INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

FINDING THE RIGHT BALANCE BETWEEN TRANSPARENCY AND DIGITAL ERASURE UNDER SECTION 8(1)(J) OF THE RTI ACT, 2005

AUTHORED BY - PRAGATI BAJPAI
Designation - Research Scholar

Abstract

The Right to Information (RTI) Act, 2005[1] and the emerging Right to Be Forgotten (RTBF) present two seemingly conflicting rights—the public's right to access government-held information and the individual's right to privacy. Section 8(1)(j)[2] of the RTI Act exempts personal information from disclosure when such disclosure would cause an unwarranted invasion of privacy, unless the larger public interest justifies it. The constitutional recognition of privacy as a fundamental right in Justice K.S. Puttaswamy v. Union of India[3] and the enactment of the Digital Personal Data Protection Act, 2023[4] (DPDPA) have transformed the understanding of informational privacy and the public's right to know.

This paper examines the evolving jurisprudential interplay between transparency and digital dignity, focusing on how RTBF can be reconciled within the RTI framework without undermining government accountability or freedom of expression. It argues that privacy exemptions under Section 8(1)(j)[5] must be interpreted in a manner consistent with constitutional values, balancing individual dignity with democratic transparency. The study highlights challenges posed by expanding digital footprints and persistent data availability in government repositories, which complicate the exercise of RTBF rights alongside RTI obligations.

The paper explores the implications of the DPDPA for RTI applications, emphasizing the need for legal clarity and procedural mechanisms to address conflicts between privacy and public information demands. Through comparative analyses and doctrinal scrutiny, the paper

[1] Right to Information Act, Act No. 22, Acts of Parliament, 2005 (India).
[2] Right to Information Act, S. 8(1)(j), Act No. 22, Acts of Parliament, 2005 (India).
[3] Justice K.S. Puttaswamy v. Union of India (2017) 10 SCC 1.
[4] Digital Personal Data Protection Act, Act No. 22, Acts of Parliament, 2023 (India).
[5] Supra note 2.

ISSN: 2582-6433

proposes a framework aligning RTI laws with contemporary data protection principles to foster accountability while respecting digital autonomy. In conclusion, the paper advocates for an integrated approach that harmonizes the RTI Act's transparency goals with the RTBF's privacy imperatives, ensuring robust democratic governance and protection of individual rights in India's digital age.

Keywords: Right to Information, Right to Be Forgotten, Privacy, Data Protection, Transparen cy, Digital Dignity.

1. INTRODUCTION

Transparency and privacy represent twin pillars of India's constitutional democracy. The RTI Act, 2005 signals a nationwide shift towards governmental accountability, empowering citizens through access to previously opaque administrative records. With rising digitization and the advent of information technologies, the storage and dissemination of personal data have increased dramatically, making individual privacy more vulnerable. The rise of the digital era has amplified the complexity surrounding the conciliation of information access and privacy concerns.[6]

Both the right to information and the right to privacy are critical human rights that primarily serve to ensure government accountability to the individual.[7] However, the request for personal information stored by government bodies inevitably leads to a discrepancy between these rights.[8]

The legislative journey in India has attempted to manage this conflict, first through the RTI Act and its exceptions, and now through the comprehensive data protection framework of the DPDP Act, 2023.[9] Supreme Court jurisprudence, especially Retd. Justice K.S. Puttaswamy v. Union of India[10], has aligned privacy with human dignity and autonomy, heightening the stakes for balancing state transparency and personal honor.

[6]Markkula Center for Applied Ethics, Rights, available at: https://shorturl.at/mquS1 (last visited on September 10, 2025).
[7] Vijay Pal Dalmia, "India: Data Protection Laws in India - Everything You Must Know" Mondaq, December 13, 2017, available at: https://www.mondaq.com/india/data-protection/655034/data-protection-laws-in-india--everything-you-must-know (last visited on September 10, 2025).
[8] Ibid.
[9] P Arun, "A Soft Tone with a Tiger Claw-A Critical Commentary on the Digital Personal Data Protection Bill, 2022" 58 (6) Economic and Political Weekly 10 (2023)
[10] Justice K.S. Puttaswamy v. Union of India (2017) 10 SCC 1.

