DIGITAL PERSONAL DATA PROTECTION ACT, 2023: BALANCING PRIVACY AND TRANSPARENCY UNDER RIGHT TO INFORMATION ACT

Siddharth Rathee, LLB, Maharishi Dayanand University

ABSTRACT

The recognition of the right to privacy as a fundamental right in *Justice K.S. Puttaswamy (Retd.) v. Union of India* transformed the legal landscape surrounding personal data protection in India. The enactment of the Digital Personal Data Protection Act, 2023 (DPDPA) marks a significant legislative step towards operationalising privacy protections in the digital era. However, this development introduces complex challenges for the Right to Information Act, 2005 (RTI Act), a cornerstone of government transparency and accountability. While the RTI Act embodies the democratic principle that citizens have a right to know, the DPDPA prioritises safeguarding personal data through stringent consent-based processing and broad definitions of privacy. This article examines the intersections and potential conflicts between these two statutes, particularly in the context of public access to information that contains personal data. It analyses constitutional principles, statutory provisions, and comparative international frameworks, and proposes a harmonised approach that safeguards individual dignity while preserving the public's right to hold the state accountable.

I. Introduction

The twin ideals of privacy and transparency have long coexisted in constitutional democracies, albeit in uneasy tension. In India, the Right to Information Act, 2005 ("RTI Act") empowered citizens to demand accountability by accessing information held by public authorities, significantly altering the balance between the state and the individual.[1] Its transformative impact has been evident in exposing corruption, improving governance, and enabling informed public participation.

Yet, the constitutional recognition of privacy as a fundamental right in *Justice K.S. Puttaswamy (Retd.) v. Union of India* in 2017 shifted the legal narrative, elevating personal data protection to a matter of constitutional dignity under Article 21.[2] The Digital Personal Data Protection Act, 2023 ("DPDPA") operationalises this right in the digital sphere, introducing a consent driven framework for processing personal data, imposing obligations on data fiduciaries, and granting enforceable rights to data principals.[3]

This legislative development, while laudable for its privacy focus, raises pressing questions about its interaction with the RTI Act. Specifically, when an RTI request seeks information containing personal data, should the default presumption favour disclosure in the public interest, or should the individual's privacy prevail absent explicit consent? Without clear harmonisation, public authorities may adopt inconsistent interpretations, potentially undermining either transparency or privacy.

This article interrogates these tensions, examining the constitutional foundations, statutory overlaps, and international approaches, before advancing recommendations for a coherent legal framework that balances these two democratic imperatives.

1. The Right to Information Act, No. 22 of 2005, INDIA CODE (2005).
2. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
3. The Digital Personal Data Protection Act, No. 22 of 2023, INDIA CODE (2023).

II. Constitution and Legal Background

The interaction between the Right to Information and the right to privacy is rooted in the Indian Constitution, where both derive their legitimacy from fundamental rights but operate in different normative spaces.

A. Right to Privacy

The landmark judgment in *Justice K.S. Puttaswamy (Retd.) v. Union of India* unequivocally affirmed that the right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as part of the freedoms guaranteed by Part III of the Constitution. The Supreme Court characterised privacy as encompassing bodily integrity, informational self determination, and decisional autonomy. The judgment specifically recognised that informational privacy — the ability to control the dissemination of one's personal data — required legislative protection in the digital era.

Following *Puttaswamy*, the call for a comprehensive data protection law intensified, leading to the Justice B.N. Srikrishna Committee's 2018 report[4] and, ultimately, to the passage of the Digital Personal Data Protection Act, 2023 ("DPDPA"). The Act seeks to create a consent driven, rights based regime for personal data processing, thereby embedding privacy protections into statutory law.

4. Justice B.N. Srikrishna Comm., Report of the committee of Experts on Data Protection Framework for India(2018).

B. Right to Information

Conversely, the Right to Information, though not explicitly mentioned in the Constitution, has been recognised by the Supreme Court as flowing from Article 19(1)(a) — the right to freedom of speech and expression.[5] In *State of Uttar Pradesh v. Raj Narain*, the Court held that "the people of this country have a right to know every public act, everything that is done in a public way, by their public functionaries."[6]

This principle was given legislative force through the RTI Act, 2005, which mandates the disclosure of information held by public authorities, subject to limited exemptions. Among these exemptions, Section 8(1)(j) is of particular relevance: it prohibits disclosure of personal information which has no relationship to any public activity or interest, or which would cause unwarranted invasion of privacy, unless a larger public interest justifies disclosure.[7]

