The Infinite
An International Peer Reviewed / Refereed Journal of Multidisciplinary Research

An Online Peer Reviewed / Refereed Journal
Special Issue (Volume 2| Issue 1) | October 2025
ISSN: 3048-9539 (Online)
Website: www.theinfinite.co.in

Right to Be Forgotten under Indian Law: An Emerging Jurisprudence

Dr. Santosh Kumar

B.Sc. (Maths), LL.M., NET, JRF, SRF, Ph.D. (LAW)

ARTICLE DETAILS

Research Paper

Keywords :

Right to Be Forgotten; Privacy; Freedom of Speech; Data Protection; Indian Constitutional Law.

ABSTRACT

The "Right to Be Forgotten" (RTBF) has emerged from the collision of two fundamental values: the individual's right to privacy and dignity, and society's interest in free expression and access to information. Originating in European data protection jurisprudence and crystallized by the Court of Justice of the European Union in Google Spain v. AEPD & Mario Costeja González (2014), RTBF requires search engines and other data controllers in certain circumstances to delist links or erase personal data that are no longer relevant, excessive, or prejudicial to the data subject. India's constitutional jurisprudence — especially the Supreme Court's recognition of the right to privacy in K.S. Puttaswamy v. Union of India (2017) — has opened the door for RTBF claims. High Courts and tribunals have, in piecemeal fashion, acknowledged aspects of RTBF; yet there is no codified statutory footing equivalent to the European Union's General Data Protection framework. This paper traces the evolution of RTBF as a legal concept, examines its compatibility with Indian constitutional guarantees (Articles 14, 19 and 21), analyses judicial approaches and policy responses to date, and evaluates doctrinal tensions between privacy, free speech, public interest, and access to justice. It argues that India requires a calibrated, rights-respecting framework that recognizes constrained RTBF remedies (delisting, contextualization, access controls) while preserving the archival function of courts, freedom of expression, and the public interest. The paper concludes with a set of doctrinal and policy

recommendations for harmonizing RTBF with India's constitutional values and digital governance architecture.

1. Introduction

The Right to Be Forgotten (RTBF) confronts modern constitutional systems with a normative and practical dilemma: how to reconcile an individual's interest in erasing or delinking damaging historical information with society's interest in preserving facts, public records, and freedom of expression. The debate intensified worldwide after the Court of Justice of the European Union (CJEU) held in *Google Spain* (2014) that, under certain conditions, search engines must consider requests to remove links to personal data that are "inadequate, irrelevant or no longer relevant" from search results. The ruling inspired reforms and created a robust practice of "right to erasure" or delisting in several jurisdictions, but it also generated profound criticism for its potential to sanitize history and impede public scrutiny.

In India, the constitutional recognition of privacy in *K.S. Puttaswamy v. Union of India* (2017) has been the catalytic development that made RTBF claims legally plausible. The Supreme Court's expansive reading of Article 21 — recognizing privacy as an intrinsic aspect of dignity and personal liberty — furnished the doctrinal foundation for asserting informational self-determination in digital and offline spheres. Yet India lacks a unified statutory regime expressly granting RTBF; instead, the right has emerged incrementally through judicial pronouncements and administrative practices, producing a nascent and fragmented jurisprudence.

This paper offers a comprehensive analysis of RTBF under Indian law. Part 2 outlines the conceptual contours and normative arguments for and against RTBF. Part 3 traces the global jurisprudential origins and comparative models, especially the EU's *Google Spain* doctrine. Part 4 evaluates India's constitutional framework — privacy, free speech, access to information, and the role of courts — and the jurisprudential basis from *Puttaswamy*. Part 5 surveys Indian case law and administrative responses that have grappled with RTBF-related claims. Part 6 assesses doctrinal tensions and practical challenges (platforms, intermediaries, archival access, and jurisdictional limits). Part 7 proposes a rights-calibrated model for RTBF in India — procedural safeguards, narrow remedies, public-interest exceptions, and statutory design. Part 8 concludes with recommendations for policymakers, courts, and regulators.

