain statistical and definitive records encompass personnel records, financial statements, payroll accounts, and operational metrics used for corporate governance, compliance, and analytical oversight. Digital platforms driven by rising cybercrimes, data breaches, corporate exploitation for targeted advertising, and national security threats, "**Data Protection**" has emerged as a critical regulatory framework. Consequently, global jurisdictions are enforcing strict legal mandates to secure data, mitigate vulnerabilities, and prevent cyber threats."

Legislative shift heavily impacts administrative transparency and accountability, as critical records regarding government schemes, recruitments, and public spending can now be withheld under the guise of data privacy. Striking a harmonious balance amid safeguarding individual privacy and upholding the citizen's *Right to Information* remains a critical challenge for future legal interpretation and global governance.

In constitutional law, *Privacy & Transparency* exist in a state of reciprocal tension. While transparency ensures public accountability by disclosing government actions, privacy protects individual autonomy from state intrusion. To resolve conflicts between these two principles, the judiciary employs proportionality or balancing test. Consequently, any legislative measure compelling public disclosure must serve a legitimate state interest and be narrowly tailored to avoid unjustifiably infringing upon fundamental privacy rights.¹

The DPDP Act 2023 conflicts with the RTI Act 2005 by removing the public-interest balancing test, allowing authorities to shield personal data from citizen requests. This legislative framework evolved significantly via MeitY between 2019 and 2023 to combat critical data security violations—such as theft and cyber warfare—that threaten individual privacy and national sovereignty.

¹ <https://articles.manupatra.com/article-details/From-Constitutional-Rights-to-Data-Protection-Article-21-and-Comparative-Perspectives-on-Privacy>

TIMELINE OF DRAFTING ACT:

- **Proposal** (December 2019): The **Personal Data Protection Bill, 2019** was introduced in the Lok Sabha, proposing strict rights-based rules and data localization mandates and referred to JPC committee.²
- **Committee Review** (December 2021): The Joint Parliamentary Committee (JPC) reviewed the bill and recommended over 80 amendments to resolve high compliance costs and excessive government exemptions.³
- **Withdrawal** (August 2022): The government officially withdrew the Bill to design a simplified, more comprehensive legal framework aligned with digital infrastructure.⁴
- **Public Draft** (November 2022): MeitY released a streamlined draft version for public review & consultation.⁵
- **Enactment** (August 2023): By incorporating stakeholder's feedback, Parliament officially passed the revised bill, culminating in the formal final enactment of the **Digital Personal Data Protection (DPDP) Act, 2023** to regulate digital data through an outcome-oriented system for regulating digital personal data.⁶

This legislative shift elevates the right to privacy into an absolute shield against public scrutiny, effectively eliminating the statutory balancing test that once favored government accountability. The **Digital Personal Data Protection (DPDP) Act, 2023**, has created a significant legal conflict with the **Right to Information (RTI) Act, 2005**, by redefining the boundaries between individual privacy and public transparency in India. Previously, the RTI Act allowed the disclosure of personal information if it served a larger public interest. However, Section 44(2) of the DPDP Act amends Section 8(1) (j) of the RTI Act⁷, creating a blanket ban on the disclosure of all personal data held by public authorities.

This conflict severely impacts democratic oversight, as critics argue the amendment weakens the RTI Act by allowing public officials to withhold critical information under the guise of data privacy. Crucial data regarding government appointments, corruption investigations, and the distribution of public welfare benefits can now be legally concealed from citizens.

² <https://prsindia.org/billtrack/the-personal-data-protection-bill-2019>

³ https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3569465

⁴ <https://prsindia.org/billtrack/the-personal-data-protection-bill-2019>

⁵ <https://www.activemind.legal/guides/india-dpdp/>

⁶ <https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf>

⁷ <https://www.scoobserver.in/cases/constitutionality-of-the-digital-personal-data-protection-act-2023/>

Here is the structured comparison table of PENALTIES AND PUNISHMENTS under the Personal Data Protection (PDP) Bill, 2019 & the Digital Personal Data Protection (DPDP) Act, 2023:

ASPECT OF PENALTY	PERSONAL DATA PROTECTION (PDP) BILL, 2019	DIGITAL PERSONAL DATA PROTECTION (DPDP) ACT, 2023
Nature of Liability	This law imposes civil fines and up to 3 years' imprisonment for unlawful data collection, sale, transfer, or re-identification. These specific data offences are legally classified as cognizable and non-bailable.	Exclusively civil in nature. There is no criminal liability or imprisonment; enforcement focuses entirely on monetary penalties and corrective directions.
Maximum Financial Penalty	Up to 4% of global turnover or ₹15 crore, whichever is higher. ⁸	Imposes civil penalties up to ₹250 crore per breach, determined by a statutory schedule of specified defaults rather than global turnover. ⁹
Enforcing Authority	Enforced by a Data Protection Authority (DPA) equipped with extensive rule-making powers.	Adjudicated by the Data Protection Board of India (DPBI), acting as an independent adjudicatory body.
Penalty Assessment Criteria	Calculated using rigid, highly prescriptive rules and turnover-based formulas.	Penalties are evaluated individually based on the breach's severity, duration, and harm, alongside the organization's cooperation and response efforts.
Penalties on Individuals (Data Principals)	Included no statutory duties or penalties for Data Principals.	Introduces statutory duties for Data Principals, including penalties for non-compliance such as filing false or frivolous complaints .

