International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2025: 7.089

Balancing Privacy and State Power: A Constitutional Analysis of India's Digital Personal Data Protection Act, 2023 in Light of Puttaswamy and the GDPR

Hansapriya S

Symbiosis Law School, Pune
Symbiosis International (Deemed University), Pune, India.

Abstract: ***The digital revolution has vastly increased the collection and processing of personal data by both governments and corporations. In India, the landmark Supreme Court judgment Puttaswamy v. Union of India (2017) unequivocally recognized privacy as a fundamental right essential to individual dignity and autonomy. Global frameworks like the EU's GDPR set high benchmarks for data protection. In this context, India enacted the Digital Personal Data Protection Act, 2023 (DPDP Act) on August 11, 2023. The Act seeks to balance citizens' right to protect their personal data with legitimate social needs. This paper critically examines the DPDP Act's provisions, especially its "consent-based" model for private entities and its expansive exemptions for state agencies. We analyze whether the new law incorporates the constitutional standards of Puttaswamy (such as strict necessity and proportionality) and how it measures up against GDPR's principles. Our research finds that while the Act introduces a comprehensive framework of rights (access, correction, erasure) and duties (security safeguards, breach notification) for data fiduciary, it omits certain individual rights (like data portability) and grants broad, ill-defined powers to the state. We recommend legislative and institutional reforms - for instance, narrowing exemption clauses and strengthening the Data Protection Board – to realign India's law with constitutional ideals. The paper concludes that embedding privacy-by-design and proportionality in law is essential if India is to reconcile effective digital governance with the fundamental right to privacy.***

Keywords: Data Privacy, Digital Personal Data Protection Act, 2023, K.S. Puttaswamy, Consent, State Surveillance, GDPR

1. Introduction

The rapid digitization of society has transformed personal data into a critical asset, raising urgent privacy concerns. As governments and companies collect vast quantities of information for welfare, security, and commercial purposes, individuals face unprecedented risks of profiling, surveillance, and misuse of their data. In India, this tension came to the fore with the Supreme Court's unanimous decision in *Justice K.S. Puttaswamy (Retd.) v. Union of India*,[1] which recognized privacy as a fundamental right under Article 21. The Court held that privacy encompasses informational autonomy and human dignity, and it imposed a strict proportionality test on state intrusions. Concurrently, nations worldwide enacted comprehensive data protection laws; notably, the EU's General Data Protection Regulation (GDPR) is widely regarded as the global benchmark for data privacy.

Building on these developments, India's Parliament enacted the *Digital Personal Data Protection Act, 2023* (DPDP Act) on 11 August 2023. By its own Preamble, the Act "recognizes both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes." [2] It imposes a consent-based regime on companies (data fiduciaries) and enumerates certain rights for individuals (data principals). However, observers note a critical caveat: the Act grants broad exemptions to the State, allowing government agencies to bypass many core obligations on general grounds of sovereignty, security, or public order. This has raised questions about whether the DPDP Act faithfully implements the *Puttaswamy* standards and how it aligns with international norms.

This study conducts a deep dive into these issues. We map the constitutional background of privacy in India and outline the new legal framework (including the IT Act 2000 provisions and the DPDP Act).[3] We then analyze the DPDP Act's key features and fault lines: its consent model, fiduciary duties (like security safeguards and breach notification), and special regimes (e.g. for children and "significant" data fiduciaries). A focal point is the Act's State exemptions – whether they comply with *Puttaswamy*'s necessity and proportionality requirements or risk diluting privacy in practice.[4] We contrast India's approach with the GDPR's, noting common principles but crucial differences in scope, rights, and enforcement. Finally, we identify emerging challenges (AI, biometric data, children's privacy) and propose reforms. Throughout, we ground our analysis in connected legal sources and scholarship to ensure accuracy and depth.

2. Objectives and Research Questions

The primary objective is to assess India's DPDP Act considering constitutional privacy norms and global standards. Concretely, we address questions such as: (i) Does the Act align with the fundamental right to privacy as articulated in *Puttaswamy* (i.e., is state data collection subject to strict justification)? (ii) How does the new law compare with the GDPR and other international frameworks in terms of individual rights, consent requirements, and enforcement mechanisms? (iii) What gaps or conflicts arise

in the DPDP Act's provisions – especially regarding state surveillance, technological risks (profiling/AI), and corporate data practices? (iv) How might Indian data protection be strengthened to safeguard autonomy and dignity?[5] [6]

To answer these, we examine: constitutional judgments (notably *Puttaswamy I & II*), the DPDP Act text, and established statutes (IT Act 2000 and rules). We also draw on scholarly analyses and policy documents that critique or explain the DPDP Act. A comparative lens with the GDPR helps identify best practices (e.g., rights to portability, strict data minimization) that India could emulate. By integrating doctrinal study with policy review, the paper aims to offer a comprehensive understanding of India's evolving data privacy regime. [7] [8] [9]

3. Methodology

This research adopts a doctrinal legal approach combined with comparative analysis. We analyze constitutional provisions (Articles 21, 19) and Supreme Court jurisprudence, including pre-*Puttaswamy* cases (like *M.P. Sharma* and *Kharak Singh*) and landmark judgments (*Puttaswamy* 2017 and the *Aadhaar* decision in 2019). [10] [11] [12] The statutory framework the DPDP Act 2023 and its rules is examined in detail, alongside the IT Act 2000 and its data protection rules. We review the text of GDPR (EU Regulation 2016/679) for comparison, as well as academic commentary (law journal articles, government reports) on privacy and DPDP. Key terms and definitions from the Act are considered, and provision-by-provision analysis is performed, especially focusing on consent, exemptions, and fiduciary duties. [13] [14] [15] Comparative insights are drawn from authoritative analyses (e.g., Latham & Watkins comparison, law review critiques) to highlight differences and lessons. This blend of statutory and case law analysis aims to identify both legal conflicts and normative benchmarks. [16] [17]

