

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS



Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

**Copyright © International Journal for Legal Research & Analysis.
All rights reserved.**

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IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines.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.

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.

THE “RIGHT TO BE FORGOTTEN” VS. PUBLIC ACCESS TO INFORMATION ANALYZING THE LEGAL TENSION BETWEEN DIGITAL PRIVACY RIGHTS AND FREEDOM OF EXPRESSION IN THE AGE OF PERSISTENT ONLINE DATA

AUTHORED BY - PRIYA S

(V BALLB) STUDENT

GOVERNMENT LAW COLLEGE, TRICHY

Abstract

The “Right to be Forgotten” (RTBF) has emerged as a critical legal and ethical challenge in the digital age, where the permanence of online data creates an inherent tension between individual privacy rights and society’s interest in accessing information. This article examines the conceptual foundations of RTBF, tracing its origin from the European Court of justice’s landmark Google Spain decision to its evolving recognition in Indian Jurisprudence through cases like Karthick Theodore and Jorawar Singh Mundy. The study analyzes the core legal conflict between privacy, dignity and personal autonomy on one hand and freedom of expression, open justice, and democratic transparency on the other. Current issues are explored including digital stigma affecting acquitted individuals inconsistent judicial outcomes in the absence of statutory codification technological enforcement challenges and the chilling effect on journalism and historical records. The article proposed a comprehensive policy framework to address these challenges, including legislative codification with clear eligibility criteria and exceptions a seven part balancing test for courts differentiated treatment of information types (court judgements, news articles, social media content), technological solutions such as automated redaction and time-limited indexing, and public awareness initiatives. Drawing comparative insights from the EU’s GDPR, ARTICLE 17’s policy recommendations and emerging Indian case law, this article argues that RTBF should not be an absolute right but must be balanced through context-sensitive adjudication that protects individuals from perpetual digital stigma while preserving the public right to know and maintaining archival integrity. The Supreme Court of India’s pending decision to establish a nuanced framework that can serve as a global precedent for reconciling privacy and transparency in an era of persistent online data.

Keywords: Right to be forgotten, Digital Privacy, freedom of Expression, Data protection, Open Justice, Personal Autonomy, DPDPA 2023, Article 21, GDPR, Public Interest.

In the digital age, where information is perpetually stored and instantly accessible, one of the most pressing legal and ethical challenges is the tension between an individual's **"Right to be Forgotten" (RTBF) and society's** right to access to information. This conflict sits at the intersection of privacy, dignity, freedom of expression and transparency values that are foundational to democratic societies but often pull in opposite directions when applied to the persistent nature of online data.

I. Conceptual Foundations: What is the "Right to be Forgotten"?

A. Definition and Origin

The Right to be Forgotten also known as the "Right to Erasure" refers to an individual's entitle, under certain conditions to have personal data removed from internet search results, data bases or public platforms. Though not explicitly recognized in international human rights instruments, the RTBF emerged prominently from European data protection law, particularly through the Court of Justice European union's (CJEU) landmark 2014 decision in *Google Spain SL V. Agencia Espanola de Proteccion de datos*.

In that case, the CJEU held that EU citizens could request search engines to de-index links containing personal information that was "inadequate, irrelevant no longer relevant or excessive. This ruling laid the groundwork for Article 17 of General data Protection Regulation (CGPR), which codifies the right to erasure under specific grounds such as withdraw consent, unlawful processing or data no longer being necessary.

B. Philosophical and Legal Rationale

The RTBF is grounded in the broader right to privacy and personal autonomy. The idea that individual should have control over how their personal information is disseminated and used. In the analog era, information naturally faded over time; newspaper aged, records were archived and public memory moved on. The internet, however, creates digital permanence, where past mistakes, accusations or embarrassing moments remain perpetually accessible, potentially causing lasting reputational, professional and psychological harm.

As Justice Kaul observed in the Indian Supreme Court's *K.S.Puttaswamy v. Union of India (2017)* judgment, which recognized privacy as a fundamental right under Article 21 of the Constitution, individuals should be able to remove information that is no longer necessary,

relevant or is incorrect and serves no legitimate interest.

II The Counterweight: public access to information and freedom of expression

A. The Public Interest in transparency

Opposing the RTBF is the Public's Right to Know, rooted in principles of freedom expression, open justice and public records serve critical functions. They inform citizens, enable scrutiny of power and preserve historical truth.