ISSN: 2582-6433

The DPDP Act, in conjunction with the *Puttaswamy*[11] judgment, marks a crucial milestone in the voyage of the right to privacy, making "Consent" paramount for data processing and ensuring information self-determination for the "Data Principal."[12] The Act promotes transparency and accountability by assigning rights and duties to the Data Principal and the Data Fiduciary.[13]

Section 8(1)(j) is central in this dynamic landscape, acting both as a safeguard for privacy and a gatekeeper for legitimate public interest. The doctrinal and procedural evolution of this provision illuminates broader trends in Indian regulatory thought – oscillating between maximal public access and vigorous individual protection.

This paper will demonstrate that while the DPDP Act strengthens privacy, its amendment to the RTI Act compromises the carefully calibrated balance that previously existed, necessitating a renewal of the public interest test.

2. The Pre-DPDP Paradigm: Section 8(1)(j) and the Public Interest Override

2.1. The Constitutional Basis and Original Conflict

Prior to 2023, the Right to Information (RTI) Act, 2005, and the burgeoning Right to Privacy stood in a state of dynamic equilibrium, primarily regulated by Section 8(1)(j) of the RTI Act.[14] The genesis of this conflict lies in the Indian Constitution itself: the Right to Information is an indispensable derivative of Article 19(1)(a)[15], guaranteeing freedom of speech and expression, which inherently includes the public's right to know about governmental functions. The Right to Privacy, recognized as a fundamental and inalienable component of the Right to Life under Article 21[16] following the landmark judgment in *Justice K.S. Puttaswamy v. Union of India* (2017)[17], ensures an individual's control over their personal information and digital dignity.

The very purpose of the RTI Act is to ensure government accountability and openness; however, in seeking to attain this goal, it often necessitates the disclosure of records that contain

[11] Ibid.
[12] Digital Personal Data Protection Act, Sec. 2(i), Act No. 22, Acts of Parliament, 2023 (India).
[13] Digital Personal Data Protection Act, Sec. 2(j), Act No. 22, Acts of Parliament, 2023 (India).
[14] Right to Information Act, S. 8(1)(j), Act No. 22, Acts of Parliament, 2005 (India).
[15] The Constitution of India, Article 19(1)(a).
[16] The Constitution of India, Article 21.
[17] Justice K.S. Puttaswamy v. Union of India (2017) 10 SCC 1.

ISSN: 2582-6433

private, third-party information. This is where the discrepancy between the two rights—both crucial to democratic governance—arises. Section 8(1)(j) was therefore crafted as a "constitutional bridge" between transparency and privacy, providing an exemption for personal data only where specific conditions were met. The provision exempted from disclosure:

"...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."[18]

The latter clause—the 'unless' proviso—was the pivotal mechanism. It demanded a nuanced, rights-based interpretation consistent with constitutional values, recognizing that while privacy is fundamental, it is not absolute, like other rights, and must yield to a compelling "larger public interest."[19] The proviso was often considered the "acid test" of the Section, requiring the Information Officer to make a subjective, yet judicially reviewable, assessment based on a quasi-legislative standard: whether the information would have been denied to Parliament or the State Legislature before refusing a citizen's request. The Section thereby aimed to fine-tune the balance between one's personal information and the need for transparency in public life.[20]

2.2. Judicial Interpretation of the Balancing Test

The pre-DPDP regime was characterized by a jurisprudence that stressed the balancing act as a "herculean task" but necessary to attain the common goal of government accountability. The Supreme Court and various Information Commissions established clear principles for the application of Section 8(1)(j) to ensure that the fundamental right of RTI was not unnecessarily constricted:

- Restriction to Third-Party Information: The applicability of Section 8(1)(j) was strictly restricted to the disclosure of third-party information, which, if released, would constitute an unwarranted invasion of the individual's private domain. This implied that information pertaining to a public servant's professional activity or performance, as long as it related to their official duties and public interest, could not be automatically protected under this provision.

