Global Perspectives on the Right to Be Forgotten: A Comparative Legal Analysis

by

MR. SWASTIK KUMAR

&

DR. KRITIKA NAGPAL

ABSTRACT

The Right to Be Forgotten (RTBF) has emerged as one of the most debated digital rights in contemporary legal discourse. Rooted in the European Union's data protection framework, particularly the General Data Protection Regulation (GDPR), RTBF embodies the right of individuals to have personal data erased or delisted from public access when it no longer serves a legitimate purpose. This research paper undertakes a comparative analysis of RTBF across multiple jurisdictions, including the European Union, the United States, the United Kingdom (especially post-Brexit), and selected Asian and Latin American nations. The paper highlights the diverse constitutional and legal approaches to balancing privacy with freedom of speech and the right to information.

The European Union, through the landmark Google Spain v. AEPD & Costeja González case, has institutionalized RTBF with enforceable procedural safeguards. In contrast, the United States resists RTBF on First Amendment grounds, prioritizing free expression over privacy claims. The UK, following Brexit, maintains a hybrid stance, retaining GDPR principles but slowly redefining them in a national context. Latin American countries like Brazil and Colombia, and Asian jurisdictions like South Korea and Japan, are beginning to localize RTBF within their constitutional and cultural landscapes.

This paper argues that India, while progressing in its data protection landscape, lacks a coherent RTBF framework and can benefit significantly from international models. The study concludes by emphasizing the need for India to integrate RTBF in a manner that respects its constitutional values, including freedom of speech and privacy, while also addressing technological and enforcement challenges.

INTRODUCTION

The digitalization of personal information has raised critical concerns about the permanence of online data and its potential to harm personal dignity, reputation, and autonomy. As individuals seek to reclaim control over their digital identities, the Right to Be Forgotten (RTBF) emerges as a key tool to navigate the tension between informational privacy and the public's right to know. This paper explores the global evolution of RTBF and its complex legal contours, particularly through a comparative study of its adoption and resistance across jurisdictions.

RESEARCH QUESTIONS

- How have different jurisdictions interpreted and implemented the Right to Be Forgotten?
- What constitutional and legal tensions arise between RTBF and freedom of expression?
- How can India develop a balanced RTBF framework that aligns with its constitutional values and evolving digital ecosystem?

LITERATURE REVIEW

The Right to Be Forgotten (RTBF) has garnered significant scholarly attention, particularly since the landmark Google Spain1 decision in 2014, which catalyzed the global discourse on digital privacy and personal data control. The literature spans various themes, including the philosophical underpinnings of memory and identity, the legal conflict between privacy and free speech, the role of internet intermediaries, and comparative regulatory frameworks.

Viktor Mayer-Schönberger, in his influential work Delete: The Virtue of Forgetting in the Digital Age (2009)2, provides the foundational philosophical argument in favor of forgetting as a social and psychological necessity in the digital era. He argues that the internet's inherent tendency to remember everything disrupts human capacity for change and second chances. This forms the normative bedrock upon which many RTBF claims are constructed.

Jeffrey Rosen (2012) raises a cautionary counterpoint by viewing RTBF as potentially incompatible with democratic values such as transparency and press freedom. In his Stanford

[1] *Google Spain SL v. AEPD*, Case C-131/12, CJEU (2014)
[2] Viktor Mayer-Schönberger, *Delete: The Virtue of Forgetting in the Digital Age* (Princeton Univ. Press 2009)

Law Review3 article, Rosen criticizes the European Court of Justice's interpretation in Google Spain4 as granting excessive power to individuals to suppress truthful information. He warns against the risk of creating a private censorship regime governed by search engines and bureaucrats rather than courts.

Reuben Binns (2018), in his article Data Protection and the Ethics of the Right to be Forgotten5, addresses the ethical and algorithmic implications of automated content moderation. He emphasizes the need for transparent and contestable processes, especially when private tech companies act as arbiters of digital memory. His work intersects RTBF with the broader challenge of algorithmic governance.

