YourLawArticle

Open Access Law Journal, ISSN (O): 3049-005

Editor-in-Chief – Prof. (Dr.) Amit Kashyap; Publisher Reet Parihar

Analysis of the Right to Be Forgotten on Social Media Platforms: Facebook and Twitter

Meghana Laxman Hadawale, L.L.M, Chhatrapati Shivaji Maharaj University, Panvel, Navi Mumbai

&

Dr Piyush Maheshwari, Associate Professor, Department of Law, Chhatrapati Shivaji Maharaj University, Panvel, Navi Mumbai

Published on: 3nd June 2025

Abstract

The Right to Be Forgotten (RTBF) has emerged as a crucial legal and ethical principle in the age of digital permanence, offering individuals the right to request the erasure of personal data that is outdated, irrelevant, or damaging. This paper critically analyses the application of RTBF on social media platforms such as Facebook and Twitter, where content dissemination is rapid, decentralized, and global. It examines the conceptual evolution of RTBF, anchored in the landmark Google Spain *case and codified under Article 17 of the EU's General Data Protection Regulation (GDPR), while exploring its developing status in India under the Digital Personal Data Protection Act, 2023. The paper further explores challenges posed by AI-generated deepfakes, immutable blockchain systems, and the absence of global legal harmonization. Through case studies, comparative analysis, and platform-specific practices, the study highlights the balance required between individual privacy and freedom of expression. It concludes with practical recommendations for legislators, platforms, and users, emphasizing the need for technological innovation and international cooperation to make RTBF effective in the evolving digital ecosystem.*

Keywords: *Right to Be Forgotten, Digital Privacy, Social Media, GDPR, Deepfakes*

Introduction

The digital revolution has transformed how personal data is stored, shared, and remembered. Social media platforms such as Facebook and Twitter serve as hubs of self-expression, activism, and social interaction, but they also retain vast amounts of user-generated content, some of which may no longer reflect current identities or contexts. The **Right to Be Forgotten (RTBF)** has emerged as a legal mechanism allowing individuals to request the erasure of personal data that is outdated, irrelevant, or no longer necessary, thus restoring autonomy over one's digital footprint. However, its application to social media remains complex and contested due to competing interests in privacy, public interest, and freedom of expression.

Concept and Evolution of the Right to Be Forgotten

The RTBF originates from the broader right to privacy and is defined as the ability of individuals to request that certain data about them be erased from digital records when it is no longer necessary, lawful, or consented to. The landmark judgment by the **European Court of Justice (ECJ)** in *Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* recognized this right, compelling search engines to delist links to outdated or irrelevant personal data where no overriding public interest existed .[1]

This ruling became the cornerstone for **Article 17** of the **General Data Protection Regulation (GDPR)** of the European Union, which codified the RTBF and laid down its applicability to data controllers across all sectors, including social media platforms .

Legal Framework and Global Comparisons

European Union

Under **Article 17 of the GDPR**, individuals can request erasure of personal data in cases including: lack of necessity, consent withdrawal, unlawful processing, or legal obligation.

[1] *Google Spain SL v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (C-131/12) [2014] ECR I-317.

However, this right is **not absolute** and is balanced against **freedom of expression**, **legal compliance**, and **public interest** .[2]

India

While the **Indian Constitution** does not explicitly mention the RTBF, the **Supreme Court in Justice K.S. Puttaswamy v Union of India**[3] recognized the **right to privacy** as a **fundamental right** under Article 21 . The **Digital Personal Data Protection Act, 2023 (DPDPA)** contains clauses allowing data principals to request data erasure, forming the backbone of an emergent RTBF regime. Courts in India have addressed the RTBF in a **case-by-case** manner. For example, in *Jorawar Singh Mundy v Union of India*[4], the Delhi High Court allowed the removal of online judgments from public domains to protect an acquitted individual's reputation .

