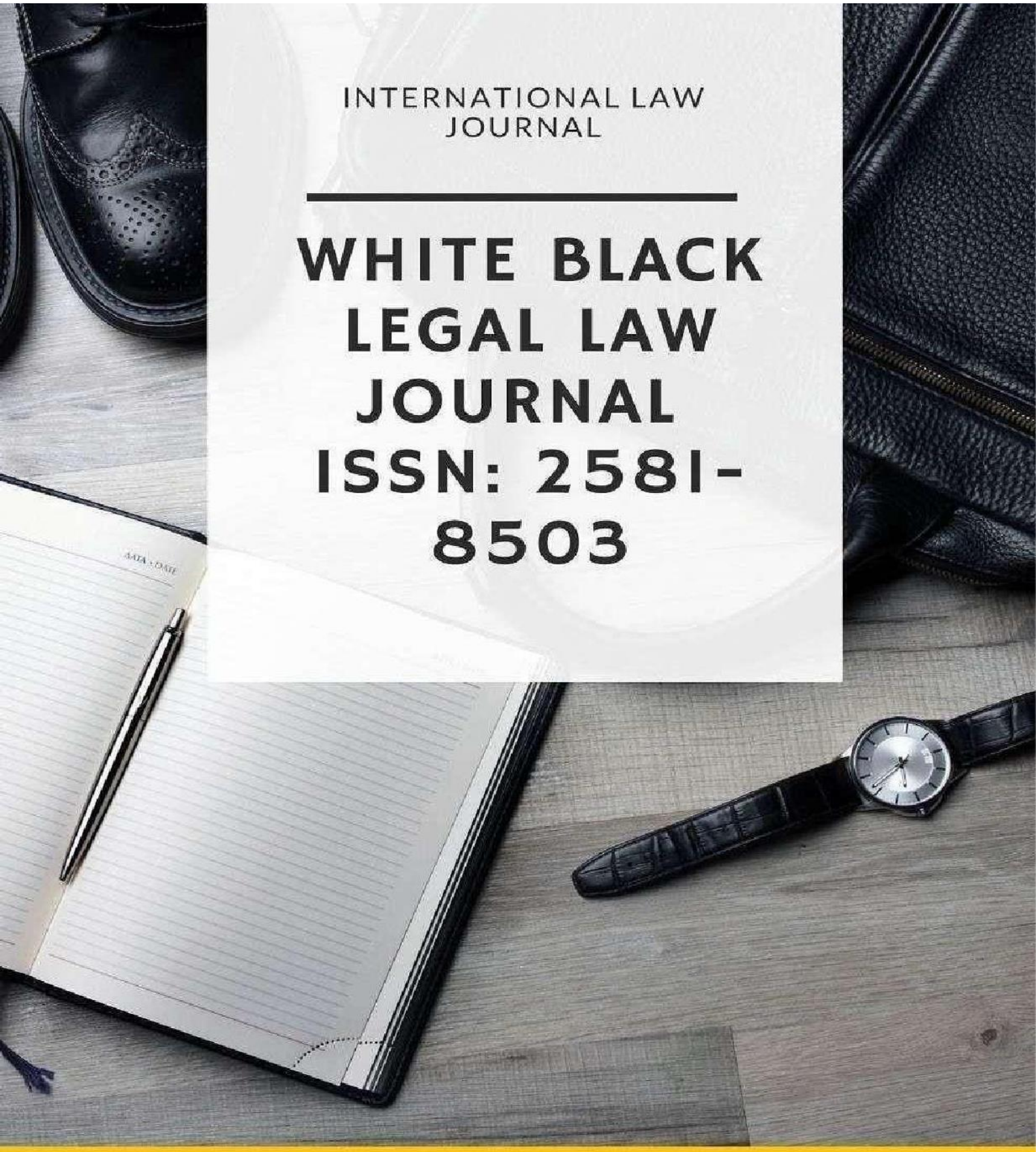


INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

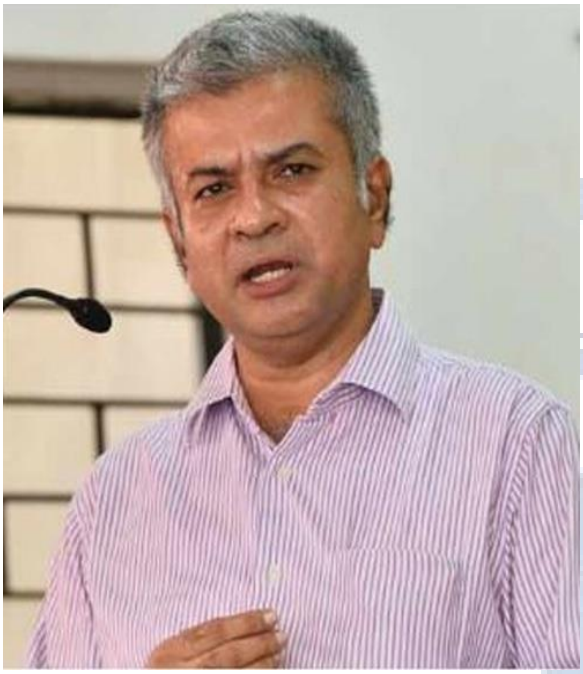
DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Editor-in-chief of White Black Legal – The Law Journal. The Editorial Team of White Black Legal holds the copyright to all articles contributed to this publication. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of White Black Legal. Though all efforts are made to ensure the accuracy and correctness of the information published, White Black Legal shall not be responsible for any errors caused due to oversight or otherwise.