4. Evolution of Privacy in Indian Law

4.1 Pre-*Puttaswamy* Landscape

For much of India's constitutional history, the right to privacy had no explicit recognition. Early Supreme Court cases like *M.P. Sharma v. Satish Chandra* (1954) and *Kharak Singh v. State of U.P.* (1963) outright denied a freestanding privacy right. [18] [19] These rulings viewed privacy as merely implicit in other liberties, vulnerable to broad state exceptions. Although later decisions cautiously acknowledged privacy interests in contexts like telephone tapping or medical confidentiality, there was no settled doctrine. As Justice Seervai observed, this "fragmented recognition" left individuals exposed to unchecked state surveillance, especially as innovative technologies emerged. [20] [21]

4.2 *K.S. Puttaswamy v. Union of India* (2017) and Aftermath

This changed radically with *Puttaswamy I* (2017), where a nine-judge bench unanimously held that privacy is a fundamental right under Article 21. The Court conceptualized privacy not just as "freedom from intrusion," but as essential to autonomy, dignity, and democratic participation. Crucially, it overruled past precedents and imposed a structured proportionality test: any state data collection or surveillance must be lawful, necessary, and narrowly tailored. The judgment explicitly envisaged "informational privacy" individuals' control over their personal data as a constitutional foundation. [22] [23]

In *Puttaswamy II* (the Aadhaar case, 2019), the Court reaffirmed that digital identity programs must respect privacy, striking down indiscriminate collection of biometric data. It emphasized that even welfare schemes cannot override privacy without rigorous safeguards. These jurisprudential developments set a high bar: the state must justify any coercive handling of personal data, and individuals gain a right to informational self-determination. The Supreme Court also noted that rights like free speech (Art.19) and privacy must be balanced through reasonable restrictions, underscoring that privacy is not absolute. The *Puttaswamy* framework thus became the constitutional benchmark for all future data protection law in India. [24] [25] [26]

5. Indian Legal Framework for Data Privacy

Before 2023, India's data protection obligations were scattered across statutes. The Information Technology Act, 2000 and its rules provided limited safeguards. Notably, Section 43A of the IT Act made corporate entities liable to compensate individuals for failure to protect "sensitive personal data or information," and the 2011 SPDI Rules required companies (including social media platforms) to have privacy policies and implement "reasonable security practices".[27] [28] Section 72A even criminalized unauthorized disclosure of personal information in breach of a lawful contract. These provisions were sectoral and modest: for example, 43A offered only civil remedies for data breaches. They lacked general regulatory authority or a comprehensive rights framework.

The Digital Personal Data Protection Act 2023 (DPDP Act) overhauled this regime. It applies broadly to *digital* personal data processed in India, as well as to processing outside India connected to offering goods or services to individuals in India. (Notably, non-digital offline data remains outside its scope.) Under the Act, every Data Principal (the individual to whom data relates) is entitled to certain rights, and every Data Fiduciary (the person determining the purpose and means of data processing) has correlative duties. [29] [30] [31]

Key features of the DPDP Act include:

- **Consent and Notice:** Personal data can be processed only with the data principal's free, specific, informed, and unambiguous consent. Data fiduciaries must provide clear notice of purpose before seeking consent. The Act's consent standard mirrors GDPR's emphasis on informed choice. Consent can be withdrawn anytime, triggering deletion of the data unless retention is required by law. [32]

- **Data Principal Rights:** The Act enumerates rights including access to information about processing, correction and erasure of one's data, grievance redress, and nomination of a representative if the person is incapacitated. However, unlike GDPR, it does not explicitly grant a general data portability right or a broad right to object to processing. [33]
- **Fiduciary Obligations:** Data fiduciaries must ensure the accuracy, completeness, and consistency of data they use (especially if it affects decisions about a person), and implement appropriate technical and organizational measures to safeguard data. They are required to notify both the Data Protection Board and affected individuals of any data breach. Importantly, once the purpose of processing is fulfilled or consent is withdrawn, the fiduciary must erase the personal data (subject only to narrow legal exceptions).
- **Significant Data Fiduciaries:** The government may designate certain large or sensitive entities as "significant." These must take extra steps, such as appointing a Data Protection Officer (to oversee compliance and liaise with authorities), conducting periodic data-protection impact assessments, and undergoing independent audits. [34]
- **Children's Data:** The Act defines a *child* as anyone under eighteen and requires verifiable parental consent for processing a child's data Crucially, it prohibits any tracking, behavioral monitoring, or targeted advertising directed at children. These provisions aim to offer heightened protection for minors' privacy. [35]
- **Regulatory Authority:** A *Data Protection Board of India* is established as the primary regulator. It can enforce compliance, impose penalties, and issue guidance. However, scholars have raised concerns about its independence, noting that executive control over appointments could undermine impartiality. [36] [37]
- **Exemptions for the State:** Most strikingly, the Act exempts the government and its agencies from core obligations on broad grounds. Under Section 18, the Central Government may exempt any public body from any data-protection duty if it deems the purpose falls under sovereignty, security, public order, etc. These exemption clauses lack clear definitions or oversight mechanisms, a point to which we return. [38] [39]

In sum, the DPDP Act creates a structured, rights-and-duties framework for personal data in India, reflecting modern privacy principles. It goes well beyond the IT Act by codifying consent requirements and fiduciary duties. But some design choices, especially regarding state power and individual rights scope will determine how effective it is in practice. [40]

6. Critical Analysis of the DPDP Act, 2023

The DPDP Act adopts many internationally recognized principles (inspired by the GDPR), but its execution is mixed.