C. The Privacy-Transparency Tension

Even prior to the enactment of the DPDPA, the judiciary navigated the fine line between transparency and privacy under the RTI Act. In *Girish Ramchandra Deshpande v. CIC*, the Supreme Court held that personal information relating to service records and disciplinary proceedings of a public servant could not be disclosed unless there was an overriding public interest.[8] Similarly, in *Thalappalam Service Cooperative Bank Ltd. v. State of Kerala*, the Court stressed that the term "information" under the RTI Act did not encompass every detail about an individual, particularly where it would lead to an invasion of privacy.[9]

5. *State of Uttar Pradesh v. Raj Narain*, (1975) 4 SCC 428.
6. Id. § 5.
7. *Girish Ramchandra Deshpande v. Cent. Info. Comm'n*, (2013) 1 SCC 212
8. Id. § 7.
9. *Thalappalam Serv. Coop. Bank Ltd. v. State of Kerala*, (2013) 16 SCC 82

The DPDPA 2023 introduces a broader, more formalised privacy protection regime, potentially expanding the scope of what qualifies as "personal data" and heightening consent requirements. This raises the possibility that public authorities may interpret privacy exemptions under RTI more expansively, thereby limiting access to information that was previously available.

Thus, the constitutional and legal foundations reveal an inherent tension: both rights are constitutionally recognised, yet neither is absolute. The task lies in ensuring that their intersection is governed by a principled framework that serves both democratic transparency and individual dignity.

III. Key Provisions of the Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 ("DPDPA") represents India's first dedicated data protection legislation, enacted to give statutory effect to the right to informational privacy recognised in *Puttaswamy*. Its provisions apply to both public and private entities engaged in the processing of digital personal data, whether within India or outside, if such processing is in connection with offering goods or services in India.

A. Definition and Scope

The DPDPA adopts a broad definition of "personal data" as "any data about an individual who is identifiable by or in relation to such data."[10] "Processing" is defined expansively to include the entire lifecycle of data handling — from collection to storage, use, sharing, and erasure.[11] This expansive terminology means that a large volume of information that might be sought under the Right to Information Act ("RTI Act") could qualify as personal data under the DPDPA.

10. Id. § 3.
11. Id. § 3.

B. Rights of Data Principals

The Act grants several enforceable rights to individuals (termed "data principals"):

1. Right to access information about personal data processing.[12]
2. Right to correction and erasure of personal data.[13]
3. Right to grievance redressal through the data fiduciary and, if unsatisfied, through the Data Protection Board of India.[14]

These rights reinforce individual control over personal information but may also limit disclosure obligations under other laws when personal data is involved.[15]

C. Obligation of Data Fiduciaries

Entities processing personal data ("data fiduciaries") are required to:

• Obtain free, specific, informed, and unambiguous consent from the data principal, unless processing is for a "legitimate use" defined under the Act.

• Ensure purpose limitation (processing only for the purpose specified at collection) and storage limitation (retaining data only for as long as necessary).

• Implement reasonable security safeguards to prevent breaches.

For public authorities, the consent requirement can become a limiting factor when complying with RTI requests involving personal data.[16]

12. Id. § 3.
13. Id. § 3.
14. Id. § 3.
15. Id. § 3.
16. Id. § 3.

D. Government Exemptions

Section 17 of the DPDPA grants the Central Government power to exempt any of its instrumentalities from compliance with certain provisions of the Act in the interests of sovereignty, integrity, security, public order, or preventing incitement to offences. While exemptions for state functions are common in data protection regimes globally, the breadth of these clauses in the DPDPA raises concerns that they could be invoked to deny RTI disclosures.[17]

E. Penalties

The Act prescribes significant penalties, up to ₹250 crore for non-compliance with its obligations creating a strong incentive for public authorities to err on the side of caution when faced with conflicting demands under RTI and DPDPA.