[18] Centre for Right to Information, Yashada, Pune, Data Privacy and Right to Information
[19] Shailesh Gandhi, Critical Analysis of Supreme Court Judgements on the RTI Act, 2005.
[20] Mr. Dharmendra Kumar, Impact of the Digital Personal Data Protection Act, 2023 on Third-Party Information under the Right to Information Act, 2005: A Critical Analysis

ISSN: 2582-6433

- The Non-Absolute Nature of Privacy: The courts reiterated that privacy, though fundamental post-*Puttaswamy*, was subject to reasonable restrictions, including those imposed by the necessity of information access for democracy. The disclosure of information was required to be justified by a larger public interest, effectively requiring the application of a proportionality test to weigh the harm to the individual's privacy against the public benefit derived from the disclosure.
- Landmark Pro-Transparency Benchmarks: The Supreme Court's judgment in *Reserve Bank of India v. Jayantilal N. Mistry & Ors.* (2015)[21] stands as a significant pro-transparency benchmark. The ruling strongly affirmed the spirit of the RTI Act and the vitality of the public interest override, particularly concerning institutional and systemic information, demonstrating a clear judicial inclination towards disclosure when government accountability was at stake.

This robust mechanism ensured that information disclosure decisions were made on a case-by-case basis, rather than through a blanket rule. By emphasizing the requirement of public interest and the principle of proportionality, the legal framework had, before the 2023 amendment, found a delicate and rights-based methodology for maintaining the dynamic equilibrium between transparency and privacy in the Indian context.

3. The Paradigm Shift: The DPDP Act, 2023 and the Unqualified Exemption

3.1. The Legislative Mandate of the DPDP Act

The enactment of the Digital Personal Data Protection Act, 2023 (DPDP Act), fundamentally reshaped India's legal landscape concerning informational privacy. It establishes a rigorous, principles-based framework intended to govern the processing of digital personal data, thereby ensuring data protection and self-determination for the "Data Principal."[22] This legislative move was a direct response to the Supreme Court's mandate in the *Puttaswamy* judgment, which declared privacy a fundamental right under Article 21, thereby necessitating a statutory mechanism to safeguard personal data and the individual's control over its dissemination.

The Act's core tenets revolve around "Consent" being paramount for all data processing actions, promoting transparency and accountability by assigning explicit rights and duties to both the Data Principal and the Data Fiduciary. While the DPDP Act is primarily designed to regulate

[21] Reserve Bank of India v. Jayantilal N. Mistry & Ors. AIR 2016 SUPREME COURT 1.
[22] Digital Personal Data Protection Act, Sec. 2(i), Act No. 22, Acts of Parliament, 2023 (India).

ISSN: 2582-6433

data processing in the private and public sectors, its legislative sweep was broad enough to impact pre-existing laws, specifically the RTI Act, where the two statutes intersected over the release of personal information.

3.2. The Amendment to Section 8(1)(j)

The most significant and debated impact of the DPDP Act on the RTI regime is the amendment to Section 8(1)(j), accomplished through Section 44(3) of the new law.[23] This amendment did not merely tweak the wording; it dramatically altered the mechanism for balancing the conflicting rights by eliminating the critical 'public interest' override that had previously defined the equilibrium.

The original clause, which allowed for disclosure *unless* the larger public interest justified it, was entirely removed. The amended Section 8(1)(j) now essentially substitutes the specific conditions and balancing test with a generic reference to the DPDP Act, effectively stating that personal information shall not be disclosed, subject to the DPDP Act's provisions.

This legislative change has the profound effect of transforming privacy from a qualified exemption into an unqualified, or absolute, exemption from information disclosure under the RTI Act.[24] In simple terms, where the previous law required the Information Commission to actively weigh the individual's privacy interest against the larger public benefit of disclosure, the new law makes the existence of personal data a near-automatic barrier to disclosure.

