

Right To Be Forgotten Versus Right to Know: The Constitutional Conflict Under the DPDP Act, 2023

A Legal Analysis of Competing Fundamental Rights in India's Digital Governance Framework

Adv. Yashwant Shailendra Soni

I. INTRODUCTION

Privacy and transparency have always lived in creative tension within democratic legal systems. In India, that tension has been elevated, in the age of the internet, to the level of a constitutional confrontation. The right to informational privacy which finds its most consequential modern expression in the Right to be Forgotten (RTBF) sits uneasily alongside the right of citizens, journalists, and civil society to access public information. Both are legitimate, both are constitutionally grounded, and yet each, when pushed to its logical extreme, threatens to extinguish the other.

The problem has acquired particular urgency following the enactment of the *Digital Personal Data Protection Act, 2023* (DPDP Act). ¹Far from settling the debate, the Act has sharpened it. On one side, Section 12 of the DPDP Act provides individuals with a statutory mechanism to demand erasure of their personal data. On the other, Section 44(3) of the same Act quietly rewrote a foundational provision of the *Right to Information Act, 2005* (RTI Act) in a manner that, critics argue, has severely curtailed the public's right to access government information. The result is a legal landscape where privacy and transparency have been left to collide without an adequate statutory referee.

This article examines the constitutional dimensions of that collision. It begins by tracing how the RTBF has been recognised under Indian constitutional law, particularly following *K.S. Puttaswamy v. Union of India* (2017). ² It then analyses how the DPDP Act's structural choices on erasure rights, the publicly available data exemption, and the RTI amendment have altered the legal landscape. It draws on the Delhi High Court's landmark 2026 ruling in *Laksh Vir Singh Yadav v. Union of India* ³to examine how courts are attempting to reconcile these competing

¹The Digital Personal Data Protection Act, 2023, No. 22 of 2023 (India) [hereinafter DPDP Act].

² *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1 (India). The nine-judge bench unanimously held that privacy is a fundamental right under Article 21 of the Constitution

³ *Laksh Vir Singh Yadav v. Union of India & Ors*, 2026 DHC 4891 (Delhi High Court, May 29, 2026, J. Sachin Datta) [consolidated judgment on the Right to be Forgotten, de-indexing, and masking of judicial records].

interests in the absence of adequate legislative guidance. Finally, it offers an original set of policy proposals to restore a principled balance.

II. THE CONSTITUTIONAL ROOTS OF THE RIGHT TO BE FORGOTTEN IN INDIA

To understand the RTBF, it is important to first understand what it is not. It is not a right to rewrite history, nor a mechanism for sanitising a person's public record at will. The RTBF is, more precisely, the legally enforceable interest of an individual to demand that personal data which is no longer accurate, relevant, or proportionate be removed from active digital circulation. It operates not against the existence of historical records, but against their perpetual, unmediated amplification through commercial search infrastructure.

Indian jurisprudence recognises a conceptual predecessor in what one might call the 'Right to Forget' the idea that historical events should, by virtue of time and distance, naturally recede from public consciousness. Physical archives faded; newspaper clippings yellowed; public memory was limited by geography and attention. The digital revolution, however, destroyed these natural mechanisms of informational decay. Search engines transformed every publicly archived fact into a permanent, instantly retrievable data point, no matter how old, how minor, or how personally devastating to the individual concerned.

The foundational legal recognition of the RTBF in India came through the Supreme Court's landmark nine-judge bench ruling in *K.S. Puttaswamy v. Union of India* (2017).⁴ The plurality opinion established that the right to privacy is a fundamental right protected under Article 21 of the Constitution of India. Crucially, the Court held that privacy encompasses 'informational self-determination' the individual's ability to control the collection, storage, dissemination, and retrieval of information about themselves. This principle constitutes the direct constitutional foundation for the RTBF in India.

However, the Court was equally clear that privacy is not an absolute value. It must be balanced against competing fundamental rights, including the right to freedom of speech and expression under Article 19(1)(a)⁵ and the public interest in transparency and accountability. The tension this creates is not a weakness in the constitutional framework; it is, in fact, the very thing that makes the framework honest. The challenge has been to translate that constitutional balance into workable statutory and judicial mechanisms and this is precisely where the Indian legal system has struggled.

