International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

THE RIGHT TO BE FORGOTTEN UNDER GDPR: LEGAL SCOPE AND PRACTICAL CHALLENGES

Anushree Chaudhary[1], Prof. (Dr.) S.P.S Shekhawat[2]

[1]PhD Scholar Law, [2]Head and Dean
Faculty of Law, Jagannath University, Jaipur, Rajasthan

Abstract:
The *Right to Be Forgotten* (RTBF), enshrined under Article 17 of the General Data Protection Regulation (GDPR), represents a pivotal shift in the landscape of data privacy and digital rights in the European Union. This right empowers individuals to request the erasure of personal data when it is no longer necessary for the purpose it was collected, when consent is withdrawn, or when the processing is unlawful. Rooted in the landmark *Google Spain SL v. Agencia Española de Protección de Datos (2014)* decision, the RTBF underscores the growing tension between *privacy rights* and *freedom of expression*, especially in the digital ecosystem dominated by global tech giants. This abstract explores the legal scope of the RTBF, examining the conditions, limitations, and exceptions under GDPR. It also evaluates the extraterritorial applicability of the right, particularly in cross-border data flows, and the complex balance it seeks to achieve between personal autonomy and public interest. The paper investigates practical challenges in enforcing this right, such as defining the threshold of "public interest," handling requests across multiple jurisdictions, ensuring compliance by data controllers, and the risk of censorship. Moreover, it highlights concerns about technological enforcement, especially the feasibility of complete erasure in decentralized systems like blockchain or widespread internet archives. The role of search engines, the ambiguity around delisting versus deletion, and the implications for media archives are also critically analyzed. Through comparative insights and recent case law developments, this work underscores that while the RTBF is a significant advancement in data protection, it remains fraught with operational ambiguities and ethical dilemmas in the age of the internet.

Keywords: Right to Be Forgotten, GDPR, Data Privacy, Freedom of Expression, Digital Erasure, Cross-border Data Protection.

1. INTRODUCTION AND EVOLUTION OF THE RIGHT TO BE FORGOTTEN

The advent of the digital age has significantly transformed the way personal data is created, stored, and disseminated. As the internet became an integral part of modern life, concerns about the long-term availability and misuse of personal information grew considerably. In this context, the *Right to Be Forgotten* (RTBF) has emerged as one of the most contentious and significant aspects of data protection laws globally. It reflects a growing recognition of individuals' rights to digital privacy and control over their personal information in the face of rapid technological change and massive data accumulation.[1]

Historical Background of the Right to Be Forgotten

The conceptual foundation of the RTBF predates the formal legal articulation found in the General Data Protection Regulation (GDPR). Its roots can be traced to European traditions of privacy and dignity, particularly in civil law jurisdictions like France and Germany. In France, the concept of "le droit à l'oubli" (the right to oblivion) has long granted individuals the ability to move beyond past convictions or events after a certain period, reflecting a societal value placed on personal redemption and privacy.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), Official Journal of the European Union, L 119, 4.5.2016.

Before GDPR, fragmented national-level privacy regulations existed in EU member states. These often provided some form of recourse for individuals seeking to remove outdated or irrelevant personal data. However, these protections lacked harmonization, enforceability, and clarity, making cross-border application nearly impossible. The increasing ubiquity of search engines and digital archives further compounded the issue, necessitating a more unified legal framework.

The Google Spain Case: A Turning Point

The landmark 2014 judgment in *Google Spain SL v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* by the Court of Justice of the European Union (CJEU) was a pivotal moment in the evolution of the RTBF. The case involved a Spanish national, Mario Costeja González, who requested Google to remove links to a 1998 newspaper article about his past financial troubles, which had been resolved but remained prominently visible online through search engine results.

