THE RIGHT TO BE FORGOTTEN: LEGAL INSIGHTS AND A ROADMAP FOR INDIA

Anumodan Tiwari*

ABSTRACT

The "Right to be Forgotten" (RTBF) is a critical aspect of digital privacy, empowering individuals to control their personal information online. It enables people to request the removal or de-indexing of personal data that is outdated, irrelevant, or harmful from internet platforms. While this right is explicitly enshrined in the European Union's General Data Protection Regulation (GDPR), its recognition and implementation in India remain uncertain. This ambiguity stems from the absence of a comprehensive data protection law and the inherent tensions between privacy, freedom of expression, and public interest. This paper explores the RTBF's conceptual foundation and its relevance in the Indian context, analyzing judicial interpretations such as the landmark Justice K.S. Puttaswamy v. Union of India case, which recognized the right to privacy as a fundamental right. Despite this, the RTBF lacks statutory backing, with only vague references in the Draft Digital Personal Data Protection Bill, 2023. The challenges to implementation are manifold, including legal conflicts, technological hurdles, and potential misuse to suppress free speech or public records. Through a detailed analysis, this research identifies the gaps in the current framework and proposes a balanced approach to implementing the RTBF in India. It advocates for clear legal guidelines, an independent adjudicatory authority, and the integration of advanced technological solutions to address enforcement challenges. Furthermore, it emphasizes the need for public awareness and education to ensure the responsible use of the RTBF while preserving constitutional values. This study contributes to the discourse on privacy rights in India, offering actionable insights into harmonizing individual privacy with collective freedoms in the digital age.

Keywords: Right to be Forgotten, Digital Privacy, Data Protection, Indian Constitution, Freedom of Expression.

*BBA LLB, SECOND YEAR, UILS, CHANDIGARH UNIVERSITY.

INTRODUCTION

The digital revolution has transformed the way information is created, shared, and consumed. With vast amounts of personal data stored online, concerns over privacy and data misuse have intensified, leading to the emergence of the "Right to be Forgotten" (RTBF). This right, rooted in the principle of informational self-determination, empowers individuals to request the removal of personal data that is outdated, irrelevant, or harmful to their reputation or safety. The RTBF is a cornerstone of digital privacy in jurisdictions like the European Union (EU), where the General Data Protection Regulation (GDPR) provides a robust legal framework for its enforcement.

In India, however, the concept remains in a nascent stage. While privacy has been recognized as a fundamental right by the Supreme Court in the landmark *Justice K.S. Puttaswamy v. Union of India* case, the RTBF lacks explicit statutory recognition.[1] The Draft Digital Personal Data Protection Bill, 2023, acknowledges the RTBF but leaves its scope and application vague.[2] This lack of clarity creates legal uncertainty, posing significant challenges for individuals seeking to assert this right and for organizations navigating compliance obligations.

The RTBF's implementation in India raises critical questions about the balance between privacy and other constitutional rights, such as freedom of speech and the public's right to access information.[3] It also highlights the technological challenges of enforcing this right across global digital platforms, where data may be stored in multiple jurisdictions and shared widely.

This research delves into these complexities, aiming to bridge the gap between legal theory and practical enforcement. By exploring the RTBF's origins, analyzing its implications in the Indian context, and proposing a balanced implementation framework, this paper seeks to contribute to the evolving discourse on digital privacy rights in India.

UNDERSTANDING THE RIGHT TO BE FORGOTTEN

The *Right to Be Forgotten* (RTBF) is a modern legal principle that provides individuals with the ability to seek the removal of personal information from public domains, particularly online

[1] *Justice KS Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1 (India).
[2] Draft Digital Personal Data Protection Bill 2023, Bill No XX, cl 13 (India).
[3] See Constitution of India, arts 19(1)(a), 19(1)(g); see also *Shreya Singhal v Union of India* (2015) 5 SCC 1.

platforms when such information is outdated, irrelevant, or harmful to their reputation. This concept recognizes the need to protect individuals' dignity and privacy in the digital age, where data permanence often exacerbates the risks of reputational damage and misuse of personal information.[4]

DEFINITION AND SCOPE

At its core, the RTBF allows individuals to exercise greater control over their digital footprint by requesting that certain personal data be delisted or removed from search engines, websites, or other platforms. However, this right is not absolute. Its scope typically includes situations where the information in question:

1. Is no longer relevant or necessary for the purpose for which it was collected.
2. Has become outdated or misleading over time.
3. Causes undue harm to an individual's personal or professional reputation.