III. THE DPDP ACT, 2023: THE STATUTORY FRAMEWORK AND ITS LIMITATIONS

India's first comprehensive data protection legislation, the DPDP Act, 2023⁶, does not expressly use the phrase 'Right to be Forgotten.' Nevertheless, Section 12 of the Act which codifies the

⁴ *Id* 2

⁵ Constitution of India, 1950, Art. 21 (Right to Life and Personal Liberty); Art. 19(1)(a) (Freedom of Speech and Expression).

⁶ DPDP Act, 2023, s. 12 (Right to correction and erasure of personal data).

‘right to correction and erasure of personal data’ operationalises its core content.⁵ Under Section 12, a data principal (the individual whose data is processed) may demand that a data fiduciary (the entity processing the data) erase their personal data when that data is no longer necessary for the purpose for which it was collected, unless retention is required for legal compliance or statutory performance.

The procedural framework for the Act was further established by the Digital Personal Data Protection Rules, 2025, notified on November 14, 2025.⁷ Together, they create an 18-month compliance runway for data fiduciaries, with full enforcement projected for May 2027. The Data Protection Board of India, established under the Act, functions as the primary adjudicatory authority for data protection disputes.

A. The Publicly Available Data Exemption: A Critical Blind Spot

The most consequential limitation of the DPDP Act’s erasure regime is found in Section 3(c), which carves out an exemption for ‘publicly available’ personal data.⁸ Under this provision, data that was either voluntarily made public by the data principal or was required to be made public under any law in force falls entirely outside the Act’s protective scope. This means that any secondary processor including commercial search engines and AI developers can scrape, index, and indefinitely process such publicly available data without seeking consent or offering any erasure right to the individual concerned.

The practical implications of this gap are serious. News articles, court judgments, government gazettes, and other public records all of which frequently contain identifying personal information about private individuals are beyond the reach of Section 12. An acquitted person whose name appears in a published court order, or a welfare beneficiary whose details appear in a government notification, has no statutory remedy under the DPDP Act to prevent a search engine from making that information permanently and prominently accessible. Their only recourse is to approach the constitutional courts directly under Article 21 an expensive, slow, and inaccessible process for most citizens.

This is not merely a technical drafting gap. It reflects a fundamental policy choice to protect the integrity of public records at the cost of individual privacy a choice that has been made without any explicit statutory acknowledgment of the trade-off involved, and without providing any guidance on how that balance should be struck in contested cases.

IV. SECTION 44(3) AND THE DILUTION OF THE RIGHT TO INFORMATION

While the DPDP Act’s erasure provisions have attracted most of the academic commentary on privacy, the Act’s most significant impact on public life may, paradoxically, be in the domain of transparency. Section 44(3) of the DPDP Act amended Section 8(1)(j) of the RTI Act, 2005 - the

⁷ Digital Personal Data Protection Rules, 2025, notified on November 14, 2025 (India).

⁸ DPDP Act, 2023, § 3(c) (Applicability exemptions - publicly available personal data).

provision most frequently invoked to withhold personal information in response to public information requests.⁹ The nature of this amendment represents a fundamental recalibration of the balance between citizen access to government information and individual privacy.

A. The Original Framework: A Nuanced Balancing Test

The original Section 8(1)(j) of the RTI Act was deliberately crafted as a qualified exemption.¹⁰ Public Information Officers (PIOs) were required to apply a three-part contextual test: they had to evaluate whether the personal information had a relationship to any public activity or interest, whether disclosure would constitute an ‘unwarranted invasion of privacy,’ and whether a larger public interest justified disclosure. The burden of proof rested on the public authority to demonstrate that withholding was justified.

The provision also contained a critical structural safeguard a Parliamentary proviso stipulating that information which cannot be denied to Parliament or a State Legislature cannot be denied to an ordinary citizen. This proviso operationalised a basic principle of popular sovereignty: that citizens, as the ultimate holders of democratic authority, cannot be placed in a position of informational inferiority relative to their elected representatives when it comes to government activities.