- **Consent-Based Model:** The Act firmly places *informational self-determination* at its core. Consent is defined to be "free, specific, informed, unconditional and unambiguous." Processing of personal data is allowed only for the purposes consented to by the data principal unless a statutory exception applies. In practice, this means organizations must design processes around obtaining clear consent and providing full transparency. The Act acknowledges the importance of individual choice: indeed, commentators note that it marks a shift toward individual control, recognizing "informational self-determination as a foundational principle."
- **Enumerated Rights:** To support consent, the DPDP Act grants data principals' rights like those in GDPR, albeit limited. Data principals can access the data held about them, request corrections, or deletion, and seek redress for grievances. There is also a novel right to nominate a representative (e.g., for a deceased person's data). This set of rights enhances transparency and accountability in data processing. However, there are notable gaps remaining. The Act does *not* guarantee a broad right to data portability or a general right to object to processing, both of which are key features of GDPR that empower individuals. In effect, an Indian individual's agency is strong in refusing consent and erasing data, but weaker in transferring data between services or halting processing for other reasons. [41]
- **Fiduciary Duties:** Companies (data fiduciaries) face concrete obligations under the Act. They must ensure data accuracy when it affects decisions, implement "appropriate technical and organisational measures," and take "reasonable security safeguards to prevent personal data breach." This includes notifying the Board and affected individuals of any breach. There are penalties for non-compliance, with fines that can reach remarkably elevated levels (e.g., up to INR 2.5 billion or about €23.5M). The requirement to erase data after consent withdrawal or completion of purpose is particularly important for data minimization. These provisions align with global best practices: in GDPR, data controllers must also ensure accuracy, security, and breach notification.

Areas of Concern: Several features of the DPDP Act raise red flags considering privacy principles:

- **No Legitimate Interest Clause:** Unlike the GDPR, the DPDP Act does not recognize a broad "legitimate interest" basis for processing. Instead, it allows only certain legitimate use (e.g., voluntary data sharing, compliance with law, employment purposes, medical emergencies). This narrower basis means that any processing outside explicit consent or listed exceptions is impermissible, which is privacy-protective in theory but can limit flexibility. Conversely, it could encourage broad invocation of these exceptions.
- **Limited Individual Rights:** As noted, the omission of portability and objection rights weakens individual control. Additionally, the Act does not explicitly articulate a right to be forgotten in the GDPR sense (beyond erasure upon consent withdrawal). There is also no explicit collective redress or public-interest reporting mechanism.
- **Significant Data Fiduciary Framework:** Designating big platforms as "significant" is positive, but the criteria and enforcement remain unclear. In principle, significant fiduciaries must appoint a Data Protection Officer and conduct regular impact assessments and

audits. In practice, until rules specify the classes of entities, this power is latent.

- **Data Protection Board:** The establishment of a regulatory board is necessary. However, its executive-centric structure is worrisome. The Board can enforce penalties and guidelines, but scholars warn that lack of tenure security and government control may compromise its independence. An independent authority is essential for impartial enforcement (as GDPR experience shows).
- **Exemption Clauses:** The most controversial aspect is the Act's treatment of the State as a data fiduciary. On paper, governmental bodies are bound by the same principles as private actors. Section 18 allows the central government to exempt any public authority from any obligation of the Act on broadly defined grounds (sovereignty, integrity, security, public order, etc.). These grounds are not clearly defined, and the Act imposes no mandatory review or approval process. As a result, the executive has "wide latitude to determine the scope of its own data protection obligations." [42]
- **This flip-flops the logic of Puttaswamy:** whereas private companies are stringently regulated, the State may choose to avoid safeguards. Critics note that this "reverses the logic" that should apply to the State, which wields coercive power and ought to be subject to even greater accountability. Indeed, while the Act rhetorically acknowledges state processing, its substantive design privileges administrative convenience. Comparative experience suggests that security or public order exceptions must be narrowly tailored. For example, *Puttaswamy* requires any data-driven government program to demonstrate a pressing need and adopt the least invasive means. The DPDP Act's blanket exemptions threaten to "de-center privacy" precisely where constitutional protection is most needed. [43]

In summary, the DPDP Act embodies a mix of progress and pitfalls. It advances India's private-sector data protection by codifying modern norms (consent, purpose limitation, security) and imposing significant fines. Yet it falls short in curbing state surveillance and fully empowering individuals. As one study observes, the Act "strengthens data protection vis-à-vis private actors" but "falls short in adequately constraining State power." The next sections explore these constitutional and comparative dimensions in detail.

7. Data Privacy and State Surveillance

India's state has launched ambitious digitization projects (e.g., Aadhaar, health IDs, welfare databases). These involve compulsory biometric and demographic data collection on millions, raising privacy risks. Under *Puttaswamy*, such schemes must satisfy legality, necessity, and proportionality. However, the DPDP Act's broad exemptions effectively insulate many government systems from these principles. [44]

For instance, the Act allows the government to declare any state agency exempt from *any* obligation, simply by deeming its purpose within undefined national interest categories. These categories (sovereignty, security, public order) are so sweeping that they could cover routine data gathering. There is no statutory requirement for the government to justify each exemption through a compelling test. As commentators note, this creates a "two-tiered" system: private entities face stringent rules, while the State can "opt out of core safeguards."

The constitutional implications are stark. Without independent oversight, "routine data collection can be retrospectively justified under the umbrella of security," as the exemption language permits indiscriminate justification. Similarly, any data processing claims to be in the interest of public order or sovereignty escapes scrutiny. In practice, this means that citizens may have no legal recourse if a state program collects or processes their data without consent, if the government invokes an exemption. This undermines the *Puttaswamy* mandate that privacy rights must yield only to concrete and narrowly tailored State objectives.