The foundational principles of the Indian democratic framework—transparency (derived from Article 19(1)(a)) and personal autonomy (guaranteed by Article 21)—create a persistent legal tension when a citizen's right to access public records overlaps with the privacy rights of an individual. While these two rights are generally co-supportive in holding the government accountable, their inherent contradiction surfaces precisely when a request for information mandates the disclosure of personal data stored by a public authority.[25] Addressing this friction requires a syncretic jurisprudence, ensuring that statutory safeguards from both the data protection and information access regimes are applied consistently and in a harmonized

[23] Ibid sec. 44.
[24] Mohammad Omar Hashmi; Adnan Ahmad, "Data Protection Bill: A Comparative Study of the Indian Data Privacy Dilemma" 3(3) Jus Corpus Law Journal 515 (2023).
[25] Angad Haksar, "Analysing the Digital Personal Data Protection Bill, 2022" 5 Indian Journal of Law and Legal Research 4 (2023).

ISSN: 2582-6433

manner.

Prior to the recent amendments, the unamended Section 8(1)(j) of the Right to Information Act, 2005, was crafted to serve this function. It provided a qualified exemption that protected the release of "personal information" which had no demonstrable connection to any public activity or interest, thereby shielding an individual's private domain from unwarranted invasion. Crucially, the section was not an absolute barrier; it contained the pivotal public interest override, which explicitly mandated that information *must* be disclosed if the larger public interest in transparency outweighed the potential harm to the individual's privacy. This proportionality test empowered Information Commissioners to make a nuanced, rights-based determination on a case-by-case basis.

By establishing this fluid equilibrium, the provision effectively ensured that the twin pillars of constitutional governance—the public's right to know and the individual's right to digital dignity—could coexist, preventing the use of privacy as a blanket shield for official secrecy while upholding democratic scrutiny.[26]

The recognition of personal information as an absolute exemption aligns with the goal of aggressively safeguarding the fundamental right of privacy as envisioned post-2017. However, this absolute protection comes at the cost of compromising democratic accountability. By eliminating the public interest override, the amendment significantly diminishes the discretionary powers of Information Commissioners who previously acted as constitutional arbiters in this conflict.[27] This shift prevents the disclosure of personal data even in cases of blatant corruption, misuse of public office, or systemic failure, where the larger public interest in transparency is overwhelmingly evident.[28] The outcome is a potential legislative imbalance, prioritizing the fundamental right to privacy in an unqualified manner over the derived, yet equally vital, fundamental right to information, leading to the risk of increased governmental secrecy under the guise of data protection.

[26] The Hindu Bureau, "Digital Personal Data Protection Bill, 2023 passes in Lok Sabha; govt. shrugs off exemptions" The Hindu, August 07, 2023, available at: https://www.thehindu.com/news/national/data-bill passes-in-lok-sabha-govt-shrugs-off-exemptions/article67167943.ece (last visited on March 10, 2025).
[27] Lalit Dadwal, "Right to Information" M.D.U. Law Journal, Vol. X. Part 1, 2005.
[28] Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy" 4(5) Harvard Law Review 193-220 (1890). 1890.

ISSN: 2582-6433

4. Critical Analysis: Eroding Transparency and Global Isolation

The legislative decision to amend Section 8(1)(j) of the RTI Act through the provisions of the DPDP Act, 2023, marks a significant moment of retreat in India's journey towards comprehensive public transparency. While seemingly a logical extension of the fundamental right to privacy established by *Puttaswamy*, the practical effect of converting the personal information exemption into an absolute bar, unqualified by the public interest, is to create a new mechanism for governmental opacity. The resulting paradigm shift elevates the right to privacy to an unchallenged supremacy over the right to know, leading to a critical erosion of democratic accountability and placing India in an isolated position compared to other major democracies.

