RIGHT TO BE FORGOTTEN: BALANCING PRIVACY (DIGITAL PERSONAL DATA PROTECTION ACT, 2023) WITH FREE SPEECH & ARCHIVES IN INDIA

Advocate Amit Maheshwari, Practicing Advocate, Phagi, Jaipur, Rajasthan

Ms. Aarya Goswami, BBA LLB, LL.M.

Advocate Akansha Singh, Practicing Advocate, Rajasthan High Court, Jodhpur, Rajasthan

ABSTRACT

The Right to Be Forgotten (RTBF) has emerged as a pivotal issue in the digital era, where personal data and online records persist indefinitely, often shaping reputations and identities long after their relevance has diminished. This research paper critically examines the evolution, legislative framework, and judicial interpretations of RTBF in India, particularly in light of the Digital Personal Data Protection Act (DPDPA), 2023. While the Act grants individuals' significant control over their personal data, it does not explicitly codify RTBF, leaving its implementation dependent on judicial balancing and regulatory discretion. The study explores the inherent conflict between RTBF and freedom of speech under Article 19(1)(a) of the Constitution, analyzing case law where courts have sought to reconcile privacy, reputation, and public interest with archival integrity and press freedom. Ethical and social dimensions, including digital rehabilitation, stigma, censorship risks, and technological challenges such as de-indexing, anonymisation, and AI-based filters, are evaluated to highlight the complexities of operationalizing RTBF. Comparative insights from the European Union, United Kingdom, and United States provide valuable perspectives for shaping India's approach. The paper concludes with recommendations for codifying RTBF as a distinct statutory right, supported by institutional mechanisms, transparent criteria, and robust safeguards against misuse. It further emphasizes the role of digital literacy, public awareness, and responsible digital citizenship in ensuring a balanced framework that harmonizes individual privacy with democratic values of free speech and archival preservation.

Keywords: Right to Be Forgotten (RTBF), Privacy, Free Speech, Digital Personal Data Protection Act, 2023 and Digital Literacy.

I. INTRODUCTION

"Privacy is the fountainhead of all other rights."

\- ***Edward Snowden***[1]

Cyberspace is a vast digital environment that lives inside our physical world to accommodate our various requirements and tastes. Its pervasiveness has significantly changed our way of life. Its growth is driven by data, which has made it an indispensable aspect of our lives in recent years. Without a doubt, everybody who has ever used digital media has received several warnings to avoid disclosing private or sensitive information online.[2] Protecting the privacy of personal information has grown more difficult. In the modern world, a person's reputation and personality can be made or broken by their internet presence. Maintaining a decent and professional image in one's internet identity is therefore essential, and our personal and professional lives may suffer greatly if we do not do so.[3]

The right to privacy states to the exact right of an individual to regulate the collection, use and disclosure of his personal information. The term Personal information can be explained in the form of personal habits, various activities, family, educational, communications, clinical and monetary records. Right to Privacy is synonymous with the ***"right to be let alone."***[4] **According to Black's Law Dictionary** *"right to be let alone; the right of a person to be free from any unwarranted publicity; the right to live without any unwarranted interference by the public in matters with which the public is not necessarily concerned" is defined as Privacy."*[5]

The Right to be Forgotten is an important legal principle in a time where digital fingerprints and the ubiquitous nature of internet information are the norm. It acknowledges that information shared online can affect a person's personal and professional life in long-lasting and frequently unexpected ways. Thus, it is evident why this right should be implemented: it protects individual rights and encourages a sensible strategy for data protection in the digital

[1] Edward Snowden, 'Edward Snowden's quotes on the importance of privacy' (Yourstory, June 21, 2017), <https://yourstory.com/2017/06/edward-snowden-quotes-privacy> accessed 10 September 2025.
[2] Gayathri G., 'Letting Bygones Be Bygones; Implementing the Right to Be Forgotten in India' (2024) 2(1) Lawfoyer International Journal Doctrinal Legal Research <https://lijdlr.com/2024/05/06/letting-bygones-be-bygones-implementing-the-right-to-be-forgotten-in-india/> accessed 10 September 2025.
[3] Luciano Floridi, 'The Right to Be Forgotten: A Philosophical View' (2015) 23 Jahrbuch far Recht und Ethik Annual Review of Law and Ethics <https://philarchive.org/rec/FLOQRT> accessed 11 September 2025.
[4] *Justice K.S. Puttaswamy v Union of India [2017],* [2017] 10 SCC 1.
[5] *Black's Law Dictionary* (10th Ed, Thomson Reuters 2014).

era.[6] Moreover, its significance extends beyond individual privacy; it influences criminal law, public opinion, and numerous other facets of modern life.