Given India's history of surveillance (from telephone tapping to social media monitoring), many fear these provisions could legalize excessive profiling. Scholars urge that safeguards such as judicial authorization, prior impact assessments, or mandatory review be imposed on any state surveillance activities. In their absence, the DPDP Act's state clauses risk normalizing unchecked data-driven governance. It is thus essential to scrutinize and constrain these powers to uphold the constitutional balance. [45]

8. Data Privacy and Private Corporations

On the corporate side, digital platforms and data brokers hold vast personal information. Business models now often depend on targeted advertising, algorithmic profiling, and cross-selling of user data. The DPDP Act addresses this to an extent: it requires companies to adhere to purpose limitation, obtain valid consent, and protect data with security measures. Significant fiduciaries (e.g., large tech companies) will have to appoint officers and conduct audits, potentially increasing accountability. [46]

However, several challenges remain:

- **Information Asymmetry and Behavioral Profiling:** Individuals typically lack transparency about how their data is collected and used by algorithms. The Act improves transparency (through mandatory privacy notices) but does not fully close the information gap. For example, it obliges fiduciaries to secure data and report breaches, but it does not require them to explain automated decision-making processes to users. In practice, users may still consent blindly to complex terms. The Act's consent requirement (free, informed consent with clear opt-in) attempts to empower users, but in a world of asymmetric information, genuine consent is hard to ensure.
- **Limited Remedies for Abuse:** If a private firm misuses data (say, covertly transfers it to affiliates, or employs it for undesired profiling), the only recourse is through the Data Protection Board. The Act permits penalties for fiduciaries that violate obligations, but individual remedies (beyond erasure/correction) are limited. There is no class-action mechanism for systemic corporate abuse.

- **Children and Vulnerable Groups:** The DPDP Act makes strong provisions here. As noted, it bans targeted advertising to children and requires parental consent for their data. This goes beyond many laws globally and is a positive step. It reflects recognition that minors are especially vulnerable to exploitation by algorithms. [47]

In sum, the Act gives private entities clear rules to follow, but it does not fundamentally alter the corporate incentive to collect data. Indian tech giants and foreign platforms operating in India will need to overhaul compliance (especially for security and consent), but the law stops short of regulating business models themselves. Ongoing oversight and perhaps competition or consumer law interventions may be needed to ensure that companies do not skirt the spirit of privacy protection.

9. Comparative Analysis: India vs. GDPR

India's DPDP Act was explicitly inspired by global norms. A detailed comparison highlights both convergence and divergence from the EU's GDPR.

- **Scope:** The GDPR applies broadly to *any* personal data of EU residents, whether processed inside or outside the EU. It covers *sensitive personal data* (health, genetic, biometric) with extra care. In contrast, the DPDP Act applies primarily to "digital personal data" processed in India, or data of Indians processed abroad in connection with services. Notably, *purely offline* data (e.g., paper records) falls outside its ambit. Also, the DPDP Act excludes data that the principal themselves has made publicly available. In short, GDPR is more expansive in data scope and geography; India's law is narrower (though still covering most modern data flows). [48]
- **Individual Rights:** Both regimes guarantee core rights of data subjects. Like GDPR, the DPDP Act gives rights to access, rectify, erase personal data, and to complain to authorities. However, GDPR explicitly includes additional rights such as data portability (the right to transfer data to another service) and a general right to object to processing. The Indian Act has neither. It does create a unique right to nominate a representative, which GDPR does not have. Thus, GDPR is somewhat stronger on user empowerment. [49]
- **Legal Bases for Processing:** Under GDPR, data may be processed on several lawful bases: consent, contract performance, legal obligation, vital interests, public task, or *legitimate interests*. The DPDP Act recognizes only *consent* and a limited list of "legitimate uses" (e.g., compliance with law, emergencies). Importantly, there is no open-ended "legitimate interests" clause. This makes the Indian law more restrictive: any processing outside the enumerated grounds is effectively disallowed.
- **Consent Standard:** Both laws require "unambiguous" consent with clear affirmative action. The DPDP Act explicitly requires consent to be "free, informed, specific, and unambiguous," mirroring GDPR's standard.
- **Exemptions for Government:** GDPR has no blanket exemptions for state surveillance; it applies even to public authorities (with some nuance for national security, which EU law generally leaves to member states). The DPDP Act's expansive state exemptions have no close GDPR counterpart. In fact, global practice would consider India's approach unusual. Other democracies subject government data collection to stringent checks (often through separate surveillance laws or judicial warrants).
- **Cross-Border Data Transfers:** GDPR strictly regulates transfers outside the EU, requiring adequate protection or binding mechanisms. The DPDP Act also addresses cross-border flows: it permits transfers to countries on a (so far unannounced) restricted list. The government must set conditions by notification for transfers, but at present no countries have been specified. In practice, this means Indian companies may transfer data abroad freely, unless future lists restrict certain nations.
- **Enforcement:** GDPR is enforced by independent Data Protection Authorities in each country, with significant investigatory powers and fines up to 4% of global annual turnover. The DPDP Act allows fines up to ₹250 crore (about €30M) for certain breaches, which could be lower or higher depending on the company size. The Indian Data Protection Board is empowered to impose penalties and direct corrective measures. However, its structural independence is doubtful. In contrast, GDPR authorities are required to be institutionally separate from government.

In summary, the DPDP Act embodies many GDPR-like principles, but with key differences: its geographical scope is more limited, it lacks some data subject rights, and it allows broader state discretion. As one analysis notes, India's law "aligns with global standards like GDPR" in aspiration, yet "differences exist in scope, user rights, [and] enforcement mechanisms." Indian regulators and courts will therefore play a crucial role in filling gaps and interpreting the law in line with international benchmarks.