The RTBF is most commonly invoked in cases involving personal data such as financial histories, outdated criminal records, or sensitive information that, if left accessible, can cause psychological or social harm.[5]

ORIGINS OF THE RTBF

The RTBF gained global attention following the landmark case of *Google Spain SL v. Agencia Española de Protección de Datos (AEPD)* in 2014. In this case, the Court of Justice of the European Union (CJEU) ruled that individuals have the right to request the removal of personal data from search engine results if it infringes on their privacy or dignity. This judgment effectively embedded the RTBF within the European Union's General Data Protection Regulation (GDPR), making it a statutory right across EU member states.[6]

The CJEU's ruling highlighted the balance between an individual's right to privacy and the public's right to access information. While search engines and platforms have a responsibility

[4] Wolfgang Schulz and Stephan Dreyer, 'The Right to Be Forgotten in Data Protection Law: A No-Go for Public Data?' (2010) 2(2) International Journal of Communications Law and Policy 13.
[5] Paul Schwartz and Daniel Solove, 'The PII Problem: Privacy and a New Concept of Personally Identifiable Information' (2011) 86 NYU Law Review 1814.
[6] General Data Protection Regulation, art 17.

to provide information, the judgment underscored that such obligations must be tempered by respect for individual rights.[7]

IMPLICATIONS FOR DATA PRIVACY

In the digital age, where data is created, shared, and stored at an unprecedented scale, the RTBF serves as a powerful tool for safeguarding privacy. It addresses several critical concerns:

1. **Data Permanence**: Information published online often remains accessible indefinitely, even if its relevance diminishes over time. The RTBF offers individuals a means to mitigate the long-term consequences of such permanence.

2. **Reputational Harm**: Negative or outdated information can severely impact personal and professional lives. The RTBF provides a mechanism for individuals to protect their reputations from unjustified harm.

3. **Power Asymmetry**: The RTBF empowers individuals in a digital ecosystem dominated by large technology companies, ensuring that personal data is not exploited or misused without recourse.

However, the RTBF also raises significant concerns, particularly regarding its potential to conflict with freedom of expression and the public's right to know. For instance, removing certain types of information, such as past criminal offenses or corporate controversies, may impede journalistic freedoms or historical accountability.[8]

In the Indian context, the RTBF holds immense relevance as the country navigates the complexities of digital privacy within a rapidly growing online population. While the Supreme Court has recognized the right to privacy as a fundamental right, there is no explicit statutory provision for the RTBF.[9] As such, India must carefully consider its implementation to strike a balance between individual rights and societal interests.

By examining its definition, origins, and implications, the RTBF emerges as a vital component of modern data protection frameworks, offering individuals a means to reclaim autonomy over

[7] *Google Spain SL v AEPD (n 4).*
[8] Andrew Murray, *Information Technology Law: The Law and Society* (3rd edn, OUP 2019) 168.
[9] Draft Digital Personal Data Protection Bill 2023 (India).

their digital identity while challenging lawmakers and technology platforms to navigate its nuanced complexities.

RESEARCH QUESTIONS

1. What is the legal status of the RTBF in India?

2. What challenges arise in implementing the RTBF?

3. How can India adopt a balanced framework for RTBF enforcement?

Section 1: The Concept of the Right to Be Forgotten

1.1 Origins and Global Perspective

The "Right to be Forgotten" (RTBF) originated as a response to the growing challenges posed by the digital age, where personal data is perpetually accessible and difficult to erase. The concept gained global attention through the landmark case of *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* in 2014.[10] The European Court of Justice (ECJ) ruled in favor of González, allowing him to request the removal of outdated and irrelevant information about his past from search engine results.[11] This case set a precedent, ultimately leading to the formal recognition of the RTBF under Article 17 of the General Data Protection Regulation (GDPR) in the European Union.[12]

The GDPR codifies the RTBF as the "right to erasure," enabling individuals to request data controllers and processors to delete personal information under certain conditions. These include situations where the data is no longer necessary for the original purposes of processing, the data subject withdraws consent, or the information is unlawfully processed.[13] While the RTBF under the GDPR has specific exceptions—such as the need to uphold freedom of expression, public interest, and archival purposes—it has set a global benchmark for data privacy rights.

