ERASING DIGITAL SHADOWS: RECONCILING PRIVACY AND PRESS FREEDOM THROUGH THE RIGHT TO BE FORGOTTEN IN INDIA

Christi Anna George, Research Scholar, Department of Law, Banaras Hindu University

ABSTRACT

This paper examines the nascent yet critical intersection of the right to be forgotten (RTBF) and the constitutionally protected freedom of the press within India's evolving digital landscape. This paper analyses the inherent tension between an individual's right to privacy, as articulated through the RTBF, and the journalistic imperative to inform the public. While acknowledging the RTBF's grounding in principles of human dignity and the need to control one's digital narrative, particularly concerning outdated or irrelevant personal information, the paper recognizes the potential chilling effect on journalistic freedom posed by unfettered RTBF implementation.

Drawing comparative insights from the European Union's GDPR-driven approach to the RTBF and the contrasting system of sealed court records in the United States, this paper explores the jurisprudential development of the RTBF in India, tracing its trajectory through key judicial pronouncements.

The central argument posits that a balanced approach is essential, one that acknowledges the legitimate privacy concerns underlying RTBF requests while safeguarding the essential function of a free press as a watchdog of public interest. Specifically, the paper advocates for the establishment of a self-regulatory framework within journalistic organizations, grounded in ethical principles and best practices, to adjudicate RTBF requests on a case-by-case basis. This framework should incorporate a nuanced assessment of the enduring public interest value of specific information against the potential for disproportionate and unwarranted harm to individuals.

By analyzing the delicate equilibrium between privacy rights and press freedom, this paper seeks to contribute to the ongoing legal and policy discourse surrounding the RTBF in India, proposing a pragmatic and principled framework that respects both individual autonomy and the indispensable role of a free and robust press in a democratic society.

Keywords: Right to be forgotten, press freedom, privacy, journalistic ethics, GDPR.

INTRODUCTION

The digital revolution has fundamentally reshaped the way information is created, disseminated, and accessed, ushering in an era of unprecedented connectivity and knowledge sharing. However, this transformative shift has also presented novel and complex challenges to individual privacy. One particularly pertinent issue arises from the enduring nature of online content, where digital footprints, once easily accessible, can persist indefinitely, casting a long shadow over an individual's present and future. This permanence of digital information has brought to the forefront the concept of the "right to be forgotten" (RTBF), a legal and ethical principle that seeks to empower individuals to control their online narrative by enabling the removal of outdated, irrelevant, or inaccurate personal information from the internet.

The RTBF, rooted in the fundamental right to privacy, acknowledges the inherent human dignity and autonomy of individuals to shape their own identities and reputations. It recognizes that past actions, mistakes, or even victimhood, once publicly available online, can have lasting and often detrimental consequences, hindering personal growth, professional opportunities, and social reintegration. The RTBF aims to provide a mechanism for individuals to reclaim control over their digital presence, allowing them to move forward without being perpetually defined by past events. This concept, however, intersects with and potentially conflicts with other fundamental rights, most notably freedom of expression and the freedom of the press. The tension between an individual's right to privacy and the public's right to information forms the crux of the ongoing debate surrounding the RTBF.

This paper delves into the multifaceted dimensions of the RTBF, exploring its evolution, implementation, and implications, particularly within the distinct legal frameworks of India and the European Union. The EU has been a pioneer in recognizing and implementing the RTBF, most notably through the General Data Protection Regulation (GDPR), which grants individuals specific rights regarding the processing and erasure of their personal data. The GDPR has served as a catalyst for discussions and legislative developments regarding the RTBF globally, including in India. This paper examines the jurisprudential underpinnings of the RTBF, tracing its development in the EU, where it has achieved significant legal recognition and practical application, and comparing this with its nascent yet evolving presence in India.