The cumulative effect of these provisions is to create a consent centric privacy regime with an expansive scope of protected data and strong compliance pressures. In the absence of express harmonisation with the RTI Act, public authorities may interpret privacy exemptions broadly, leading to an implicit contraction of transparency obligations. This statutory architecture sets the stage for the conflicts analysed in the next section.[18]

17. Id. § 3.
18. Id. § 3.

IV. Areas of Conflict between RTI and DPDPA, 2023

The *Right to Information Act, 2005* ("RTI Act") and the *Digital Personal Data Protection Act, 2023* ("DPDPA") pursue distinct yet equally legitimate constitutional objectives of transparency in governance and protection of individual privacy. However, their operational mandates often intersect, and without explicit harmonisation, this intersection can give rise to practical and legal conflicts.

A. Consent Requirements vs. Presumption of Disclosure

The RTI Act operates on a foundational presumption that information held by public authorities should be disclosed unless an exemption applies. Conversely, the DPDPA enshrines consent as the primary basis for processing personal data, subject to limited "legitimate use" exceptions.

Example: An RTI applicant seeks details of beneficiaries under a government housing subsidy scheme. Under RTI, such data could be disclosed unless it is deemed to cause an unwarranted invasion of privacy. Under DPDPA, however, disclosure would require the consent of each beneficiary unless it falls within a legitimate use exception which is practically unfeasible requirement that may lead to outright denial.

B. Expanded Definition of Personal Data

Section 2(13) of the DPDPA defines "personal data" broadly, potentially encompassing information that was previously considered disclosable under RTI. This includes not only sensitive personal identifiers (such as Aadhaar numbers or bank details) but also seemingly benign information that can be linked to an identifiable person.

Example: Publication of contractors' names and payment details for public works projects may now be withheld on the grounds that they constitute personal data,

even though such disclosures have historically served as anti-corruption measures under RTI.

C. Overlap with RTI's Section 8(1)(j)

Section 8(1)(j) of the RTI Act exempts personal information from disclosure if it has no relationship to any public activity or interest, unless public interest outweighs privacy concerns. However, the DPDPA does not expressly incorporate a public interest override for disclosure suggesting that information could be denied under DPDPA even where RTI's balancing test would favour release.

Example: Information about disciplinary action taken against a senior public official may be withheld entirely under DPDPA despite a strong public interest in transparency about official misconduct.

D. Government Exemptions and Potential Overreach

Section 17 of the DPDPA allows the Central Government to exempt its agencies from the Act's provisions for reasons such as sovereignty, integrity, or public order.[19] While aimed at national security, such exemptions could be applied broadly to restrict RTI disclosures, particularly in sensitive policy areas.

Example: A citizen requesting procurement details from a defence public sector undertaking could be denied access on the dual grounds of "security interests" and personal data protection, even if the information is primarily financial in nature.

19. Id. § 3.

E. Chilling Effect from High Penalties

With penalties of up to ₹250 crore, public authorities may adopt an overly cautious approach, preferring to reject RTI requests rather than risk a DPDPA violation. This risk aversion could erode the culture of transparency cultivated over 18 years of RTI implementation.

In sum, these conflicts reveal that without statutory guidance on how the RTI Act and DPDPA interact, public authorities are left to reconcile competing legal duties on an ad hoc basis. The result is a high risk of inconsistent application, legal uncertainty, and a gradual erosion of transparency norms in the name of privacy protection.

V. Comparative Perspective: International Framework and Insights for India

While the tension between privacy and transparency is pronounced in India's RTI-DPDPA framework, similar challenges have arisen in other jurisdictions that have adopted both data protection and freedom of information (FOI) laws. These experiences offer useful models for legislative and judicial harmonisation.

A. United Kingdom: Data Protection Act 2018 & Freedom of Information Act 2000

The UK operates under two complementary regimes: the Freedom of Information Act 2000 (FOIA)[20] ensures public access to information held by public authorities, while the Data Protection Act 2018 (DPA)[21] implementing the GDPR[22] safeguarding personal data.

20. Freedom of Information Act 2000, c.36 (UK).
21. Data Protection Act 2018, c.12 (UK).
22. General Data Protection Regulation (Regulation (EU) 2016/679)

Under FOIA's Section 40, personal data is exempt from disclosure if doing so would contravene data protection principles. However, FOIA incorporates a public interest test for certain categories of personal data, especially where disclosure relates to the conduct of public officials. This allows balancing on a case-by-case basis rather than an absolute bar on disclosure.

Key Insight for India: A statutory public interest override, as in the UK, ensures that privacy protection does not become a shield for official misconduct.