B. The Post-Amendment Framework: An Unqualified Barrier

The amendment introduced by Section 44(3) of the DPDP Act replaced this nuanced framework with a blunt instrument.¹¹ The revised text simply exempts ‘information which relates to personal information’ without any qualification regarding public relevance, the nature of the activity, or the proportionality of non-disclosure. The Parliamentary proviso was deleted entirely.

The consequences have been immediate and significant. PIOs now routinely invoke the amended Section 8(1)(j) to deny requests for information that courts and Information Commissions had, for nearly two decades, consistently treated as public: the names and designations of civil servants involved in public contracts; the academic credentials of government officials; disciplinary records of public functionaries; details of welfare scheme beneficiaries. A telling example emerged in early 2025, when an activist seeking the names of employees involved in a municipal road contract awarded by the Bruhat Bengaluru Mahanagara Palike (BBMP) was refused disclosure on the ground that it would violate the DPDP Act. This directly contradicts long-settled RTI

⁹ Right to Information Act, 2005, No. 22 of 2005, s. 8(1)(j) (India) [hereinafter RTI Act], as amended by DPDP Act, 2023, s.44(3).

¹⁰ RTI Act, 2005, s. 8(1)(j) (original text, prior to DPDP Act amendment): "information which relates to personal information the disclosure of which has no relationship to any public activity or interest, or which would cause unwarranted invasion of the privacy of the individual unless the Central Public Information Officer or the State Public Information Officer or the appellate authority, as the case may be, is satisfied that the larger public interest justifies the disclosure of such information.

¹¹ Karnataka State Information Commission, Function Test ruling (2025–26): personal data relating to official functions of public servants remains disclosable under the RTI Act notwithstanding the DPDP Act amendment.

jurisprudence establishing that public servants' identities in the exercise of official functions are matters of public record.

This gap has produced a troubling divergence among State Information Commissions. The Karnataka SIC has adopted a 'Function Test,' holding that data relating to the official performance of public functionaries remains disclosable regardless of the amendment.²⁰ The Maharashtra SIC, by contrast, applies a 'Contextual Harm Test,' allowing redaction of even official data where specific circumstances suggest a risk of individual harm¹². The existence of two fundamentally opposed approaches within the same national legal framework is a sign of serious structural failure.

The deletion of the Parliamentary proviso carries its own distinct constitutional weight. Citizens now have fewer rights to government information than their elected representatives an inversion of the logic of popular sovereignty that animated the RTI Act in the first place. The challenges to Section 44(3) now pending before the Supreme Court are therefore not merely technical legal disputes; they raise foundational questions about what kind of democracy India intends to be in the digital age.

V. JUDICIAL RESOLUTION: THE DELHI HIGH COURT'S FRAMEWORK IN LAKSH VIR SINGH YADAV

In the absence of a balanced statutory framework, the Indian judiciary has stepped into the space left by the legislature. The Delhi High Court's consolidated judgment of May 29, 2026 in *Laksh Vir Singh Yadav v. Union of India & Ors*¹³ represents the most comprehensive judicial elaboration of the RTBF in India to date. The judgment, delivered by Justice Sachin Datta, addresses what the legislature conspicuously failed to: how privacy and transparency are to be practically reconciled in the context of digital judicial records.

A. The Open Justice–Indexing Distinction

The analytical heart of the judgment lies in Justice Datta's distinction between 'open justice' as a matter of record-keeping integrity, and 'commercial name-based indexing' as a distinct act of informational amplification. The Court held that the principle of open justice requires that judicial records exist, remain authentic, and remain retrievable through structured, purposive legal searches by case number, citation, court, or date. What open justice does not require is that a private citizen's name function as a permanent, globally searchable commercial keyword on platforms like Google.

This distinction is both intellectually sound and practically important. A search engine is not a passive repository; it is an active data processor that organises and retrieves information in ways designed to maximise retrieval frequency and visibility. When a person's name becomes a search

¹² Maharashtra State Information Commission, Contextual Harm Test ruling (2025–26): official data may be redacted under amended § 8(1)(j) if specific facts indicate risk of harassment or personal harm to the individual.