United States

The **US legal framework** does not recognise the RTBF. The **First Amendment**, protecting free speech, often trumps privacy concerns. However, limited data deletion rights exist under the **California Consumer Privacy Act (CCPA)** and **Children's Online Privacy Protection Act (COPPA)** .[5]

Other Jurisdictions

- **Russia** and **Turkey** have adopted limited RTBF-like provisions.
- **Canada** and **South Korea** are exploring legislation that echoes RTBF principles, particularly in the context of consent-based erasure.

Application on Social Media Platforms

Social media platforms such as Meta (Facebook, Instagram) and X (formerly Twitter) are not mere passive conduits of user-generated content; they act as data controllers and processors under data protection laws, especially within jurisdictions governed by the General Data Protection Regulation (GDPR). As data controllers, they determine the purposes and means of

[2] Regulation (EU) 2016/679 (General Data Protection Regulation) art 17.
[3] *Justice K.S. Puttaswamy (Retd.) and Anr. v Union of India* (2017) 10 SCC 1.
[4] Jorawar Singh Mundy v Union of India 2021 SCC OnLine Del 2306.

[5] California Consumer Privacy Act 2018; Children's Online Privacy Protection Act 1998.

processing personal data, while as processors, they execute these functions on behalf of the user and other stakeholders. This dual role places significant legal responsibility on such platforms to facilitate, process, and respond to RTBF requests.

User-Initiated Deletion

One of the most immediate and accessible mechanisms for data removal is the ability of users to delete content they have personally uploaded, such as status updates, tweets, images, or videos. However, this mechanism is technically limited in scope:

- Shared Content: When a user deletes their own post, the original content is removed from their profile, but any shares, reposts, or quoted content may continue to exist on other profiles.
- Third-party Archives: In some cases, deleted content may already be captured via screenshots or archived by third-party services (e.g., the Internet Archive), rendering true erasure ineffective.
- Residual Metadata: Even when content is removed, metadata (e.g., timestamps, locations, or interactions) may persist in backend systems, log files, or data lakes.

Thus, user-initiated deletion offers limited protection, especially in cases involving viral or defamatory content that has rapidly spread across the digital ecosystem.[6]

Platform-Assisted Requests

To address the limitations of self-deletion, platforms provide formal content removal pathways:

- These typically involve reporting tools embedded within the interface, where users can flag content as abusive, harassing, private, misleading, or infringing.
- In the context of RTBF, platforms are expected to remove content that is inaccurate, outdated, or damaging, particularly when it has been posted without consent or has no legitimate public interest value.

[6] Mike Hydes, 'Right to Be Forgotten: Empowering Privacy in the Digital Age' (LinkedIn, 2023) https://www.linkedin.com/pulse/right-forgotten-empowering-privacy-digital-age-mike-hydes-3zvie accessed 30 May 2025.

- Many platforms also allow third parties (e.g., parents of minors or legal representatives) to submit requests for removal on behalf of users, especially in cases involving non-consensual pornography, revenge porn, or cyberbullying.

However, these takedown mechanisms often lack transparency and consistency, with decisions being taken algorithmically or without clear appeal procedures. Moreover, content moderation standards differ across platforms, leading to inconsistent enforcement.[7]

Legal and Regulatory Enforcement

Under Article 17 of the GDPR, data controllers must comply with erasure requests where:

- The personal data is no longer necessary,
- The individual withdraws consent,
- The processing is unlawful,
- Or the data subject objects to the processing and there are no overriding legitimate grounds.