[10] *Google Spain SL v. Agencia Española de Protección de Datos (AEPD)*, Case C-131/12, 2014 E.C.R. I-317.
[11] Ibid.
[12] See General Data Protection Regulation, art 17 (n 4).
[13] Ibid.

1.2 Indian Context

In India, the RTBF has yet to receive a comprehensive legal foundation, but its relevance has been highlighted in several court judgments and policy discussions. The Supreme Court's recognition of privacy as a fundamental right in *Justice K.S. Puttaswamy v. Union of India* laid the groundwork for privacy-related rights, including the RTBF.[14] Indian courts have addressed RTBF-like cases, albeit on a case-by-case basis. For example, in *Jorawer Singh Mundy v. Union of India*, the Delhi High Court directed the removal of judgment references to protect the petitioner's dignity and reputation.[15]

Despite these developments, the RTBF's status remains ambiguous under Indian law. The Draft Digital Personal Data Protection Bill, 2023, makes passing references to this right but fails to provide a detailed framework for its implementation.[16] This gap has created uncertainty for both individuals seeking recourse and digital platforms tasked with compliance.

1.3 The Need for the RTBF in India

In a society where the internet increasingly serves as a repository of personal histories, the RTBF holds significant relevance. Individuals often face reputational harm, psychological distress, or discrimination due to outdated or irrelevant information remaining accessible online. For instance, information about past mistakes, such as criminal charges that were later acquitted, can continue to negatively impact a person's career, social relationships, or mental health.[17]

Moreover, the RTBF aligns with the principle of rehabilitation and second chances, allowing individuals to move past errors that should not define their present or future. However, implementing this right in India requires navigating its complex socio-legal landscape, where the public's right to know and freedom of expression coexist with an individual's right to privacy.[18]

This section establishes the foundation for further exploration of the RTBF's practical implications and the challenges of incorporating it into India's legal and technological

[14] *Supra* (n 1).
[15] Jorawer Singh Mundy v Union of India, WP (C) 3918/2021 (Del HC, 2021).
[16] *Supra* (n 2).
[17] Jonathan L Zittrain, *The Future of the Internet—And How to Stop It* (2008) 52.
[18] Constitution of India, arts 19(1)(a), 21

framework. By understanding its origins, global applications, and contextual nuances, we can better analyze how this right can be harmonized with India's democratic values.

Section 2: Challenges in Implementation

The implementation of the Right to Be Forgotten (RTBF) in India faces significant challenges due to the country's complex legal, technological, and social environment. While the concept is gaining traction globally, its application in India is hindered by multiple factors, including legal ambiguity, conflict with constitutional rights, and practical enforcement barriers.

2.1 Legal Ambiguity

One of the primary challenges is the absence of a robust legal framework explicitly recognizing the RTBF. While the Draft Digital Personal Data Protection Bill, 2023, acknowledges the right in principle, it fails to define its scope or establish clear guidelines for its enforcement.[19] The lack of statutory clarity leaves individuals uncertain about their rights and organizations unsure of their obligations.

Moreover, Indian courts have approached RTBF-related cases on a case-by-case basis, leading to inconsistent interpretations.[20] For instance, while some judgments have granted individuals relief by directing the removal of personal data from public platforms, others have emphasized the need to protect freedom of expression and the public's right to access information.[21] This inconsistency reflects the broader challenge of balancing competing constitutional values.

2.2 Conflict with Freedom of Expression and Public Interest

Implementing the RTBF requires a delicate balance between an individual's right to privacy and the public's right to freedom of expression under Article 19(1)(a) of the Indian Constitution. Removing or de-indexing information can lead to censorship or suppression of public records, particularly in cases involving news, historical documentation, or public interest matters.

[19] *Supra* (n 2).
[20] *Supra* (n 9).
[21] *Shreya Singhal v Union of India (2015) 5 SCC 1 (India).*

For example, requests to erase information about a public figure's controversial past could be perceived as an attempt to rewrite history or manipulate public perception.[22] Similarly, information about criminal cases, even if the individual is acquitted, often holds public relevance, particularly for ensuring transparency and accountability.[23] This creates a potential conflict between individual privacy and the democratic principle of an informed citizenry.