¹³ *Id* 3

keyword that instantly surfaces a decades-old acquittal, discharge, or private civil dispute, the privacy intrusion is qualitatively different from and far greater than the original act of making the judicial record public. The Court's framework correctly identifies this amplification as the source of the harm, not the existence of the record itself.

B. The Three-Tier Test for De-Indexing

To operationalise the RTBF in this context, the Court established a rigorous Three-Tier Test for determining eligibility for de-indexing orders:¹⁴

First, the character of the information and the outcome of concluded proceedings. Relief is primarily available where proceedings concluded in acquittal, discharge, quashing, or mutual settlement outcomes that carry a legal presumption of innocence or the extinguishment of public interest. Conversely, convictions for serious offences, crimes against women and children, or violations of public trust attract a strong presumption against relief.

Second, the public role of the individual. Public officials and those who have voluntarily entered public life carry heightened transparency expectations with respect to their exercise of public duties. They cannot invoke the RTBF to curate their public image or suppress information about their official conduct. However, this is not an absolute bar a public official involved in a purely private or matrimonial dispute retains the same privacy interest as an ordinary citizen.

Third, accuracy and relevance over time. The Court must assess whether the information has become obsolete, excessive, or misleading through the passage of time. This imports a temporal proportionality dimension into the analysis recognising that information which was once legitimately public may, over decades, become so disconnected from any current public interest as to justify restricting its active digital promotion

C. Masking: A Complementary Remedy

Beyond de-indexing, the Court also addressed the remedy of 'masking' the practice of redacting personal identifiers such as names from published judgments and replacing them with neutral placeholders. Drawing on its consolidated consideration of *Abhishek Beri v. Union of India*,¹⁵ the Court established strict parameters: masking orders can only be passed by the court that authored the original judgment, preserving judicial supervisory authority over its own records. Only identifiers are redacted; the substantive legal reasoning remains intact and fully accessible. Unredacted versions are permanently preserved in internal court records. And masking applies both retrospectively and prospectively to digital databases.

The Court also addressed the critical question of territorial scope, holding that de-indexing orders must operate globally not merely on national domain extensions like google.co.in. The practical

¹⁴ Laksh Vir Singh Yadav, 2026 DHC 4891 (Three-Tier Test for eligibility for de-indexing: (i) character of information and outcome of proceedings; (ii) public role of the individual; (iii) accuracy and relevance of information over time).

¹⁵ *Abhishek Beri v. Union of India* (consolidated in Laksh Vir Singh Yadav, 2026 DHC 4891), holding that masking orders can only be passed by the court that authored the original judgment.

reasoning is compelling: restricting orders to national domains is trivially circumvented by switching to google.com. A remedy that can be bypassed with a single keystroke is no remedy at all. The Court further confirmed that writ petitions under Article 226 are maintainable directly against private intermediaries like Google and Indian Kanoon, whose processing operations directly cause the constitutional harm under Article 21 and who are bound by statutory duties under the IT Rules, 2021.¹⁶

VI. COMPARATIVE PERSPECTIVES: WHAT INDIA CAN LEARN

India's constitutional dilemma is not unique. Two international models offer instructive, though imperfect, guidance.

A. The European Union: Dignity-First, Balanced by Exceptions

The European Union's General Data Protection Regulation (GDPR) provides the most developed statutory framework for the RTBF anywhere in the world. Article 17 of the GDPR codifies a 'Right to Erasure,' allowing individuals to demand deletion of personal data when it is no longer necessary, when consent is withdrawn, or when there is no overriding legitimate interest in continued processing.¹⁷ Crucially, however, Article 17(3) contains explicit balancing exceptions, protecting processing necessary for the exercise of freedom of expression and information, legal compliance, public health, and archival and research purposes in the public interest.¹⁸

The GDPR model is notable for institutionalising the balancing exercise within the statute itself. Rights and exceptions are set out at the same legislative level, preventing either value from being structurally privileged over the other. The enforcement architecture through independent Data Protection Authorities also provides an expert administrative intermediary that can develop contextual norms over time. This stands in contrast to India's current situation, where the absence of statutory balancing is forcing case-by-case constitutional adjudication.