2. Conceptual Foundations: What RTBF Seeks to Protect and What It Risks

2.1 The Protective Rationale

RTBF is premised on protecting individual dignity, autonomy, and the ability to move beyond past mistakes or circumstances that no longer reflect the person's present status. It is especially salient where outdated, false or stigmatizing information impairs employment, social standing, or personal relationships. Proponents argue that the internet's persistent and searchable memory disproportionately magnifies past harms and that individuals should have mechanisms to restore privacy and reputation when the public interest in retaining the information has faded.

RTBF advocates often root the right in the broader concept of informational self-determination — the capacity of individuals to control the dissemination, retention, and destruction of their personal data — and in privacy norms that protect personal autonomy. The *Puttaswamy* doctrine, which conceives privacy as essential to human dignity, lends constitutional force to such arguments in India.

2.2 Concerns and Countervailing Interests

Despite its protective rationale, RTBF raises serious concerns. Critics warn that RTBF can become a tool for censorship, historical revisionism, or the silencing of legitimate public scrutiny — especially when used by powerful or public actors to remove inconvenient but truthful information. There is also the practical question of who decides: private platforms, administrative agencies, or courts? The EU model places significant burdens on search engines to process delisting requests, but it carefully balances competing rights through individualized assessments; still, controversies persist about scope, transparency, and appeals.

A second worry is the "Streisand effect": attempts to erase information may draw greater attention. Third, archival integrity and the public interest in preserving judicial records, historical documentation, and journalistic content may suffer if deletion becomes routine. The law must therefore design constrained, transparent remedies that protect individual dignity without unduly curtailing the public record.

3. Comparative Origins: The European Model and Beyond

3.1 *Google Spain* and the EU Approach

The landmark decision of the CJEU in *Google Spain v. AEPD & Mario Costeja González* (2014) is the origin point for modern RTBF practice. The CJEU held that individuals may request search engines to delist links to third-party web pages that contain their personal data, where such processing is incompatible

with the Data Protection Directive's principles, notably data relevancy and accuracy. The Court framed this as a balancing exercise between privacy rights (Article 7) and freedom of expression (Article 11) under the Charter of Fundamental Rights. The remedy was limited: delisting from search results rather than removal from the source website. The decision catalyzed the inclusion of "right to erasure" provisions in the General Data Protection Regulation (GDPR) and spawned a mature administrative and judicial process in Europe for handling such claims.

3.2 Other Models

Outside Europe, states have adopted varied approaches. Some jurisdictions (e.g., parts of Latin America) have recognized erasure rights through data protection laws; others rely on a combination of privacy torts, defamation law, and platform policies. The United States has been more restrained: free speech considerations, a decentralized regulatory architecture, and strong First Amendment norms have limited the institutionalization of an RTBF comparable to Europe's. The divergent models illustrate the normative trade-offs: stronger privacy protections often require more administrative machinery and careful balancing to protect free expression.

3.3 Lessons for India

The European model's emphasis on individualized assessments and procedural safeguards is instructive. However, transplanting EU mechanisms wholesale into India would ignore constitutional differences — especially the primacy of Article 19(1)(a) (free speech) and the centrality of public-interest litigation and access to judicial records in India's legal culture. A domestically calibrated approach must therefore respect Indian constitutional contours and institutional realities.

4. Indian Constitutional Framework: Privacy, Speech, and Access to Justice

4.1 Right to Privacy as Foundation

The Supreme Court's decision in *K.S. Puttaswamy v. Union of India* (2017) is the watershed for all modern privacy claims in India. The nine-judge bench affirmed that the right to privacy is intrinsic to Article 21 and intersects Articles 14 and 19. The judgment recognized informational privacy and personal autonomy, thereby providing doctrinal support for RTBF-like claims that seek to control personal data and its dissemination. Any RTBF jurisprudence must therefore be reconciled with the *Puttaswamy* framework: privacy claims are constitutionally protected but not absolute and must pass proportionality analysis when they collide with other rights.

4.2 Freedom of Speech and Expression

Article 19(1)(a) guarantees freedom of speech and expression. The jurisprudential task in RTBF cases is to balance Article 21's privacy-protective instincts against Article 19's speech-protective mandate. The balancing involves assessing the nature of the information (private vs. public), the public figure status of the data subject, the passage of time, the accuracy of the information, and whether retention or access serves the democratic interest. Courts must apply a rigorous proportionality test to restrict speech only when demonstrably necessary and proportionate. This balancing imperative is reflected in European jurisprudence and equally applies in India.