4.1. Impact on Accountability and Third-Party Information

The unqualified nature of the new exemption creates significant challenges by arguably prioritizing privacy over transparency, particularly concerning third-party information held by public authorities. The DPDP Act, in its effort to enhance personal data protection, may inadvertently compromise transparency by severely limiting access to data that is demonstrably in the public interest, most notably the operational details and conduct of public functionaries. The constitutional jurisprudence on transparency has always rested on the principle that the public servant, by accepting a position of authority, subjects their professional life to a higher degree of public scrutiny. This constitutional expectation of accountability is rooted in the very nature of public office, where the actions undertaken are on behalf of the populace. By removing the public interest override, the new regime compromises the ability of citizens to exercise their right to scrutinize governmental actions.

The practical consequences of this legislative overreach are substantial:

- **Reduced Public Servant Accountability:** Information relating to public servants' performance, disciplinary records, discretionary decision-making, or even certain asset declarations—which may be broadly construed as "personal information"—could now be absolutely shielded from disclosure, even in cases of suspected malfeasance or gross negligence. The potential chilling effect is clear: a citizen requesting a public servant's performance appraisal to assess their suitability for a high-level post, or details of a land allotment made to a third-party developer, could be summarily denied on the grounds that such disclosure constitutes an unwarranted invasion of privacy, regardless of the compelling public interest in preventing corruption or cronyism. The loss of the

ISSN: 2582-6433

override essentially provides a "secrecy cloak" to public officials, contradicting the fundamental premise that public servants operate under the constitutional expectation of public scrutiny.

- **Encouragement of Judicial Activism or Legislative Inertia:** The policy gaps resulting from the lack of a balanced public interest test and the potentially vague application of the term 'personal information' are destined to generate legal uncertainties and inconsistent application across various Information Commissions. This confusion directly threatens the RTI Act's historical role in ensuring quick and effective accountability. The Information Commissions, which were once vested with the crucial quasi-judicial power to perform this balancing act, now find their authority significantly curtailed[29]. This procedural gap creates a void that will likely be filled by an increased burden on the already-strained higher judiciary, forcing it to develop bespoke proportionality tests on a case-by-case basis—a process the RTI Act was meant to streamline and decentralize.

4.2. The Right to Be Forgotten (RTBF) and Digital Erasure

The DPDP Act's framework also introduces the concept of the Right to Be Forgotten (RTBF), an integral component of the right to digital erasure and the control over one's digital footprint.[30] The RTBF grants individuals the power to demand the deletion or de-indexing of their personal information when it is no longer necessary for the purpose for which it was collected or when its retention is unjustified.

The core legal challenge at this juncture is the fundamental conflict between the RTBF's mandate for *erasure* and the RTI's mandate for *public record retention and disclosure*. [31]Public records, by their very nature, are intended to be permanent, serving as historical evidence of governmental action and a check against executive overreach. Allowing an individual (even a public figure) to demand the erasure of records detailing their past official actions, even if old, potentially undermines the historical accountability function of public documents.

The previous qualified exemption under Section 8(1)(j) was a mechanism designed to manage this specific tension through proportionality before a RTBF claim could even be fully

[29] Gaurav Pathak, "Need for a Data Privacy Law" 57 (34) Economic and Political weekly 5 (2022).
[30] Karishma Sundara and Nikhil Narendran, "Protecting Digital Personal Data in India in 2023 is the lite approach, the right approach?" 24 (1) Computer Law Review International Journal 9 (2023).
[31] Angad Haksar, "Analysing the Digital Personal Data Protection Bill, 2022" 5 Indian Journal of Law and Legal Research 4 (2023).

ISSN: 2582-6433

articulated.[32] It enabled the Information Officer to weigh the public's right to access an individual's past official actions (e.g., decisions, expenditures, official correspondence) against the individual's right to digital dignity and the right to correct or minimize their persistent digital footprint. By removing the public interest criterion, the DPDP Act's influence risks making the public record ephemeral whenever it touches upon "personal data."

To mitigate this, a nuanced approach is imperative: promoting the anonymization of sensitive data before publication, especially for older records, and strengthening the proactive disclosure of non-personal information can help resolve conflicts between RTI obligations and RTBF rights without resorting to full erasure or denial.[33] This is the only way to safeguard both the historical accountability of the State and the individual's autonomy over their data.