B. The United States: Speech-First, at the Cost of Individual Privacy

The United States represents the opposite pole. American jurisprudence categorically rejects any general right to be forgotten, treating it as a form of government-mandated censorship incompatible with the First Amendment. In *Cox Broadcasting Corp. v. Cohn* (1975) and *Florida Star v. B.J.F.* (1989),¹⁹ the Supreme Court of the United States established that once truthful information is obtained from lawfully accessible public court files or official records, the state

¹⁶ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (India), Rule 3 (obligations of significant social media intermediaries).

¹⁷ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), Art. 17 [hereinafter GDPR].

¹⁸ GDPR, Art. 17(3) (exceptions to the right to erasure for freedom of expression, legal obligations, public health, and archival purposes in the public interest).

¹⁹ *Cox Broadcasting Corp. v. Cohn*, 420 U.S. 469 (1975); *Florida Star v. B.J.F.*, 491 U.S. 524 (1989).

cannot constitutionally sanction the press for publishing it. The American model treats historical accuracy and the free flow of information as presumptively superior to individual privacy interests, permitting only narrow exceptions.

The American approach provides robust protections for journalism, archival scholarship, and democratic accountability. However, it also leaves individuals with no legal recourse against the permanent digital exhibition of embarrassing, harmful, or simply outdated information about them. In a world where private actors not government agencies control the dominant channels of information access, a framework that relies almost entirely on the voluntary editorial policies of media organisations offers inadequate protection for personal dignity.

C. India's Calibrated Path

India's constitutional tradition positions it between these two extremes. The Puttaswamy judgment's recognition of privacy as a fundamental right reflects the dignity-centred approach of the European model. But India's constitutional framework also contains robust free speech protections and a strong commitment to the structural necessity of public information in a democracies values closer to the American tradition. The Justice Srikrishna Committee Report (2018)²⁰ recognised this through its proposed five-factor balancing test, and early legislative drafts like the Personal Data Protection Bill, 2019²¹ attempted to codify it. The DPDP Act's abandonment of this nuanced framework in favour of a simplified erasure right and an unqualified RTI exemption represents a step backward from the sophisticated balance those earlier formulations had attempted to achieve.

VII. THE PENDING SUPREME COURT CHALLENGES

The constitutional fault lines created by the DPDP Act have now reached the Supreme Court of India. Clubbed together in early 2026, the pending petitions challenge three structural features of the Act:

The challenge to Section 44(3) argues that converting the qualified RTI exemption into an unqualified barrier violates the fundamental right to information under Article 19(1)(a), and fails the three-pronged test of legality, legitimate aim, and proportionality established in Puttaswamy itself. The argument is structurally compelling: using a privacy law to weaken the primary instrument of governmental transparency without providing any alternative mechanism for citizens to access public interest information cannot satisfy a proportionality analysis under constitutional law.

The second challenge targets the Act's removal of civil remedies for individuals harmed by data breaches. Earlier legislative drafts had preserved the right of data principals to seek civil damages

²⁰ Justice B.N. Srikrishna Committee, 'A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians' (Ministry of Electronics and Information Technology, Government of India, 2018).

²¹ Personal Data Protection Bill, 2019 (India), Cl. 20 (Right to be forgotten — five-factor balancing test drawn from the Srikrishna Committee Report).

in ordinary courts for negligent or unauthorised data processing. The DPDP Act, 2023, channels all grievance redressal exclusively through the Data Protection Board, a state-appointed body without providing for direct access to judicial remedies. Petitioners argue this unconstitutionally restricts the right to an effective judicial remedy, a right that flows from both Article 21 and the basic structure of the Constitution.

The third challenge addresses the Act's broad exemptions for government agencies, which permit processing of personal data without consent for national security, law enforcement, and public order purposes, without requiring independent judicial oversight. Critics contend that these exemptions, in combination, create a statutory foundation for a mass surveillance architecture, the very threat that the Puttaswamy judgment was most acutely concerned with preventing.