From a comparative legal perspective, Gloria González Fuster (2014)6 examines how the European Union elevated data protection to the level of a fundamental right, culminating in the GDPR. Her research unpacks the genealogy of Article 17, situating RTBF within the evolution of EU privacy norms.

In the Indian context, legal scholarship remains relatively nascent but is growing following the Supreme Court's recognition of privacy as a fundamental right in Justice K.S. Puttaswamy v. Union of India (2017)7. The Srikrishna Committee Report (2018)8 marked a watershed moment, recommending a statutory framework for data protection, including RTBF-like provisions. However, Indian academic contributions still grapple with reconciling RTBF with free speech under Article 19(1)(a) of the Constitution.

International perspectives from Latin America, particularly in Brazil and Colombia, are emerging through local judicial interpretations of constitutional dignity and digital rights. In Asia, Japan and South Korea have begun integrating RTBF into their data protection regimes, often balancing cultural sensitivities and technological enforcement mechanisms.

In sum, the literature reflects both the promise and peril of RTBF. While scholars like Mayer-Schönberger and González Fuster argue for stronger individual data rights, critics like Rosen and Binns caution against unintended consequences for freedom of expression and

---

[3] Jeffrey Rosen, The Right to Be Forgotten, 64 *Stan. L. Rev. Online* 88 (2012).
[4] *Google Spain SL v. AEPD*, Case C-131/12, CJEU (2014)
[5] Reuben Binns, Data Protection and the Ethics of the Right to be Forgotten, *Philos. & Tech.* 31, 311–328 (2018).
[6] Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer 2014).
[7] *Google Spain SL v. AEPD*, Case C-131/12, CJEU (2014)
[8] Committee of Experts on a Data Protection Framework for India, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (2018)

democratic accountability. The challenge lies in translating these theoretical insights into workable, rights-sensitive legal frameworks, especially in jurisdictions like India, where legal and technological infrastructures are still evolving.

DEFINING THE RIGHT TO BE FORGOTTEN (RTBF)

The **Right to Be Forgotten (RTBF)** refers to the ability of individuals to request the removal of personal information from internet search results, databases, and other publicly accessible sources. This right is deeply rooted in the principles of **privacy, data protection, and individual autonomy** in the digital age, where information can persist indefinitely, affecting a person's reputation, professional opportunities, and personal life.

ORIGIN OF THE RTBF CONCEPT

The concept of RTBF has evolved alongside the rapid expansion of the internet and digital technologies. Traditionally, legal systems have recognized the right to privacy, but the advent of **search engines, social media platforms, and digital archives** has created new challenges where personal data remains permanently accessible. RTBF gained global attention following the landmark case **Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González (2014)**[9], where the European Court of Justice (ECJ) ruled that individuals have the right to request the removal of outdated or irrelevant personal data from search results.

RTBF IN THE CONTEXT OF DIGITAL PRIVACY

RTBF is an extension of **data protection rights**, emphasizing an individual's control over their personal data. It allows for the **erasure or de-indexing of information** that is no longer relevant, excessive, or defamatory. However, RTBF does not mean absolute deletion; rather, it focuses on restricting the visibility of certain data, particularly in search engine results, while the original source may still retain the information.

KEY COMPONENTS OF RTBF

RTBF primarily involves:

- **De-indexing of URLs:** Search engines like Google can be required to remove links to specific information upon request.

[9] *Google Spain SL v. AEPD*, Case C-131/12, CJEU (2014)

- **Data Erasure Requests:** Websites and online platforms may be asked to delete certain personal data under privacy laws.
- **Balance with Public Interest:** RTBF is not an absolute right; it must be balanced with the public's right to access information, particularly concerning newsworthy events and public figures.