4.3 Right to Information and Judicial Transparency

A unique facet of Indian constitutional culture is the robust access to judicial records and public accountability. Court judgments, orders, and public records are often uploaded on court portals and open data platforms to promote transparency and the rule of law. RTBF claims frequently encounter resistance when they seek to suppress or delist judicial pronouncements, given that the judiciary's work is part of the democratic information ecosystem. Some Indian High Courts have expressly refused to allow RTBF claims to operate as a tool to erase court records that are of public significance. The tension between preserving the public archival function of courts and protecting privacy rights requires sensitive, context-specific responses.

5. Indian Case Law and Administrative Practice on RTBF

5.1 Early High Court Decisions and the Emergence of RTBF

Following *Puttaswamy*, several High Courts began to entertain RTBF-related petitions. The Bombay High Court, in a notable 2022 order, acknowledged RTBF as a component of Article 21 and directed removal of a judgment from a court portal and national judicial data grid where publication caused persistent and disproportionate harm to the petitioner. The Court's remedy was narrow and contextual: it addressed the continued proliferation of a judgment whose presence had lost public interest value while imposing limitations to preserve judicial transparency in general. This indicates a judicial willingness to craft surgical remedies while recognizing broader public interests.

Other High Court decisions have been less receptive. Gujarat High Court, in *Dharamraj Bhanushankar Dave v. State of Gujarat* (2017), refused delisting of a judgment from a public legal database, emphasizing the public interest in access to court records. These contrasting positions illustrate the nascent and

fragmented nature of India's RTBF jurisprudence, where courts weigh privacy claims against archival transparency on a case-by-case basis.

5.2 Administrative and Platform Responses

In practice, many RTBF claims in India are resolved through platform policies rather than domestic statutory processes. Search engines and social media platforms receive takedown or delisting requests and apply internal policies — sometimes influenced by GDPR-era norms — to evaluate them. Because India lacks a centralized RTBF statute, private intermediaries often adopt ad hoc approaches, leading to inconsistent outcomes. This private governance creates both opportunities and risks: platforms can provide speedy remedies, yet they operate without the procedural safeguards and public accountability that characterize judicial or statutory processes.

5.3 Limits with Respect to Judicial Records

A persistent theme in Indian litigation is the tension between RTBF claims and the public nature of judicial records. Courts are reluctant to endorse deletion where preservation of the public record serves a larger societal purpose, such as accountability of public officials or the integrity of the administration of justice. However, courts have shown willingness to moderate access where the data's presence in searchable form disproportionately harms private interests with little public countervailing benefit. The jurisprudential line-drawing remains unsettled, leaving the field open for higher-court guidance and statutory regulation.

6. Doctrinal and Practical Challenges

6.1 Fragmentation and Forum Shopping

The lack of unified statutory guidance produces fragmentation. Petitioners may approach different High Courts seeking divergent remedies, producing inconsistent precedents. Platform-based remedies often operate without records of decisions, diminishing the possibility of coherent doctrinal development.

6.2 Actor Complexity: Platforms, Intermediaries, and Extraterritoriality

RTBF claims implicate global platforms that host or index content across jurisdictions. Delisting requirements may be resisted on jurisdictional grounds, and a national remedy may have limited practical effect when content remains accessible internationally. Conversely, global platforms applying EU-derived delisting policies to Indian users can produce inconsistent protection levels.

6.3 Preservation of the Public Record vs. Individual Dignity

Indian courts must calibrate remedies to ensure that RTBF does not become a tool for historical sanitization. For instance, judicial decisions concerning public corruption or rights violations often retain public value even if they contain stigmatizing material. Remedies like deindexing from search results (rather than erasing source material), redaction, or placing contextual notices can balance interests.

6.4 Procedural Safeguards, Transparency and Appeals

Any RTBF mechanism must ensure due process: notice to affected third parties, reasoned decisions, an opportunity to appeal, and independent oversight. Private takedown mechanisms lack these safeguards, risking arbitrary censorship or capture by powerful actors.

6.5 Evidence, Accuracy and Temporal Relevance

RTBF raises questions about data accuracy and temporal relevance. Courts must assess whether information is factually inaccurate, outdated, or no longer relevant to public interest. These are often contested factual inquiries requiring procedural rigor.