WHITE BLACK
LEGAL

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer



Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala. He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and diploma in Public a professional Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB, LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

WHITE BLACK LEGAL

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi, Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

WHITE BLACK LEGAL

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

WHITE BLACK LEGAL

THE CONSTITUTIONAL DILEMMA: HARMONIZING THE RIGHT TO ERASURE WITH FREEDOM OF INFORMATION IN THE ERA OF AI WITHIN INDIAN JURISPRUDENCE

AUTHORED BY - JOSEPH THOMAS

Executive Overview

India's legal position emanates from the fundamental Right to Privacy as articulated in the judgment K.S. Puttaswamy (2017)[1], which constitutionally anchors the Right of Correction and Erasure (RTE) enshrined under the Digital Personal Data Protection (DPDP) Act, 2023. However, RTE, is not absolute, requiring judicial scrutiny to balance it against the imperatives of public interest, freedom of expression, and other statutory obligations. In this context, India's enduring commitment to transparency, as embodied in the Right to Information Act (RTI), 2005, stands in profound constitutional tension with the emerging recognition of the Right to Be Forgotten (RTBF).

In contrast to the US, which mostly dismisses the RTBF due to First Amendment concerns, and the EU, which offers clear statutory guidelines, India depends on varied judicial interpretations to settle disputes, especially those involving government documents. The rise of Artificial Intelligence (AI) further complicates this structural lack of clarity. The dependence of Generative AI on extensive, permanent datasets directly contradicts the legal requirement for data deletion, making the right technically ineffective unless sophisticated methods like Machine Unlearning are strictly implemented. Resolving this issue necessitates legislative changes to formalize the "public interest" evaluation, transfer the settlement of difficult constitutional disagreements away from private Data Fiduciaries, and impose technical compliance criteria on AI platforms.

The Origins and Development of the Right to Be Forgotten

- Historical Evolution

Roots are traced back to the French legal notion of the "Right to Oblivion," which permitted persons to remove any historical information that had lost its public relevance by a request. The contemporary

[1] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).

formulation of this right was established in Europe in 1998, prompted by the Mario Costeja González case. González, a Spanish citizen, suffered damage to his reputation because an old newspaper ad about a property auction, published when he was facing financial difficulty, remained accessible online well after his problems were sorted out.

Distressed by the persistent online presence of his personal information, González approached the court seeking its erasure. The matter culminated before the **European Court of Justice (ECJ),** which, in its judgment against Google, recognised that individuals within the **European Union (EU)** possess the right, under defined circumstances, to request that their personal data be excluded from **public records and search engine listings.** This being a landmark judgment laid the jurisprudential foundation for **the Right to Be Forgotten (RTBF)** and marked its formal **recognition in the modern digital landscape**.

- The EU's Position

In 2014, **General Data Protection Regulation (GDPR)** framework was formally incorporated, the **Right to Be Forgotten (RTBF)** by the **European Union (EU)**. Under this regime, individuals are entitled, in specific circumstances, to seek deletion of their personal data, when such information has outlived its original purpose of collection, When consent has been withdrawn and no lawful ground justifies its continued retention, or when the individual raises an objection to its processing for purposes of direct marketing. Nonetheless, this entitlement is not absolute. Requests for erasure may be lawfully declined where processing of the data is necessary to preserve freedom of speech and expression, to uphold public health objectives advancing societal welfare, or to perform a task mandated by official authority in the public interest, thereby reflecting the delicate balance between the right to data privacy and competing public and constitutional freedoms. Thus, the EU framework maintains a calibrated equilibrium among competing public and constitutional freedoms and the right to data privacy.

- The US Position

Unlike Europe, the United States has not incorporated within its legal framework the Right to Be Forgotten (RTBF), deeming it fundamentally incompatible with the First Amendment's guarantees of the public's right to know and freedom of expression. In Florida Star case (1989)[2], the ruling of

[2] *Florida Star v. B.J.F.*, 491 U.S. 524 (1989).

the U.S. Supreme Court affirmed that laws cannot restrict the publication of truthful or sensitive information, so long as such information has been lawfully obtained, under the protection of the First Amendment. This reasoning was later reinforced by the Connecticut Supreme Court in Martin case (2015)[3], which reaffirmed that "historically accurate news reports" must not be erased or altered. Consequently, the American legal tradition prioritises the collective interest in open information over individual privacy concerns. Hence, while Europe safeguards personal dignity and informational autonomy through the RTBF, the United States remains steadfast in defending unrestrained speech reflecting two sharply contrasting constitutional philosophies in reconciling privacy with public access to information.