RTBF VS. OTHER DIGITAL RIGHTS

RTBF intersects with other legal rights, including:

- **Right to Privacy:** Ensures personal autonomy and data protection.
- **Freedom of Expression:** Concerns about potential censorship and information suppression.
- **Right to Reputation:** Protection against defamation and unwanted digital permanence.

CRITICISM AND CONTROVERSY

RTBF has sparked debates around censorship, historical record alteration, and the **chilling effect** on journalism. Critics argue that it places a significant burden on private companies (such as search engines) to determine what information should be removed, potentially leading to **subjective enforcement** and legal inconsistencies across jurisdictions.

PHILOSOPHICAL AND LEGAL JUSTIFICATION FOR RTBF

The RTBF is deeply rooted in both **philosophical principles and legal doctrines**, reflecting evolving societal values regarding **privacy, personal autonomy, and digital ethics**. The justifications for RTBF stem from **natural rights theories, constitutional law, human rights instruments, and evolving judicial interpretations**.

PHILOSOPHICAL FOUNDATIONS OF RTBF

JOHN LOCKE'S THEORY OF PERSONAL AUTONOMY

Lockean philosophy asserts that individuals have **ownership over their personal identity and information**. RTBF aligns with this notion by allowing people to control their digital footprint, akin to **controlling their property and personal affairs**.

KANTIAN ETHICS AND HUMAN DIGNITY

Immanuel Kant emphasized **human dignity and individual autonomy**. Under this framework, individuals should have the **moral right to control their personal narrative**, which aligns with the modern demand for RTBF.

MILL'S HARM PRINCIPLE AND RTBF

John Stuart Mill's **harm principle** suggests that restrictions on information should only occur when harm is caused to an individual. RTBF supports this by ensuring that outdated or misleading personal data does not cause unjust harm to a person's reputation or future opportunities.

LEGAL JUSTIFICATIONS FOR RTBF

EUROPEAN UNION'S GDPR (GENERAL DATA PROTECTION REGULATION)[10]

The most formal legal recognition of RTBF is enshrined in **Article 17 of the GDPR**, which provides individuals with the **right to request the erasure of personal data** under specific conditions:

- The data is no longer necessary for its original purpose.
- The individual withdraws consent.
- The data was processed unlawfully.
- The individual objects to data processing on legitimate grounds.

INTERNATIONAL HUMAN RIGHTS LAW

The **Universal Declaration of Human Rights (UDHR)** and the **International Covenant on Civil and Political Rights (ICCPR)** emphasize **privacy as a fundamental right**. RTBF aligns with these principles by protecting individuals from excessive exposure of personal data.

NATIONAL LEGAL FRAMEWORKS

- **European Union:** Established through GDPR and ECJ rulings.
- **United States:** No formal RTBF, but privacy laws such as the **California Consumer Privacy Act (CCPA)** provide limited data control.

[10] Regulation (EU) 2016/679 (General Data Protection Regulation)

- **India:** RTBF is an emerging concept, with references in the **Puttaswamy Judgment (2017)**[11], which recognized **privacy as a fundamental right**.
- **Other Jurisdictions:** Countries like Argentina and Canada are exploring RTBF implementations within their legal systems.

BALANCING RTBF WITH FREEDOM OF EXPRESSION

A major legal challenge is ensuring that RTBF does not infringe on **press freedom and access to information**. Courts have developed balancing tests, weighing **personal privacy rights against public interest and journalistic freedoms**.

ETHICAL CONSIDERATIONS AND FUTURE LEGAL DEVELOPMENTS

Ethically, RTBF raises concerns about the **erasure of historical records, potential misuse by public figures, and jurisdictional enforcement issues**. Moving forward, legal scholars suggest:

- Developing **clearer global frameworks** for RTBF enforcement.
- Establishing **independent review bodies** to evaluate removal requests.
- Encouraging **technological solutions**, such as AI-based content moderation, to balance privacy with free speech.