The CJEU ruled in favor of González, stating that individuals have the right to request search engines to remove links to personal data under certain conditions. The judgment emphasized that search engines are data controllers and, thus, subject to EU data protection laws. This ruling effectively established a judicially created right to be forgotten and mandated search engines to delist links to personal data that is "inadequate, irrelevant or no longer relevant, or excessive" in relation to the purposes of the data processing.[2]

This decision was groundbreaking for several reasons:

- It reinforced the concept of data minimization and proportionality in digital contexts.
- It recognized the evolving nature of privacy rights in response to technological advances.
- It imposed new responsibilities on private companies, particularly tech giants, to balance privacy and public interest.

Codification in the General Data Protection Regulation (GDPR)

Building upon the momentum of the Google Spain ruling, the European Union codified the RTBF in the GDPR, which came into effect on 25 May 2018. Article 17 of the GDPR provides individuals with the right to obtain the erasure of personal data concerning them without undue delay, subject to specific grounds and limitations.

Under Article 17(1), the RTBF can be exercised in the following situations:

- The personal data is no longer necessary in relation to the purposes for which it was collected or processed.
- The data subject withdraws consent on which the processing is based.
- The data subject objects to the processing and there are no overriding legitimate grounds.
- The personal data has been unlawfully processed.
- The personal data has to be erased for compliance with a legal obligation.
- The data was collected in relation to the offer of information society services to a child.

However, Article 17(3) outlines exceptions where the RTBF does not apply, including when processing is necessary for exercising the right of freedom of expression and information, compliance with a legal obligation, the performance of a task in the public interest, public health purposes, archiving in the public interest, scientific or historical research, or for the establishment, exercise, or defense of legal claims.[3]

Philosophical and Legal Underpinnings

The RTBF sits at the intersection of various legal principles, including data protection, privacy, human dignity, and freedom of expression. In European jurisprudence, privacy is seen not merely as a negative right to be left alone but as a positive entitlement to develop one's personality without unwarranted interference. This

[2] Court of Justice of the European Union (CJEU), Case C-131/12, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González, ECLI:EU:C:2014:317.
[3] Kuner, C. (2017). The GDPR: Understanding the General Data Protection Regulation. Oxford University Press.

normative framework explains the robust emphasis on privacy in the EU and the recognition of RTBF as an extension of personal autonomy and informational self-determination.
This is contrasted with the approach in common law jurisdictions, especially in the United States, where freedom of expression is often prioritized over individual privacy. As a result, the RTBF has received considerable criticism and skepticism outside the EU, particularly concerning its impact on press freedom, public knowledge, and censorship.[4]

Digital Context and the Need for RTBF

In the digital era, information has become virtually indelible. Unlike the analog world, where the passage of time naturally leads to the obscurity of events, the internet preserves information indefinitely, making it accessible at any time and from anywhere. This digital permanence can have profound implications for individuals, especially when outdated or irrelevant personal data continues to define their online identities.
Instances abound where people have suffered reputational harm, professional setbacks, or personal distress due to lingering digital records. This includes old criminal records, financial disputes, personal controversies, or even unflattering news reports. The RTBF seeks to address these harms by offering a mechanism to recalibrate one's digital footprint.
Moreover, the emergence of powerful data analytics and profiling technologies has exacerbated privacy risks. Data once shared innocently can be aggregated, repurposed, or weaponized, often without the knowledge or consent of the individual concerned. The RTBF, in this context, empowers individuals to reclaim control over their data and mitigate unintended consequences.[5]

Global Debate and Normative Tensions

The RTBF has ignited a global debate on the appropriate limits of privacy in the digital age. Proponents argue that it is a necessary tool to protect human dignity, prevent online harassment, and enable second chances. They view it as a corrective mechanism in an era where personal data can be easily and permanently misused.
Critics, on the other hand, contend that the RTBF poses significant risks to freedom of speech and the right to information. They warn that it could lead to arbitrary censorship, revisionism, or the suppression of legitimate public interest material. This is particularly concerning when RTBF claims involve news media, political figures, or corporate accountability.
There is also a practical concern about the extraterritorial application of the RTBF. The CJEU, in its 2019 *Google v. CNIL* decision, held that while the RTBF applies within the EU, it does not necessarily extend globally. This highlights the challenges of reconciling divergent legal systems and cultural values in an interconnected world.[6]