In simpler terms, the "right to forget" refers to the already intensively reflected situation that a historical event should no longer be revitalized due to the length of time elapsed since its occurrence. The "right to be forgotten" reflects the claim of an individual to have certain data deleted so that third persons can no longer trace them.[7] Therefore, the right to be forgotten is based on the autonomy of an individual becoming a right holder in respect of personal information on a time scale; the longer the origin of the information goes back, the more likely personal interests prevail over public interests.[8]

Basically, the **"Right to be forgotten" or "Right to be erased"** provides a right to individual to request for removal of his/her personal data floating around through Internet.[9] The basic tenet of data erasure is that the data owner must voluntarily consent to the use of the data. Therefore, the owner has the right to have his data deleted when the consent is revoked. Also, when the data controller has no legal right to process the data, the data should be erased.[10] Determining what constitutes "personal data" is a major technological obstacle to the implementation of the "Right to be forgotten". According to ***Article 17 of European Union (EU) Directives***, the term "personal data" means any information relating to the individual.[11] Such a definition creates uncertainties regarding things like collective information, which may not specifically identify any individual but may point to the family.

II. HISTORICAL AND CONCEPTUAL FRAMEWORK OF RIGHT TO BE FORGOTTEN

The concept of ***le droit a l'oubli (the right to be forgotten)*** was first proposed in France in 2010, acknowledging that ex-offenders had the right to have their names removed from official records because the information pertaining to them was "outdated."[12] It enables people to begin

[6] *Supra Note 2.*
[7] Prashant Mali, 'Privacy Law: Right to Be Forgotten in India' (2018) 7(1) NLIU Law Review <https://nliulawreview.nliu.ac.in/journal-archives-2/volume-vii/> accessed 12 September 2025.
[8] *Supra Note 7.*
[9] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, (General Data Protection Regulation), article 17 and 19.
[10] *Ibid art. 18, 19.*
[11] *Ibid art. 11.*
[12] Gargee Yadav, 'Unravelling the Emergence of Right to Be Forgotten in India' (2023) 1(2) Lawfoyer International Journal of Doctrinal Legal Research <https://lijdlr.com/2023/08/05/unravelling-the-emergence-of-right-to-be-forgotten-in-india/> accessed 12 September 2025.

their lives over, free from the weight of their history. It is also important to note that a delicate balance needs to be established between other fundamental rights, for instance, freedom of speech and expression, the right to information, right to press, and the right to dissent that play an important role in safeguarding the democratic character of a country.[13]

The data protection directive of the European Union was officially accepted in 1995 and aimed at regulating the processing of personal data. However, this directive did not explicitly mention the right to be forgotten. The court of justice of the European Union recognised this right in the case of ***Google Spain v. Gonzalez (2014)***[14]. Gonzalez, a Spanish national, filed a complaint against Google Spain, Google Inc., and the Spanish daily *La Vanguardia* in 2010 for publishing all of its newspapers from 1881 to 2009 online, including the 1998 auction of Gonzalez's property. To recoup his social security debt, his property was put up for auction. A Google search of the plaintiff's name revealed that he had paid off all of his obligations nearly ten years prior, and that the newspaper had placed all of its records online in 2009. Because the information was out of date and irrelevant, he filed a lawsuit against Google.[15]

By looking at how Google handles data when users search for anything on its search engine, the question of whether it processes data may be answered. After comparing the search query with the index, Google's query processor shows the most pertinent match. Google uses this to get the best match for the query after first temporarily storing it in its cache memory.[16] The court also pointed out that users may be able to search for a person's name using the information aggregation, which would allow anyone to obtain a comprehensive profile of that person just by entering their name. Therefore, the court noted that there is a violation of the right to privacy.[17] The court held that the search engines do fall within the ambit of the data protection directive *95/46* of the European Union.[18]

---

[13] Anuprash Rajat & Gaurav Bharti, 'Right to Be Forgotten in India: A Critical Legal Analysis' (2022) 4 (1) Indian JL & Legal Rsch <https://www.ijllr.com/post/right-to-be-forgotten-in-india-a-critical-legal-analysis> accessed 14 September 2025.

[14] Tejashree J., 'The Need for the Right to Be Forgotten in India' (2018) 5(1) RGNUL Financial & Mercantile Law Review <https://www.rfmlr.com/_files/ugd/0fa0b3_a397a0db5fc8407288c2ae7bcd1a9837.pdf> accessed 16 September 2025.

[15] *Ibid.*

[16] Andrew Kenyon, *'Comparative Defamation and Privacy Law'* (Cambridge University Press 2016).

[17] Lisa Owings, 'The Right to Be Forgotten' (2015) 9 (1) Akron Intellectual. Property Journal <https://ideaexchange.uakron.edu/akronintellectualproperty/vol9/iss1/3/> accessed 14 September 2025.

[18] Herke Kranenborg, 'Google and the Right to Be Forgotten' (2015) 1(1) European Data Protection Law Review 70-79 <https://www.researchgate.net/publication/327546121_Google_and_the_Right_to_Be_Forgotten> accessed 15 September 2025

However, until the ***K.S. Puttaswamy judgement*** in 2017, the right to privacy wasn't officially acknowledged in India. It is a basic yet incredibly complex right. Although it can be determined that removing personal information from public forums is a significant part of this, neither the legislature nor the judiciary have taken a consistent position on the subject.[19] **The Information Technology Act of 2000**[20] prescribes punishments for publishing or transmitting images of private parts or other explicit images of individuals without consent.[21] Despite differing opinions of the different , it is evident that the notion in question has already been recognized by the current legal system and legislation. However, the words "forgotten" and "erasure" were not specifically mentioned. Discourses evolved over time over the same.