GOVERNMENT MEASURES & ENFORCEMENT:

The Digital Personal Data Protection (DPDP) Act effectively stops businesses from exploiting personal data, but applying its strict rules to government bodies limits public transparency. As a result, Indian courts must find a balance between the right to privacy and

⁸ <https://www.consent.in/blog/dpdp-act>

⁹ <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2190655®=48&lang=2>

the right to information, ensuring that data protection does not destroy the public's ability to hold the government accountable.

- **Commercial Misuse vs. Public Transparency:** The DPDP Act is highly successful at preventing private companies to toss around or abusing your personal information. However, when the same strict privacy rules are applied to the government, it becomes difficult for citizens to access public records, investigate corruption or to ensure institutional checks and balances.¹⁰
- **Competing Rights:** The text highlights a clash between two fundamental rights:
 - *Right to Privacy:* The right of an individual to keep their personal details safe.
 - *Right to Information:* The right of citizens to see government data to ensure that officials are doing their jobs honestly.
- **The Role of the Judiciary:** Because the law sparks a dispute between privacy and transparency, The Indian judiciary is required to act as a neutral mediator to harmonize both rights, so that protecting an individual's privacy does not completely block¹¹ the public's right to question the government.

DOCTRINAL BREAKDOWN & FEDERAL AFTERMATHS

ISSUE:

Tech conglomerates that control major platforms like **WhatsApp, Facebook, Instagram, and Google** routinely harvest consumer data through manipulative privacy policies. By burying data-sharing clauses within dense terms of service, these platforms obtain technical consent to track user locations and deploy Artificial Intelligence (AI) algorithms that serve targeted advertisements. This collected information is then monetized and shared with third-party enterprises, such as insurance providers and e-commerce platforms without the consent of the data holder. This corporate data ecosystem is highlighted in the web series *Escapade*

¹⁰ <https://www.legal500.com/intelligence/india/privacy/india's-digital-personal-data-protection-act-and-the-dpdp-rules-2025-phased-commencement-core-obligations-and-a-board-ready-compliance-strategy>

¹¹ <https://www.thehindu.com/news/cities/Coimbatore/judiciary-at-a-crossroads-introspection-necessary-to-restore-neutrality-justice-anand-venkatesh/article71485597.ece>

Live on Disney+ Hotstar, which dramatizes the backend mechanics of digital platforms and their reliance on user data for revenue generation¹².

The WhatsApp privacy policy controversy highlighted the tension over digital autonomy when Meta pressured users to accept deeper data integration, sparking fears of aggressive corporate targeting. While data privacy risks escalate when organizations exploit personal information without explicit consent, a critical transparency deficit emerges when governments do the same under broad "legitimate uses" clauses. Consequently, the state now shields public spending, beneficiary lists, and official appointments under the guise of protected "personal information".¹³ This ultimately prevents citizens from using the RTI Act to demand necessary institutional disclosures and government accountability:

- The Root Cause: Data privacy issues occur when organizations collect, process, or share personal data without obtaining explicit user consent or providing clear disclosures.
- The Transparency Deficit: A critical imbalance exists because the government is legally permitted to process and use citizens' personal data without explicit consent under broad "legitimate state uses".
- Vague privacy policies: How algorithms utilize consumer habits, preventing individuals from understanding the true scope of their data exposure.¹⁴
- Hidden third-party tracking: Hide and unmapped data sharing directly violate data minimization principles,¹⁵ creating massive vulnerabilities for unauthorized surveillance and breaches.

EVALUATION:

The themes of manipulative policies, non-consensual data sharing, and the urgent need for robust legislation are unfolding in real-time. Big Tech data collection practices have escalated from a hidden corporate strategy into a high-stakes legal battleground.