Conclusion of the Evolutionary Overview

The evolution of the Right to Be Forgotten from a philosophical notion to a legally enforceable right under GDPR marks a significant development in the field of data protection. It reflects the European commitment to human dignity, privacy, and the ethical use of technology. However, its emergence also underscores the complexity of regulating digital environments, where multiple rights, jurisdictions, and technologies converge.
The RTBF is not a silver bullet but a dynamic legal tool that continues to evolve through judicial interpretation, regulatory guidance, and societal discourse. Its future will depend on how well it balances individual privacy with collective interests, and how it adapts to the ever-changing contours of the digital world.

[4] Mantelero, A. (2013). The EU Proposal for a General Data Protection Regulation and the Roots of the 'Right to be Forgotten'. Computer Law & Security Review, 29(3), 229–235. https://doi.org/10.1016/j.clsr.2013.03.010
[5] Rosen, J. (2012). The Right to Be Forgotten. Stanford Law Review Online, 64, 88–92.
[6] Ausloos, J. (2012). The 'Right to Be Forgotten' – Worth Remembering?. Computer Law & Security Review, 28(2), 143–152. https://doi.org/10.1016/j.clsr.2012.01.006

2. LEGAL FRAMEWORK AND SCOPE UNDER GDPR

The General Data Protection Regulation (GDPR), which came into force on May 25, 2018, revolutionized the data protection landscape in the European Union (EU) and beyond. Article 17 of the GDPR formally recognizes the Right to Be Forgotten (RTBF) under the title "Right to erasure ('right to be forgotten')." This section outlines the legal contours of this right, defining when it can be exercised, the obligations it imposes on data controllers and processors, and the exceptions where this right may be lawfully restricted.[7]

Legal Basis and Conditions for Erasure

The RTBF grants individuals the right to request the erasure of personal data concerning them under specific legal grounds. Article 17(1) enumerates six such grounds:

1. **Data no longer necessary**: If the data is no longer necessary in relation to the purposes for which it was originally collected or otherwise processed.
2. **Withdrawal of consent**: If the data subject withdraws consent, and there is no other legal ground for processing.
3. **Objection to processing**: If the data subject objects to processing under Article 21(1) and there are no overriding legitimate grounds, or under Article 21(2) concerning direct marketing.
4. **Unlawful processing**: If the personal data has been unlawfully processed.
5. **Legal obligation**: If the data must be erased to comply with a legal obligation in Union or Member State law.
6. **Children's data**: If the personal data was collected in relation to the offer of information society services to a child under Article 8.

Obligations of Data Controllers

When a valid erasure request is submitted, the data controller is obligated to act "without undue delay." This requires prompt action and communication with the data subject. Additionally, under Article 19, the controller must inform any third-party recipients about the erasure, unless this proves impossible or involves disproportionate effort.

A unique obligation arises under Article 17(2), which pertains to controllers who have made personal data public. They are required to take reasonable steps, including technical measures, to inform other controllers processing the data (e.g., search engines) of the erasure request.[8][9]

Exceptions to the Right to Erasure

Article 17(3) provides six key exceptions where the RTBF does not apply:

- **Freedom of expression and information**
- **Compliance with a legal obligation or performance of a task in the public interest**
- **Public health purposes**
- **Archiving in the public interest, or for scientific or historical research or statistical purposes**
- **Exercise or defense of legal claims**

These exceptions reflect the EU's intent to balance individual privacy with other fundamental rights and societal interests. Notably, the "freedom of expression and information" exception has become central to legal and academic debates, especially regarding journalism and media archives.