III. LEGISLATIVE FRAMEWORK

A. Pre-DPDPA Legal Framework

India's approach to data protection and the ***Right to Be Forgotten (RTBF)*** was disjointed, reactive, and largely dependent on judicial discretion prior to the passage of the ***Digital Personal Data Protection Act (DPDPA), 2023***.[22] Although the Information Technology Act of 2000 and its related regulations provided some limited protections, they lacked a thorough, rights-based framework based on human control over personal data.

The distribution of private or explicit photos without consent is punishable under the ***Information Technology Act of 2000.***[23] To preserve people's privacy, courts have frequently mandated that such content be taken down. In a significant instance, the Supreme Court ordered Google to remove defamatory content from Ban Asbestos India, but it made it clear that removal must be done in accordance with a formal order rather than merely a complaint. Although this represents aspects of the Right to Be Forgotten, judicial discretion was primarily relied upon in these rulings due to the absence of consistent legal norms.[24]

Following the historic Puttaswamy case, Indian courts carefully examined the parameters of the Right to Be Forgotten (RTBF) within the larger framework of privacy rights in the

[19] *K.S. Puttaswamy (Retd.) & Anr. v Union of India & Ors [2017],* [2017] AIR SC 4161.
[20] Act No. 21 of 2000.
[21] Information Technology Act 2000, s 67.
[22] Act No. 22 of 2023.
[23] Information Technology Act 2000, s 66E, 67 and 67A.
[24] *Supra Note 2.*

absence of explicit statutory recognition.

B. Right to Be Forgotten under the Digital Personal Data Protection Act, 2023

The phrase ***"Right to Be Forgotten" (RTBF)*** is not used specifically in the ***Digital Personal Data Protection Act, 2023 (DPDPA)***, but it is implied in a number of its clauses. The Act gives people—known as Data Principals—the ability to meaningfully manage their digital personal information. The cornerstone of informational autonomy is provided by Section 12(1), which grants a Data Principal the right to request the correction, completeness, updating, or deletion of personal data processed with their permission.[25]

Section 12(3) further broadens this right by requiring a Data Fiduciary to delete personal data upon receiving a legitimate request for erasure from the Data Principal, unless the data must be kept to fulfill the original purpose or to adhere to legal obligations.[26] Furthermore, Section 8(7) reinforces this erasure need by requiring Data Fiduciaries to remove data when the intended use has been completed or consent has been revoked.[27] By guaranteeing that data is not kept permanently, this clause protects individual privacy and reduces needless exposure. Section 8(8) of the Act also establishes a practical presumption that, in the event that the Data Principal has not communicated with the Data Fiduciary for a certain amount of time and has not exercised any of her data rights during that time, the indicated purpose is deemed to be no longer valid.[28] By enabling the system to start deletion based on user inactivity even in the absence of express withdrawal, this clause successfully complies with the objectives of RTBF.

Although it is not specifically codified as a stand-alone right, the DPDPA adopts a functionally analogous concept of RTBF from a legal and policy standpoint. This sets it apart from the General Data Protection Regulation (GDPR) of the European Union, where Article 17 expressly guarantees RTBF. The DPDPA, on the other hand, prohibits arbitrary or abusive deletion requests by limiting the right to erasure on legal compliance and the data's relevance to the stated purpose. This well-rounded strategy protects legitimate institutional, economic, and public interests while still preserving individual privacy. Notably, inactivity-based triggers for deletion are included, providing a practical and

[25] The Digital Personal Data Protection Act 2023, s 12(1).
[26] *Ibid* § 12(3).
[27] *Supra Note 25 s 8(7).*
[28] *Supra Note 25 s 8(8).*

automatic means of implementing data reduction guidelines. However, the practical implementation of this right will probably rely on future rule-making and court interpretation due to the lack of a specific RTBF clause or comprehensive processes.

C. *Role of the Data Protection Board of India and Enforcement of RTBF with the remedies and its limitations*

A key player in the enforcement of data rights, including the recently developed ***Right to Be Forgotten (RTBF)***, is the ***Data Protection Board of India (DPBI)***, which was founded in accordance with ***Section 18*** of the ***Digital Personal Data Protection Act, 2023 (DPDPA)***. In accordance with ***Section 27(1)(b)***, the Board, a quasi-judicial entity, has the authority to hear complaints from Data Principals and investigate claims of infractions by Data Fiduciaries, including failures to delete personal data upon legal order.[29] Due process, reasoned decision-making, and the opportunity to be heard are among the natural justice principles that must be adhered to in order for procedures to be fair, as stipulated by Section 28.[30] Depending on the seriousness of a violation, the Board may additionally levy heavy fines, up to ₹250 crore, as specified in Section 33.[31] This regulatory structure reflects a commitment to both accountability and deterrence in the handling of personal data.