RTBF IN CONTEXT OF PRIVACY, DATA PROTECTION, AND FREEDOM OF EXPRESSION

The Right to Be Forgotten (RTBF) stands at the crossroads of three fundamental legal principles: privacy, data protection, and freedom of expression. As digital interactions grow exponentially, personal data becomes more vulnerable to misuse, leading to increasing concerns over how information is stored, shared, and accessed. RTBF seeks to grant individuals greater control over their digital footprint, but its enforcement raises critical challenges in balancing personal privacy with public interest. While privacy and data protection support an individual's right to request the erasure of personal data, freedom of expression and the public's right to access information often come into direct conflict with such claims. Examining RTBF

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

through the lens of these three principles is essential to understanding its scope, applicability, and limitations.

PRIVACY AS A FOUNDATION OF RTBF

The foundation of RTBF is rooted in the right to privacy, which has been recognized as a fundamental human right in international legal instruments such as Article 12 of the Universal Declaration of Human Rights (UDHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR). Privacy laws aim to protect individuals from arbitrary interference in their personal lives, and as digital platforms continue to amass and disseminate personal data, this right has evolved to encompass online activities. RTBF extends the right to privacy into the digital domain by allowing individuals to request the removal of personal data that is no longer relevant or necessary.

Legal frameworks across jurisdictions approach privacy differently. In Europe, the European Convention on Human Rights (ECHR) recognizes privacy under Article 8, which has been interpreted broadly by the European Court of Human Rights to include control over personal information. The landmark General Data Protection Regulation (GDPR) of the European Union explicitly codifies RTBF under Article 17[12], affirming that individuals can request data erasure under specific conditions. In India, the Supreme Court in *Justice K.S. Puttaswamy v. Union of India (2017[13])* declared privacy a fundamental right under Article 21 of the Constitution. While this decision strengthened the legal foundation for RTBF, India still lacks a dedicated law enforcing such a right. The privacy rationale behind RTBF is clear: individuals should not be permanently haunted by outdated or irrelevant personal data, especially when its continued availability serves no legitimate public interest.

However, the challenge in enforcing RTBF purely as a privacy measure lies in its potential misuse. Privacy claims could be used to erase inconvenient but truthful information, such as past financial misdeeds or criminal records, leading to conflicts between personal privacy and accountability. In democratic societies, where transparency and informed public discourse are valued, determining when privacy should prevail over public knowledge is a crucial legal and ethical challenge.

[12] Regulation (EU) 2016/679 (General Data Protection Regulation)
[13] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1

RTBF AND DATA PROTECTION LAWS

Data protection laws provide the statutory basis for enforcing RTBF by regulating how personal information is collected, stored, and deleted. GDPR[14] remains the most comprehensive framework in this regard, specifically recognizing RTBF under Article 17. Under GDPR, individuals can request data deletion if their information is no longer necessary for the purpose it was collected, if consent is withdrawn, or if data has been processed unlawfully. However, GDPR also acknowledges that RTBF is not absolute and must be weighed against factors such as freedom of expression, legal obligations, and public interest.

Different countries approach RTBF within their own data protection laws. The United States, for example, takes a free speech-centric approach, where the First Amendment[15] limits the extent to which personal data can be erased from public records. There is no equivalent of RTBF under U.S. federal law, although certain state laws, such as the California Consumer Privacy Act (CCPA), provide limited data deletion rights. India's proposed Digital Personal Data Protection (DPDP) Bill, 2022[16], introduces a version of RTBF, but its scope remains unclear, with concerns over its implementation and possible governmental overreach.

The enforcement of RTBF within data protection laws also raises questions regarding extraterritorial jurisdiction. The *Google Spain v. AEPD & Mario Costeja González* case established that search engines must comply with RTBF requests[17], but it also created uncertainty over whether such obligations extend globally or only within the European Union. The broader question of how RTBF interacts with cross-border data flow remains a complex legal issue.