Genesis and Evolution of the Right to be Forgotten in India

- Article 21 and Right to Privacy

The Right to Be Forgotten (RTBF) according to the laws of Indian was firmly grounded through landmark judgment of *Justice K.S. Puttaswamy (2017)*, wherein its foundation was laid down by the Hon'ble Supreme Court of India. It was universally affirmed through this verdict that the Right to Privacy forms an integral element of the Right to Life and Personal Liberty enshrined under Article 21 of the Constitution of India.[4]. The decision underscored the need for informational privacy and the lasting nature of digital records, stressing that individuals must maintain the capacity to change, grow, and not be forever characterized by their history online.[5] This concept of informational self-determination furnished the constitutional basis required for the RTBF to develop, positioning it as crucial for individual independence and personal respect.[6]

Before the right was formally codified into law, High Courts throughout India started interpreting and employing the RTBF concept on an individual, case-by-case basis. Such judicial pronouncements generally pertained to sensitive or acquittal-related cases, wherein the continued public accessibility of past incidents was deemed to violate an individual's right to dignity. In the ABC case[7], the Delhi High Court recognised

[3] *Martin v. Hearst Corp.*, 777 F.3d 546 (2d Cir. 2015).
[4] Anjani Agarwal & Aman Singh, *The Right to Be Forgotten Under the Digital Personal Data Protection Act, 2023: A Missed Opportunity in India's Data Privacy Regime*, 11 **Int'l J. L.** 57 (2025), https://www.lawjournals.org/assets/archives/2025/vol11issue6/11131.pdf..
[5] Raunak Dhillon, Jeezan Pakhliwal & Gunav Gujral, *The Right to Be Forgotten: Reclaiming Dignity in Digital Age*, Cyril Amarchand Mangaldas: Dispute Resolution Blog (Sept. 10, 2025), https://disputeresolution.cyrilamarchandblogs.com/2025/09/the-right-to-be-forgotten-reclaiming-dignity-in-digital-age/.
[6] *Data Protection Laws in India*, DLA Piper: Data Protection Laws of the World (Jan. 6, 2025), https://www.dlapiperdataprotection.com/index.html?t=law&c=IN.
[7] *ABC v. State (NCT of Delhi)*, Civil Appeal No. 28367 of 2015 (India).

RTBF as an essential facet of personal dignity, directing that judicial records be anonymised by replacing real names with generic identifiers in public search results. Similarly, in the Rakesh Jagdish Kalra case, the Delhi High Court directed that defamatory content associating the petitioner with criminal allegations be removed following his acquittal, holding that the right to privacy may justifiably outweigh Article 19 of the Indian Constitution when the disclosed information no longer holds public significance. Although these rulings provided necessary relief, they also underscored a substantial regulatory gap, as the principle continued to be applied inconsistently owing to the lack of a uniform legislative framework.

- Codification by Statute, The Digital Personal Data Protection Act, 2023 (DPDP Act)

Legislative framework governing data processing is embodied in the Digital Personal Data Protection Act, 2023. Although the DPDP Act was intended to create a comprehensive regulatory mechanism, it consciously avoids explicitly mentioning the Right to Be Forgotten. The essence of this right, however, is implicitly embedded within the broader Right of Correction and Erasure (RTE) as articulated in Section 12.[8] of the statute. This decision by the legislature to replace the well-known RTBF phraseology with the more restricted RTE, is noteworthy, especially when contrasted with prior data protection bills in India. Earlier legislative drafts, such as the 2018 and 2019 versions of the Personal Data Protection Bill, had expressly incorporated provisions recognising an individual's entitlement to restrict the dissemination of personal data online, thereby explicitly codifying the Right to Be Forgotten within their framework.

The legislature's measured approach is evident in the final 2023 Digital Personal Data Protection (DPDP) Act, which omits the right altogether, particularly concerning the most debated facet of the Right to Be Forgotten (RTBF) the obligation imposed upon search engines to de-index truthful and publicly accessible information.

The DPDP Act, by narrowing or limiting the right to erasure, primarily concentrates on the information held by Data Fiduciaries (DFs) for specific purposes, rather than imposing the broad de-indexing requirement characteristic of the European regulatory model.