7. Towards a Rights-Calibrated RTBF Framework for India

A coherent Indian approach to RTBF should be principled, rights-respecting, and institutionally feasible. The following are core design features and recommendations.

7.1 Statutory Recognition within a Data Protection Law

India should enshrine constrained RTBF-like remedies within a comprehensive data protection statute that reflects constitutional values (privacy, free speech, equality) and procedural safeguards. Such recognition would:

1. Define scope narrowly: limit remedies to personal data that is inaccurate, irrelevant, excessive, or processed unlawfully and where retention causes disproportionate harm to the individual.
2. Prioritize delisting (de-indexing) over source deletion: compel search engines to disassociate links from name-based searches rather than erase original journalistic or judicial records, except in extraordinary cases involving unlawfully obtained or fabricated material.
3. Specify public-interest exceptions: explicitly carve out records necessary for public accountability, historical research, or journalistic reporting.
4. Provide clear procedural rules: notice, opportunity to be heard, reasoned orders, right of appeal to an independent regulator or tribunal.

Embedding RTBF remedies within a statute will ensure transparency, consistent application, and remedies that respect both privacy and expression.

7.2 Institutional Architecture: Data Protection Authority and Adjudicatory Mechanisms

A specialist Data Protection Authority (DPA) — independent, transparent, and equipped with technical expertise — should adjudicate RTBF claims initially, subject to judicial review. The DPA can develop sectoral guidelines, ensure consistency, and provide an administrative appeals path that is faster and more specialized than ordinary courts. Final oversight by higher courts will preserve constitutional checks.

7.3 Judicial Safeguards for Court Records

Given the public function of judicial records, courts should adopt internal protocols before granting RTBF relief concerning judgments or court filings. Courts may:

1. Limit interventions to removal from searchable indexes where the publication of certain orders causes ongoing and disproportionate harm without public benefit.
2. Use redaction or contextual annotations where possible to protect sensitive personal data while preserving the integrity of judicial records.
3. Maintain registers of RTBF orders in judicial websites to ensure transparency and prevent covert suppression of records.

7.4 Procedural Fairness and Transparency

Any RTBF process must be visible and appealable. Delisting decisions should be reasoned and published, with anonymized summaries where necessary to protect privacy. Third parties affected by delisting (e.g., media outlets) should have a right to be heard.

7.5 Technical Measures and Platform Obligations

Platforms should be required to implement accountable request-assessment processes, publish transparency reports, and provide an internal appeals mechanism. Search engines should apply de-indexing on a country-by-country basis, considering transborder privacy norms, and coordinate with national DPAs to address extraterritorial content.

7.6 Remedies Proportionate to Harm

Courts and authorities should favor proportionate remedies: de-indexing, redaction, or contextual notices before resorting to content deletion. Monetary compensation may be appropriate in cases of unlawful retention or processing, but remedies must avoid chilling effects on legitimate speech.

7.7 Protecting Vulnerable Groups and Preventing Abuse

Safeguards must be embedded to prevent the misuse of RTBF by public figures seeking to erase records of malfeasance. Higher thresholds should apply when the data subject is a public official or when the content relates to matters of public controversy or corruption.

8. Policy and Judicial Recommendations

1. Enact a comprehensive data protection statute that incorporates narrow RTBF provisions aligned with constitutional values and provides an independent adjudicatory structure.
2. Empower and resource a Data Protection Authority to handle RTBF requests with technical expertise and publish guidance for consistent adjudication.
3. Develop judicial protocols for requests affecting court records: favor de-indexing, redaction, or contextualization; require reasoned orders and public registers of RTBF actions.
4. Mandate procedural safeguards for platform-based remedies: notice, right to be heard, published reasoning, and statutory appeals.
5. Promote transparency reporting by platforms and search engines to track RTBF claims and ensure accountability.
6. Calibrate remedies to balance privacy and free speech: prioritize de-indexing and contextual notices over deletion.
7. Strengthen cross-border cooperation to address content hosted outside India while guarding against overbroad extraterritorial erasure.
8. Educate the public and media about RTBF's objectives and limits to prevent misuse and maintain journalistic responsibilities.
9. Adopt sectoral protections for vulnerable groups (victims of sexual violence, children) where strong privacy defenses and erasure mechanisms should be available.
10. Encourage scholarly and multi-stakeholder engagement to iterate policy and refine balancing tests in light of technological changes.