RTBF AND FREEDOM OF EXPRESSION

The most significant opposition to RTBF comes from concerns over freedom of expression and the public's right to know. Freedom of expression, enshrined in Article 19 of the UDHR and Article 10 of the ECHR, ensures that individuals and the media can share and access information without undue restrictions. Critics argue that RTBF, if applied broadly, could lead to censorship, erasing history under the pretext of privacy.

[14] Regulation (EU) 2016/679 (General Data Protection Regulation)
[15] U.S. Const. amend. I
[16] Committee of Experts on a Data Protection Framework for India (2018)
[17] *Google Spain SL v. AEPD*, Case C-131/12, CJEU (2014)

Cases such as *Google Spain*[18] and *NT1 & NT2 v. Google LLC*[19] illustrate how courts attempt to balance RTBF with free speech. While RTBF applies to outdated, irrelevant, or misleading personal data, it does not extend to public figures or information that remains in the public interest. Nevertheless, the chilling effect remains a concern—if RTBF is not carefully regulated, it could allow powerful individuals or corporations to suppress negative but truthful information.

COMPARATIVE ANALYSIS: RTBF VS OTHER DIGITAL RIGHTS

While RTBF is a significant digital right, it does not exist in isolation. It must be examined in relation to other digital rights such as the right to access information, the right to rectification, and the right to data portability. These rights often overlap or conflict, making it necessary to establish a nuanced framework for balancing them.

RTBF VS. RIGHT TO ACCESS INFORMATION

The right to access information ensures that individuals and society at large can obtain knowledge, which is fundamental to democracy and accountability. RTBF, in contrast, allows individuals to request the removal of certain information. This inherent conflict raises legal and ethical dilemmas. Should RTBF allow a former criminal to erase past convictions from search engines? Should news archives be altered to accommodate privacy claims? Courts have generally held that RTBF does not extend to public records, but the boundary between private and public interest remains contentious.

RTBF VS. RIGHT TO RECTIFICATION

The right to rectification, recognized under Article 16 of GDPR, allows individuals to correct inaccurate data but does not grant the right to complete erasure. The distinction between the two rights is significant—RTBF enables individuals to remove outdated or irrelevant information, while rectification ensures that existing data is factually correct. In some cases, individuals might seek both rectification and erasure, such as when a wrongly accused person wants to delete search engine results while also correcting official records.

[18] *Google Spain SL v. AEPD*, Case C-131/12, CJEU (2014)
[19] *NT1 & NT2 v. Google LLC*, [2018] EWHC 799 (QB)

RTBF VS. RIGHT TO DATA PORTABILITY

The right to data portability, under Article 20 of GDPR, allows users to transfer their data from one service provider to another. While both RTBF and data portability empower individuals over their data, their objectives differ. RTBF focuses on erasure, while data portability ensures continuity of access. For example, a social media user seeking to delete their account may request RTBF for unwanted posts while also invoking data portability to transfer their content to another platform.

RTBF VS. DIGITAL FORGETTING MECHANISMS

Digital forgetting mechanisms refer to automated processes where data is erased after a predetermined period, such as ephemeral messaging or time-bound data retention policies. Unlike RTBF, which requires an active request, digital forgetting is often built into the system. While digital forgetting aligns with RTBF in reducing digital permanence, legal frameworks need to address scenarios where automated deletions conflict with evidentiary requirements or public interest considerations.

CONCLUSION

The Right to Be Forgotten represents a transformative development in digital privacy jurisprudence, offering individuals a mechanism to reclaim control over their personal data in an era of pervasive digital memory. Through this comparative analysis of jurisdictions such as the European Union, the United States, the United Kingdom, and select Asian and Latin American countries, it becomes evident that RTBF is interpreted not as a universal right but as a context-dependent legal construct, shaped by each region's constitutional values, legal traditions, and cultural attitudes toward privacy and free expression.