In India, the RTBF has emerged through a combination of judicial pronouncements and

legislative initiatives. While not explicitly enshrined in the Indian Constitution, the right to privacy has been recognized as an intrinsic part of Article 21, which guarantees the right to life and personal liberty. The judiciary has played a crucial role in shaping the understanding and application of the RTBF in India, with landmark judgments highlighting the importance of protecting individual privacy in the digital age. Furthermore, legislative efforts, such as the Personal Data Protection Bill, 2019[1] (although subsequently withdrawn and replaced by the Digital Personal Data Protection Act, 2023), have sought to provide a legal framework for the RTBF, although the specifics of its implementation and enforcement remain a subject of ongoing debate. This paper analyzes the similarities and differences in the RTBF's interpretation and application in these two jurisdictions, aiming to illuminate the diverse legal and philosophical approaches to balancing individual privacy with the public's right to information.

Beyond the EU and India, the United States offers a different approach to managing potentially harmful online information through the practice of "sealing court records." This mechanism allows for the restriction of access to certain court documents, often in cases involving minors, rehabilitation, or sensitive personal information. While distinct from the RTBF, the concept of sealing court records shares a common goal of protecting individuals from the potentially damaging consequences of publicly available information.

This paper explores the US system as a comparative lens, contrasting it with the RTBF as implemented in the EU and proposed in India. By examining these different approaches, the paper seeks to identify best practices and potential pitfalls in the design and implementation of legal frameworks for managing online information.

Ultimately, this analysis seeks to provide a comprehensive understanding of the RTBF, its challenges, and its potential impact on the future of digital privacy in a globalized world. As technology continues to advance and the volume of online information grows exponentially, the need for robust legal frameworks to govern digital privacy becomes increasingly urgent. This paper aims to contribute to the ongoing legal and policy discourse surrounding the RTBF, exploring the delicate balance between individual autonomy and the public interest, and proposing a framework for navigating the complex interplay between privacy, freedom of

[1] The Personal Data Protection Bill, 2019, Bill No. 373 of 2019, PRS Legislative Research, https://prsindia.org/billtrack/the-personal-data-protection-bill-2019 (last visited Feb. 9, 2025).

expression, and the enduring nature of digital information.

THE RIGHT TO BE FORGOTTEN

The "right to be forgotten" allows individuals to have specific online data deleted, making it untraceable by third parties.[2] It's the right to keep quiet about past events, whether they happened or not. Essentially, it enables individuals to remove information like photos or videos about themselves from online records, preventing search engines from displaying them. Before 2011, there was limited recourse for harms stemming from incidents like revenge porn or the sharing of compromising images. The right to be forgotten differs from the right to privacy: privacy protects information that is *not* publicly known, while the right to be forgotten concerns deleting information that *was* public at some point, restricting future access. The terms Right to Be Forgotten and Right to Forget are often used interchangeably, but they have distinct meanings. The Right to Forget pertains to the notion that a historical event should no longer be revived or recalled due to the passage of a significant amount of time. In contrast, the Right to Be Forgotten refers to an individual's request for the removal of specific personal data or information, preventing third parties from accessing or tracing it.

EVOLUTION OF THE RIGHT TO BE FORGOTTEN

In 1998*, Spaniard Mario Costeja González* faced financial difficulties and was forced to auction his property, placing an advertisement in a newspaper that later became available online. Even after resolving his financial troubles, search engines continued to display this outdated information, leading to reputational harm. Seeking redress, González took legal action, which ultimately resulted in the recognition of the Right to Be Forgotten.

The European Court of Justice (ECJ) ruled against Google, affirming that under certain conditions, individuals in the European Union (EU) could request the removal of personal information from search engine results and public databases.[3] However, in a 2019 ruling, the court limited this right to the EU jurisdiction.

The Right to Be Forgotten, often associated with the broader Right to Erasure, is rooted in the

[2] Rolf H. Weber, Right to Be Forgotten: More than a Pandora's Box?, 2 JIPITEC 120 (2011), http://www.jipitec.eu/issues/jipitec-2-2-2011/3084/jipitec%202%20-%20a%20-%20weber.pdf.
[3]Case C-507/17, Google LLC v. Commission Nationale de l'Informatique et des Libertés (CNIL), ECLI:EU:C:2019:772.

idea that individuals have a civil right to safeguard their digital identity and ensure a dignified life by having irrelevant or outdated personal data removed. To make this right effective, a structured mechanism must be in place to ensure that deleted data is also erased from backup storage.