10. Emerging Challenges in Data Privacy

The digital landscape is evolving rapidly, raising new privacy challenges that the law must address over time. Prominent issues include:

- **Artificial Intelligence and Automated Profiling:** AI systems can analyze personal data to make predictions or decisions about individuals (for credit, job screening, policing, etc.). This raises concerns about lack of transparency and potential bias. The DPDP Act does not explicitly regulate AI or profiling, but its principles apply: for instance, use of personal data for profiling would require clear consent and purpose. Judicial and regulatory clarification may be needed on how automated decision-making is handled (as GDPR's Article 22 does). [50]
- **Biometrics and Surveillance Technology:** Technologies like facial recognition, gait analysis, or big data analytics can identify individuals in public spaces without their knowledge. Such surveillance tools challenge the notion of anonymity in public. India has already experimented with biometric ID (Aadhaar). Privacy experts warn that unchecked state or private use of such tech could violate autonomy. The DPDP Act's applicability to biometric data depends on whether it is in digital form (it usually is). Any covert use of biometrics by government would have to rely on the Act's state

exemptions, underscoring the need for judicial oversight. [51]

- **Data Re-identification and Aggregation Risks:** Even anonymized datasets can sometimes be re-identified when combined with other information. This poses a risk that goes beyond straightforward consent models. Legislatures may need to develop stronger data minimization and anonymization standards to counter this threat.
- **Children's Online Privacy:** As noted, the DPDP Act takes a strong stance on children's data: it forbids profiling or targeted ads towards minors and requires parental consent. Globally, protecting children's digital privacy is a key concern. Ensuring that these provisions are enforced (e.g., through age verification and penalties for violations) will be important.
- **Emerging Sectoral Uses:** New applications (health wearables, smart education, smart cities) gather sensitive data. The law will have to adapt to ensure privacy is built in. For example, location tracking and IoT devices pose constant surveillance risks. Embedding privacy-by-design – as recommended below – will be critical to meet these challenges.

While some of these issues are not yet squarely addressed in legislation, India's constitutional commitment to privacy provides a guiding framework. Courts and regulators will evolve the law (or rules under it) to tackle novel technologies, ideally in dialogue with global developments.

11. Privacy and Freedom of Expression

In India's constitutional scheme, the right to privacy coexists with fundamental freedoms of speech and the press (Article 19). Neither right is absolute, and they must be balanced through the proportionality principle laid down in *Puttaswamy*. For instance, investigative journalism often involves publishing personal information. The privacy right cannot be used as a "shield" to suppress legitimate public interest disclosures. Conversely, freedom of expression does not justify arbitrary violation of privacy. [52]

The DPDP Act does not expressly specify how to handle such conflicts. Implicitly, legitimate uses include news reporting, but there is no carve-out clause. In practice, resolving these tensions will fall to the courts, which will have to weigh privacy under Article 21 against Article 19(1)(a) on a case-by-case basis, using the same proportionality framework. The Act should thus be interpreted in harmony with the Right to Information and free-speech guarantees. Future case law may clarify, for example, that publishing personal data in the public domain (e.g., MP lists, crime data) may not violate consent requirements, whereas commercial exploitation of personal details without consent would. [53]

12. Key Findings

Our analysis reveals several key insights:

- **Constitutional Alignment:** The DPDP Act partially operationalizes *Puttaswamy*, but not fully. It institutionalizes the consent principle and some informational autonomy, yet its broad state exemptions and lack of strict procedural safeguards suggest a gap between constitutional ideals and statutory practice. Without reform, there is a risk that in contexts like welfare databases or national security, privacy protections become nominal. [54]
- **Rights vs State Power Imbalance:** The law clearly enhances rights against private misuse of data – individuals can withdraw consent, demand erasure, and authorities can fine errantly companies. However, when it comes to government data practices, the balance tips in the opposite direction. The Act's architecture effectively allows the state to self-certify its own compliance, which undermines the "transformative promise" of *Puttaswamy* in protecting citizens from overreaching surveillance. As one critique puts it, while the Act "introduces a long-overdue statutory architecture for personal data protection," its exemptions "risk de-centering privacy." [55]
- **Comparative Gaps:** Relative to the GDPR, India's regime has a narrower scope (digital data only) and omits some user-friendly rights (portability, objection). India's enforcement machinery is still nascent. For instance, GDPR authorities have issued guidance on AI and are actively fining non-compliant firms; India's Data Protection Board is not yet fully functional and may rely on administrative controls. On the positive side, India's prohibition on child profiling goes beyond what GDPR mandates (though GDPR also restricts automated profiling of minors by default). [56]
- **Technological and Social Challenges:** Emerging technologies (AI, IoT, surveillance tools) and social changes (e.g., more online services) will continually test the law. The Act's effectiveness will depend on detailed rules and guidelines issued by the Board and on judicial interpretation to keep pace with innovation. A forward-looking finding is that legal principles like necessity and data minimization must be embedded early in system design ("privacy by design") to truly protect individual autonomy in the digital era. [57]

13. Recommendations

To address the gaps identified, we propose several reforms:

1) **Narrow and Define State Exemptions:** The exemption clauses should be curtailed. Grounds like "national security" or "public order" must be defined with clear criteria and limited in duration. For example, an amendment could require that any exemption from core obligations must specify a concrete threat and include a sunset clause. Alternatively, the Act could mandate prior judicial or parliamentary review of such exemptions. [58]
2) **Codify Proportionality:** The statute should explicitly incorporate a proportionality requirement for state data collection. This could take the form of a written necessity and proportionality assessment for any major government program, demonstrating why less intrusive methods are inadequate. Embedding these tests in law would translate the *Puttaswamy* framework into enforceable standards. [59]
3) **Strengthen Oversight Institutions:** The Data Protection Board of India must be made fully independent. Appointment processes should be

transparent, terms of office secured, and funding protected. Importantly, its mandate should explicitly include oversight of state data practices, not just enforcement against private entities. Supplementary bodies (e.g., parliamentary committees with technical advisers) could review government data initiatives, and an independent audit regime could be imposed on public databases.