¹² <https://timesofindia.indiatimes.com/web-series/reviews/hindi/escaype-live/escaype-live-season-1/seasonreview/91648989.cms>

¹³ <https://dokumen.pub/data-protection-in-a-profiled-world-9048188644-9789048188642.html>

¹⁴ <https://luthresearch.com/glossary/understanding-algorithmic-consumer-behavior-insights-for-modern-businesses/>

¹⁵ <https://www.kiteworks.com/risk-compliance-glossary/data-minimization/>

The "take-it-or-leave-it" metadata sharing policy¹⁶ introduced by WhatsApp has shifted from a public outcry into severe regulatory and legal action, The Supreme Court of India actively reprimanded Meta and WhatsApp regarding their data-sharing practices, explicitly criticizing the exploitation of personal data as akin to "data theft. The Competition Commission of India levied a ₹213.14 crore (\$25 million) penalty against Meta for abusing its dominant market position by forcing users to share data to enable targeted advertising.¹⁷ Meta is legally contesting this fine in the Supreme Court.

The context noted how companies use AI to track and target consumers. The challenge has evolved as The Big Tech is no longer just selling data to insurance or shopping apps—they are actively feeding consumer data directly into Generative AI models.¹⁸ Tech organizations face massive scrutiny for scraping public and user data to train AI tools without explicit consumer consent.

The Constitutional legislation mandates lawful, transparent data handling, forcing companies to provide clear privacy notices and user rights. However, evaluating transparency from an Indian perspective reveals a severe systemic conflict, as the state frequently utilizes broad "legitimate uses" to process citizen information without explicit consent. Consequently, by broadly expanding the definition of "personal information," this framework restricts the RTI shielding public spending and appointments from vital citizen scrutiny¹⁹ which leads to:

- **Impede Accountability:** Consequently, citizens can no longer use the Right to Information (RTI) Act to demand disclosures on public spending, beneficiary lists, or government appointments, as the state shields this data under the blanket of protected "personal information."
- **The Role of Legislation:** Robust Data Protection Laws are vital to protect individual privacy, enforce transparent consent frameworks, and defend the fundamental right to digital autonomy.
- **Legal compliance requires:** Companies to provide clear "privacy notices at or before collection," granting users full rights to access, rectify, or delete their information.
- **Legal frameworks:** India's DPDP Act 2023 mandate that data handling must be lawful, fair, and transparent.

¹⁶ <https://indiankanoon.org/doc/165750198/>

¹⁷ <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2074431®=48&lang=2>

¹⁸ <https://www.mdpi.com/2504-2289/10/2/46>

¹⁹ <https://jkexamlibrary.in/app-blog/116-rti-act-right-to-information-act-2005--complete-jkssb-notes?page=0>

IMPACT:

Governments are introducing strict, phased legislation to protect the individual right to choose and eliminate manipulative policies like dense, confusing terms of service. At the center of these new rules there is a mandatory framework for Consent Managers²⁰ interoperable platforms providing a single dashboard where users can explicitly grant, review, or revoke data consent. Full compliance deadlines for major tech firms will roll out in legally binding phases.

- *Data Sharing:* Regulators are banning the forced integration of WhatsApp data into Meta's ad ecosystem, legally separating private chat metadata from corporate advertising profiles. This ensures that using essential messaging tools is no longer conditional on surrendering sensitive data to track user habits. By creating this strict boundary, data protection becomes an enforceable rule rather than a passive user burden. Ultimately, this safeguards your digital autonomy, ensuring personal communication remains private instead of weaponised for profit.²¹ For Example; Competition Commission of India (CCI) vs. Meta Supreme Court Case.
- *Manipulative Privacy Policies:* "Consent Architecture" reframes data protection by replacing deceptive "dark patterns" with user-friendly control dashboards and granular opt-out choices. Models like India's DPDP Rules and US State Privacy Laws return ownership of sensitive browsing and location data to consumers.²² By eliminating all-or-nothing data harvesting, this framework forces Big Tech to explicitly earn consumer trust and establishes digital privacy as a fundamental right.
- *AI Targeting & Consumer Control:* Legal limits on consumer data and biometrics prevent tech firms from harvesting facial prints, voices, and browsing habits to fuel AI profiling algorithms without explicit consent. Using frameworks like the EU AI Act, these regulations establish biometric and behavioral data as non-negotiable personal assets.²³ By providing clear opt-out rights, the law stops corporations from using autonomous AI systems to quietly predict, manipulate, and capitalize on intimate consumer behaviors.

²⁰ <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2190655®=48&lang=2>

²¹ <https://vajiramandravi.com/current-affairs/meta-whatsapp-data-case/>

²² <https://www.ijlrr.com/post/comparative-study-of-data-protection-laws-usa-vs-india>

²³ <https://policyreview.info/articles/analysis/general-purpose-ai-regulation-and-ai-act>

Section 44(3) of the DPDP Act 2023 stripped the "**public interest override**" from the **RTI Act 2005**, turning privacy into a barrier that shields public officials and welfare lists from scrutiny.²⁴ This creates a paradox: the state processes citizen data without consent under broad "**legitimate uses**" but invokes privacy to block institutional transparency. Ultimately, bypassing oversight compromises government accountability and shifts power away from citizens.