The concept of the Right to Be Forgotten (RTBF), though relatively new in India, has roots in legal principles that have existed for decades. While RTBF has gained significant attention due to digital privacy concerns, its evolution in Indian jurisprudence can be traced back to earlier legal principles and judicial interpretations.

The origins of RTBF in India can be linked to *State of Punjab* v. *Gurmit Singh*[4] where the Supreme Court underscored the importance of protecting the identity of rape victims. The Court held that the identities of rape survivors should remain anonymous throughout legal proceedings and should be conducted in-camera. Although RTBF was not explicitly recognized in this case, the ruling laid the foundation for protecting individuals from the long-term consequences of public disclosure of personal information.

A similar principle was reinforced in *State of Karnataka* v. *Puttaraja*[5], where the Supreme Court referred to Section 228-A of the Indian Penal Code, 1860, which prohibits the disclosure of a rape victim's identity. This provision, aimed at preventing social ostracism, aligns with the intent of RTBF by ensuring that sensitive personal information does not remain publicly accessible, thereby protecting the dignity and privacy of individuals.

The first explicit mention of RTBF in Indian courts arose in *Dharamraj Bhanushankar Dave* v. *State of Gujarat*[6]. The Gujarat High Court, however, did not recognize the right in this case. The petitioner, acquitted of criminal charges, sought to have his court judgment removed from online platforms, arguing that it negatively impacted his reputation. The Court ruled against the plea, stating that publication of judicial records did not violate Article 21 (Right to Life and Personal Liberty) of the Indian Constitution, thereby highlighting the tension between RTBF and the public's right to information.

[4] *State of Punjab v. Gurmit Singh* AIR [1996] SC 1393.
[5] *State of Karnataka v. Puttaraja* AIR [2003] SCW 6429.
[6] *Dharamraj Bhanushankar Dave v. State of Gujarat* Special Civil Application No. 1854 of [2015].

The need for RTBF was further debated in *Mr. X* v. *Hospital Z*[7], where the Supreme Court addressed the conflict between privacy and public interest. The case involved a hospital disclosing a patient's HIV status to his fiancé without his consent. The Court ruled that the fiancé's right to a healthy life, as protected under Article 21, superseded the individual's privacy concerns. This case illustrated that RTBF is not an absolute right and must be balanced against other fundamental rights.

JUDICIAL INTERPRETATION & THE RIGHT TO BE FORGOTTEN

The right to privacy, a fundamental right under Article 21 of the Indian Constitution, forms the basis for the evolving right to be forgotten (RTBF). Article 21, guaranteeing the right to life and personal liberty, has been interpreted broadly by the Supreme Court to encompass various other rights, including privacy. In *Justice K.S. Puttaswamy (Retd.)* v. *Union of India*[8], the Supreme Court affirmed an individual's control over their personal data and online presence, recognizing the permanence of digital information and the challenges it poses to personal rehabilitation. The internet's persistent memory, even after content deletion attempts, makes "forgetting" a continuous struggle in the digital age.

The Delhi High Court, in *Zulfiqar Ahman Khan* v. *M/S Quintillion Business Media Pvt. Ltd.*[9], emphasized the importance of being "forgotten and left alone" as integral to life and existence under Article 21. The court acknowledged the impact of online information on an individual's reputation and the increasing prevalence of online harassment and rumor-mongering. While the RTBF isn't explicitly codified in Indian law, courts have increasingly recognized it as a crucial aspect of the right to privacy. Several petitions seeking the removal of personal data from the internet, court records, and news articles are currently before the Delhi High Court, with some petitioners successfully obtaining relief.

The *K.S. Puttaswamy* judgment served as a milestone, with the court noting that the Personal Data Bill (now the Digital Personal Data Protection Act, 2023) also supported the concept of forgotten rights. The Orissa High Court has indicated that it would enforce such a right through court processes if necessary. While India lacks specific legislation on the RTBF, the General Data Protection Regulation (GDPR) in Europe provides a comparative framework, recognizing

[7] *Mr. X v. Hospital Z* AIR [1999] SC 495.
[8] *Justice K.S. Puttaswamy (Retd.) v. Union of India* 4 [2019] 1 SCC 1.
[9] *Zulfiqar Ahman Khan v. M/S Quintillion Business Media Pvt. Ltd* CS (OS) 642 [2018].

the right to erasure when data is no longer needed or consent is withdrawn. The challenge lies in balancing the benefits of a permanent digital record against the difficulties individuals face in overcoming past mistakes. People evolve and change, and the RTBF aims to provide a chance for reinvention, free from the constraints of past actions.