B. European Union: General Data Protection Regulation & Public Access Regulation (1049/2001)

The EU's GDPR[23] provides robust privacy safeguards but recognises the need to reconcile them with the principle of transparency under Regulation 1049/2001[24], which governs access to EU institutions' documents. Article 86 of the GDPR explicitly permits the disclosure of personal data in official documents "in accordance with Union or Member State law" reconciling the right to data protection with freedom of information.

The European Court of Justice has stressed that such reconciliation requires case-specific proportionality assessments, weighing the necessity of disclosure against potential harm to privacy (*Bavarian Lager* case)[25].

Key Insight for India: Explicit legislative provisions mandating proportionality and case-by-case balancing could prevent blanket denials under DPDPA.

23. Id. § 22
24. Regulation (EC) No 1049/2001 of the European Parliament and of the Council, OJ L 145/43.
25. Case C-28/08 P, *European Commission v. Bavarian Lager Co. Ltd* [2010] ECR I-6055.

C. **Canada**: Privacy Act & Access to Information Act

Canada's Access to Information Act[26] includes exemptions for personal information, but also a public interest clause (Section 20(6)) allowing disclosure if the public interest in transparency outweighs the resulting invasion of privacy. The Canadian courts have interpreted "public interest" broadly, especially for information concerning public health, safety, and integrity of public officials.[27]

Key Insight for India: A legislated "public interest override" combined with clear guidance to public information officers can provide certainty while preserving both transparency and privacy.

D. Lessons for India

1. *Codified Balancing Mechanism:* Both privacy and transparency are constitutional values; legislation should expressly mandate a proportionality assessment rather than defaulting to non-disclosure.
2. *Public Interest Override:* An explicit statutory clause could ensure that personal data is disclosed where non-disclosure would undermine democratic accountability.
3. *Guidelines & Training:* International experience shows that without practical guidance, officials default to denial; structured guidelines can ensure consistent decision making.

26. Access to Information Act, R.S.C. 1985, c. A-1 (Canada).
27. *Canada (Information Commissioner) v. Canada (Minister of National Defence)*, 2011 SCC 25.

VI. Recommendations and Harmonization Framework

The coexistence of the Right to Information Act, 2005 (RTI Act) and the Digital Personal Data Protection Act, 2023 (DPDPA) presents a statutory tension that cannot be resolved solely through ad hoc case law. To ensure both transparency and privacy are protected as constitutional values, a harmonisation framework is essential. The following recommendations are aimed at legislative, administrative, and judicial stakeholders.

A. Legislative Measures

1. Introduction of a public override in DPDPA

The DPDPA should incorporate a provision similar to Section 8(2) of the RTI Act, allowing disclosure of personal data where the public interest in disclosure outweighs potential harm to privacy.

This override should be explicitly linked to principles of proportionality under *K.S. Puttaswamy v. Union of India*.

2. Clarification of interaction between RTI and DPDPA

Parliament could insert a non-obstante clause in the RTI Act stating that, in case of conflict, both Acts should be read harmoniously and subject to proportionality tests.

Alternatively, an interpretive provision in the DPDPA could affirm that it does not override RTI's transparency mandate except in clearly defined privacy-sensitive contexts.

B. Administrative and Procedural Measures

1. Guidelines for Public Information Officers (PIOs)

The Department of Personnel and Training (DoPT) should issue detailed guidance on handling RTI requests involving personal data, including step-

by-step proportionality assessments.

Templates for balancing tests and redaction protocols can standardise decisions.

2. **Training and Capacity Building**

Regular workshops for PIOs, appellate authorities, and judicial officers should cover DPDPA compliance and RTI balancing, with practical case studies.

C. Judicial Role

1. **Developing Proportionality Jurisprudence**

The higher judiciary should lay down structured guidelines for proportionality analysis, including factors such as the nature of the personal data, the role of the data subject, and the degree of public interest in the information.

2. **Promoting Case Specific Balance**

Blanket denials should be discouraged; courts should reinforce that privacy is not an absolute right and must be balanced against transparency on a case-by-case basis.

Conclusion

India's legal framework stands at a crossroads where informational privacy and democratic transparency must be reconciled rather than pitted against each other. International experience, constitutional jurisprudence, and statutory interpretation all point toward a balanced approach anchored in proportionality and public interest. If adopted, the proposed harmonization framework could transform potential conflict between RTI and DPDPA into a synergistic relationship, strengthening both privacy and the right to know as pillars of a robust democracy.