4.3. Comparative Global Isolation

India's decision to eliminate the public interest override in the RTI Act stands as a significant divergence from the established democratic practice of leading jurisdictions around the world.[34] The absence of this key balancing mechanism risks isolating India from global best practices in information governance.

Comparative analysis reveals that other mature democracies have successfully institutionalized a calibrated public interest test to resolve the privacy-transparency conflict:

- **European Union (EU) - General Data Protection Regulation (GDPR):** The GDPR, considered the global gold standard for data protection, explicitly allows personal data processing and disclosure *without consent* when necessary for compliance with a legal obligation *or* when it is "necessary for reasons of substantial public interest." Crucially, the GDPR itself (Article 86) permits Member States to reconcile the right to personal data protection with the right to freedom of expression and information.[35] The EU model thus provides a definitive mechanism where the Data Protection Authority and the freedom of information regime must coexist and use a public interest test to arbitrate conflicts.

[32] Supranote 25.
[33] Vijay Pal Dalmia, "India: Data Protection Laws in India - Everything You Must Know" Mondaq, December 13, 2017, available at: https://www.mondaq.com/india/data-protection/655034/data-protection-laws-in-india--everything-you-must-know (last visited on September 10, 2025).
[34] Markkula Center for Applied Ethics, Rights, available at: https://shorturl.at/mquS1 (last visited on September 10, 2025).
[35] The General Data Protection Regulation, 2018, (EU 679 of 2016).

ISSN: 2582-6433

- **United Kingdom (UK) - Freedom of Information Act, 2000 (FOIA):** The UK FOIA employs a strong two-part public interest test for exemptions related to personal information (Section 40). Disclosure is permitted if, on balance, the public interest in disclosure outweighs the public interest in maintaining the exemption. This standard ensures that the public's right to know remains the primary consideration in cases involving official actions, thereby safeguarding government accountability and preventing excessive secrecy[36].

India's new law, by creating an absolute and unqualified exemption for personal data under the RTI Act, effectively contravenes the animating spirit of its own constitutional architecture—which requires fundamental rights to be balanced and subjected to reasonable restrictions—and represents a significant step away from these global democratic norms.[37] The desideratum, therefore, is not the wholesale acceptance of either privacy or disclosure, but the cultivation of a syncretic jurisprudence where both rights coalesce harmoniously through statutory mechanisms of proportionality and independent adjudication.

5. Harmonizing the Rights: Recommendations for a Syncretic Jurisprudence

The conflict arising from the DPDP Act's unqualified amendment to the RTI Act demands a constructive, legislative response to ensure that the fundamental rights of both transparency and privacy are not mutually exclusive. To restore the democratic *telos* of the Indian Republic and guarantee that governance remains both transparent and legitimate, a syncretic jurisprudence—where both legal frameworks are harmonized—is essential. This necessitates a deliberate re-engagement with the principle of proportionality, resurrecting the public interest override through new statutory mechanisms, and adopting institutional reforms that ensure both rights are respected in the digital age.

5.1. Reinstatement of a Balanced Public Interest Test

The most crucial step toward harmonizing the frameworks is a legislative amendment to reinstate a balanced public interest test within Section 8(1)(j) or as a clear exception within the DPDP Act itself. This move is paramount for balancing and harmonizing data protection with

[36] The Hindu Bureau, "Digital Personal Data Protection Bill, 2023 passes in Lok Sabha; govt. shrugs off exemptions" The Hindu, August 07, 2023, available at: https://www.thehindu.com/news/national/data-bill passes-in-lok-sabha-govt-shrugs-off-exemptions/article67167943.ece (last visited on March 10, 2025).
[37] Aditya Bashambu; Lavanya Chetwani, "Critical Analysis: Digital Personal Data Protection Bill 2022" 3 (2) Jus Corpus Law Journal 530 (2022).