Interplay with Other Provisions of GDPR

The RTBF must be interpreted in conjunction with other GDPR provisions. For instance, Article 6 (lawfulness of processing) and Article 9 (processing of special categories of data) also influence the legitimacy of data

[7] Lynskey, O. (2015). The Foundations of EU Data Protection Law. Oxford University Press.
[8] Solove, D. J. (2013). Privacy Self-Management and the Consent Dilemma. Harvard Law Review, 126(7), 1880–1903.
[9] CJEU, Case C-507/17, Google LLC v Commission nationale de l'informatique et des libertés (CNIL), ECLI:EU:C:2019:772.

retention and deletion. Articles 12 and 13 ensure that data subjects are informed of their rights, and Article 15 empowers them with the right of access, which often precedes erasure requests.
Similarly, Recital 65 of the GDPR underlines the importance of allowing data subjects to have personal data erased when retention is unnecessary, with special reference to online data processing. Recital 66 highlights the additional obligation on controllers to inform downstream users about the erasure request.[10]

Procedural Mechanism
The GDPR establishes a clear procedure for exercising the RTBF. A data subject can initiate a request either in writing or electronically. Upon receipt, the controller must verify the identity of the requester, assess the validity of the request based on Article 17(1) and (3), and respond within one month, extendable by two months for complex cases.
Controllers may refuse the request based on lawful grounds under Article 17(3), but they must provide a reasoned justification. Data subjects dissatisfied with a controller's response may lodge complaints with supervisory authorities or pursue judicial remedies.

Enforcement and Penalties
Non-compliance with RTBF obligations can result in significant administrative fines. Under Article 83(5), infringements related to the rights of data subjects, including Article 17, can attract penalties of up to €20 million or 4% of the annual global turnover, whichever is higher. These stringent provisions highlight the EU's commitment to enforce data subject rights effectively.[11]

3. TENSION WITH COMPETING RIGHTS AND INTERESTS
The implementation of the Right to Be Forgotten under GDPR introduces a complex matrix of competing interests and rights. Chief among these are the tensions between individual privacy and the broader societal values of freedom of expression, access to information, and media freedom. This section examines these normative conflicts, analyzing how courts, regulators, and commentators have approached the delicate balancing act required.

Privacy vs. Freedom of Expression
Perhaps the most significant tension arises between the RTBF and the right to freedom of expression and information, as enshrined in Article 11 of the Charter of Fundamental Rights of the European Union. The GDPR acknowledges this by explicitly exempting certain data from erasure when it is processed "for exercising the right of freedom of expression and information."
However, the interpretation and application of this exemption remain contentious. Media organizations, historians, and public watchdogs often argue that erasing personal data, particularly from news archives or public databases, compromises journalistic integrity, public memory, and democratic accountability.[12]

The Google Spain and Google v. CNIL Cases
In the *Google Spain* case, the CJEU acknowledged that the RTBF must be balanced against the public's interest in accessing information. The court did not establish a categorical rule but emphasized contextual assessment, considering the nature of the information, its relevance to the public, and the role of the data subject (e.g., public figure vs. private individual).

[10] Tene, O., & Polonetsky, J. (2013). Big Data for All: Privacy and User Control in the Age of Analytics. Northwestern Journal of Technology and Intellectual Property, 11(5), 239–273.
[11] Information Commissioner's Office (ICO). (2021). Guide to the General Data Protection Regulation (GDPR). Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/
[12] Article 29 Data Protection Working Party. (2014). Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12. WP225.

This balancing approach was reaffirmed in *Google v. CNIL* (2019), where the CJEU ruled that the RTBF does not apply globally and must be restricted to EU member states. This decision reflects the court's recognition of divergent international views on privacy and speech and reinforces territorial limitations on RTBF enforcement.

Public Interest and News Archives

Journalistic archives pose a unique challenge for RTBF enforcement. Removing or delisting content related to past events may hinder investigative reporting, alter historical narratives, and obscure the public's understanding of political, social, or criminal events.

Courts and data protection authorities have adopted a cautious stance, often favoring retention of data in cases involving public figures or matters of legitimate public interest. The European Data Protection Board (EDPB) recommends assessing factors such as the age of the data, its accuracy, the data subject's role in public life, and the impact of continued availability.