In *Sri Vasunathan* v. *Registrar General*,[10] the court, while acknowledging foreign jurisprudence on the matter, upheld a woman's RTBF. The Supreme Court, in *K.S. Puttaswamy*, clarified that the RTBF is subject to restrictions and cannot be invoked if the information is necessary for exercising Article 19 rights, fulfilling legal obligations, protecting public interest, or for scientific/historical purposes, among other reasons. More recently, the Madras High Court, in a case concerning the continued online presence of an acquitted individual's name in a judgment, ruled that the RTBF does not apply to court judgments. In *Jorawer Singh Mundy* v. *Union of India*[11], the Delhi High Court directed Google to remove a judgment acquitting a man in a drug case, citing its impact on his professional life. These diverse judicial interpretations highlight the ongoing evolution and nuanced application of the RTBF in India.

DIGITAL PERSONAL DATA PROTECTION ACT, 2023

India's Digital Personal Data Protection (DPDP) Act, 2023,[12] introduced to regulate data privacy, partially recognizes the Right to Be Forgotten (RTBF) but does not explicitly define it as a fundamental right. The Act provides individuals with limited control over their personal data but lacks the broad erasure rights granted under the European Union's General Data Protection Regulation (GDPR).[13]

Key Provisions of DPDP Act, 2023 Related to RTBF

1. Right to Erasure (Section 12): The Act allows individuals (data principals) to request data fiduciaries (organizations handling data) to delete or modify personal data once it is no longer necessary for the original purpose of collection.

2. Data Storage Limitation (Section 8): The Act mandates that personal data must not be retained beyond the required period, indirectly supporting the RTBF by requiring

[10] S*ri Vasunathan* v. *Registrar General*, W.P. No. 62038 of 2016 (Karn. H.C. Jan. 23, 2017).
[11] *Jorawer Singh Mundy v. Union of India* [2021] SCC OnLine Del 2306.
[12] Digital Personal Data Protection Act, No. 22 of 2023, INDIA CODE (2023).
[13] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), 2016 O.J. (L 119) 1.

organizations to delete unnecessary data.

3. Right to Correction and Update (Section 13): Individuals can request corrections to their data, but the Act does not explicitly grant them the absolute right to have their information erased upon request.

4. Adjudicatory Mechanism: Unlike the GDPR, which allows individuals to directly request data removal, the DPDP Act requires individuals to file an appeal before the Data Protection Board of India (DPBI) to exercise this right.

Limitations of RTBF under the DPDP Act

- No Direct Right to Be Forgotten: Unlike the earlier Personal Data Protection Bill, 2019, which explicitly mentioned RTBF, the DPDP Act does not define it separately.

- Public Interest & Freedom of Expression: Requests for data deletion can be denied if the information is deemed necessary for public interest, law enforcement, or journalistic purposes.

- No Search Engine Delisting: The Act does not address the issue of removing personal data from search engine results, unlike the EU's GDPR, which allows individuals to request delisting.

RIGHT TO BE FORGOTTEN IN EUROPEAN UNION

India's journey with the right to be forgotten (RTBF) is still unfolding. From the *Gurmit Singh* case in 1996 to the more recent *Laksh Vir Singh Yadav* case, the concept has been gradually evolving, though at a slower pace than in other jurisdictions. India's progress involves recognizing the need to remove objectionable data and strengthening privacy laws.[14]

In stark contrast, the EU has a fully developed and legally enshrined RTBF, recognized as a fundamental right. Recent cases across EU member states demonstrate this. For instance, in Germany, two brothers who murdered an actor, after serving their sentence, sued Wikimedia Foundation to remove their names from the website, citing reputational harm. A similar case

[14] Two German Killers Demanding Anonymity Sue Wikipedia's Parent, available at <http://www.huffingtonpost.com/2009/11/13/twogerman-killers-demand_n_356380.html> accessed 9 February 2025.