This decision moves the main duty for resolving intricate de-indexing disputes involving publicly accessible data, like court documents, back to the judiciary for constitutional resolution. This results in regulatory ambiguity until the Supreme Court issues conclusive direction on current cases.[9] Under the DPDP Act, a Data Principal (DP) is empowered through the Right of Correction and Erasure (RTE) to seek the removal of personal data where such data has been processed unlawfully, has outlived the purpose for which it was collected, or where the DP has withdrawn consent for its further use.

[8] Agarwal & Singh, *supra* note 1, at 57.

[9] *Right to Be Forgotten in India: A Comparative Guide to Compliance*, AMLEGALS (2025), https://amlegals.com/a-comparative-guide-to-compliance-with-the-right-to-be-forgotten-in-india/#

- Restrictions and Range of the RTE within the DPDP Act

The **RTE** is not absolute and needs **careful judicial review,** where **public interest and freedom of expression** are weighed before allowing any deletion of data. The DPDP Act sets forth distinct statutory grounds where a Data Fiduciary is not obligated to delete personal data. These exceptions come into play if data retention is: (1) essential for compliance with legal mandates; (2) necessary for advancing legal proceedings; or (3) serving the public interest, for activities like journalism, statistical evaluation, or historical research. This framework is similar to the European model, recognizing that the right to privacy must be assessed against other key societal interests.[10] Nevertheless, the Act's applicability to public information, such as court documents, remains ambiguous, resulting in ongoing contradictory judicial interpretations even after its enactment. Despite High Courts actively affirming the RTBF's role in safeguarding individual dignity, especially for exonerated or vulnerable people, the persistent need for these specific judicial interventions points to a practical failing in the DPDP Act concerning public domain data protection. The courts reactive, instance specific use of the RTBF produces inconsistent results and criteria, underscoring the necessity for a complete legislative structure that offers definitive methods for resolving major disputes.[11]

Part II: The Imperative of Openness: Freedom of Information in India

- The Right to Information Act, 2005 (RTI Act)

Enacted to replace the **Freedom of Information Act, 2002,** the **Right to Information Act, 2005** stands as India's foremost legislation promoting **transparency and accountability in governance**. It rests on the belief that an informed citizenry is better equipped to monitor public authorities, thereby strengthening **governmental** responsibility.[12] At its core, the RTI Act is founded on the constitutional linkage between the Right to Know and the fundamental freedom of speech and expression under Article 19(1)(a). Through this framework, the Act provides an effective mechanism enabling citizens to obtain information from public authorities, thereby fostering transparency and accountability in governance.

[10] *Digital Personal Data Protection Act, 2023: Rules and Implementation Framework*, Ministry of Electronics & Information Technology, Govt. of India (2024), https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf.

[11] Dhillon et al., *supra* note 3.

[12] *Right to Information Guidelines, 2018*, Labour Bureau, Ministry of Labour & Employment, Government of India, https://labourbureau.gov.in/assets/images/pdf/RTI_Guidelines_2018.pdf.

- Statutory Exclusions within the RTI Act

To protect crucial state operations, the RTI Act includes several legal exemptions. Information may be withheld from release if its disclosure would harm national security, sovereignty, or financial interests (Section 8). Additionally, Section 24 grants a special exemption to select Central agencies, including the Research and Analysis Wing (RAW), the Central Bureau of Investigation (CBI), and the Intelligence Bureau (IB), which are engaged in intelligence and security operations. This exclusion is justified by the requirement to safeguard confidential intelligence activities and law enforcement abilities. Importantly, these exclusions are conditional. The law recognises that transparency in cases of wrongdoing takes precedence over institutional secrecy; therefore, information relating to these exempt agencies must still be disclosed when it concerns human rights violations or allegations of corruption.[13]

- The Key Point of Convergence: Third-Party Data and Public Interest

The RTI Act requires a cautious balancing act when the release of information involves a third party, which frequently includes personal data. Data pertaining to commercial trust, proprietary secrets, or intellectual property is usually excluded from disclosure if its release would damage the third party's market standing. Nonetheless, this exclusion can be superseded by the application of the "larger public interest" standard. If the appropriate authority determines that disclosure is warranted in the broader public interest, such information must be made public.. Legal protections require that the third party be given a complete chance to argue for non-disclosure before a final determination is reached.

A major difficulty stems from the lack of a precise, formalized definition for "larger public interest" in the RTI Act. This ambiguity is especially troubling since the DPDP Act uses a similar, potentially contradictory, "public interest" exception to reject the Right to Erasure. Depending on an undefined standard generates uncertainty and guarantees that disputes will be settled through different interpretations across the two legal frameworks. This core conflict is intensified by the philosophical difference between the two laws: the RTI Act assumes disclosure unless an explicit exemption applies, while the DPDP Act assumes privacy, meaning access must be warranted by either consent or valid interests. Following the direction of the Puttaswamy judgment, the State must now provide a rationale for keeping or sharing personal data that would have previously been readily available under RTI, thereby shifting the balance of power between the citizen's right to information and their protecting private data.[14]

[13] *Exempted Authorities Under Section 24 of the RTI Act: An In-Depth Analysis Across Jurisdictions*, SCC Online Blog (Sept. 9, 2025), https://www.scconline.com/blog/post/2025/09/09/exempted-authorities-under-section-24-of-the-rti-act-an-in-depth-analysis-across-jurisdictions/.