4) **Enhance Individual Rights:** Consider introducing additional rights to match global norms. For instance, adding a right to data portability and a general right to object (with appropriate safeguards) would empower users and improve interoperability. Similarly, establishing clear consequences for breaches of specific rights (beyond general penalties) could provide better remedies.
5) **Transparency and Public Participation:** The government should mandate regular transparency reports on data usage. Any state agency invoking an exemption should publish anonymized statistics or rationales to enable democratic scrutiny. More broadly, privacy impact assessments and algorithmic transparency reports (subject to narrow confidentiality rules) should be required for significant digital projects. Involving the public (through consultations and complaints portals) can ensure the law evolves with citizens' interests.
6) **Data Minimization and Design Principles:** Both government and industry should adopt privacy-by-design: limit data collection to what is strictly needed, anonymize data whenever possible, and build privacy safeguards into technology from the outset. This may require new standards or guidelines (for example, sectoral rules for health data or education data).
7) **Education and Awareness:** Finally, empowering individuals through education about data rights is crucial. People should understand how to manage consent and seek redress. Civil society and academia can play a role in raising awareness of privacy and shaping norms.

Implementing these measures would move India's legal framework closer to both its constitutional ideals and international best practices. As constitutional scholars stress, "privacy should be treated as an enabling condition for dignity, autonomy and democratic participation, not as a regulatory obstacle."

14. Conclusion

India stands at a pivotal moment in data governance. The *Puttaswamy* judgment established that privacy is a structural constitutional guarantee, providing tools of legality, necessity, proportionality, and due process to reconcile individual rights with societal needs. The Digital Personal Data Protection Act, 2023 is a landmark legislative response: it acknowledges that citizens have rights over their data and that misuse by corporations must be checked. On the other hand, its broad carve-outs for the State risk undermining the very privacy rights *Puttaswamy* sought to protect. [60]

Our deep-dive analysis finds that without course correction; there is a danger of "erosion" of privacy through executive convenience. Conversely, aligning the Act with constitutional values can strengthen India's democracy in the digital era. This means not only tightening legal rules (as recommended above) but also fostering a culture of privacy-by-default and transparency. If India treats data protection as complementary to good governance rather than as a hindrance it can achieve both innovation and individual dignity. As *Puttaswamy* teaches, the legitimacy of data-driven policies rests on safeguarding fundamental rights. The true test of the DPDP Act will be whether future courts and regulators interpret it in the spirit of *Puttaswamy*, ensuring that "effective governance and constitutional fidelity are mutually reinforcing." [61] [62]

References

[1] Guruswamy M, "Justice K.S. Puttaswamy (Ret'd) and Anr v. Union of India and Ors" (2017) 111 American Journal of International Law 994 https://www.cambridge.org/core/journals/american-journal-of-international-law/article/abs/justice-ks-puttaswamy-retd-and-anr-v-union-of-india-and-ors/ED631B8F922039BEC5400086C8E34338
[2] Chail A and Lahel RS, "India's DPDP Act 2023 and Draft DPDP Rules 2025: Operational Considerations for Hospitals" (2026) 15 Journal of Dr. YSR University of Health Sciences. 4 https://doi.org/10.4103/jdrntruhs.jdrntruhs_107_25
[3] Garg A and Pathak SN, "Privacy Rights in India: Evolution, Legal Developments, and Contemporary Challenges in the Digital Age" [2025] Zenodo (CERN European Organization for Nuclear Research) https://zenodo.org/records/17937575
[4] Sahoo AS, "From Puttaswamy to DPDP: Tracing the Legislative Journey of Data Privacy in India" [2026] International Journal of Science and Research (IJSR) 1012 https://www.ijsr.net/getabstract.php?paperid=SR26317112521
[5] Malhotra C and Malhotra U, "Putting Interests of Digital Nagriks First: Digital Personal Data Protection (DPDP) Act 2023 of India" (2024) 70 Indian Journal of Public Administration 516 https://doi.org/10.1177/00195561241271575
[6] Parashar C, "Governing Data in Corporations; A Critical Analysis of DPDP Act 2023 and Its Compliance Lacunas" [2026] Open MIND https://zenodo.org/records/18606326
[7] Yadav V, "Crossing Borders: Comparative Perspectives on Data Protection Laws in India, the EU, and the US" (2025) 1 Journal on Development of Intellectual Property and Research 38 https://journal.cdipr.ac.in/index.php/jdipr/article/view/40
[8] "DATA PROTECTION IN INDIA AFTER THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023: A CRITICAL EVALUATION OF PRIVACY AND STATE POWER – Indian Journal of Legal Review [ISSN – 2583-2344]" https://ijlr.iledu.in/v6i114/
[9] Nair A, "From IT Act to Data Protection: A Comparative Socio-Technological Study of India's Response to Cybercrime" (2025) 7 International