In India, the open court system is a constitutional principle ensuring that judgement are publicly accessible. As Chief Justice Chandrachud remarked during the Supreme Court hearing on the *Karthick Theodore Case*, "Once a judgement is delivered by a court, it is a part of the public record. How can anybody direct that the judgement should be pulled down?"

B. Freedom of expression, protected under article 19(1)(a) of the Constitution and Article 10 of the European convention on Human Rights, includes the right to impart and receive information. The RTBF, by enabling removal or re-indexing of information, inherently restricts this freedom.

The CJEU itself acknowledged this tension, noting that the RTBF "cannot exist without balancing other relevant interests like the freedom of expression, compliance with legal obligations, public health, research or legal claims.

III The Core Legal Tension: privacy v. Transparency

A. Where the conflict arises

The tension between RTBF and public access manifest in several scenarios:

- Acquitted individual whose names remain associated with criminal allegations online, harming employment and social prospects
- Public figures whose past conduct remains searchable, raising questions about whether public interest outweighs privacy.
- Rape survivors seeking anonymity to avoid social stigma, despite judgements being publicly accessible.
- Historical records and journalistic archives that may be altered or removed, potentially rewriting history.

- Permanence vs. Redemption: The internet's memory is infinite, but human being evolve. Should a person's past mistake define them forever?
- Individual Harm vs. Public interest: Does the public benefit from knowing every detail of a person's past, especially after acquittal or rehabilitation?
- Search Engines as Gatekeepers: Should private companies like Google decide what information is accessible or should courts oversee such decision
- Global vs. Local Enforcement: If information is de-indexed in one jurisdiction, it may remain accessible elsewhere, raising questions about the RTBF's effectiveness.

IV. CURRENT ISSUES AND EMERGING CHALLENGES

A. The Indian context:

Judicial recognition without Statutory framework for the RTBF. The Digital Personal Data Protection Act, 2023 (DPDPA), though a significant step, does not explicitly recognize the RTBF. Instead, Section 12(3) allows individuals to request erasure of personal data once its purpose is fulfilled, subject to legal exceptions.

In the absence of legislation, Indian courts have developed RTBF jurisprudence on a case-by-case, often invoking Article 21 (Right to Privacy) and Article 19 (Right to freedom of expression).

Notable Indian Cases:

1. Karthick Theodore v. Madras High Court (2024)

An acquitted individual sought redaction of his name from a 2011 judgement. The Madras High Court allowed limited anonymization, but the Supreme Court stayed the Order, questioning whether judgement can be "Pulled Down".

2. Jorawar Singh Mundy v. UOI (Delhi HC, 2021)

An acquitted American citizen of Indian origin sought de-indexing of judgements affecting his career. The Court recognized RTBF as part of privacy and directed search engines to remove the links.

3. Vysakh K.G v. UOI (Kerala HC, 2022)

The court held that RTBF is not absolute and must be balanced against open justice. Relief was granted only in sensitive cases e.g., child custody, passport issues.

4. Rakesh Jagdish Kalra v. India Today (Delhi HC, 2024) Post-acquittal, media outlets were directed to remove prejudicial content, recognizing that privacy can outweigh expression when no public interest remains.

B The Supreme court Pending decisions

The Supreme court is currently hearing multiple petitions, including Karthick Theodore and Alka Malhotra v. UOI, to determine whether RTBF can be enforced against judicial archives and legal databases like Indian Kanoon. This decision will set a precedent for balancing dignity and privacy against open justice and transparency.

C Global Perspectives

European union: The GDPR provides a structured RTBF framework with clear exceptions for freedom of expression and public interest.

United states: The U.S prioritizes First Amentments Rights, making RTBF claims difficult to enforce. Courts often reject RTBF as incompatible with free speech.

Latin America: Countries like Argentina and Brazil have recognized RTBF in limited contexts, emphasizing proportionality and public interest tests.

V. Specific Issues

1. Digital Stigma and Social Harm

Individuals acquitted of crime or who have served sentences often face continued stigma due to persistent online records. This can lead to:

- Employment discrimination
- Social ostracization
- Psychological distress
- Inability to relocate or travel (e.g., visa denials)

2. Chilling Effect on Journalism and Historical record

If RTBF is applied too broadly, it may:

- Discourage investigative journalism
- Enable powerful individuals to erase inconvenient truths
- Undermine archival integrity and historical research

3. Inconsistent Judicial outcomes

Without statutaory guidance, courts apply RTBF inconsistently. Somr grant relief in sensitive cases; others prioritize open justice. This creates legal uncertainly and unequal protection.