[14] Luciano Floridi, *Soft Ethics and the Governance of the Digital*, **Phil. Trans. R. Soc. A** 376, 20180087 (2018), https://royalsocietypublishing.org/doi/10.1098/rsta.2018.0087.

Part III: The Constitutional Intersection: Weighing the RTBF against FOI

- The Unavoidable Collision: Article 21 Versus Article 19(1)(a)

Conflict between **Article 19(1)(a) (Freedom of Information)'s guarantees of free expression and the Right to Know and the Right to Be Forgotten, which stems from Article 21's protections of dignity and privacy,** reflects a profound constitutional tension between two equally vital fundamental rights.[15] Resolution demands a proportionate strategy, one that guarantees the protection of privacy does not lead to the right being exploited for censorship or the rewriting of history.[16]

- The Principle of Proportionality and Double Proportionality

Indian legal theory resolves disputes between fundamental rights by employing the doctrine of proportionality. For scenarios involving two conflicting constitutional rights, a meticulous assessment called "double proportionality" becomes necessary. This procedure establishes a stringent standard and cannot be treated as a routine or mechanical step; it requires a concurrent evaluation of why limitations may be imposed on privacy rights and why similar restrictions may apply to freedom of expression. Before any reconciliation is attempted, each right's importance must be independently and meticulously assessed to determine which should prevail in the specific context.[17]

This process of balancing must also include an evaluation of temporal relevance. Data that was highly pertinent for public examination during an event, like an arrest or accusation, may lose its relevance or become unfairly damaging once the initial reason is fulfilled, for example, following an acquittal. For instance, if published reports about an acquitted plaintiff persist online without serving any current public interest, the right to privacy should ultimately be prioritized.[18] Consequently, over time, the threshold of public interest necessary to justify disclosure ought to diminish, thereby shifting the burden onto the party resisting deletion to demonstrate the information's continuing relevance for archival, statistical, or journalistic purposes.[19]

WHITE BLACK LEGAL

[15] Suryansh Pandey & Harshit Pathak, *Striking the Balance: Right to Be Forgotten v. Right to Information Under DPDP Act, 2023*, NLIU-CLT Blog (Sept. 2025), https://clt.nliu.ac.in/?p=1189.
[16] *Right to Be Forgotten in India: Balancing Privacy and Public Interest*, Int'l J.L. Liberty & Reform Blog (2025), https://www.ijllr.com/post/right-to-be-forgotten-in-india-balancing-privacy-and-public-interest.
[17] Suryansh Pandey & Harshit Pathak, *Striking the Balance: Right to Be Forgotten v. Right to Information Under DPDP Act, 2023*, NLIU-CLT Blog (2025), https://clt.nliu.ac.in/?p=1189.
[18] *Right to Be Forgotten in India: Digital Privacy & Law*, Neeti Niyaman (2025), https://neetiniyaman.com/right-to-be-forgotten-india-digital-privacy/.
[19] Dhillon et al., *supra* note 3

C. Structural Weakness in the DPDP Framework

The DPDP Act, particularly Section 12, introduces a major systemic problem by assigning the preliminary settlement of disputes to private Data Fiduciaries (DFs). This section provides DFs with wide-ranging exceptions (e.g., retention required for 'adherence to any other statute') and does not clearly instruct DFs to perform the intricate balancing assessment needed to weigh free speech against the RTE. This choice essentially delegates the arbitration of a fundamental constitutional dispute to non-state, commercial entities. Handing over the quasi-judicial duty of balancing abstract democratic principles (like historical integrity or freedom of the press) against specific demands for individual dignity to DFs risks demoting the constitutional RTBF to a simple matter of contract or regulatory compliance. As the Srikrishna Committee observed, it is fundamentally impractical to expect private entities to carry out the impartial, constitutional review mandated by the double proportionality principle. For the Right of Correction and Erasure (RTE) to be effectively enforced, responsibility must rest with an independent judicial or quasi-judicial authority, such as India's Data Protection Board (DPBIA), to adjudicate and resolve these intricate disputes.