As far as remediation goes, the DPDPA provides people with the option to seek the deletion of personal information under Section 12, which serves as the foundation for RTBF.[32] Furthermore, all Data Fiduciaries are required by Section 13 to have efficient grievance resolution procedures in place, which must be used first before bringing issues to the Board.[33] The Appellate Tribunal may hear appeals of the Board's decisions under Section 29, and Section 39 streamlines the adjudication process by prohibiting civil courts from getting involved in subjects under the Board's jurisdiction.[34] To further encourage compliance without drawn-out litigation, Section 32 permits organizations to submit voluntary undertakings to the Board.[35]

RTBF enforcement is not without restrictions, though. As seen in Section 8(7), where banks

[29] *Ibid s 27(1)(b).*
[30] *Ibid s 28.*
[31] *Ibid s 33.*
[32] *Ibid s 12.*
[33] *Ibid s 13.*
[34] *Ibid s 29, 39.*
[35] *Supra Note 25 s 32.*

are obligated to retain customer records for ten years, data fiduciaries are not compelled to remove data if its keeping is permitted by law.[36] Furthermore, data processing pertaining to national security, state operations, or active legal actions is excluded from the RTBF under Section 17.[37] Additionally, the Act does not provide for the automated deletion of data; instead, the Data Principal must formally request it and have it evaluated. Furthermore, the consistency and predictability of decisions pertaining to RTBF may differ since the Board has considerable discretion in interpreting and applying the legislation.

Although the DPBI provides a formalized channel for redress, how fairly and effectively it uses its power will determine how effective it is in practice. This illustrates a larger conflict in Indian data protection law: striking a balance between the rights of individuals to privacy and legal, regulatory, and public interest factors.

IV. CONFLICT BETWEEN THE RIGHT TO BE FORGOTTEN AND FREEDOM OF SPEECH

The recognition of the ***Right to be Forgotten (RTBF)*** in Indian jurisprudence has prompted a complex constitutional debate, especially when placed in juxtaposition with ***Article 19(1)(a) of the Indian Constitution***, which guarantees the right to freedom of speech and expression. This tension reflects the broader global struggle to reconcile digital privacy with democratic values of transparency, freedom of the press, and the public's right to know. The RTBF, rooted in informational self-determination, asserts that individuals should have control over their personal data, including the right to remove or delink information that is no longer relevant or necessary. However, the assertion of this right frequently collides with the interests of free expression, open access to information, and journalistic freedoms, necessitating a careful judicial balancing act.

A. Article 19(1)(a) vs. Emerging Privacy Rights

Article 19(1)(a) enshrines a citizen's right to free speech, which includes the freedom to access and disseminate information.[38] However, this right is not absolute and is subject to reasonable restrictions under Article 19(2), including grounds such as defamation, decency,

[36] *Ibid* s *8(7) illus. II.*
[37] *Ibid s 17.*
[38] The Constitution of India 1950, art. 19(1)(a).

and public order.[39] On the other hand, privacy as a fundamental right was recognized in the landmark decision of ***Justice K.S. Puttaswamy (Retd.) v. Union of India (2017)***, where the Supreme Court held that privacy is an essential facet of the right to life under Article 21.[40] Within this broader right, informational privacy and the RTBF have emerged as integral components, particularly in the context of digital permanence—the indelibility of online data and its potential to cause reputational harm.

The doctrinal conflict lies in the competing claims of two fundamental rights: the right of an individual to digitally disappear versus the right of the public to remember and access information. This dichotomy becomes sharper in the age of internet archives, search engines, and social media platforms, where personal data once public becomes permanent. The RTBF seeks temporal limitation on speech, suggesting that past information may lose its public relevance and deserve erasure, a claim that arguably clashes with the democratic imperative of memory and historical continuity.

B. Judicial Interpretations Balancing Individual Reputation And Public Interest

Indian courts have begun to cautiously recognize the RTBF, particularly in cases involving acquitted individuals, victims of sexual offences, and persons seeking to delink personal data from search engines. However, the judiciary has also emphasised that the RTBF cannot be viewed in isolation and must be harmonised with competing interests such as press freedom, judicial transparency, and archival integrity.

In ***K.S. Puttaswamy v. Union of India***, the Supreme Court acknowledged RTBF as part of the right to informational privacy, albeit with reservations about its implementation in a democratic society. Justice Sanjay Kishan Kaul, in his concurring opinion, referred to RTBF as a right "in the context of the individual's autonomy over personal data," but also noted that it must be balanced against free speech and archival responsibilities.[41]

In ***Subhranshu Rout v. State of Odisha (2020)***, the Orissa High Court recognized that in some cases, an individual's right to be forgotten may override public interest in retaining information.[42] Conversely, in ***Gautam Navlakha v. National Investigation Agency (2021)***,

[39] The Constitution of India 1950, art. 19(2).
[40] *K.S. Puttaswamy (Retd.) v. Union of India [2017],* [2017] 10 SCC 1.
[41] *Supra Note 40.*
[42] *Subhranshu Rout v. State of Odisha [2020],* [2020] SCC Online Ori 878.

the Delhi High Court declined a plea to redact the petitioner's details from judicial records, citing public interest and the need for transparency in legal proceedings.[43] The courts have thus followed a case-by-case balancing approach, weighing factors such as the nature of the offence, the relevance of the information, the status of judicial proceedings, the impact on the individual's dignity and rehabilitation, and the broader public interest.

