INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 6 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

PRIVACY AGAINST TRANSPARENCY: ENFORCEMENT CHALLENGES AT THE INTERSECTION OF THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023 AND THE RIGHT TO INFORMATION ACT, 2005

AUTHOR – BEROZ SHERIM J* & R. THENDRALARASI**

* STUDENT AT SCHOOL OF LAW, VELS INSTITUTE OF SCIENCE, TECHNOLOGY AND ADVANCED STUDIES (VISTAS)

** ASSISTANT PROFESSOR AT SCHOOL OF LAW, VELS INSTITUTE OF SCIENCE, TECHNOLOGY AND ADVANCED STUDIES (VISTAS)

BEST CITATION – BEROZ SHERIM J & R. THENDRALARASI**,** PRIVACY AGAINST TRANSPARENCY: ENFORCEMENT CHALLENGES AT THE INTERSECTION OF THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023 AND THE RIGHT TO INFORMATION ACT, 2005, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR),* 6 (6) OF 2026, PG. 427-434, APIS – 3920 – 0001 & ISSN - 2583-2344. DOI - https://doi.org/10.65393/IJLRV6I643

1. ABSTRACT:

The enactment of the Digital Personal Data Protection Act, 2023 (DPDP Act) marks a defining moment in Indian information governance. Yet the statute's most consequential provision — Section 44(3), which amends Section 8(1)(j) of the Right to Information Act, 2005 (RTI Act) — has received insufficient scholarly scrutiny. By substituting a nuanced, proportionality-driven public interest override with an unqualified reference to 'personal data', the legislature has created a conflict of constitutional and institutional magnitude. This article examines the doctrinal foundations of both the right to information and the right to privacy as co-equal fundamental rights under the Indian Constitution, analyses the specific legislative and institutional conflicts generated by the DPDP-RTI interface, and draws on comparative frameworks from the European Union, the United Kingdom, and South Africa to advance a case for a harmonised privacy-transparency framework. The article concludes that Section 44(3) fails the proportionality test articulated in Justice K S Puttaswamy v Union of India and proposes legislative, institutional, and interpretive reforms necessary to restore constitutional coherence.

Keywords: Digital Personal Data Protection Act 2023; Right to Information Act 2005; Section 44(3); privacy; transparency; proportionality; Data Protection Board of India; Central Information Commission; GDPR; constitutional law.

2. INTRODUCTION:

India confronts an unprecedented constitutional tension. For the first time in its legislative history, two major statutes — the Right to Information Act, 2005 and the Digital Personal Data Protection Act, 2023 — occupy the same normative space and pull in opposite directions. The RTI Act democratised governance by empowering citizens to demand information from public authorities; the DPDP Act regulates the collection, processing, and protection of digital personal data. Each statute gives effect to a distinct fundamental right. Yet the legislature, in enacting the DPDP Act, has altered their relationship in a manner that raises serious constitutional and practical concerns.

The conflict crystallises in Section 44(3) of the DPDP Act, which amends Section 8(1)(j) of the

RTI Act[815]. The original provision balanced personal privacy against public accountability through a calibrated public interest override. Section 44(3) sweeps this balance away entirely, substituting a compressed exemption for 'information which relates to personal data' — with no public interest exception, no proportionality mechanism, and no institutional guidance on resolution. [1] The implications reach into every domain where governmental power intersects with individual identity: procurement decisions, disciplinary proceedings, employment records, official correspondence, and the full sweep of information about how the Indian state conducts itself.

This article undertakes a systematic analysis of the enforcement challenges that arise from this legislative conflict. It examines the constitutional foundations of both statutes, identifies the doctrinal vulnerabilities created by Section 44(3), evaluates the institutional architecture of the Data Protection Board of India and the Central Information Commission, and draws comparative lessons from jurisdictions that have managed the privacy-transparency interface with greater sophistication. The article concludes with a set of legislative, institutional, and interpretive reforms designed to restore what the DPDP Act has disrupted: a principled, proportionality-based equilibrium between two co-equal constitutional rights.

3. CONSTITUTIONAL FOUNDATIONS: PRIVACY AND TRANSPARENCY AS CO-EQUAL RIGHTS:

The right to information and the right to privacy have followed parallel constitutional trajectories in India, each receiving recognition as fundamental rights through landmark judicial decisions. Their convergence in the present statutory conflict can only be understood against this constitutional backdrop.

The constitutional foundation of the right to information derives from Article 19(1)(a) of the Constitution, which guarantees freedom of speech and expression. In S P Gupta v Union of India,[2] the Supreme Court established that an open government is foundational to participatory democracy: citizens cannot exercise democratic rights in any meaningful sense unless they possess information about how state power is being used. This reasoning informed the RTI Act's transformative architecture — mandatory proactive disclosure, a presumption in favour of information sharing, and a right of access subject only to narrowly framed exemptions.