In this context, social media platforms must respond to legitimate RTBF requests within one month, with a possible extension to two months for complex cases. Failure to comply can result in severe administrative fines:

For example, in 2023, Meta Platforms Ireland was fined €1.2 billion by the Irish Data Protection Commission for failing to ensure adequate safeguards for the data transfers of European users to the US, which indirectly touched upon data minimisation and retention concerns relevant to the RTBF framework. Furthermore, platforms are obligated to notify third-party controllers who have access to the data, ensuring complete ecosystem-wide erasure, where feasible. This "notification obligation" creates a cascading responsibility for data deletion across multiple systems and services, which can be both technically and administratively burdensome.[8]

[7] Peter K Yu, 'The Right to Be Forgotten Across the World' (2019) 1(1) International Review of Law, Computers & Technology 1.
[8] United Nations General Assembly, 'Right to Privacy in the Digital Age' A/RES/73/179 (17 December 2018).

Challenges in RTBF Enforcement on Social Media

1. Global Disparity in Compliance: Platforms often operate globally, but RTBF enforcement is jurisdiction-specific. What must be deleted under the GDPR in the EU may remain publicly accessible in jurisdictions like the US, where freedom of speech is prioritised.
2. Automated Moderation vs. Human Oversight: The sheer volume of content means that platforms rely heavily on AI-based moderation tools. These systems may fail to understand context, satire, or cultural nuances, leading to both over-removal and under-removal of content.
3. Appeal and Accountability: The lack of standardized appeals mechanisms across platforms undermines due process and procedural fairness, especially when legitimate requests are denied or ignored.

Importance and Societal Impact

The Right to Be Forgotten (RTBF) plays a vital role in upholding the moral and ethical fabric of a digitally interconnected society. In an age where information is instantly searchable and indefinitely archived, digital permanence can cause irreversible harm to individuals' reputations and mental well-being. The RTBF seeks to restore balance between the public's right to know and the individual's right to be forgotten, particularly when content is outdated, irrelevant, or unnecessarily harmful. Its significance extends beyond legal boundaries, offering societal redress to those unfairly judged or perpetually haunted by their past.[9]

One of the most powerful justifications for the RTBF is its potential to combat digital stigma. In many instances, individuals who were wrongfully accused, acquitted, or involved in minor past infractions continue to suffer reputational harm long after their legal or social consequences have ended. Search engine results and old social media content often resurface during employment background checks, academic admissions, or even personal relationships, perpetuating a cycle of judgment and exclusion. By enabling individuals to request the removal of outdated or irrelevant content, the RTBF serves as a mechanism of dignity restoration, ensuring that people are not indefinitely punished for past actions that are no longer reflective of who they are.

[9] Lawrence Lessig, *Code and Other Laws of Cyberspace* (Basic Books 1999).

Furthermore, the RTBF significantly aids in the rehabilitation and reintegration of individuals into society. For example, former convicts who have served their sentence and are seeking to rebuild their lives often face insurmountable barriers due to persistent digital records of their criminal past. Even whistleblowers, who act in public interest, may suffer professional and social retaliation long after the matter has been resolved. In such cases, the RTBF allows these individuals to transition into a new phase of life without being endlessly burdened by information that serves no continuing public purpose. This aligns with the broader principles of restorative justice, which emphasize healing, reintegration, and second chances over perpetual punishment.[10]

Additionally, the psychological toll of being digitally exposed or shamed cannot be underestimated. Online harassment, revenge porn, cyberbullying, and defamatory content can leave lasting scars on an individual's mental health. Victims may experience anxiety, depression, social withdrawal, and a diminished sense of self-worth. The RTBF provides a legal remedy through which such individuals can seek the removal of harmful content, allowing them a pathway to mental and emotional recovery. It validates the emotional suffering caused by digital violations and reaffirms the individual's right to control their narrative. In doing so, it also contributes to a more compassionate and accountable online ecosystem.

In summary, the RTBF is not just a legal doctrine, it is a moral imperative and social safeguard. It embodies the evolving understanding that human identity is dynamic and that people deserve the right to evolve without being shackled by permanent digital judgments. By reducing stigma, supporting rehabilitation, and protecting mental health, the RTBF fosters a society that values privacy, redemption, and digital dignity.[11]

Criticisms and Controversies

Despite its utility, RTBF is not without criticism.