- Case Review: RTBF and Court Records

The tension is especially severe when personal information is embedded within publicly available judicial documents. Since court judgments are historically public, a direct conflict arises when an individual seeks to have their data redacted or de-indexed following legal acquittal to reclaim their dignity. The Supreme Court is presently examining this matter in the Ikanoon case, which arose from a Madras High Court order directing the deletion of the name of a man who had been acquitted in a sexual assault judgment.[20] The Supreme Court's decision to stay the order of the Madras High Court—an order that had upheld the right to privacy in this instance—underscores the complexity and delicate nature of the matter. The eventual ruling in Ikanoon is anticipated to be a landmark decision, likely defining the precise boundaries of the RTE regarding authoritative, non-confidential judicial records, an area the current DPDP Act structure is poorly suited to resolve on its own.[21]

Part IV: Comparative Jurisprudence: Parallels in Western Law

To understand India's developing legal structure, one must conduct a comparative study of the two main Western frameworks, the European Union's model, which centres on individual rights, and the United

[20] Vikrant Rana, Anuradha Gandhi & Rachita Thakur, *Will Right to Be Forgotten Be Applicable in Judicial and Publicly Available Documents?*, S.S. Rana & Co. (Aug. 20, 2024), https://ssrana.in/articles/right-to-be-forgotten-judicial-publicly-available-documents/.

[21] *Data Privacy and Cyber Security Newsletter – August 2024*, Dentons Link Legal (Aug. 16, 2024), https://www.dentonslinklegal.com/en/insights/newsletters/2024/august/16/data-privacy-and-cyber-security-newsletter/data-privacy-and-cyber-security-newsletter-august.

States' approach, which prioritizes freedom of expression.

- The European Union (EU) Framework: GDPR and the Clear RTBF

The **EU framework,** grounded in the **Fundamental Right to Data Protection under Article 8 of the Charter of Fundamental Rights,** finds its principal expression in the **General Data Protection Regulation (GDPR),** where **Article 17 explicitly defines the Right to Erasure (RTBF)**.This system allows for strong enforcement, particularly against search engine operators, where individuals can enforce the removal of links to their old data, even if the source content is still legally accessible on the internet.[22] The GDPR establishes specific and enforceable exceptions, offering legal clarity for both transparency and free expression. Erasure rights do not apply in circumstances where data processing is essential for upholding freedom of expression and access to information, for complying with legal obligations or fulfilling public duties, or when the processing is undertaken for objectives related to public interest, historical or scientific research, or statistical analysis.

This detailed categorization differs from India's general dependence on a vague "public interest" exception within the DPDP Act.[23] Implementing the EU's level of detail would increase legal predictability for Data Fiduciaries and offer solid protection for valid archival and journalistic concerns in India. Moreover, the EU upholds a freedom of information system through Regulation (EC) No 1049/2001, which governs access to documents held by EU institutions.[24] A disclosure request may be refused if it jeopardizes institutional decision-making, except where a compelling public interest justifies its release, following a balancing approach akin to the public interest override under India's RTI Act.[25]

[22] *Right to Erasure ("Right to Be Forgotten"),* Art. 17, Regulation 2016/679, General Data Protection Regulation (GDPR), https://gdpr-info.eu/art-17-gdpr/.

[23] *Right to Erasure*, Information Commissioner's Office (ICO), UK GDPR Guidance (Aug. 2024), https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/right-to-erasure/.

[24] *Revision of the Access to Documents Regulation*, Eur. Parl. Legis. Train Schedule (Apr. 20, 2025), https://www.europarl.europa.eu/legislative-train/theme-protecting-our-democracy-upholding-our-values/file-revision-of-the-access-to-documents-regulation.

[25] *Regulation (EC) No. 1049/2001 of the European Parliament and of the Council of 30 May 2001 Regarding Public Access to European Parliament, Council and Commission Documents*, 2001 O.J. (L 145) 43, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32001R1049

- The United States (US) Model: The Dominance of the First Amendment

The legal framework of the US presents a distinct opposite to both India and the EU. US courts and legal experts mostly dismiss the central European idea of the RTBF, considering it to be fundamentally opposed to the tenets of the First Amendment. The main apprehension is that compelling service providers to delete or de-index accurate, historically truthful content amounts to an unacceptable practice of forced speech or censorship. The assumption of newsworthiness is significantly prioritized over individual privacy claims concerning factual public data.[26] Although a sweeping RTBF is rejected, limited privacy safeguards are available at the state level, permitting the sealing or deletion of certain damaging records, such as juvenile offenses or bankruptcy filings. Yet, even these targeted protections are structured to prevent the violation of substantial First Amendment interests. Regardless of the US position, American firms with international operations are still required to comply with the GDPR's RTBF obligations for EU residents, which underscores the functional challenge of extraterritorial compliance enforced by rights-focused data protection legislation. As India finalizes its data protection framework, international platforms will confront a comparable jurisdictional issue in handling Indian RTE demands.[27]

- Comparative Legal Foundations for the Right to Erasure/Forgotten (India vs. EU)

Structurally, India's approach mirrors that of the EU in requiring a formal balancing process while recognising data protection as a fundamental right.. Nevertheless, cultural distinctions remain, whereas the **EU emphasises strong individualism,** India is often seen as an **inherently collective society,** shaping how **public interest** is weighed against individual rights**.**

The table below highlights the principal structural distinctions between India's RTE and the EU's RTBF.