ACTIONABLE REFORMS: STRATEGIC ALTERNATIVES & JUSTIFICATIONS

The Digital Personal Data Protection (DPDP) Act, 2023 drastically updated the 2022 draft by narrowing the Data Protection Board of India into a purely quasi-judicial enforcement body. Instead of making policy, the DPBI strictly investigates data breaches, orders corrections, and penalizes non-compliant companies. Additionally, the Act replaces traditional consent with a strict requirement for unambiguous, specific, and revocable permission. Data Fiduciaries must now give individuals a clear, detailed notice outlining the exact purpose of data collection before processing it, ensuring users retain total control and the permanent right to revoke their consent.

Under the **DPDP Act, 2023**, designated Significant Data Fiduciaries must appoint an India-based Data Protection Officer (DPO) and hire independent auditors for security evaluations. Furthermore, Section 8 mandates that all Data Fiduciaries deploy robust technical safeguards—such as advanced encryption and access controls—to prevent data breaches, alongside a mandatory internal grievance redressal mechanism that users must exhaust before escalating disputes to the Data Protection Board of India.²⁵ Failure to implement these security controls or resolve grievances constitutes a material breach, shifting the regulatory burden onto corporate actors through continuous operational auditing to ensure systemic accountability.

- **Data Protection Board: Section 27 of the DPDP Act 2023** establishes the Data Protection Board of India (DPBI) strictly as an independent, quasi-judicial adjudicatory body rather than a general regulator. It is empowered to investigate

²⁴ <https://www.alsedunation.com/current-affairs?q=Indian%20Polity%20&%20Governance>

²⁵ <https://www.dpdpa.com/dpdpa2023/chapter-2/section8.html>

data breaches, direct urgent remedial actions, and levy non-compliance penalties up to ₹250 crore.²⁶

- Appointment of Data Protection Officer: Under **Section 10 of the DPDP Act 2023**, Significant Data Fiduciaries must appoint an India-based Data Protection Officer (DPO) to manage grievances and handle regulatory representation. They are also legally required to hire an independent Data Auditor to conduct periodic security and compliance audits.
- Authorized Consent: The DPDP Act 2023 mandates that organizations obtain free, specific, informed, and unconditional consent through clear, accessible data-collection notices. Individuals retain the ultimate right to grant or withdraw permission at any time.
- End to End Encryption: **Section 8(5) of the DPDP Act 2023** explicitly shifts the focus from specific technologies like encryption to a broader legal obligation, mandating that every Data Fiduciary must implement reasonable security safeguards—including technical and organizational measures—to completely prevent personal data breaches during processing and transfer.²⁷
- Grievance Redressal Cell: Under **Section 13 of the DPDP Act 2023**, all Data Fiduciaries must establish an easily accessible grievance redressal mechanism. Data Principals are legally required to exhaust this internal channel before they can escalate unresolved complaints to the Data Protection Board of India.

CONCLUSION

The shift of **PDP Bill 2019** to the current framework establishes a tightly controlled digital ecosystem by mandating **free consent**, protecting **minors' data**, and enforcing **end-to-end encryption** alongside application permission policies. While it introduces strict **finest for breaches**, dedicated **grievance redressal cells**, and **algorithmic accountability**, the framework simultaneously cements a **superior role for the government** with expansive data-erasure powers. Ultimately, data sharing based on explicit **written permission** must be strictly regulated to ensure state oversight does not compromise or dismantle the fundamental **Right to Privacy**.

²⁶ <https://www.tcsa.in/frameworks/dpdp/penalties-enforcement>

²⁷ <https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf>

The **DPDP Act 2023** creates a direct conflict between data privacy and transparency by altering the **RTI Act 2005**. By dismantling the historic balancing test between these two principles, the amendment turns the right to privacy into an absolute barrier against public oversight and government accountability.

While the DPDP Act, 2023 introduces critical regulatory safeguards against corporate data exploitation, cyber threats, and unauthorized commercial profiling, its application to public administrative bodies creates a severe transparency deficit. The complete elimination of the public interest exception under Section 8(1)(j) converts individual privacy into an absolute barrier against state scrutiny, insulation of public officials, and democratic oversight. To prevent blanket rejections, PIO must apply Section 10 of the RTI Act to redact personal identifiers and disclose governance data, using Section 8(2) to let public interest override exemptions. Ultimately, the paper emphasizes that the Indian judiciary and policymakers must restore a harmonious proportionality balance between protecting fundamental privacy rights and upholding constitutional transparency to maintain institutional government accountability.