Risk of Censorship and Revisionism

One of the primary criticisms of the RTBF is its potential to be misused for censorship or historical revisionism. Individuals may attempt to erase unfavorable truths under the guise of privacy, thereby manipulating digital memory and evading accountability.

This risk is particularly acute in politically sensitive contexts, where erasure requests could serve as tools for image control or narrative manipulation. Transparency, proportionality, and rigorous scrutiny are essential safeguards against such misuse.[13]

Data Controllers as Arbiters of Speech

A practical concern is the growing role of private tech companies, especially search engines, in adjudicating RTBF claims. Companies like Google receive thousands of removal requests annually and must decide whether to delist content based on privacy-public interest assessments. This privatized form of censorship has raised alarms about due process, transparency, and the consistency of decision-making.

Efforts have been made to introduce oversight mechanisms, such as internal ethics committees and external advisory boards. Still, the delegation of such crucial decisions to corporate actors remains a fundamental concern.[14]

The Need for Clearer Standards

Given the complexities involved, there is a pressing need for clearer legal standards and consistent criteria for balancing rights. Judicial precedents offer some guidance, but more comprehensive regulatory frameworks and international cooperation are required to harmonize practices and avoid legal fragmentation.

4. PRACTICAL AND TECHNOLOGICAL CHALLENGES IN IMPLEMENTATION

The enforcement of the Right to Be Forgotten (RTBF) in practice presents a host of logistical, technical, and operational challenges. Although the legal framework under the GDPR is well-defined, translating these rules into effective action is often a daunting task, especially for data controllers and processors operating across complex digital ecosystems.

Jurisdictional Complexity and Cross-border Enforcement

One of the foremost practical issues is the cross-border nature of the internet. While the GDPR is applicable within the European Union, websites and online platforms often operate globally. As a result, enforcing an

[13] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), Official Journal of the European Union, L 119, 4.5.2016.

[14] Court of Justice of the European Union (CJEU), Case C-131/12, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González, ECLI:EU:C:2014:317.

erasure order across jurisdictions is not straightforward. The CJEU, in *Google v. CNIL*, clarified that global delisting is not mandatory under the GDPR, limiting enforcement to EU member states.
However, this poses a risk of forum shopping and digital reappearance of the same information through non-EU domains. For instance, a delisted article on "google.fr" might still appear on "google.com" or other regional domains. Such fragmentation undermines the efficacy of the RTBF and creates regulatory blind spots.[15]

Technical Limitations and Incomplete Erasure
Even when erasure requests are granted, the complete removal of data is not always feasible. Cached pages, backups, screenshots, and mirrored content may continue to exist on third-party servers or archival platforms. Moreover, in decentralized systems like blockchain, data is designed to be immutable and permanent, making erasure virtually impossible.
The practical question becomes: what does deletion really mean in a digital context? Removing a hyperlink from a search engine index does not equate to deletion from the original source. Therefore, the RTBF often results in de-indexing rather than actual data erasure.[16]

Identification and Verification of Data Subjects
Verifying the identity of individuals requesting erasure is critical to prevent fraudulent or malicious claims. However, this often involves collecting additional personal information, creating a paradox where data minimization is challenged by verification requirements.
Organizations must strike a balance between adequately authenticating users and not collecting excessive data. Failure to do so can result in identity theft, denial-of-service risks, or non-compliance with GDPR's principles of necessity and proportionality.