4. Technological and Enforcement Challenges

- De-indexing Vs. Deletion: Most RTBF orders require de-indexing (removing from search results) rather than deletion (removing fom source).
- Global Enforcement : A de-indexing order in India ma not affect servers in other jurisdiction.
- Intermediary Liability : Should platforms like google, Indian Kanoon, or social media sites be held liale for hosting public records?

Solution:

The tension between the Right to be Forgotten (RTBF) and public access to information demands a multi layered, context sensitive policy framework the balances individual dignity with democratic transparency. India's Digital Personal Data Protection Act, 2023 (DPDPA), while a significant step toward data privacy, falls short of explicitly recognizing the RTBF, leaving courts to navigate this complex terrain on a case by case basis. A comprehensive statutory framework is essential to provide legal certainty, uniformity, and procedural clarity, ensuring that RTBF claims are neither arbitrarily granted nor blanketly denied. Such legislation must establish strict eligibility thresholds, carve out narrow exceptions for freedom of expression and public interest, and embed robust procedural safeguards to prevent abuse while protecting genuine privacy harms.

To prevent frivolous or abusive RTBF claims, legislation should establish strict eligibility thresholds that require applicants to demonstrate that the information in question is private, irrelevant, or no longer necessary for any legitimate public interest or ongoing legal purpose. For instance, a decade old news report about a minor offense, post acquittal, may qualify for removal, whereas a recent corruption scandal involving a public official would not. Applicants must provide concrete evidence of substantial harm, such as employment discrimination. Mere embarrassment or inconvenience should not suffice, as this would open the door to excessive censorship and undermine the public's right to know. Furthermore, public figures politicians, celebrities, corporate leaders should have a lower expectation of privacy due to their societal role, and information related to ongoing investigations, public health crises, or national security should remain accessible to ensure democratic accountability and public safety.

To balance RTBF with other fundamental rights, legislation must carve out narrow,

well defined exceptions that protect freedom of expression, public interest, and legal obligations. Journalistic integrity must be preserved, meaning investigative reports, editorials, and news archives should be protected unless proven false or malicious. Similarly, artistic and literary works biographies, documentaries, creative expressions should not be subject to RTBF unless they violate privacy laws independently. Public interest exceptions must cover information related to health and safety, and legal obligations. Court judgments, orders, and legal filings are part of the public record and should generally remain accessible, subject to redaction in sensitive cases involving rape survivors, minors, or acquitted persons where no ongoing public interest exists.

To prevent arbitrary or opaque RTBF decisions, robust procedural mechanisms are essential. Only courts or independent data protection authorities such as India's proposed Data Protection Board should decide RTBF requests, avoiding delegation of this power to private intermediaries like Google or Facebook, which lack accountability and may prioritize commercial interests. Data publishers, including news outlets and legal databases, must receive prior notice of RTBF requests and have the opportunity to contest them, ensuring due process and preventing unilateral takedowns that could undermine transparency. Search engines and platforms should publish annual transparency reports detailing the number of RTBF requests received, the number granted or denied, and the categories of information affected, promoting accountability and enabling scrutiny of RTBF enforcement.

Courts should adopt a structured, multi factor test to balance RTBF against freedom of expression, drawing from ARTICLE 19's policy brief, which proposes seven criteria to ensure nuanced, context sensitive adjudication.

First, courts must assess whether the information is private in nature, distinguishing between personal details that require a higher threshold for removal.

Second, courts must evaluate whether the applicant had a reasonable expectation of privacy, considering context for instance, a person arrested but later acquitted may have a reasonable expectation that the acquittal, not the arrest, defines their public persona while recognizing that individuals who voluntarily shared information may have a lower expectation of privacy.

Third, courts must determine whether the information serves a legitimate societal purpose, such as exposing corruption, informing voters, or preserving history; if so, RTBF should generally be denied unless the harm to the individual is disproportionate.

Fourth courts must consider whether the information pertains to a public figure, recognizing that politicians, celebrities, and corporate leaders have a reduced expectation of privacy due to their influence on public affairs, whereas ordinary citizens deserve stronger privacy protections, especially post acquittal or rehabilitation.