- **Censorship Allegations**: Critics claim that RTBF could be misused to rewrite history or suppress truths, especially by public figures or corporations.

[10] Eleni Kosta, 'Taking the European "Right to Be Forgotten" to the Next Level' (2017) 19(2) *Vanderbilt Journal of Entertainment & Technology Law* 233.
[11] Julie E Cohen, Configuring the Networked Self: Law, Code, and the Play of Everyday Practice (Yale University Press 2012).

- **Technical Impracticalities**: Decentralised content, screenshots, data mirrors, and third-party archives can make total erasure nearly impossible.
- **Jurisdictional Disparities**: What qualifies as removable in the EU may not be in the US, making global enforcement incoherent.

Case Studies and Precedents

- **Google Spain Case (2014)**: Set a global precedent for search engine de-indexing.
- **Jorawar Singh Mundy (India)**: Highlighted the tension between open court principles and individual privacy.
- **Facebook's Oversight Board Decisions**: Reflect the growing trend of platform-driven quasi-judicial RTBF decisions, especially concerning misinformation and political content.

7. The Future of RTBF

AI and Deepfakes

The emergence of generative artificial intelligence (AI) and deepfake technology poses one of the most pressing challenges to the effective enforcement of the Right to Be Forgotten. Synthetic media in which a person's likeness is replaced or manipulated using AI can be indistinguishable from authentic content. When such content is maliciously used for purposes like defamation, revenge porn, or misinformation, it significantly infringes on an individual's right to privacy, autonomy, and reputation. What makes these tools especially problematic is their anonymity and speed. Deepfakes can be created and circulated globally within minutes, leaving little room for timely response or damage control. From an RTBF perspective, the issues are twofold: identification and removal. First, it is often difficult to establish authorship or hold creators accountable due to anonymous posting and AI-generated proxies. Second, even when the harmful content is identified, its viral nature and multi-platform proliferation make comprehensive erasure nearly impossible. This necessitates the development of new legal tools and technological partnerships between governments, platforms, and AI developers to identify and flag AI-generated content and to enforce takedowns effectively. The traditional RTBF

framework must evolve to include automated detection and proactive moderation mechanisms to counteract these new-age violations of digital dignity.[12]

Blockchain Dilemmas

Blockchain's immutable ledger poses a direct challenge to data deletion rights. "Right to Erasure" is technically impossible in systems built on permanence. Once data is recorded on a blockchain, it is replicated across nodes in a decentralized network, and cannot be altered or deleted without undermining the entire system's integrity. This immutability is particularly problematic when personal data, such as transaction histories, personal identifiers, or smart contract metadata, is stored on-chain. Unlike centralized databases where data can be edited or deleted by an administrator, blockchain's decentralized consensus mechanism lacks a single point of control. Efforts to introduce RTBF into blockchain systems have included storing only encrypted references on-chain while keeping actual personal data off-chain. However, even this does not fully eliminate the risk of traceability and re-identification. Therefore, legal scholars and technologists are now calling for "privacy by design" frameworks in blockchain development, incorporating concepts like zero-knowledge proofs and privacy-preserving protocols that can mitigate conflicts between blockchain permanence and personal data erasure. Still, the fundamental incompatibility between RTBF and blockchain remains an unresolved tension in privacy jurisprudence.[13]

Global Standardization: The Push for Harmonized Digital Rights

One of the most critical challenges to enforcing the RTBF is the lack of uniform global standards. While the European Union, through the General Data Protection Regulation (GDPR), has robustly enshrined the RTBF, other jurisdictions like the United States, China, or many countries in the Global South either lack similar laws or prioritise different values, such as freedom of expression or state surveillance. This fragmentation creates confusion not only for individuals but also for multinational platforms, which must navigate a complex web of conflicting legal obligations. For instance, a social media post that must be delisted under EU law may still be accessible from US servers, where the First Amendment guarantees broad speech protections. Recognising these inconsistencies, international organisations such as the

[12] United Nations General Assembly, 'Right to Privacy in the Digital Age' A/RES/73/179 (17 December 2018).
[13] Daskal J, 'Borders and Bits: The Right to Be Forgotten in a Global Context' (2018) 49(1) *Vanderbilt Journal of Transnational Law* 1.