The constitutional status of privacy followed a more contested path. Early decisions in M P Sharma v Satish Chandra[816] and Kharak Singh v State of Uttar Pradesh[4] declined to recognise privacy as a distinct fundamental right. The doctrinal shift began with R Rajagopal v State of Tamil Nadu[5] which treated privacy as an aspect of the right to life under Article 21. The definitive constitutional settlement arrived with the nine-judge bench decision in Justice K S Puttaswamy v Union of India (2017),[6] which unanimously held that privacy is a fundamental right under Articles 14, 19, and 21. Justice D Y Chandrachud's lead opinion identified informational privacy — control over personal data — as a core constitutional interest deserving protection from state intrusion.

The critical constitutional consequence of Puttaswamy is not merely the recognition of privacy as a right, but the articulation of the framework within which restrictions on both privacy and transparency must be evaluated. The judgment adopted a three-part proportionality test: any restriction on a fundamental right must be prescribed by law, must pursue a legitimate aim, and must be proportionate — meaning the least restrictive means of achieving that aim must be employed.[7] This framework applies equally to restrictions on the right to information and to restrictions on the right to privacy. It is precisely this framework that Section 44(3) of the DPDP Act violates, by imposing an absolute restriction

[815] RTI Act

[816] M P Sharma v Satish Chandra

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 6 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

on information access without any proportionality mechanism.

4. THE LEGISLATIVE CONFLICT: SECTION 44(3) AND ITS CONSEQUENCES

A. THE ARCHITECTURE OF THE ORIGINAL SECTION 8(1)(J):

The original Section 8(1)(j) of the RTI Act created what administrative law scholars describe as a qualified exemption with a public interest override. Information relating to personal matters was exempt from disclosure only where it had no relationship to any public activity, or where disclosure would cause an unwarranted invasion of privacy. Even then, the exemption yielded where the public interest in disclosure clearly outweighed the privacy interest. Over two decades, the Central Information Commission built a sophisticated jurisprudence around this provision, distinguishing between genuinely private information — attracting strong exemption — and information about the exercise of official power, which was generally held disclosable despite its personal character.[8]

B. THE TRANSFORMATION EFFECTED BY SECTION 44(3)

Section 44(3) replaces this carefully calibrated provision with four words: 'information which relates to personal data'.[817] The substitution eliminates two essential operative elements of the original provision. First, the qualification that the information must have 'no relationship to any public activity' disappears: all personal data is now exempt regardless of its connection to governmental function. Second, and more critically, the public interest override is abolished entirely. There is no mechanism for an Information Commissioner to weigh the public interest in exposure of official misconduct against the privacy interest of the official concerned.

The consequences are amplified by the DPDP Act's definitional framework. Section 2(t) defines 'personal data' as 'any data about an individual who is identifiable by or in relation to such data'.[10] This definition is unqualified. It encompasses a government servant's name and designation, official correspondence, asset declarations, performance appraisals, and records of disciplinary proceedings. Under the amended provision, each of these categories — long held disclosable by the CIC where public accountability was engaged — is potentially shielded from RTI access. The risk is not theoretical: public authorities have already begun invoking DPDP grounds to resist RTI disclosure, and a pattern of refusals citing personal data protection is taking shape in the Commission's appeals caseload.

C. THE CONSTITUTIONAL VULNERABILITY

The proportionality analysis is, on any view, adverse to Section 44(3). The provision satisfies the first limb of the Puttaswamy framework — it is prescribed by law. It may satisfy the second — protecting privacy is a constitutionally recognised aim. It fails the third. A blanket exemption for all personal data from RTI disclosure, without any calibration for the distinction between private conduct and the exercise of public power, is not the least restrictive means of protecting privacy. It is a categorical prohibition that sacrifices the right to information entirely in every case where personal data is involved, rather than undertaking the principled balancing exercise that both the Constitution and the judicial consensus demand.[11] The Supreme Court in *Girish Ramchandra Deshpande v Central Information Commissioner*[12] preserved the public interest override as a meaningful operative mechanism. Section 44(3) has reversed that preservation without doctrinal justification.

5. INSTITUTIONAL ARCHITECTURE AND JURISDICTIONAL CONFLICTS

The constitutional challenge posed by Section 44(3) is compounded by institutional design failures that generate jurisdictional uncertainty and enforcement incoherence. The DPDP Act creates the Data Protection Board of India as its

[817] Section 44(3)

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 6 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

adjudicatory body, while the RTI Act vests adjudicatory authority in the Central Information Commission. The legislature has provided no mechanism for resolving the conflicts that inevitably arise when these two bodies are called upon to address overlapping questions.