C. Case Studies from Indian Courts

Several Indian cases demonstrate how courts are navigating the complex terrain of RTBF and free expression:

a) ***Jorawar Singh Mundy v. Union of India (2021)***: This case marked a significant milestone in Indian jurisprudence on RTBF. The Delhi High Court ordered the removal of a judgment from online platforms involving an NRI who had been acquitted of sexual harassment charges. The Court noted that continued online availability of the judgment caused undue harm to his reputation and professional prospects, even after legal exoneration. The judgment emphasised that *"public interest in accessing an acquittal decision of an unknown foreign national is negligible compared to the impact on his life and career."* This case underscores a rehabilitative approach to RTBF and the differentiation between public relevance and voyeuristic curiosity.[44]

b) ***XYZ v. Union of India (2021)***: Here, the Kerala High Court considered the plea of a woman who sought to erase a matrimonial case order from online platforms. The Court acknowledged her plea for dignity and privacy, especially in the context of her future marriage prospects, and agreed that RTBF could be invoked where judicial records serve no larger public interest. However, the Court also highlighted that removal from digital platforms does not imply tampering with court records, thereby ensuring archival continuity while offering digital erasure.[45]

c) ***Name Redacted v. Registrar General (2022), (Madras High Court)***: In a criminal case involving the accused who had been acquitted, the Court allowed anonymisation of the

[43] *Gautam Navlakha v. National Investigation Agency [2021],* [2021] 7 SCC 329.
[44] *Jorawar Singh Mundy v. Union of India [2020],* [2021] SCC Online Del 2306.
[45] *XYZ v. Union of India [2021],* [2021] 10 SCC 630.

name in the judgment available online. The Court underscored the need to protect acquitted individuals from digital stigma in perpetuity.[46]

D. RTBF In Media, Journalism, And Online Records

The application of RTBF in the realm of journalism and online media introduces a constitutional paradox. On one hand, the media functions as a watchdog in a democracy, holding institutions accountable and chronicling contemporary events. On the other hand, sensational or outdated news content, especially when algorithmically amplified, can stigmatize individuals indefinitely, even when they have been acquitted or have reformed.

Indian courts have grappled with this issue in a cautious manner. In ***Rakesh Kumar v. Union of India (2021)***, a plea to remove news reports about a past arrest was denied, with the Court observing that factual reporting of public records could not be retroactively censored unless it was proven false or malicious.[47] However, some judgments have encouraged media self-regulation, suggesting that portals update stories to reflect acquittals or provide context to prevent reputational harm.

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, provide a basic grievance redressal mechanism but fall short of codifying a robust RTBF regime. In the absence of specific legislation, individuals often resort to invoking ***Article 21***[48] read with ***Article 19(2)***[49] of the Indian Constitution to claim privacy over past narratives, creating ambiguity in the legal framework. Moreover, digital platforms, particularly search engines, become critical gatekeepers in this context. Since these platforms control the visibility and accessibility of information, Indian courts may soon need to follow the EU's lead and mandate search engine de-indexing in specific RTBF cases, ensuring reputational fairness without erasing public records.

V. ETHICAL, SOCIAL AND TECHNOLOGICAL DIMENSIONS OF THE RIGHT TO BE FORGOTTEN

The ***Right to be Forgotten (RTBF)*** has emerged as a contentious yet critical digital right in the

[46] *Name Redacted v. Registrar General [2021],* [2021] SCC Online Mad 2755.
[47] *Rakesh Kumar v. Union of India [2021],* [2021] 6 SCC 156.
[48] The Constitution of India 1950, art. 21.
[49] *Supra Note 39.*

era of mass datafication. It reflects a fundamental tension between privacy and public interest in the digital age, where individual data persists indefinitely in cyberspace. As a derivative of the right to privacy and informational self-determination, the RTBF asserts that individuals should have the power to request the removal of personal information from online platforms when it no longer serves a legitimate public interest.