Journal for Multidisciplinary Research https://www.ijfmr.com/research-paper.php?id=56159
[10] Sandhu P and others, "Safeguarding Privacy in the Age of Artificial Intelligence: Legal Implications and Challenges" (2025) 3 International Research Journal on Advanced Engineering and Management (IRJAEM) 2256 https://goldncloudpublications.com/index.php/irjaem/article/view/1052
[11] Lakra R and Shrivastava A, "Confronting the Metadata Dilemma in India: A Turn to Context and Proportionality" (2024) 32 International Journal of Law and Information Technology https://doi.org/10.1093/ijlit/eaae012
[12] "Safeguarding Privacy in the Age of Artificial Intelligence: Legal Implications and Challenges" (2025) 3 International Research Journal on Advanced Engineering and Management (IRJAEM) 2256 https://goldncloudpublications.com/index.php/irjaem/article/view/1052
[13] Bhushan V, "EMPOWERING INDIVIDUALS: A DEEP DIVE INTO THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023" (2024) 12 International Journal of Advanced Research 891 https://www.journalijar.com/article/48771/empowering-individuals:-a-deep-dive-into-the-digital-personal-data-protection-act,-2023/
[14] Saha S and Mukhopadhyay S, "A New Age of Data Privacy Laws in India: Review of Digital Personal Data Protection Act, 2023" [2024] International Journal of Law and Social Sciences 84 https://www.journalsalliancepub.com/index.php/ijls/article/view/114
[15] "OSF" https://osf.io/preprints/lawarchive/r7ydq_v1
[16] Kuhar A, "A Comparative Analysisof Data Protection Laws in India, UK, and the USA. From Consent to Compliance" (2025) 7 International Journal for Multidisciplinary Research https://www.ijfmr.com/research-paper.php?id=45887
[17] Abiad HA and Masadeh A, "Law Comparison as a Research Method in Legal Studies, and Its Importance in Promoting Uniformity in Legal Systems" [2024] Lecture Notes in Civil Engineering 446 https://doi.org/10.1007/978-3-031-56121-4_42
[18] Dubey K and Singh J, "The Right to Privacy in India: Evolution and Developments" (2025) 7 International Journal for Multidisciplinary Research https://www.ijfmr.com/research-paper.php?id=42002
[19] Dalal P and Richa, "The Right to Privacy in India: Historical Evolution and Contemporary Challenges in the Digital Age" (2025) 10 RESEARCH REVIEW International Journal of Multidisciplinary 46 https://old1.rrjournals.com/index.php/rrijm/article/view/1709
[20] "The Right to Privacy in India: Historical Evolution and Contemporary Challenges in the Digital Age" (2025) 10 RESEARCH REVIEW International Journal of Multidisciplinary 46 https://old1.rrjournals.com/index.php/rrijm/article/view/1709
[21] Tripathi S, "JUSTICE K.S. PUTTASWAMY (RETD.) AND ANR. VS. UNION OF INDIA AND ORS. (2017) 10 SCC 1" [2026] Open MIND https://zenodo.org/records/18986900
[22] Parmar B, "K.S. Puttaswamy v. Union of India" [2026] Open MIND https://zenodo.org/records/18987178
[23] Bioni BR and others, "A Landmark Ruling from the Brazilian Supreme Court: Data Protection as an Autonomous Fundamental Right and Informational Due Process" (2020) 6 European Data Protection Law Review 615 https://edpl.lexxion.eu/article/EDPL/2020/4/21
[24] "Justice K.S. Puttaswamy (Ret'd) and Anr v. Union of India and Ors" (2017) 111 American Journal of International Law 994 https://www.cambridge.org/core/journals/american-journal-of-international-law/article/abs/justice-ks-puttaswamy-retd-and-anr-v-union-of-india-and-ors/ED631B8F922039BEC5400086C8E34338
[25] Kamboj A, "Judicial Response to Personal Data Protection in India" (2025) 7 International Journal for Multidisciplinary Research https://www.ijfmr.com/research-paper.php?id=59926
[26] Saji A, "Data Protection and Privacy Laws in India" [2026] Open MIND https://zenodo.org/records/18990711
[27] Chaudhary J, "Enhancing Data Privacy in Cyberspace: A Comprehensive Study on Strategies, Regulations, and Technologies" (December 28, 2024) https://jisem-journal.com/index.php/journal/article/view/9334
[28] Sharma N and Kumar A, "Legal Framework for Developing and Implementing Robust Cybersecurity Policies in India" [2024] Journal for ReAttach Therapy and Developmental Diversities https://jrtdd.com/index.php/journal/article/view/2738
[29] Gaurav, Ayarekar DrS and Kadam DrS, "A Comparative Legal and Regulatory Analysis of India's Digital Personal Data Protection Act (2023) and the EU GDPR: Implications for FinTech Governance and Audit Automation" [2025] Zenodo (CERN European Organization for Nuclear Research) https://zenodo.org/records/18063751
[30] Yadav R, "THE FIDUCIARY LIABILITY OF CONSENT MANAGERS: STATUTORY DUTIES VS. TORTIOUS NEGLIGENCE UNDER THE DIGITAL PERSONAL DATA PROTECTION ACT 2023" [2026] Open MIND https://zenodo.org/records/18771708
[31] Christopher D and others, "India's Data Protection Regime Notified: Overview of the Act and Rules" (November 1, 2025) https://kluwerlawonline.com/journalarticle/Global+Privacy+Law+Review/6.1/GPLR2025023
[32] Chaurasiya VR and Chaurasiya VR, "CONSENT MECHANISMS UNDER THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023: A COMPARATIVE LEGAL ANALYSIS WITH GDPR AND CCPA/CPRA - LIJDLR" (LIJDLR - India's Most Indexed Legal Journal in Global Databases, June 26, 2025) https://lijdlr.com/2025/06/26/consent-mechanisms-under-the-digital-personal-data-protection-act-2023-a-comparative-legal-analysis-with-gdpr-and-ccpa-cpra/