Volume of Requests and Resource Allocation
Tech companies and large data controllers receive thousands of RTBF requests, straining their operational capacity. Evaluating each request demands legal, contextual, and often subjective analysis. Determining whether information is outdated, irrelevant, or in the public interest requires nuanced judgment.
To manage the volume, many companies have set up automated systems for preliminary sorting, followed by manual review by legal teams. Still, the workload can be overwhelming and lead to inconsistent outcomes or unjustified refusals.[17]

Cost Implications and SME Challenges
Implementing RTBF mechanisms also carries financial implications, particularly for small and medium enterprises (SMEs). Unlike tech giants, SMEs may lack the infrastructure, legal expertise, or dedicated staff to handle erasure requests. This creates an uneven playing field and raises concerns about access to rights.
The European Commission has acknowledged this disparity and continues to support awareness programs and GDPR toolkits to assist smaller organizations in compliance efforts.[18]

Balancing RTBF with Cybersecurity and Audit Requirements
Erasing data may conflict with obligations to retain records for cybersecurity, fraud detection, or audit trails. Organizations often face difficult decisions about reconciling RTBF requests with regulatory or contractual obligations requiring data retention.

[15] Kuner, C. (2017). The GDPR: Understanding the General Data Protection Regulation. Oxford University Press.
[16] Mantelero, A. (2013). The EU Proposal for a General Data Protection Regulation and the Roots of the 'Right to be Forgotten'. Computer Law & Security Review, 29(3), 229–235. https://doi.org/10.1016/j.clsr.2013.03.010
[17] Rosen, J. (2012). The Right to Be Forgotten. Stanford Law Review Online, 64, 88–92.
[18] Ambrose, Meg Leta & Ausloos, Jef. (2013). The Right to Be Forgotten Across the Pond. Journal of Information Policy, 3, 1–23.

For example, financial institutions may need to keep transaction records for a statutory period, even if an individual requests erasure. In such cases, legal grounds for continued processing under Article 17(3) must be clearly documented and communicated.

5. COMPARATIVE JURISPRUDENCE AND GLOBAL PERSPECTIVES

The Right to Be Forgotten, though prominently developed within the EU legal framework, has found resonance—albeit with variation—across other jurisdictions. This section explores how different countries have interpreted or responded to the concept of RTBF and highlights comparative jurisprudence to illustrate broader global trends and tensions.[19]

United States: Free Speech First

In the United States, the RTBF faces significant legal and cultural resistance. The First Amendment's strong protection of freedom of speech often outweighs privacy concerns. Courts in the U.S. have generally been reluctant to endorse broad erasure rights, viewing them as a potential threat to press freedom and public discourse.

Although some privacy rights are recognized under statutes like the California Consumer Privacy Act (CCPA), these do not provide a full-fledged RTBF equivalent. CCPA's "right to delete" is limited and subject to various business-related exceptions. Moreover, the notion of delisting from search engines has not gained legal traction in the U.S.

India: Emerging Recognition

India has seen growing judicial and legislative interest in the RTBF, especially following the Supreme Court's landmark ruling in *Justice K.S. Puttaswamy v. Union of India* (2017), which recognized privacy as a fundamental right under Article 21 of the Constitution.

Several High Courts have addressed RTBF claims in contexts such as matrimonial disputes, criminal acquittals, and employment cases. However, decisions have been inconsistent due to the absence of a comprehensive data protection law. The proposed Digital Personal Data Protection Act, 2023 seeks to include provisions akin to RTBF, but its implementation and interpretation remain to be seen.

Canada and Latin America

In Canada, privacy is constitutionally protected under Section 7 of the Charter of Rights and Freedoms, and statutory protections exist under PIPEDA. However, there is no explicit RTBF. The Office of the Privacy Commissioner has supported greater control over personal information but emphasized the need for public consultations and careful balance with free expression.

In Latin America, countries like Brazil and Argentina have taken steps to align with GDPR through their data protection laws (e.g., Brazil's LGPD). Although RTBF is not always explicitly stated, principles of data minimization and rectification allow for similar functionality.[20]

Asia-Pacific Region

Japan, South Korea, and Singapore have also enacted robust privacy laws, though RTBF adoption is limited. In Japan, courts have occasionally ordered delisting in cases involving reputational harm, but these are judged on a strict balancing test. South Korea's PIPA provides deletion rights, but again within specific limits.