The Supreme Court's refusal in February 2026 to grant an interim stay on the RTI amendment, citing the need for deep constitutional adjudication and referring the matter to a larger bench, signals the gravity of the issues at stake. The outcome of these proceedings will define the constitutional boundaries of data governance in India for a generation.

VIII. TOWARDS A PRINCIPLED FRAMEWORK: POLICY RECOMMENDATIONS

The current legal framework leaves both privacy and transparency in an unstable, contested position. The following three structural reforms would establish a principled and durable equilibrium.

A. Restore Contextual Balancing to the RTI Act

The absolute language introduced by Section 44(3) should be replaced with a statutory balancing test. Drawing on the Srikrishna Committee's recommendations¹² and the pre-amendment text of Section 8(1)(j),²² Parliament should require PIOs to evaluate: the sensitivity of the personal data concerned; its relationship to any public activity or duty; the temporal gap between the data's creation and the disclosure request; the potential harm of disclosure to the individual; and whether a larger public interest justifies disclosure. The Parliamentary proviso ensuring parity between citizens and legislators in access to government information must be reinstated. Balancing tests are more administratively demanding than bright-line rules, but in this domain, nuance is not optional: it is constitutionally required.

B. Integrate Privacy-by-Design into Judicial Records Management

The current model where individuals must pursue expensive constitutional litigation to achieve de-indexing or masking is structurally unjust. Most people whose privacy is harmed by the permanent digital amplification of old legal proceedings lack the resources, knowledge, or time to approach the High Court under Article 226. A systematic solution is needed.

²² SUPRA 21

Court management systems should be redesigned to incorporate privacy-by-design protocols. Cases resulting in acquittal, discharge, or quashing should trigger an automatic review of whether the judgment is appropriate for name-masking before digital publication. Parties in private matrimonial or family law proceedings should be able to apply for pseudonymisation at the time of filing, not merely after the harm has already occurred. Unredacted versions should be preserved in internal, access-controlled court archives. This systemic approach would deliver privacy protection at scale, without requiring individual litigants to navigate the constitutional courts.

C. Legislatively Define the Public–Private Boundary

Regulatory and judicial guidance has attempted to distinguish between a public servant’s official conduct and their private life, but this distinction urgently needs legislative codification. Parliament should establish a clear statutory presumption: that information relating to the exercise of public office, the use of public funds, and the making of administrative decisions carries a strong public interest that overrides privacy claims under both the RTI Act and the DPDP Act. Conversely, intimate personal data medical records, domestic addresses, family relationships, and disputes entirely unrelated to official duties should receive strong protection from public disclosure unless a direct systemic public interest is affirmatively demonstrated.

This clear demarcation would resolve the current divergence between State Information Commissions and provide PIOs, courts, and the Data Protection Board with a workable framework for the thousands of individual decisions they must make each year.

IX. CONCLUSION

The conflict between the Right to be Forgotten and the Right to Know is not a conflict between good values and bad ones. Both privacy and transparency are indispensable to a functioning democratic society: privacy protects individuals from the disproportionate consequences of their digital footprint; transparency holds public power accountable and enables citizens to make informed choices about those who govern them. The error the DPDP Act, 2023, has made is not in attempting to protect privacy, but in doing so through structural choices that privilege one value over the other without adequate justification, proportionality, or balancing mechanism.

The Delhi High Court’s judgment in *Laksh Vir Singh Yadav*²³ demonstrates that principled reconciliation is not only possible but judicially achievable. The Three-Tier Test, the open justice–indexing distinction, and the global scope of de-indexing orders together constitute a sophisticated, rights-respecting framework that neither the legislature nor the executive has yet matched. The constitutional challenges now before the Supreme Court offer an opportunity to translate these judicial insights into binding constitutional doctrine.

²³ ID 3

India stands at a crossroads in its data governance journey. The question is whether it will build a framework that genuinely protects individuals while preserving the public's right to know or whether it will settle for a system where privacy becomes a shield for institutional opacity and transparency becomes an instrument for individual humiliation. The constitutional imperative, rooted in the values of both Article 21 and Article 19(1)(a), demands the former. It is now for the legislature and the Supreme Court to deliver it.