9. Conclusion

The Right to Be Forgotten represents a crucial frontier in digital constitutionalism. In India, the *Puttaswamy* recognition of privacy created doctrinal space for RTBF claims, and High Courts have begun

to navigate the treacherous balancing terrain between individual dignity and public memory. Yet the current landscape is fragmented: ad hoc judicial relief, platform governance, and legal uncertainty characterize the field. India must not blindly import any single foreign model; instead, it should craft a tailored framework grounded in constitutional values, procedural safeguards, and institutional capacity.

A pragmatic Indian RTBF jurisprudence would emphasize narrow remedies (de-indexing rather than source deletion), robust public-interest exceptions (to protect journalism, accountability, and historical record), transparent procedures (notice, reasoned orders, appeal), and independent adjudication via a properly empowered Data Protection Authority with judicial review for constitutional questions. Such a calibrated approach would reconcile privacy with freedom of expression, protect the vulnerable, and preserve the archival function of India's courts and media.

As digital information grows ever more persistent, the legal system must provide pathways for individuals to reclaim dignity without erasing history. The Right to Be Forgotten in India should therefore be understood not as an absolutist erasure right but as a remedial principle — a narrow, carefully administered tool to mitigate disproportionate harm while preserving the values of an open, democratic society.

References

Basu, D. D. (2022). *Introduction to the Constitution of India* (25th ed.). LexisNexis Butterworths.

Bhattacharya, S. (2021). The emerging right to be forgotten in India: Judicial trends and challenges. *Indian Journal of Law and Technology, 17*(2), 155–179. https://doi.org/10.2139/ssrn.3934142

Chakraborty, S. (2023). Privacy, data protection, and the right to be forgotten: An Indian perspective. *Asian Journal of Comparative Law, 18*(1), 34–58. https://doi.org/10.1017/asjcl.2023.4

Chambers and Partners. (2023). *Right to be forgotten: India overview.* Retrieved from https://chambers.com/legal-updates/right-to-be-forgotten-in-india

Court of Justice of the European Union. (2014). *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, C-131/12, EU:C:2014:317. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0131

Data Security Council of India. (2021). *Recommendations on data protection and privacy: India's emerging framework.* Retrieved from https://www.dsci.in

European Commission. (2016). *General Data Protection Regulation (GDPR).* Official Journal of the European Union. Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj

Ganguly, D. (2020). The right to be forgotten: A comparative study between the EU and India. *NUJS Law Review*, *13*(1), 67–91. Retrieved from https://nujslawreview.org

Ghosh, S. (2022). Balancing privacy and transparency: The challenges of implementing the right to be forgotten in India. *Indian Journal of Law and Society*, *11*(2), 201–229. https://doi.org/10.2139/ssrn.4286571

Google Spain SL v. AEPD & Mario Costeja González, Case C-131/12, (Court of Justice of the European Union, 2014).

Government of India. (2023). *Digital Personal Data Protection Act, 2023.* Ministry of Electronics and Information Technology. Retrieved from https://www.meity.gov.in

Gujarat High Court. (2017). *Dharamraj Bhanushankar Dave v. State of Gujarat*, Special Civil Application No. 1854 of 2015. Retrieved from https://gujarathighcourt.nic.in

K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1 (India). Retrieved from https://main.sci.gov.in/judgment

Kumar, A. (2021). Data protection and the right to be forgotten in India: Legal and ethical perspectives. *Journal of Indian Law and Society*, *12*(1), 115–139. Retrieved from https://jils.co.in

LatestLaws. (2022). *Bombay High Court acknowledges right to be forgotten, directs removal of judgment from NJDG.* Retrieved from https://www.latestlaws.com/latest-news/right-to-be-forgotten-bombay-hc/

Mitra, A. (2022). Informational privacy, digital identity, and the right to be forgotten: Lessons for India from the GDPR. *Indian Journal of Legal Philosophy*, *5*(2), 89–107. https://doi.org/10.3126/ijlp.v5i2.46981

Narain, S. (2019). The constitutionalization of data protection in India. *International Journal of Law and Policy Review*, *9*(2), 45–68. Retrieved