Fifth, courts must assess whether the information is part of the public record, such as court judgments, legislative proceedings, or official records, which are presumptively public, though sensitive details may be redacted to protect dignity without undermining open justice.

Sixth, applicants must demonstrate substantial harm through concrete, measurable evidence such as job loss, social ostracization, or mental health deterioration rather than speculative harm like mere discomfort or embarrassment.

Seventh, courts must evaluate the temporal relevance of the information recognizing that old, outdated information may no longer serve public interest, whereas recent information about ongoing scandals, investigations, or public safety concerns should remain accessible.

Not all information deserves equal treatment, and a tiered approach ensures proportionality in RTBF enforcement. Court judgments should generally remain publicly accessible to uphold open justice and legal transparency, but sensitive details such as names of rape survivors, minors, or acquitted persons in cases with no ongoing public interest may be redacted or anonymized. Courts can issue anonymized versions for public circulation in cases involving sexual offenses, family disputes, or mental health, and publish supplementary orders indicating acquittals, exonerations, or case closures to provide context without erasing the legal record. News articles, particularly those published post acquittal or post exoneration, should be updated or removed if they contain prejudicial content that no longer serves public interest, ensuring that individuals are not perpetually defined by past allegations that were legally resolved. Social media platforms and user generated content hosts should implement clear takedown policies aligned with RTBF principles, enabling individuals to request removal of harmful, outdated, or irrelevant personal information while preserving legitimate expression

and public discourse.

Technological solutions can complement legal frameworks to enable practical, scalable RTBF enforcement. Courts and legal databases can deploy automated redaction tools using artificial intelligence to anonymize sensitive information before publication, reducing the burden on litigants and ensuring consistent privacy protection. Search engines could implement time limited indexing, deprioritizing old, irrelevant information after a certain period to reduce its visibility without erasing it entirely, balancing privacy with historical preservation. De-indexing orders could be limited to specific jurisdictions, ensuring that RTBF enforcement respects local privacy norms without imposing global censorship. thereby balancing global access with local privacy rights.

Public awareness and education are critical to empowering citizens and fostering responsible media practices. Digital literacy initiatives should educate citizens about privacy settings, data rights, and RTBF mechanisms, enabling individuals to proactively manage their online persons and seek redress when necessary. Media organizations should be encouraged to update or contextualize old stories, especially post acquittal, ensuring that journalism serves both truth and dignity. Journalists can adopt ethical guidelines for reporting on past allegations, emphasizing verification, proportionality, and the public interest, while avoiding sensationalism that perpetuates stigma long after legal resolution.

In sum, curing the issues arising from the RTBF public access tension requires a holistic approach that combines legislative e codification, judicial balancing tests, differentiated treatment of information types, technological innovation, and public education. By embedding clear criteria, narrow exceptions, and robust safeguards into law, India can protect individual dignity without undermining democratic transparency, setting a global precedent for navigating privacy and freedom of expression in the digital age.

Conclusion

The tension between the right to be Forgotten and Public Access to Information is not a zero-sum. Both privacy and transparency are essential to a functioning democracy. The challenge lies in crafting a nuanced, context-sensitive framework that:

- Protect individuals from unwarranted digital system

- Preserves the public's right to know and historical integrity.
- Ensures judicial consistency and legal certainty
- Leverages technology to enable practical solution.

As the Indian Supreme Court deliberates on the scope of RTBF, it has an opportunity to set a global precedent for balancing these competing rights in the digital age. The goal should not be erase the past, but tpo ensure that individuals are not perpetually defined by it- while maintain the transparency and accountability thatunderpin democratic societies.

References

1. Google Spain Vs. Agencia Espanola de Proteccion de Datos, CJEU (2014)
2. KS Puttaswamy Vs. union of India, (2017) 10 SCC1.
3. Karthick Theodore Vs. Madras High Court, SLP(C) Np.15311/2024
4. Jorawar Singh Mundy Vs. UOI, Delhi HC (2021)
5. Vysakh KG Vs. UOI, Kerala HC (2022)
6. GDPR Article 12 (Right to Erasure)
7. Article 19 Policy Brief (2017)
8. Digital Personal Data Protection ACT, 2023 (INDIA)