The jurisdictional conflict arises acutely in a scenario that is no longer hypothetical. Suppose a citizen files an RTI application seeking information about government procurement payments — information about an identifiable contractor. The public authority refuses on DPDP grounds. The citizen appeals to the CIC. The CIC must determine whether it is bound by the amended Section 8(1)(j) to uphold the refusal, or whether it can apply its pre-amendment jurisprudence. If the CIC orders disclosure and the contractor complains to the DPDPB that the disclosure violates the DPDP Act[818], which order prevails? The two bodies operate under separate statutes with no statutory hierarchy between them, and the DPDP Act provides no guidance on this question.

The DPDP Act's institutional design raises additional concerns about the Board's independence. The Chairperson and Members of the Data Protection Board are appointed entirely by the Central Government without independent screening. The Board operates in a 'digital office' model without requiring physical hearings — a design that reduces procedural rigour in complex cases involving competing constitutional rights. The penalty regime creates further anomalies: the DPDP Act provides for penalties of up to Rs 250 crore for specified violations, but imposing financial penalties on public authorities for making disclosures ordered by the CIC would have a severe chilling effect on transparency.[819]

The accountability consequences of these design failures are significant. The RTI Act has served as India's most effective anti-corruption instrument, generating disclosures about procurement irregularities, governance failures, and official misconduct that would otherwise have remained concealed. Any ambiguity in the post-DPDP framework that allows public authorities to deploy personal data exemptions as a shield against accountability disclosures threatens this function directly.

6. COMPARATIVE ANALYSIS: LESSONS FROM MATURE FRAMEWORKS

A. THE EUROPEAN UNION: HARMONISATION OVER HIERARCHY

The GDPR — the global standard for data protection — addresses the privacy-transparency interface through Article 86, which explicitly provides that personal data in official documents held by public authorities may be disclosed for reasons of public interest in accordance with Union or Member State law.[15] This provision enshrines a principle of harmonisation rather than hierarchy: neither right automatically overrides the other. The Court of Justice of the European Union in *Google Spain SL v Agencia Española de Protección de Datos*[16] demonstrated that even the right to be forgotten must be balanced against the public interest in information access on a case-by-case basis. No categorical exclusion of personal data from transparency obligations exists anywhere in the EU framework.

B. THE UNITED KINGDOM: INTEGRATED OVERSIGHT AND QUALIFIED EXEMPTION

The United Kingdom provides the most instructive comparative model. Section 40 of the Freedom of Information Act 2000 creates only a *qualified* exemption for third-party personal data — one that requires a public interest test and is conditioned on whether disclosure would breach Data Protection Act principles.[17] Crucially, the UK Information Commissioner's Office administers both the FOIA and the Data Protection Act 2018, enabling it to develop coherent guidance on their interaction, resolve jurisdictional conflicts through internal referral, and apply consistent proportionality principles across privacy and

[818] DPDP Act
[819] CIC

transparency cases. The Supreme Court's decision in *R (Evans) v Attorney General*[18] reinforced that ministerial claims to non-disclosure must yield to judicial scrutiny and cannot frustrate legitimate public interest disclosure. India's bifurcated architecture — separate DPDPB and CIC with no coordination mechanism — stands in stark contrast to this integrated model.

C. SOUTH AFRICA: CONSTITUTIONAL SYMMETRY AND GRADUATED EXEMPTION

South Africa presents the closest constitutional analogue to India's challenge, with both privacy (section 14)[820] and access to information (section 32) explicitly guaranteed as fundamental rights in the Constitution.[19] The Protection of Personal Information Act 2013 (POPIA) and the Promotion of Access to Information Act 2000 (PAIA) address their interaction through two mechanisms: POPIA's Section 6(1) preserves processing necessary for exercising rights or obligations conferred by law — broad enough to cover RTI disclosure obligations — and PAIA's Section 34 creates a multi-factor public interest test for personal information exemptions that requires weighing privacy against corruption exposure, safety, and accountability. The South African model's most significant lesson is its refusal to treat the personal data exemption as categorical: it retains proportionality as the governing principle at every stage.

The comparative synthesis generates five findings relevant to Indian reform. First, no mature democracy has abolished the public interest override for personal data in transparency legislation. Second, institutional integration — a single body with jurisdiction over both privacy and transparency — eliminates the jurisdictional conflicts that India's bifurcated architecture creates. Third, a graduated definitional framework distinguishing between genuinely private information and information about the exercise of public power is constitutionally and practically essential. Fourth, proportionality analysis must be conducted by independent adjudicatory bodies insulated from executive influence. Fifth, explicit legislative acknowledgment of the co-equal constitutional status of both rights is necessary to guide adjudicators and public authorities.