2.3 Technological Challenges

The global and decentralized nature of the internet poses significant technological hurdles to the RTBF's implementation. Personal data is often stored across multiple servers worldwide, making it difficult to enforce removal requests uniformly.[24] Additionally, the proliferation of content through mirrors, backups, and third-party platforms complicates the task of ensuring complete erasure.

Search engines and digital platforms often face challenges in determining the legitimacy of removal requests and assessing whether they fall within the scope of the RTBF.[25] Without advanced technological tools, these platforms risk either overcomplying, which could lead to censorship, or undercomplying, which could violate privacy rights.

2.4 Lack of Awareness and Public Understanding

Another challenge lies in the limited public awareness of the RTBF. Many individuals are unaware of their rights or the procedures to request data removal. This lack of understanding not only limits the exercise of the RTBF but also increases the risk of its misuse, as individuals may seek to suppress legitimate information for personal gain.

Similarly, organizations and digital platforms may lack the training and resources required to handle RTBF requests effectively. The absence of standardized protocols further complicates the process, leading to delays and inefficiencies.[26]

[22] Wolfgang Schulz and Stephan Dreyer, 'The Right to Be Forgotten in Data Protection Law: A No-Go for Public Data?' (2010) 2(2) International Journal of Communications Law and Policy 13.
[23] *Supra* (n 1).
[24] Jonathan L Zittrain, *The Future of the Internet—And How to Stop It* (2008) 52.
[25] Ibid.
[26] Andrew D Murray, *Information Technology Law: The Law and Society* (3rd edn, 2019) 168.

2.5 Potential for Misuse

The RTBF carries the inherent risk of misuse, especially in cases where individuals seek to erase information that is lawfully in the public domain. For instance, corrupt officials or individuals with a criminal background could exploit the RTBF to suppress records of their wrongdoing, thereby obstructing justice or misleading the public.[27] Balancing this concern with the need to protect genuine privacy interests is a significant implementation challenge.

These challenges underscore the need for a well-defined legal and institutional framework to implement the RTBF effectively in India. Addressing these issues will require a multi-stakeholder approach involving the government, judiciary, technology platforms, and civil society to ensure that the RTBF safeguards individual privacy without undermining democratic freedoms. The next section explores potential solutions to these challenges, proposing a balanced framework tailored to India's unique context.

Section 3: Proposed Framework for India

The Right to Be Forgotten (RTBF) is a pivotal step toward strengthening digital privacy in India. However, its effective implementation requires a robust framework that addresses the unique legal, social, and technological challenges of the Indian context. A well-balanced approach must harmonize the RTBF with constitutional rights, technological realities, and societal needs. This section outlines a proposed framework to achieve these goals.

3.1 Legal Clarity and Comprehensive Legislation

A clear legal foundation is essential for the effective implementation of the RTBF. The first step is to enact comprehensive data protection legislation explicitly recognizing the RTBF.[28] The legislation must provide:

1. **Definition and Scope**: Clear definitions of what constitutes "outdated," "irrelevant," or "harmful" data.

[27] Paul M Schwartz and Daniel J Solove, 'The PII Problem: Privacy and a New Concept of Personally Identifiable Information' (2011) 86 NYU Law Review 1814, 1843–45.
[28] *Supra* (n 2).

2. **Eligibility Criteria**: Specific conditions under which individuals can invoke the RTBF, such as when data is no longer necessary, unlawfully processed, or violates personal dignity.

3. **Exceptions**: Provisions to protect public interest, freedom of expression, and the right to access information, especially for journalistic, academic, or archival purposes.[29]

Additionally, the law should establish mechanisms to resolve conflicts between competing rights, ensuring a balanced approach that respects both privacy and free speech.[30]

3.2 Institutional Mechanism

An independent regulatory body, such as a Data Protection Authority (DPA), should oversee the RTBF's implementation. This body would:

1. **Adjudicate Requests**: Evaluate RTBF claims on a case-by-case basis, balancing individual privacy with public interest.

2. **Issue Guidelines**: Develop clear procedures for submitting and processing RTBF requests.