[33] Sim J and others, "Technical Requirements and Approaches in Personal Data Control" (2022) 55 ACM Computing Surveys 1 https://doi.org/10.1145/3558766
[34] "Investigating Data Protection Compliance Challenges| International Journal of Innovative Science and Research Technology" https://www.ijisrt.com/investigating-data-protection-compliance-challenges
[35] Macenaite M and Kosta E, "Consent for Processing Children's Personal Data in the EU: Following in US Footsteps?" (2017) 26 Information & Communications Technology Law 146 https://doi.org/10.1080/13600834.2017.1321096
[36] Kumar AP, "The Digital Personal Data Protection Board: Persisting Questions of Constitutionality" (Economic and Political Weekly, March 12, 2025) https://www.epw.in/journal/2025/3/law-and-society/digital-personal-data-protection-board.html
[37] Saurabh S, "THE DIGITAL PERSONAL DATA PROTECTION ACT OF 2023: STRENGTHENING PRIVACY IN THE DIGITAL AGE" (2024) 3 International Journal of Law in Changing World 77 https://ijlcw.emnuvens.com.br/revista/article/view/84
[38] Kolanu M, Lakra R and Shrivastava A, "Data, Control, and Power: Decoding India's Digital Personal Data Protection Act, 2023" (November 1, 2025) https://kluwerlawonline.com/journalarticle/Global+Privacy+Law+Review/6.1/GPLR2026002
[39] Bhandari V and Sane R, "Protecting Citizens from the State Post Puttaswamy: Analysing the Privacy Implications of the Justice Srikrishna Committee Report and the Data Protection Bill, 2018" (Scholarship Repository) https://repository.nls.ac.in/slr/vol14/iss2/1/
[40] Mahajan G, "India's Emerging Data Protection Framework: A Critical Analysis of Legal Reform and Global Interoperability" (HSTalks, March 1, 2026) https://hstalks.com/article/11030/indias-emerging-data-protection-framework-a-critic/?business
[41] "A Comparative Legal and Regulatory Analysis of India's Digital Personal Data Protection Act (2023) and the EU GDPR: Implications for FinTech Governance and Audit Automation" [2025] Zenodo (CERN European Organization for Nuclear Research) https://zenodo.org/records/18063751
[42] Rahman F, "SAFEGUARDING PERSONAL DATA IN THE PUBLIC SECTOR: UNVEILING THE IMPACT OF THE NEW PERSONAL DATA PROTECTION ACT IN INDONESIA" (2025) 16 UUM Journal of Legal Studies 1 https://e-journal.uum.edu.my/index.php/uumjls/article/view/20361
[43] "Data, Control, and Power: Decoding India's Digital Personal Data Protection Act, 2023" (November 1, 2025) https://kluwerlawonline.com/journalarticle/Global+Privacy+Law+Review/6.1/GPLR2026002
[44] Sahil and Jeet S, "Predictive Policing, AI Surveillance, and Privacy in India: A Legal Analysis under the DPDP Act 2023" [2025] Zenodo (CERN European Organization for Nuclear Research) https://zenodo.org/records/18221510
[45] Tandon U and Gupta NK, "Informational Privacy in the Age of Artificial Intelligence: A Critical Analysis of India's DPDP Act, 2023" (2025) 6 Legal Issues in the Digital Age 87 https://lida.hse.ru/article/view/27529
[46] "A Comparative Legal and Regulatory Analysis of India's Digital Personal Data Protection Act (2023) and the EU GDPR: Implications for FinTech Governance and Audit Automation" [2025] Zenodo (CERN European Organization for Nuclear Research) https://zenodo.org/records/18063751
[47] Rao P and Rout KT, "Protecting the Young: Legal Protection of Children's Data under India's Digital Personal Data Protection Act, 2023" (2025) 13 International Journal of Advances in Social Sciences 177 https://ijassonline.in/AbstractView.aspx?PID=2025-13-4-2
[48] "A New Age of Data Privacy Laws in India: Review of Digital Personal Data Protection Act, 2023" [2024] International Journal of Law and Social Sciences 84 https://www.journalsalliancepub.com/index.php/ijls/article/view/114
[49] Agrawal S and Tiwari Y, "Data Privacy Governance Under India's DPDP Act, 2023 and the EU GDPR: A Comparative Study with Focus on Cross Border Data Transfers" [2025] Zenodo (CERN European Organization for Nuclear Research) https://zenodo.org/records/17649236
[50] Mandal T, "Consent and Algorithmic Decision-Making under the DPDP Act, 2023: A Regulatory Paradox" [2026] National Journal of Cyber Security Law https://lawjournals.celnet.in/index.php/njcsl/article/view/2007
[51] Kagda P. R, "Biometric Identification Systems and Human Rights: Ethical and Legal Challenges" (2024) 9 Vidhyayana https://vidhyayanaejournal.org/index.php/journal/article/view/2478
[52] Barot AS, "The Conflict between Press Freedom and Individual Privacy: A Legal Perspective" [2025] Zenodo (CERN European Organization for Nuclear Research) https://zenodo.org/records/17668618
[53] Chirtoacă L, "Unele Aspecte Din Jurisprudența CtEDO Privind Echilibrarea Drepturilor: Protecția Datelor, Libertatea de Exprimare Și Accesul La Informații [Articol]" (2025) https://msuir.usm.md/items/23ee7b94-6b5f-40f0-bff6-dc91f3f4e62d
[54] Pittman LJ, "The Elusive Constitutional Right to Informational Privacy" (Scholarly Commons @ UNLV Boyd Law) https://scholars.law.unlv.edu/nlj/vol19/iss1/5/
[55] "Data, Control, and Power: Decoding India's Digital Personal Data Protection Act, 2023" (November 1, 2025) https://kluwerlawonline.com/journalarticle/Global+Privacy+Law+Review/6.1/GPLR2026002
[56] Vaishali and Thombare J, "AI-Enabled Cybersecurity and Privacy Governance in India: Comparative Insights from the European Union" [2026] Zenodo

(CERN European Organization for Nuclear Research) https://zenodo.org/records/18885474

[57] Bolognini L and Capparelli F, "Proposals for Improving the Digital Omnibus, Rebalancing Data Protection and E-Privacy Disciplines with Innovation" [2026] Zenodo (CERN European Organization for Nuclear Research) https://zenodo.org/records/18598414

[58] Kong HL, "Thresholds, Powers, and Accountability in the Emergencies Act" (2025) 46 Manitoba Law Journal 31 https://journals.library.ualberta.ca/themanitobalawjournal/index.php/mlj/article/view/1434

[59] Anupriya and Deo SCK, "Securing Informational Privacy in India's IoT Governance: Looking through the Lens of FASTag" (HSTalks, February 25, 2025) https://hstalks.com/article/9067/securing-informational-privacy-in-indias-iot-gover/?business

[60] "EMPOWERING INDIVIDUALS: A DEEP DIVE INTO THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023" (2024) 12 International Journal of Advanced Research 891 https://www.journalijar.com/article/48771/empowering-individuals:-a-deep-dive-into-the-digital-personal-data-protection-act,-2023/

[61] Goel M, "Data Protection Bill(s): Why Has India Failed to Legislate Privacy So Far?" [2026] Zenodo (CERN European Organization for Nuclear Research) https://zenodo.org/records/18991078

[62] Apoorva, "Clicks to Control:Rethinking Data Privacy" [2026] Open MIND https://zenodo.org/records/18982539