Feature	India: DPDP Act, 2023 (RTE)	European Union: GDPR (RTBF/RTE)
Core Legal Source	Established by Statute (Section 12, Data Principal Rights); derived from the Constitutional Right to Privacy (Article 21).	Established by Statute (Article 17); derived from the Fundamental Right to Data Protection (Article 8, Charter of Rights).
Explicit Mention of 'Forgotten'	Implicitly contained within the Right to Erasure; the term 'Right to be Forgotten' is not expressly utilized.	Explicitly designated as the Right to Erasure ('Right to be forgotten').[21]

[26] David L. Hudson Jr., *Right to Be Forgotten*, First Amend. Encyclopedia (Aug. 11, 2023; updated July 2, 2024), https://firstamendment.mtsu.edu/article/right-to-be-forgotten/.

[27] Paul M. Schwartz, *Global Data Privacy: The EU Way*, 93 Wash. L. Rev. 771 (2023), https://digitalcommons.law.uw.edu/wlr/vol93/iss1/5/.

Scope of Enforcement	Mainly enforceable against Data Fiduciaries; the process for de-indexing public data/search results remains ambiguous.	Enforceable against Data Controllers, including search engines for delinking public information.[21, 22]
Major Exceptions	Necessary for adhering to legal claims/requirements, or for reasons of public interest (e.g., journalism, historical studies).	Mandatory for upholding freedom of expression/information, performing public interest duties, or pursuing legal actions.[21, 23]
Deciding Authority	Data Protection Board of India (DPBIA); the preliminary evaluation is frequently assigned to the Data Fiduciary (a non-judicial entity).	Supervisory Authorities/Judicial Review (adjudication is judicial or quasi-judicial).[21]

Part V: The Era of AI: Technical Necessities and Regulatory Deficiencies

- AI's Unlimited Memory and Data Longevity

The implementation of the Right to Erasure encounters significant technical barriers in the AI era, especially with generative systems such as Large Language Models (LLMs). These models require immense, permanent datasets for training, refinement, and function, establishing a core conflict with the right to be forgotten[28]. The difficulty is that data preservation in AI goes beyond simple storage in a database, it also involves the algorithmic retention of data's impact within the intricate parameters and design of deep learning models. After data is incorporated into a model, separating and deleting it is technically challenging and frequently impossible. The lack of transparency in these models makes it difficult to identify and remove the impact of specific data points. As a result, generative AI models can unintentionally keep and output personal data from their initial training set, thus contravening the intent of an erasure request, even if the source data has been removed. Regulatory measures must thus define erasure not just as the removal of original files, but as the verifiable elimination of data's effect from resulting outputs.[29]

- The Essential Role of Machine Unlearning

For Data Fiduciaries utilizing AI/ML systems, adhering to Section 12 of the DPDP Act (which requires correction and erasure) makes technological remedies indispensable. Machine Unlearning (MU) techniques

[28] *The Right to Be Forgotten vs. AI's Infinite Memory: A Regulatory Dilemma*, DPO India (June 27, 2025), https://www.dpo-india.com/Blogs/right-to-forgot/.
[29] *The Right to Be Forgotten vs. AI's Infinite Memory: A Regulatory Dilemma*, DPO India (June 27, 2025), https://www.dpo-india.com/Blogs/right-to-forgot/.

present a viable solution, as they are specifically engineered to eliminate the impact of particular training data from a model without demanding a full, expensive, and time-consuming retraining effort. Within the scope of the DPDP Act, Machine Unlearning changes the RTE from a theoretical entitlement into an auditable and mandatory compliance standard. Regulatory agencies need to adjust policy frameworks to institute unambiguous standards for data removal in AI settings, particularly when models continue to generate results based on data that should have been deleted.[30] Moreover, the DPDP Act's focus on consent, while posing difficulties for AI training (which often demands extensive datasets), simultaneously encourages the creation and deployment of more ethical AI systems that emphasize privacy-by-design and machine unlearning functionalities. This push is backed by global initiatives advocating for responsible AI development, including the G20 New Delhi Leaders' Declaration.[31]

- AI Governance and the DPDP Act

AI developers are **mandated by the Digital Personal Data Protection Act (DPDP Act)** to carefully balance any **requirement for large datasets in model training** with the **legal obligations of data minimisation and erasure.**Although some exceptions are provided, particularly for handling publicly accessible data and information used for genuine research, these clauses offer only restricted relief. A deep concern emerges regarding the centralization of power with the State. India's current legal structure allows the State to process personal data with very few restrictions. The increasing application of AI in State-run surveillance and profiling programs, combined with the DPDP Act's notable lack of provisions for transparency and accountability in intelligence agencies, introduces major systemic dangers. These dangers, particularly in light of the rapid adoption of AI, pose significant threats to the Right to Be Forgotten, jeopardising both the right to privacy and freedom of expression through risks such as automated content restriction and algorithmic profiling.