United Nations, OECD, and Internet Governance Forum (IGF) have begun advocating for harmonised data protection principles, including the right to erasure. The OECD Privacy Guidelines emphasise interoperability, while UN bodies have underscored the need for cross-border enforcement mechanisms to ensure that privacy rights are protected in a globally connected environment. A globally recognized RTBF regime would not only enhance legal certainty but also empower users worldwide to assert control over their digital identities, regardless of national boundaries. However, achieving this will require intense diplomatic cooperation, legal convergence, and perhaps most importantly, universal recognition of privacy as a fundamental human right.[14]

8. Recommendations

For Legislators

- Codify RTBF with clear definitions, processes, and exceptions.
- Build independent oversight bodies to resolve RTBF disputes.

For Social Media Platforms

- Incorporate privacy by design mechanisms.
- Increase algorithmic transparency in content de-indexing decisions**.**

For Users

- Educate oneself on privacy settings.
- Use content removal tools responsibly to uphold the balance between privacy and public interest.

Conclusion

The RTBF represents a significant evolution in digital rights, recognising the human need to forget and be forgotten. As social media grows omnipresent and invasive, the right provides a means to escape digital permanence. However, it must be carefully balanced with free expression, technical limitations, and global coherence. In the coming decade, RTBF will define the boundaries between memory and forgetting, privacy and expression, and technology and autonomy.

[14] European Parliamentary Research Service, 'The Right to Be Forgotten: European Implementation Assessment' (PE 615.660, 2017).

References

Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González (Case C-131/12) [2014] ECR I-317.

Regulation (EU) 2016/679 (General Data Protection Regulation), art 17.

Justice K S Puttaswamy (Retd) v Union of India (2017) 10 SCC 1.

Digital Personal Data Protection Act 2023 (India).

Jorawar Singh Mundy v Union of India 2021 SCC OnLine Del 2306.

California Consumer Privacy Act 2018 (CCPA), Cal. Civ. Code §1798.100 et seq.

Children's Online Privacy Protection Act 1998 (COPPA), 15 U.S.C. §§ 6501–6506.

Peter K Yu, 'The Right to Be Forgotten Across the World' (2019) 1(1) *International Review of Law, Computers & Technology* 1.

European Data Protection Board, 'Guidelines 5/2019 on the criteria of the Right to be Forgotten in search engines' (Adopted 7 July 2020).

Information Commissioner's Office (UK), 'Right to erasure' https://ico.org.uk accessed 2 June 2025.

Irish Data Protection Commission, 'Meta Platforms Ireland Limited – Final Decision' (May 2023).

Solove DJ, 'The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure' (2003) 53(3) *Duke Law Journal* 967.

OECD, 'Recommendation of the Council on Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data' (2013).

United Nations General Assembly, 'Right to Privacy in the Digital Age' A/RES/73/179 (17 December 2018).

Lawrence Lessig, *Code and Other Laws of Cyberspace* (Basic Books 1999).

Woodrow Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* (Harvard University Press 2018).

Eleni Kosta, 'Taking the European "Right to Be Forgotten" to the Next Level' (2017) 19(2) *Vanderbilt Journal of Entertainment & Technology Law* 233.

Julie E Cohen, *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice* (Yale University Press 2012).

European Parliamentary Research Service, 'The Right to Be Forgotten: European Implementation Assessment' (PE 615.660, 2017).

Daskal J, 'Borders and Bits: The Right to Be Forgotten in a Global Context' (2018) 49(1) *Vanderbilt Journal of Transnational Law* 1.