in France, echoing the *Costeja* case appeal, concerns the jurisdictional reach of the RTBF. The French data protection agency (CNIL) requested Google to remove specific links, which Google complied with only for its French domain, arguing a lack of jurisdiction over other country-specific Google sites. This highlights the complexities of enforcing the RTBF across borders. The *Costeja* ruling by the Court of Justice of the European Union (CJEU) in 2014 revealed the varying interpretations of the RTBF by national courts, suggesting that a single country's data protection authority cannot unilaterally dictate online content accessibility in another.[15]

These cases reveal a significant disparity between India and the EU. While India is still working towards statutory recognition of the RTBF, the EU has already integrated and applied it extensively. Furthermore, the scope of the RTBF differs considerably. In India, its application has primarily been limited to cases involving women's modesty, sexual harassment, or crimes impacting women's character. In the EU, the RTBF has a broader scope, applicable to a wider range of cases where data is deemed irrelevant, unnecessary for public view, or prejudicial to an individual, with certain exceptions. The EU is now even grappling with the complex issue of jurisdictional reach, further demonstrating its advanced stage of RTBF development.

SEALING OF COURT RECORDS IN THE USA: A CONTRASTING APPROACH

The US federal court system employs a mechanism called "sealing court records," which, while distinct from the EU's right to be forgotten (RTBF), shares a similar underlying purpose. Both aim to protect individuals' reputations and opportunities by limiting public access to certain information. Sealing court records involves restricting public access to specific case files, sometimes even leading to their eventual destruction. While sealed records can be accessed with a court order, the sealing effectively removes them from general public view.

The key difference lies in the scope: sealing court records encompasses the *entire* case file, whereas the RTBF typically focuses on redacting specific information, like names, while leaving the remaining record accessible. Sealing court records is a more comprehensive measure, granting individuals the legal right to deny involvement in the sealed case. In some

[15] Nani Jansen Reventlow, The French Court Case That Threatens to Bring the “Right to be Forgotten” Everywhere,https://www.cfr.org/blog/french-court-case-threatensbring-right-be-forgotten-everywhere accessed 9 February 2025.

jurisdictions, a sealed record is legally considered as never having occurred.

US states have varying rules governing the grounds and procedures for sealing records. Common justifications include matters of national security, trade secrets, sensitive medical information, certain family court cases, tax information, and communications between judges and staff. The lack of a uniform federal standard has led to inconsistencies and concerns about "over-sealing."

A significant issue of over-sealing came to light in 2003 with the discovery of secret dockets in Connecticut, revealing that courts had sealed records without proper legal justification, often influenced by personal gain and vested interests. Cases involving prominent figures were frequently sealed regardless of merit, and even personal matters of judges were shielded from public scrutiny.

The problem persists, as illustrated by a 2013 case involving a DEA agent's use of a fake Facebook account. While the court ruled on the case, the reasoning behind the decision, as well as the initial application for sealing, remains inaccessible to the public. This secrecy contradicts the First Amendment's guarantees of free speech and a free press.

In response to these concerns, organizations like the Civil Liberties & Transparency Clinic at the University at Buffalo School of Law, the New York Civil Liberties Union, and the Knight First Amendment Institute have proposed model rules for sealing court records. These rules aim to establish uniform standards and procedures across courts, promoting greater transparency and accountability in the process. These model rules are currently pending approval in some jurisdictions.

RIGHT TO BE FORGOTTEN & JOURNALISM

The right to be forgotten (RTBF), while seemingly beneficial in protecting individuals from the enduring consequences of their digital past, faces resistance, particularly from journalistic organizations. This resistance often stems from the perception that the RTBF infringes upon press freedom. Some argue that society should embrace a culture of forgiveness, rendering the RTBF unnecessary. They contend that a forgiving society, while ideal, is currently unrealistic in our individualistic culture. Individuals facing harm from past journalistic reports shouldn't bear the burden of societal change. Therefore, a degree of individual control over their digital

narrative is necessary. This requires a non-ideal, pragmatic approach that balances the interests of individuals and the press, rather than adhering to a utopian ideal of universal forgiveness.[16]

A common argument against the RTBF frames it as a direct assault on press freedom. Press freedom, defined as the absence of external constraints on journalistic publication, is considered crucial for a healthy democracy. Journalists, acting as watchdogs, need freedom to expose wrongdoing and hold power accountable.[17] However, this traditional view of press freedom, focused solely on combating powerful interests, may be outdated. Profit-driven media often prioritize sensationalism over public service. Furthermore, the lines between established journalistic institutions and individual online content creators are increasingly blurred. Therefore, equating any limitation on publication with an attack on core democratic values may be an oversimplification.[18] The core function of a free press – holding power accountable – is unlikely to be compromised by a carefully implemented RTBF framework.