3. **Monitor Compliance**: Ensure that organizations and digital platforms comply with the law while preventing misuse or overreach.

The DPA should also be empowered to impose penalties for non-compliance and provide a grievance redressal mechanism for individuals dissatisfied with the handling of their requests.[31]

3.3 Technological Integration

Technological advancements must be leveraged to streamline the RTBF's enforcement. This includes:

1. **AI-Driven Tools**: Use artificial intelligence to automate the identification and removal of outdated or irrelevant data.

[29] General Data Protection Regulation, art 17, 2016 OJ (L 119).
[30] *Supra* (n 1).
[31] Andrew D Murray, *Information Technology Law: The Law and Society* (3rd edn, 2019) 168.

2. **Blockchain for Transparency**: Employ blockchain technology to maintain a secure and transparent record of RTBF requests and their outcomes, ensuring accountability while protecting privacy.

3. **Global Collaboration**: Develop mechanisms for cross-border cooperation to address jurisdictional issues in data storage and removal.

By integrating these technologies, India can address the practical challenges of enforcing the RTBF across decentralized and global digital platforms.[32]

3.4 Public Awareness and Education

Educating the public about their rights under the RTBF is crucial for its success. Awareness campaigns should inform individuals about:

1. The scope and limitations of the RTBF.

2. The procedures for submitting removal requests.

3. The importance of balancing privacy with other constitutional values.

Similarly, organizations and digital platforms must receive training on handling RTBF requests ethically and efficiently. This includes understanding the law, respecting individual rights, and recognizing the broader societal implications of their actions.

3.5 Safeguards Against Misuse

To prevent misuse, the framework must include safeguards such as:

1. **Verification Mechanisms**: Ensure that requests are legitimate and supported by evidence.

2. **Public Interest Review**: Require a thorough review of cases where data removal could impact public interest or freedom of expression.

3. **Appeals Process**: Establish an appeals process for cases where a request is denied or deemed contentious.

[32] Zittrain, *supra* (n 8), 52.

These measures will ensure that the RTBF is used responsibly, protecting individual privacy while preserving transparency and accountability.

3.6 Harmonization with Constitutional Principles

The proposed framework must align with India's constitutional principles. The RTBF should complement the right to privacy while ensuring that it does not infringe on other fundamental rights, such as freedom of speech and the public's right to know. This balance can be achieved through regular judicial oversight and ongoing dialogue between stakeholders, including the government, civil society, and digital platforms.[33]

The proposed framework aims to provide a balanced and practical approach to implementing the RTBF in India. By addressing legal, institutional, technological, and societal challenges, this framework ensures that the RTBF is not only effective but also equitable and sustainable. This approach reflects India's commitment to upholding individual dignity while fostering a digital ecosystem that respects democratic values.

BALANCING THE RIGHT TO BE FORGOTTEN WITH FREEDOM OF EXPRESSION AND PUBLIC INTEREST

The Right to Be Forgotten (RTBF) often intersects with two fundamental democratic principles: freedom of expression and the public's right to access information. These principles are deeply embedded in the Indian Constitution under Article 19(1)(a), which guarantees the freedom of speech and expression, and the broader framework of transparency and accountability in governance.[34] The challenge of implementing the RTBF lies in reconciling these competing interests without undermining any of them.

Freedom of Expression

Freedom of expression is a cornerstone of democracy, enabling individuals to share ideas, engage in debates, and hold authorities accountable.[35] The RTBF, by allowing individuals to request the removal of personal data, raises concerns about censorship and the suppression of legitimate information. For instance, if public figures invoke the RTBF to erase information

[33] *Supra* (n 15).
[34] *Supra* (n 12).
[35] *Supra* (n 15).

about their controversial pasts, it could limit public discourse and hinder the electorate's ability to make informed decisions.[36]

However, proponents argue that the RTBF does not inherently conflict with freedom of expression but seeks to protect individuals from harm caused by outdated or irrelevant data.[37] The key lies in establishing a balanced framework that differentiates between private individuals seeking relief from personal harm and cases involving public interest. Courts and regulatory authorities must ensure that the RTBF is applied judiciously, with greater scrutiny in cases where its enforcement could restrict free speech.[38]

Public Interest

Public interest serves as a critical exception to the RTBF, ensuring that the removal of data does not compromise societal needs. For example, information about criminal activities, public health concerns, or corporate malpractices may remain accessible due to its relevance to transparency and accountability. Striking this balance requires a case-by-case analysis to determine whether the public benefit of retaining information outweighs the individual's privacy concerns.