A. Ethical Considerations: Rehabilitation vs. Censorship

The core ethical tension in the RTBF debate lies in reconciling the individual's right to digital rehabilitation with the collective right to access information. Ethically, the RTBF empowers individuals to detach from a digital past that may be outdated, irrelevant, or disproportionately harmful. This is particularly significant in cases involving minor legal infractions, juvenile offences, or personal missteps that hinder reintegration into society. From the perspective of rehabilitation, digital permanence often conflicts with restorative justice ideals that aim for the eventual societal reintegration of offenders and marginalized individuals.[50]

However, critics argue that RTBF veers dangerously close to censorship, especially when invoked by public figures or corporations seeking to erase accountability or suppress criticism. The line between protecting dignity and enabling erasure of historically or socially significant facts is ethically ambiguous. The de-listing of search results, especially without judicial oversight, raises concerns of unilateral power being exercised by private entities like tech platforms, potentially undermining the principle of transparency and public memory.[51] The ethics of memory in the digital age also raise philosophical questions about collective historical consciousness. The ability to forget is as vital as the ability to remember, yet digital systems are structurally biased toward memory, creating a persistent "digital scar" that can perpetuate stigma long after the event has lost relevance.[52]

B. Social Implications: Stigma, Identity, And Digital Memory

The social implications of RTBF are deeply entangled with issues of digital identity

[50] DANIEL J SOLOVE, *'THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET'* (Yale University Press 2007).
[51] Jeffrey Rosen, 'The Right to Be Forgotten' (2012) 64(88) STAN. L. REV. ONLINE <https://review.law.stanford.edu/wp-content/uploads/sites/3/2012/02/64-SLRO-88.pdf> accessed 15 September 2025.
[52] VIKTOR MAYER-SCHÖNBERGER, *'DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGE'* (Princeton University Press 2009).

formation, societal reintegration, and the persistence of stigma. In societies where digital footprints have become a primary means of forming impressions, social, professional, or legal, the existence of outdated or irrelevant data online can lead to unfair judgments, discrimination, and social exclusion. For individuals previously involved in criminal justice systems, particularly juveniles or acquitted persons, the RTBF offers a path toward reclaiming their narrative and reintegrating without being perpetually defined by past errors.

The digital enshrinement of every action violates the temporality of human error and growth, reducing complex lives to static online snapshots. However, there is also concern that social justice movements, such as #MeToo or anti-corruption campaigns, could be undermined if public figures begin to seek removal of relevant allegations under RTBF claims. This necessitates a nuanced, contextual approach to distinguishing between private harm and public interest. In India, where the ***Digital Personal Data Protection Bill (2023)*** is still evolving and the jurisprudence on RTBF remains nascent, courts have increasingly recognized the right to be forgotten, particularly in sexual harassment and criminal acquittal cases.[53] However, balancing individual rights with societal memory remains a contested domain, especially in the absence of comprehensive legislative clarity.

C. Role Of Technology In Implementing RTBF: De-Indexing, Anonymisation, And AI Filters

Technological intervention is central to the operationalization of the RTBF. De-indexing is the most widely adopted technical mechanism, wherein search engines remove links from search results associated with a person's name. Notably, de-indexing does not equate to content deletion; it merely obscures discoverability through search, which is often sufficient to address reputational harm. Anonymization and pseudonymization serve as additional layers, particularly in contexts like academic databases, legal judgments, or news archives. By redacting names and identifying details, these tools balance privacy with information retention. In India, for instance, judicial pronouncements in rape or POCSO cases are often anonymized in compliance with ***Section 228A of the IPC (now Section 72 of Bharatiya Nyaya Sanhita, 2023)***.[54]

[53] *X v. Union of India* [2021], [2021] SCC Online Del 3517.
[54] The Indian Penal Code 1860, s 228A, [Now Bharatiya Nyaya Sanhita 2023, s 72].

Emerging technologies like ***Artificial Intelligence (AI)*** and machine learning are being leveraged to automate RTBF processes, such as identifying harmful content, categorizing requests, and flagging eligible information for removal. While this offers scalability, it also introduces algorithmic bias and opacity concerns. AI filters may lack the contextual understanding needed to differentiate between private irrelevance and public relevance, thereby raising new ethical and legal challenges.[55] Moreover, blockchain-based data storage presents a technological paradox to RTBF. By design, blockchain is immutable, making data deletion technically impossible. This directly contradicts RTBF principles, indicating that technological architectures must evolve alongside legal norms to ensure compatibility between innovation and rights.

D. Stakeholders' Perspectives: Media, Tech Platforms, And Public Authorities

The RTBF implicates a broad constellation of stakeholders, each with competing rights and interests. Media outlets often resist RTBF on grounds of press freedom and the public's right to know. They argue that historical accuracy, accountability journalism, and archival integrity are fundamental to democratic discourse. A blanket RTBF, they claim, could facilitate selective amnesia that distorts collective memory and weakens scrutiny of power.

Tech platforms, particularly search engines and social media intermediaries, are frequently tasked with balancing privacy requests with free expression. The European Court of Justice's decision in the Google Spain case effectively turned private corporations into arbiters of fundamental rights, a role many argue they are neither equipped nor democratically accountable to fulfill.[56] Public authorities, including data protection regulators and courts, often struggle to articulate consistent standards for RTBF application. In jurisdictions with limited digital infrastructure or data literacy, the enforcement of RTBF is hampered by logistical, jurisdictional, and procedural barriers. Furthermore, public agencies maintaining digital records, such as courts or electoral commissions, must grapple with the implications of redacting legally or historically relevant data. Finally, civil society plays a watchdog role in ensuring that RTBF is not misused to whitewash records or

[55] Sandra Wachter et. al., 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7(2) International Data Privacy Law <https://doi.org/10.1093/idpl/ipx005> accessed 12 September 2026.
[56] *Google Spain SL v. Agencia Española de Protección de Datos,* Case C-131/12, ECLI:EU:C:2014:317, 2014 E.C.R. I-317 (CJEU).

suppress dissent.