VI. KEY FINDINGS

This study yields five principal findings. First, Section 44(3) of the DPDP Act constitutes a disproportionate restriction on the constitutional right to information under Article 19(1)(a). By eliminating the public interest override without establishing any alternative balancing mechanism, it fails the proportionality test articulated in Puttaswamy and is constitutionally suspect. The amendment cannot be justified by reference to the legitimate aim of protecting privacy alone; proportionality demands that the legislature choose the least restrictive means, which it has not done.[20]

Second, the DPDP Act's broad definitional treatment of personal data — extending without qualification to all information about identifiable individuals regardless of whether it concerns private conduct or the exercise of official power — threatens to collapse the foundational distinction between accountability information and genuinely private information. This distinction, developed over two decades of CIC jurisprudence and affirmed in Supreme Court decisions from Rajagopal to Girish Deshpande[821], is constitutionally essential and cannot be abandoned without doctrinal justification.

Third, the institutional bifurcation between the DPDPB and the CIC creates insoluble jurisdictional conflicts that the DPDP Act does not attempt to resolve. The resulting legal uncertainty harms public authorities, citizens, and the RTI framework as a whole — generating incentives for strategic invocation of DPDP exemptions and disincentives for transparency-protective decision-making.

[820] section 14

[821] Girish Deshpande

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 6 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

Fourth, comparative analysis demonstrates that India's approach is an outlier among democratic legal systems. The EU, UK, and South Africa each maintain proportionality-based balancing between privacy and transparency; each preserves some form of public interest override for personal information in transparency legislation; and each has developed institutional architectures that enable coherent adjudication of privacy-transparency conflicts. India's post-Section 44(3) framework is inferior to all three models on every dimension.

Fifth, the anti-corruption and accountability consequences are systemic. RTI has been the most powerful accountability instrument in independent India's legal arsenal. Its dilution through overbroad personal data exemptions — particularly the removal of the public interest override for information about official conduct, procurement, and governance — poses a direct threat to the accountability infrastructure that civil society, journalism, and democratic institutions depend upon.[21]

7. RECOMMENDATIONS FOR A HARMONISED FRAMEWORK

A. LEGISLATIVE REFORM

The legislature should repeal Section 44(3) of the DPDP Act and restore a reformed version of Section 8(1)(j)[822] of the RTI Act that explicitly addresses the privacy-transparency balance. The reformed provision should exempt information relating to personal data while preserving disclosure where: (a) the information concerns the discharge of official duties, public roles, or the exercise of governmental power by an identifiable individual; or (b) the public interest in disclosure clearly and demonstrably outweighs the privacy interest, having regard to the sensitivity of the data, the nature of the public interest, and the reasonable expectations of the individual in context.

A graduated definitional framework should distinguish between ordinary personal data attracting standard privacy protection and accountability-related data — information about the exercise of official power, public procurement, and governmental decision-making — which should be subject to a lower privacy protection standard and a higher public interest disclosure threshold. Both the RTI Act and the DPDP Act should include a mutual recognition provision confirming their concurrent operation and specifying that lawful RTI disclosures do not constitute DPDP violations.

B. Institutional Reform

A formal mechanism for joint adjudication should be established for cases involving both RTI and DPDP dimensions — a Joint Panel comprising members of the CIC and the DPDPB, with binding authority over both institutions. The appointment process for the Data Protection Board should be reformed to introduce independent screening, modelled on the UK ICO appointment process, insulating the Board from executive influence. Over the medium term, India should consider establishing a unified Information and Privacy Commissioner on the UK ICO model, with concurrent jurisdiction over RTI and DPDP matters, thereby eliminating the jurisdictional conflicts that the present bifurcated architecture creates.[22]

C. Interpretive Guidance

Pending legislative reform, the Supreme Court should take up the constitutional validity of Section 44(3) — either on reference from the Central Government or suo motu — given the constitutional dimensions of the privacy-transparency conflict. The CIC should issue interpretive circulars affirming that the amended Section 8(1)(j) must be read in light of the constitutional right to information; that information about the exercise of official duties remains presumptively disclosable; and that public authorities must provide specific and substantiated reasons for DPDP-based refusals, not mere invocation of the personal data label.