[19] González Fuster, Gloria. (2014). The Emergence of Personal Data Protection as a Fundamental Right of the EU. Springer.
[20] Custers, Bart. (2016). The Power of Knowledge: Ethical, Legal, and Technological Aspects of Data Mining and Group Profiling in Epidemiology. Springer.

Role of International Organizations

Bodies like the United Nations, OECD, and Council of Europe have endorsed the principle of data sovereignty and individual control, indirectly supporting RTBF concepts. However, global consensus remains elusive due to divergent legal systems and cultural values.

6. CONCLUSION AND RECOMMENDATIONS

The Right to Be Forgotten under the GDPR represents a landmark advancement in the protection of personal data and digital privacy. From its judicial recognition in *Google Spain* to its codification in Article 17, RTBF has reshaped the way individuals interact with and control their digital identities.

However, the journey from principle to practice reveals a complex terrain marked by competing rights, technological limitations, and legal fragmentation. While RTBF empowers individuals to reclaim agency over their data, it also raises critical questions about public interest, transparency, and free speech.

To ensure a balanced and effective implementation of RTBF, several steps are recommended:

- **Clearer Guidelines**: Regulatory bodies like the EDPB should issue detailed guidelines on balancing privacy with public interest, especially in cases involving media archives and public figures.
- **Standardized Procedures**: Harmonizing the verification, review, and appeal mechanisms across the EU can reduce inconsistencies and enhance procedural fairness.
- **International Cooperation**: Dialogue among jurisdictions is vital to resolve conflicts in transnational data flows and promote mutual recognition of privacy rights.
- **Technological Innovation**: Development of privacy-enhancing technologies (PETs) and AI-assisted de-indexing tools can improve the feasibility of implementing RTBF without excessive human intervention.
- **Support for SMEs**: Financial and technical support to smaller data controllers can help democratize compliance and reduce the burden of implementation.

In conclusion, the RTBF is a dynamic and evolving right that captures the challenges of privacy in the information age. Its continued relevance will depend on how societies navigate the tensions it generates and how legal systems adapt to uphold both individual dignity and democratic transparency.

Here are the references generated for your research paper **"The Right to Be Forgotten under GDPR: Legal Scope and Practical Challenges"**. These are a mix of primary sources, academic commentary, and relevant case law:

REFERENCES:

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), Official Journal of the European Union, L 119, 4.5.2016.
2. Court of Justice of the European Union (CJEU), Case C-131/12, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, ECLI:EU:C:2014:317.
3. Kuner, C. (2017). *The GDPR: Understanding the General Data Protection Regulation*. Oxford University Press.
4. Mantelero, A. (2013). The EU Proposal for a General Data Protection Regulation and the Roots of the 'Right to be Forgotten'. *Computer Law & Security Review*, 29(3), 229–235. https://doi.org/10.1016/j.clsr.2013.03.010
5. Rosen, J. (2012). The Right to Be Forgotten. *Stanford Law Review Online*, 64, 88–92.
6. Ausloos, J. (2012). The 'Right to Be Forgotten' – Worth Remembering?. *Computer Law & Security Review*, 28(2), 143–152. https://doi.org/10.1016/j.clsr.2012.01.006
7. Lynskey, O. (2015). *The Foundations of EU Data Protection Law*. Oxford University Press.
8. Solove, D. J. (2013). Privacy Self-Management and the Consent Dilemma. *Harvard Law Review*, 126(7), 1880–1903.
9. CJEU, Case C-507/17, *Google LLC v Commission nationale de l'informatique et des libertés (CNIL)*, ECLI:EU:C:2019:772.

10. Tene, O., & Polonetsky, J. (2013). Big Data for All: Privacy and User Control in the Age of Analytics. *Northwestern Journal of Technology and Intellectual Property*, 11(5), 239–273.
11. Information Commissioner's Office (ICO). (2021). *Guide to the General Data Protection Regulation (GDPR)*. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/
12. Article 29 Data Protection Working Party. (2014). *Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12*. WP225.