Several specific arguments are raised against the RTBF. First, the importance of historical integrity is cited. Preserving information in its original form is seen as crucial for historical, scientific, and statistical purposes. However, not all journalistic content holds equal archival value. A balance can be struck between respecting privacy and preserving valuable information. Information can be archived while its public visibility is reduced, mitigating individual harm without compromising the historical record. The primary function of the press is not archiving, and a shift in visibility doesn't necessarily diminish archival value.

Second, concerns about journalistic accountability are raised. It's argued that altering or anonymizing content undermines transparency and makes it difficult to verify information. However, a well-designed RTBF framework doesn't necessitate an "either/or" approach. Requests can be evaluated, and if denied, no content is altered. If granted, solutions can be found to protect privacy without compromising the verifiability of the remaining content.

Third, the economic burden on news organizations is a practical concern. Re-evaluating content is time-consuming and costly, particularly for financially struggling media outlets. However, this concern, while valid, shouldn't be the sole determining factor. News organizations can proactively address the root of many RTBF requests by focusing on informed consent.

[16] Maria Garcia-Murillo & Ian MacInnes, Così Fan Tutte: A Better Approach than the Right to Be Forgotten, 42 *Telecomm. Pol'y* 227 (2018).
[17] Julian Petley, The Leveson Inquiry: Journalism Ethics and Press Freedom, 13 *Journalism* 529 (2012).
[18] Stephen Dawes, Press Freedom, Privacy and the Public Sphere, 15 *Journalism Stud*. 17 (2014).

Journalists should ensure sources fully understand the potential long-term consequences of their participation in a story. By fostering informed consent, the number of future unpublishing requests may be reduced. This approach tackles the problem at its source, rather than simply reacting to requests after publication.

CONCLUSION

The right to be forgotten (RTBF) presents a complex challenge in the digital age, forcing a confrontation between individual privacy and the freedom of the press. This paper has explored the RTBF's evolution, its legal interpretations in India, and its comparison with related concepts in the EU and the US. While the ideal of a universally forgiving society is attractive, it remains a distant prospect. Therefore, a pragmatic approach is necessary to address the real-world harms individuals face due to the permanence of online information.

The RTBF is not a simple matter of censorship versus free speech. It requires a nuanced balancing act, weighing the public interest in information against the potential for disproportionate harm to individuals. Concerns about historical integrity, journalistic accountability, and economic burdens on news organizations, while valid, can be mitigated through careful implementation of a well-structured RTBF framework. Archiving information while limiting its public visibility, ensuring transparency in content modifications, and prioritizing informed consent from sources are key strategies.

India's legal landscape concerning the RTBF is still developing. While judicial pronouncements have acknowledged the right to privacy as encompassing aspects of the RTBF, a comprehensive legal framework is needed. The Digital Personal Data Protection Act, 2023, represents a step forward, but its limitations, particularly regarding direct access to data removal and the balancing of public interest against individual rights, require further consideration. Learning from the EU's experience with the GDPR, while also considering the distinct context of the Indian legal system, is crucial.

Ultimately, the goal is not to stifle journalistic freedom but to foster a responsible and ethical digital environment. A self-regulatory framework within journalistic organizations, guided by ethical principles and best practices, offers a promising path forward. By engaging in a case-

by-case assessment of RTBF requests, weighing the enduring public interest against the potential for individual harm, news organizations can play a vital role in striking the delicate balance between privacy and press freedom. The future of digital privacy in India depends on finding this equilibrium, ensuring that individuals have the opportunity to reclaim their digital narratives without compromising the essential function of a free and robust press in a democratic society.