8. CONCLUSION

[822] Section 8(1)(j)

The tension between the Digital Personal Data Protection Act, 2023 and the Right to Information Act, 2005 is not merely a technical legislative conflict. It reflects a deeper question about the kind of constitutional democracy India aspires to be: one where the right to privacy serves as a shield for genuine personal interests, or one where data protection law becomes an instrument for official opacity. The answer the legislature has currently provided, through Section 44(3)'s elimination of the public interest override, is constitutionally untenable and normatively unsatisfactory.

The proportionality framework of Puttaswamy[823] requires that both the right to information and the right to privacy be given their fullest constitutional expression, and that conflicts between them be resolved through principled balancing rather than categorical exclusion. Section 44(3) fails this requirement. It imposes an absolute restriction on information access without justifying why a less restrictive approach — such as a graduated framework distinguishing between genuinely private and accountability-related data, combined with a reformed public interest override — could not achieve the same privacy-protecting aim.

The comparative evidence is unambiguous: no mature democracy has taken the approach of simply abolishing the public interest override for personal data in transparency legislation. The EU, the UK, and South Africa have each developed more sophisticated, constitutionally coherent frameworks that demonstrate the viability of harmonising privacy and transparency as co-equal values. India's legislative path forward is clear: restore proportionality, reform institutional design, and affirm through explicit statutory text the constitutional commitment to both rights that the Puttaswamy judgment established.

The right to privacy and the right to information are, at their core, expressions of the same constitutional commitment: to human dignity and the accountability of power. Protecting genuinely private information and ensuring transparency about the exercise of public power are complementary, not contradictory, aims. A legal framework worthy of India's constitutional democracy must give effect to both.[824]

BIBLIOGRAPHY

Primary Sources

Legislation — India

Constitution of India 1950

Digital Personal Data Protection Act 2023 (Act 22 of 2023)

Information Technology Act 2000 (Act 21 of 2000)

Right to Information Act 2005 (Act 22 of 2005)

Legislation — Foreign

Data Protection Act 2018 (UK)

Freedom of Information Act 2000 (UK)

General Data Protection Regulation (EU) 2016/679

Promotion of Access to Information Act 2 of 2000 (South Africa)

Protection of Personal Information Act 4 of 2013 (South Africa)

Cases — India

Canara Bank v C S Shyam (2018) 8 SCC 726

Central Board of Secondary Education v Aditya Bandopadhyay (2011) 8 SCC 497

Girish Ramchandra Deshpande v Central Information Commissioner (2013) 1 SCC 212

Justice K S Puttaswamy v Union of India (2017) 10 SCC 1

Justice K S Puttaswamy v Union of India (2019) 1 SCC 1

Kharak Singh v State of Uttar Pradesh AIR 1963 SC 1295

[823] Puttaswamy

[824] constitutional democracy

M P Sharma v Satish Chandra AIR 1954 SC 300

People's Union for Civil Liberties v Union of India (2004) 2 SCC 476

R Rajagopal v State of Tamil Nadu AIR 1995 SC 264

S P Gupta v Union of India AIR 1982 SC 149

Union of India v Association for Democratic Reforms (2002) 5 SCC 294

Cases — Foreign

Google Spain SL v Agencia Española de Protección de Datos (Case C-131/12) [2014] ECR I-317

R (Evans) v Attorney General [2015] UKSC 21

South Lanarkshire Council v Scottish Information Commissioner [2013] UKSC 55

Secondary Sources

Books and Chapters

Divan S and Sengupta A, 'The Right to Information and Privacy' in Raghavan V and Khosla M (eds), The Oxford Handbook of the Indian Constitution (OUP 2019)

Greenleaf G, Asian Data Privacy Laws: Trade and Human Rights Perspectives (OUP 2014)

Mendel T, Freedom of Information: A Comparative Legal Survey (2nd edn, UNESCO 2008)

Journal Articles

Blume P, 'An Introduction to GDPR and Freedom of Information' (2019) 5(2) European Data Protection Law Review 125

Iyengar P, 'Privacy and the Information Bill' (2002) 37(25) Economic and Political Weekly 2419

Ramanathan U, 'A Unique Identity Bill' (2010) 45(35) Economic and Political Weekly 10

Reports and Official Documents

Justice B N Srikrishna Committee, 'A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians' (Ministry of Electronics and Information Technology 2018)

Law Commission of India, 'The Right to Privacy' (Report No 266, 2017)

Online Sources

Internet Freedom Foundation, 'Note on the DPDP Act and RTI' (IFF 2023) <https://internetfreedom.in> accessed 15 January 2025

Kodali S, 'Patterns of RTI Utilisation in India: An Empirical Study' (Centre for Internet and Society 2022) <https://cis-india.org> accessed 20 February 2025