VI. COMPARATIVE LEGAL ANALYSIS

The Right to Be Forgotten (RTBF), which reflects the continuous conflict between society's need to preserve public discourse and memory and an individual's right to informational autonomy, has become a key element of digital privacy legislation. This chapter critically analyzes the RTBF frameworks in the US, UK, and EU with the goal of providing insights for India's changing legal environment.

A. European Union

With ***Article 17 of the General Data Protection Regulation (GDPR)***, which creates the "right to erasure," the European Union has created the most reliable and legally binding version of RTBF. A person may request the deletion of personal data under certain conditions, such as when the data is no longer required, the person withdraws consent, or the processing is illegal, according to this clause.[57]

The Google Spain SL v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González (2014) case resulted in a historic ruling that established RTBF in the EU. According to a ruling by ***the Court of Justice of the European Union (CJEU)***, search engines are legally responsible for processing personal data that appears in search results since they are "data controllers".[58] In this instance, the Court decided that even if the original content is still legally available online, anyone might ask for links to information that is "inadequate, irrelevant, or no longer relevant" to be removed from the list.

The CJEU created a framework for striking a balance between the public's right to information (protected by Article 11) and the individual's right to privacy (covered by Articles 7 and 8 of the EU Charter of Fundamental Rights) in order to reconcile RTBF with freedom of speech.[59] The type of information, its historical significance, and whether the data subject is well-known all have an impact on this balance. In order to maintain uniformity and openness, the Article 29 Working Party—later replaced by the European

[57] 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, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 17, 2016 O.J. (L 119) 1.
[58] *Supra Note 55.*
[59] *Ibid.*

Data Protection Board—issued guidelines suggesting a case-by-case evaluation for RTBF allegations and stressing that controllers (like Google) should document and defend delisting decisions.[60]

Crucially, although the EU model gives people authority over their online persona, it has raised concerns about the transfer of judicial-like duties to private internet companies, who must now do intricate rights-balancing analyses.[61] However, while developing more intricate RTBF enforcement procedures, India might take inspiration from the EU model, which provides a legally sound and procedurally sound framework.

B. United Kingdom

Following Brexit, the UK-GDPR preserved the right to erasure under Article 17 by retaining GDPR provisions. In keeping with the common law tradition, UK courts have handled RTBF by placing more emphasis on judicial discretion and contextual balance. In this regard, ***NT1 & NT2 v. Google LLC (2018)*** is a crucial case that involved two people who wanted ties to past criminal convictions to be removed.[62] The High Court allowed the RTBF claim for NT2, who was involved in a less serious felony and had shown rehabilitation, but refused the claim for NT1, who had committed substantial financial fraud and showed no remorse. The Court applied a **three-factor test** that has since become a hallmark of UK RTBF adjudication:

a) The **nature and seriousness** of the offense,

b) The **public interest** in continued access to the information,

c) The **degree of rehabilitation** and the time elapsed since the event.[63]

Adapted to UK common law doctrine, where judges use precedential reasoning to assess conflicting rights, this test reflects the proportionality-based balancing of the EU. The UK

[60] Data Protection Working Party, Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc v. AEPD and Mario Costeja Gonzalez" (WP 225), 14/EN, 2014, art. 29.
[61] Julie E. Cohen, 'What Privacy is For' (2013) 129(117) Harv. L. Rev. <https://harvardlawreview.org/wp-content/uploads/2013/05/vol126_cohen.pdf> accessed 18 September 2025.
[62] NT1 & NT2 v. Google LLC [2018] EWHC (QB) 799 (Eng.).
[63] Emily Laidlaw, 'The United Kingdom's Right to Be Forgotten Cases: NT1 & NT2 v. Google LLC' (*Oxford University Press Blog*, May 8 2018) <https://blog.oup.com/2018/05/right-forgotten-cases-nt1-nt2-google/> accessed 18 September 2025.

model provides a workable way forward from India's perspective by offering a flexible legal norm based on context and judicial interpretation rather than codifying a strict rule.

C. United States

In stark contrast to the EU and UK, the **United States does not recognize a formal Right to Be Forgotten**, largely due to the constitutional supremacy of the **First Amendment**, which safeguards freedom of speech, press, and public access to information. As a result:

a) There is **no comprehensive federal RTBF law**,

b) RTBF-like mechanisms are limited to **sector-specific statutes**, such as laws enabling the **sealing or expungement of juvenile records**, and

c) Some states, notably **California**, have introduced **partial data privacy rights**, like the **California Consumer Privacy Act (CCPA)**, which includes limited rights to delete personal data but excludes public record content.[64]

Erasure, even when warranted by facts, is often seen as a danger to public openness and historical integrity in American legal culture. Individual privacy is frequently trumped by the public interest due to the marketplace of ideas theory and the constitution's predisposition toward transparency.[65] Therefore, the U.S. model should serve as a warning to India: overprotecting speech might expose people to digital stigma for the rest of their lives, particularly in a setting where social rehabilitation is essential.