The European Union, with its rights-based approach to data protection under the GDPR and landmark rulings like Google Spain, has institutionalized RTBF in a manner that emphasizes individual dignity and informational autonomy. Conversely, the United States has maintained a rigid resistance to RTBF, prioritizing freedom of expression under the First Amendment and viewing any broad erasure right as a threat to democratic transparency. The United Kingdom, in a post-Brexit regulatory landscape, continues to adapt RTBF principles under its domestic laws, albeit with nuanced changes to enforcement and procedural clarity.

Emerging legal regimes in Brazil, Colombia, Japan, and South Korea reflect a growing global acknowledgment of RTBF, albeit with distinct national variations. These jurisdictions

are grappling with how to localize digital rights without compromising other constitutional guarantees, particularly freedom of the press and access to information.

In the Indian context, while judicial pronouncements like Justice K.S. Puttaswamy v. Union of India have laid the groundwork by recognizing privacy as a fundamental right, the legislative framework for RTBF remains fragmented and underdeveloped. The proposed Digital Personal Data Protection Bill offers a potential vehicle for codifying RTBF, but it must be crafted with careful attention to India's democratic values, technological capacity, and institutional enforcement mechanisms.

Ultimately, RTBF must not be seen as an absolute right, but as one that necessitates a nuanced balancing exercise between the individual's right to privacy and the collective interest in preserving digital transparency. As the digital ecosystem evolves, the future of RTBF will depend on striking this balance through rights-sensitive legislation, accountable institutions, and technologically informed policy frameworks.

BIBLIOGRAPHY

CASES

- Google Spain SL v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, Case C-131/12, ECLI:EU:C:2014:317 (CJEU 2014).
- NT1 & NT2 v. Google LLC, [2018] EWHC 799 (QB) (UK).
- Cox Broad. Corp. v. Cohn, 420 U.S. 469 (1975).
- Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).

LEGISLATION AND OFFICIAL INSTRUMENTS

- Regulation (EU) 2016/679, of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation or "GDPR").
- U.S. Const. amend. I.
- Data Protection Act 2018, c. 12 (UK).
- Lei No. 13.709, de 14 de Agosto de 2018 (Brazilian General Data Protection Law or "LGPD").

BOOKS

- Viktor Mayer-Schönberger, Delete: The Virtue of Forgetting in the Digital Age (Princeton Univ. Press 2009).

- Gloria González Fuster, The Emergence of Personal Data Protection as a Fundamental Right of the EU (Springer 2014).

JOURNAL ARTICLES

- Jeffrey Rosen, The Right to Be Forgotten, 64 Stan. L. Rev. Online 88 (2012).
- Reuben Binns, Data Protection and the Ethics of the Right to be Forgotten, Philosophy & Technology, vol. 31, 311–328 (2018).
- Daniel J. Solove, A Taxonomy of Privacy, 154 U. Pa. L. Rev. 477 (2006).
- Meg Leta Ambrose, It's About Time: Privacy, Information Life Cycles, and the Right to Be Forgotten, 16 Stan. Tech. L. Rev. (2013).
- Stefan Kulk & Frederik Zuiderveen Borgesius, Google Spain: A Challenging Balancing Act Between Privacy and Freedom of Expression, 5(3) Eur. J. Risk Regul. 531 (2014).

REPORTS AND POLICY DOCUMENTS

- Committee of Experts on a Data Protection Framework for India, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians (2018) (Srikrishna Committee Report).
- European Data Protection Board (EDPB), Guidelines 5/2019 on the Criteria of the Right to Be Forgotten in the Search Engine Cases under the GDPR (Part 1) (Dec. 2019).
- UK Information Commissioner's Office (ICO), Guide to the Right to Erasure (2020).
- United Nations Human Rights Council, The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/27/37 (2014).
- OECD, Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (2013).
- Future of Privacy Forum, Comparison of Privacy Laws Worldwide (2022).