Part VI: Policy Integration and Recommendations

The Indian legal framework urgently requires regulatory and structural reforms to harmonize the equally vital Freedom of Information obligations with the fundamental Right to Be Forgotten, particularly in light

[30] Raktim Saha, *Machine Unlearning for Enterprise AI: From Right to Be Forgotten to Provable Forgetting*, Medium (June 2025), https://medium.com/@raktims2210/machine-unlearning-for-enterprise-ai-from-right-to-be-forgotten-to-provable-forgetting-2d5aadf41919

[31] *The Impact of the DPDP Act on Artificial Intelligence and Machine Learning*, Tsaaro (2025), https://tsaaro.com/blogs/the-impact-of-the-dpdp-act-on-artificial-intelligence-and-machine-learning/.

of the rapid adoption of AI technologies.

- Formalizing and Implementing the Public Interest Test

The present structure is hindered by its reliance on an undefined and uneven "public interest" benchmark that serves opposing aims, to compel disclosure under the RTI Act and to refuse erasure under the DPDP Act.[32]

- ❖ Recommendation 1: Legal Definition and Precision. The DPDP Rules should define the "public interest" test using precise, yet non-limiting, criteria, taking substantial guidance from the clear exceptions in the GDPR (e.g., distinct classifications for journalism, historical record-keeping, and statistical review). This greater level of detail will bring essential predictability for Data Fiduciaries and the courts.
- ❖ Recommendation 2: Scaled Public Interest and Temporal Relevance. The definition must include a time-based component. To lawfully override the fundamental right to dignity, the public interest in keeping or sharing the data must be shown to be current, persuasive, and essential. This guarantees that obsolete information, particularly that related to legal acquittal, can be deleted once its benefit to the public interest decreases.

- Modifying the Dispute Resolution Mechanism

The existing system's practice of assigning complicated constitutional balancing tasks to private Data Fiduciaries is a structural defect. Private entities are inherently unsuitable for carrying out the strict 'double proportionality' analysis required to weigh free speech against privacy rights.

- ❖ Recommendation 3: Independent Resolution. The task of settling RTBF requests that clash with freedom of expression, journalism, or public records must be given to an independent, judicial, or quasi-judicial body, such as the Data Protection Board of India (DPBIA) or an Appellate Tribunal, acting as the primary authority.

- Technical Compliance Requirements for AI

The discrepancy between the legal demand for data deletion and the technical endurance of generative AI necessitates forward looking regulatory action cantered on technological compliance.

- ❖ Recommendation 4: Mandatory Machine Unlearning Audits. Regulatory agencies should mandate frequent and thorough privacy impact evaluations and technical audits for AI systems, especially those categorized as high-risk. The goal of these audits must be to

[32] *Right to Erasure*, Information Commissioner's Office (ICO), UK GDPR Guidance (updated June 2025), https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/right-to-erasure/.

WHITE BLACK LEGAL

confirm that the systems are not storing or unintentionally recreating personal information that was legally required to be removed.

- ❖ Recommendation 5: Integration of Privacy-by-Design and Machine Unlearning. The DPDP Rules ought to place a distinct duty on Data Fiduciaries, particularly Significant Data Fiduciaries, to enforce "Privacy by Design" principles. This necessitates implementing demonstrable Machine Unlearning techniques right from the initial phase of model development, thereby establishing verifiable MU capability as a crucial compliance measure under Section 12.[33]

- Conclusion

India's effort to harmonise Freedom of Information with the Right to Be Forgotten is characterised by two distinct and significant legal obligations—the rights-oriented DPDP Act functioning in parallel with the disclosure-driven RTI Act. This constitutional testing ground, where Article 21 and Article 19(1)(a) intersect, requires a solution that moves past reactive court decisions. The limited legal scope of the RTE in the DPDP Act forces an ongoing dependence on the judiciary to de-index public information, resulting in systematic inconsistency. Additionally, the rapid expansion of generative AI presents a technical necessity, ensuring that the legal right to forget is not made irrelevant by AI's perpetual memory. Successful harmonization demands prompt legislative measures to formalize the undefined "public interest" criterion, centralize the constitutional resolution of these disputes, and integrate mandatory technical remedies, such as Machine Unlearning, into the regulatory framework for AI governance. Such extensive reform is the only way India can simultaneously uphold the citizen's right to dignity and the democratic requirement of transparency.

WHITE BLACK LEGAL

[33] Raktim Saha, *Machine Unlearning for Enterprise AI: From Right to Be Forgotten to Provable Forgetting*, Medium (June 2025), https://medium.com/@raktims2210/machine-unlearning-for-enterprise-ai-from-right-to-be-forgotten-to-provable-forgetting-2d5aadf41919.