VII. RECOMMENDATIONS AND CONCLUSION

A. RECOMMENDATIONS

a) Policy And Legislative Suggestions

India lacks a comprehensive framework to operationalize the Right to Be Forgotten (RTBF) in a consistent and enforceable manner. While the Digital Personal Data

[64] Omer Tene & Jules Polonetsky, 'Privacy and Big Data: Making Ends Meet' (2013) 66(35) Stan. L. Rev. Online <https://review.law.stanford.edu/wp-content/uploads/sites/3/2016/08/PolonetskyTene.pdf> accessed 20 September 2025.
[65] *Supra Note 40.*

Protection Act, 2023 gestures towards data erasure rights, it fails to clearly articulate RTBF as a standalone right balancing personal dignity and public interest. Future legislative efforts must codify RTBF as a statutory right, incorporating principles of necessity, proportionality, and fairness. Specific amendments in the Information Technology Act, 2000 and alignment with international jurisprudence are crucial to provide legal clarity, procedural safeguards, and enforceability.

b) Balancing Model: Criteria For Granting RTBF Without Suppressing Legitimate Public Interest

A normative balancing model is essential to prevent RTBF from becoming a tool of censorship. Courts and data protection authorities should assess each request based on defined criteria: the nature of the information, its relevance to public life, the role of the data subject (public figure vs private individual), the time elapsed since publication, and whether the information serves a journalistic, academic, or archival purpose.

c) Need For Institutional Mechanisms and Safeguards

Establishing independent Data Protection Authorities (DPAs) with quasi-judicial powers is vital for adjudicating RTBF claims. These bodies must be equipped with procedural standards, appellate mechanisms, and technological expertise to navigate complex privacy claims in the digital environment.

d) Role of Awareness, Education, and Responsible Digital Citizenship

The effectiveness of RTBF is not solely contingent on legislation but also on public consciousness. Digital literacy campaigns must emphasize individual responsibilities in data sharing, understanding consent, and the long-term footprint of online actions. Awareness of rights under data protection laws, and training in responsible digital conduct, can reduce the demand for post-facto data erasure by cultivating proactive digital behavior. Schools, workplaces, and civil society must be involved in embedding these values early on.

e) Reaffirmation of The Balance Between Privacy, Free Speech, And Archival Rights

RTBF must not exist in isolation but be integrated into the constitutional matrix

balancing Article 21 (Right to Privacy) with Article 19(1)(a) (Freedom of Speech) and the right to information. Judicial interpretation must evolve to create a harmonized approach, recognizing privacy as a dynamic and situational right, not an absolute claim to erasure. Further, safeguarding archival rights—particularly in academic, legal, and historical contexts—is essential to preserve the integrity of the public record.

VIII. CONCLUSION

The Right to Be Forgotten has become one of the most debated and significant digital rights in modern constitutional and data protection discussions. In an age characterized by data permanence, algorithmic amplification, and relentless digital memory, the law must address a crucial question: should persons be eternally linked to their history in cyberspace, regardless of time, change, or rehabilitation? This article illustrates that although India has made significant progress in acknowledging informational privacy—especially through judicial advancements and the implementation of the Digital Personal Data Protection Act, 2023—the Right to Be Forgotten is still insufficiently defined and inconsistently applied.

The DPDPA, though progressive in its emphasis on consent, erasure, and data minimization, stops short of expressly codifying RTBF as an independent right. As a result, its implementation relies on the discretionary interpretation of courts and the Data Protection Board of India, which raises problems regarding inconsistency, confusion, and uneven access to remedies. Judicial rulings, particularly in cases concerning acquitted individuals, survivors of sexual offenses, and marital conflicts, indicate a developing rehabilitative and dignity-focused methodology. This jurisprudence is fragmented and highly fact-dependent, highlighting the necessity for a cohesive statutory framework.

The constitutional conflict between RTBF and press, expression, and archival preservation rights is equally important. The article lays down that an unrestricted right to erasure runs the risk of undermining journalistic accountability, historical continuity, and democratic transparency. On the other hand, an absolutist dedication to free expression disproves the temporal nature of human fallibility, undermines reintegration, and sustains digital stigma. Therefore, the answer is to institutionalize a rational balancing mechanism based on proportionality, public interest, relevance, and the status of the data subject rather than giving preference to one right over another.

Comparative analysis from the US, UK, and EU highlights the value of procedural protections, contextual adjudication, and restricted de-indexing as opposed to complete removal. While keeping in mind its own constitutional principles, socio-digital realities, and developmental priorities, India must take inspiration from these examples. In the end, the Right to Be Forgotten should serve as a tool of digital dignity rather than a censorship tool, allowing people to go on without changing history and balancing privacy with accountability, free speech, and collective memory.