ISSN: 2582-6433

the right to information, replacing the current absolute ban with a nuanced approach.

- **Adopting the Proportionality Test:** The restored test must explicitly require the application of a proportionality test before disclosure of personal data. This test, a cornerstone of constitutional law, would require the Information Commission to assess three factors:
    1. **Legitimate Aim:** Does the information request serve a legitimate public interest goal (e.g., accountability, anti-corruption, public health)?
    2. **Necessity:** Is the disclosure of personal data necessary to achieve that aim, or can the aim be achieved through less restrictive means (e.g., anonymization)?
    3. **Proportionality in the Strict Sense (Balancing):** Does the public interest served by the disclosure outweigh the harm caused to the individual's privacy? This provides a mechanism that is less restrictive than an absolute ban on disclosure.
- **A "Substantial Public Interest" Standard:** Following global precedents like the GDPR, the exception should be triggered only by a demonstration of "substantial public interest," ensuring that the exemption is not easily invoked for trivial matters but reserved for genuine issues of systemic accountability and democratic functioning.[38]

5.2. Institutional and Inter-Agency Coordination

Legal clarity alone is insufficient; effective governance requires robust institutional mechanisms. The separation of powers between the data protection regulator and the information regulator presents an operational challenge that must be overcome through mandated collaboration.

- **Joint Guidelines and Dispute Mediation:** The Data Protection Board (DPB) and the Central Information Commission (CIC) must be legally obligated to collaborate on issuing joint guidelines.[39]These guidelines should clarify the practical application of both statutes, especially concerning third-party information requests for public functionaries, mediating disputes, and ensuring consistent application of both laws to safeguard democratic accountability.

[38] Saumya Tripathi and Ashish Srivastava. "Existence And Misuse of Section 8 of The RTI Act: A Critical Analysis." Indian Journal of Integrated Research in Law 5 (2025).
[39] Shreyi Singh, "Right to Privacy under the PDP Bill and RTI Act" The Right to Information, February 20, 2020, available at: https://www.thyrighttoinformation.com/2020/02/20/privacy-right-under-the-pdp-bill-and-rti act/ (last visited on October 01, 2025).

ISSN: 2582-6433

- **Specialized Tribunal/Coordination Mechanism:** To arbitrate conflicts at the interstice of privacy and transparency, a formal inter-agency coordination mechanism or the establishment of a specialized tribunal is necessary. [40]This dedicated body could hear appeals involving mixed questions of information access and data protection, ensuring a singular, expert-driven jurisprudence.
- **Strengthening Commission Expertise:** It is critical to strengthen Information Commissions with dedicated data protection expertise. Personnel within the Commissions should receive specialized training on the principles of the DPDP Act, the proportionality test, and data masking techniques.[41] This ensures that the officials making disclosure decisions are equipped to understand and apply the nuances of digital personal data protection principles while upholding the spirit of the RTI Act.

5.3. Procedural Clarity and Statutory Definitions

Ambiguity in law breeds inconsistency in practice. The successful harmonization of these two rights hinges upon eliminating legal grey areas through refined procedural rules and precise statutory definitions.

- **Clear Procedural Rules:** Public Information Officers (PIOs) require clear procedural rules for handling RTI requests that involve personal data. This includes standardized procedures for redacting, anonymizing, or seeking the consent of Data Principals when appropriate, ensuring a uniform approach across all public authorities and minimizing arbitrary denials.
- **Narrowly Tailored Definition:** The DPDP Act must be read to include a narrowly tailored definition of "personal information" when applied to the context of the RTI Act. This would prevent the overreach of the exemption by clarifying that information pertaining to the official, public acts of a public servant—such as details of tenders, decisions, or official correspondence—does not constitute *personal* information in the context of accountability.
- **Proactive Disclosure and Anonymization:**
    - Public authorities should be mandated to anonymize sensitive data before publication and actively promote the proactive disclosure of non-personal information. This strategy significantly reduces the need for citizens to file RTI

[40] Raj Kamal, EshaneeAwadhya, "Transparency & Privacy: Unconscionable or Amicable" in SairamBhat (ed.), Ashwini Arun, Sindhu V Reddy (asst. eds.), Right To Information and Good Governance 165 (NLSIU, Bengaluru, 2016).
[41] Atul Singh, "Data Protection: India in the Information Age" 59 (1) Journal of the Indian Law Institute85 (2017).