Proposed Mechanisms for Balance

To reconcile the RTBF with these democratic principles, the following mechanisms can be incorporated:

1. **Public Interest Test**: A structured framework to evaluate whether the data requested for removal serves a significant public interest. This test should consider factors such as the nature of the information, its relevance to public discourse, and the potential harm caused by its removal.[39]

2. **Role of Regulatory Bodies**: An independent Data Protection Authority (DPA) can act as an arbitrator, reviewing RTBF requests while safeguarding freedom of expression

[36] Ibid.
[37] *Supra* (n 2).
[38] Wolfgang Schulz and Stephan Dreyer, 'The Right to Be Forgotten in Data Protection Law: A No-Go for Public Data?' (2010) 2(2) International Journal of Communications Law and Policy 13.
[39] Schulz and Dreyer, *supra* (n 32), 13.

and public interest. The DPA should adopt transparent processes and issue well-reasoned decisions to maintain public trust.

3. **Judicial Oversight**: Courts should serve as a check on potential misuse of the RTBF, particularly in high-stakes cases involving public figures, media entities, or whistleblowers. This ensures that the application of the RTBF aligns with constitutional principles.

4. **Tiered Application**: Differentiate between private citizens and public figures. While private citizens should have a stronger claim to privacy, public figures may have a reduced expectation of anonymity due to their role in public life.[40]

By embedding these safeguards, the RTBF can coexist with freedom of expression and public interest, fostering a legal environment that respects individual dignity without compromising the democratic values of transparency and accountability. This balanced approach is vital to ensuring that the RTBF evolves as a tool for protecting privacy while strengthening India's commitment to democratic ideals.

CONCLUSION

The Right to Be Forgotten (RTBF) is a crucial legal concept in the age of digital information, empowering individuals to reclaim control over their personal data and safeguard their privacy.[41] However, implementing the RTBF in India is a complex endeavor due to the country's legal ambiguities, competing for constitutional rights, technological challenges, and societal nuances. Despite these hurdles, its significance cannot be overstated in a rapidly digitizing world where information permanence can have profound implications on individuals' dignity, reputation, and mental well-being.

The RTBF holds particular relevance in India, where digital penetration is increasing, and personal data is widely shared and stored on online platforms.[42] While the judiciary has acknowledged privacy as a fundamental right, the absence of a statutory framework for the RTBF creates uncertainties for both individuals seeking protection and platforms expected to

[40] *R Rajagopal v State of Tamil Nadu (1994) 6 SCC 632 (India).*
[41] General Data Protection Regulation, art 17, 2016 OJ (L 119).
[42] Internet and Mobile Ass'n of India, Digital in India: A Review of 2023 (2023).

comply. To address this gap, India must adopt a structured approach that integrates clear legal provisions, robust institutional mechanisms, and advanced technological solutions.

Balancing the RTBF with freedom of expression and public interest is critical to preserving India's democratic ethos. This requires a nuanced framework that ensures individual privacy without stifling transparency, accountability, or the public's right to information. Provisions for exceptions, public interest reviews, and safeguards against misuse are essential to prevent the RTBF from becoming a tool for censorship or the erasure of history.[43]

Furthermore, public awareness and education are indispensable for the RTBF's success. Individuals must understand their rights, and organizations must be equipped to handle requests ethically and effectively. By fostering a culture of accountability and transparency, the RTBF can become a tool for empowerment rather than conflict.[44]

Ultimately, the RTBF's implementation in India will require a multi-stakeholder approach involving the government, judiciary, digital platforms, and civil society. This collaborative effort must prioritize harmonizing privacy with democratic freedoms, ensuring that the RTBF evolves as a cornerstone of India's digital governance. By taking these steps, India can set an example for other nations grappling with the challenges of privacy in the digital age, reaffirming its commitment to individual dignity and democratic values in an increasingly interconnected world.

[43] Andrew D Murray, *Information Technology Law: The Law and Society* (3rd edn, 2019) 168.
[44] Internet and Mobile Association of India, *supra* (n 36).