ISSN: 2582-6433

applications for basic non-sensitive information, thereby reducing the burden on the system and mitigating conflicts between RTI obligations and privacy rights.

- Effective implementation of Section 4 of the RTI Act (Proactive Disclosure) is paramount. If public authorities routinely and comprehensively publish the categories of information mandated under Section 4, the reliance on reactive RTI applications, which often seek basic or slightly sensitive data, will naturally decrease. This proactive transparency is the most potent tool to balance disclosure and privacy.

6. CONCLUSION

The core task facing India's democratic and digital architecture is the careful, yet fundamental, harmonization of two cardinal constitutional entitlements: the Right to Information (RTI), which ensures governmental transparency and accountability, and the Right to Privacy (R2P), including the derivative Right to Be Forgotten (RTBF), which secures individual dignity and digital autonomy in an age where personal data has become a vulnerable and pivotal asset.

While these rights are intended to be mutually supportive, their intricate relationship becomes acutely contentious when requests for public records mandate the disclosure of personal information. Historically, the unamended Section 8(1)(j) of the RTI Act served as a crucial "constitutional bridge," operationalizing the principle that neither right is absolute. It achieved a dynamic equilibrium by offering a *qualified exemption*: disclosure was permitted even for personal data if a "larger public interest" was demonstrated, effectively subjecting privacy claims to a proportionality test to prevent the use of privacy as a blanket shield for official secrecy.

The enactment of the Digital Personal Data Protection Act, 2023 (DPDP Act), while a critical and long-overdue legislative culmination of the *Justice K.S. Puttaswamy v. Union of India* judgment and a necessary step toward informational self-determination, inadvertently threatens to dismantle this carefully calibrated balance. The DPDP Act's unqualified amendment to Section 8(1)(j) is the pivotal concern, as it removes the essential public interest override, transforming privacy from a conditional safeguard into an absolute bar on the disclosure of personal data under the RTI Act.

ISSN: 2582-6433

This legislative action, intended to aggressively safeguard the fundamental right to privacy, risks overcorrecting for the prior absence of a dedicated data law by unnecessarily restricting transparency, thereby compromising the core of democratic accountability and creating a regulatory environment where official opacity can be shielded under the guise of data protection. This divergence places India in isolation from global democratic practice; mature jurisdictions, such as the European Union's GDPR and the United Kingdom's FOI Act, explicitly maintain a robust public interest test to arbitrate the conflicting interests of privacy and information access.

The path forward, therefore, demands a commitment to syncretic jurisprudence—a legal framework where both rights are respected without one negating the other—centered on a renewed legislative commitment to the principle of proportionality. This crucial effort necessitates concrete reforms beyond mere policy suggestions: the reinstatement of a balanced public interest test within a structured proportionality framework; the mandated inter-agency coordination between the newly formed Data Protection Board and the Central/State Information Commissions to develop joint guidelines and mediate disputes; the procedural incorporation of anonymization techniques for sensitive data; and the rigorous application of a narrowly tailored definition of "personal information" to ensure that the public, official acts of public servants remain subject to scrutiny.

The debate is not about choosing between secrecy and disclosure, but about determining the appropriate legal mechanism to manage the tension between these two fundamental democratic imperatives. By reintroducing a nuanced interpretation and embracing the principle of proportionality, India can ensure that neither the democratic right to know nor individual digital dignity is compromised, thereby sustaining a government that is both accountable and legitimate. The successful harmonization of the RTI Act, the *Puttaswamy* principles, and the DPDP Act is the vital next step to strengthen the foundational pillars of the Indian Republic in the age of digital governance.