WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Social Media and the Right to Be Forgotten: Navigating Content Moderation and Free Expression in 2025

Ravina Dahiya [*] ***Dr. Anjali Dixit*** [**]

SRM University, Delhi-NCR, Sonepat, Haryana

ABSTRACT :

One big legal and ethical question that finds itself at the intersection of privacy, content moderation, and free expression asks to be discussed in the RTBF scenario, especially vis-à-vis social media platforms. This article further delves into the evolving scenario of RTBF, especially taking into account the Indian backdrop, where the constitutional guarantees of Articles 19(1)(a) and 21 strike a delicate level of harmony between human dignity and public discourse. Consideration is given to international legal developments, comparative jurisprudence, along with the Digital Personal Data Protection Act, 2023 of India-hence, with special note of Section 12(2)(a)-in order to understand the operationalization of RTBF amid growing rage over digital harm and algorithmic governance. Methodologically, the approach that is adopted is interdisciplinary, as it examines pertinent legal texts, judgements, and platform policies to locate RTBF as operationalized, contested, and interpreted across the globe. A strong focus is put on content-moderation methodologies, AI-powered decision-making, and jurisdictional balkanization faced at the social media platforms. The key findings state that, at the user level, RTBF does provide a window wherein one can strive to regain control of their online identity, but inconsistent enforcement let the whole thing down, creating yet another legal grey area by way of conflicting legal regimes, situational technological drawbacks, and the state's lack in accounting for platform governance. RTBF can aptly go against interests of the common man as a tool of the powerful to cleanse government records; hence, stronger safeguards for transparency in democracy have to be sought. The other implication from the current work then recommends that India should implement a principled, procedurally binding framework for RTBF, embedding guarantees for fairness, human review, and technological accountability to ensure in a digital democratic setting both the right to privacy and the right to know.

Keywords: Right to Be Forgotten, Digital Privacy, Content Moderation, Free Expression, Social Media, Indian Constitution, Artificial Intelligence, Data Protection Act 2023

Introduction

Paradoxically, 2025 also witnessed the increased spotlight on the interface between social media and the RTBF. However, in the modern era, the internet users generate significant personal data among themselves across several platforms and self-limiting their own access to this data has been a cause of concern. With the now expansive domains of user-generated content, people seek legal avenues to erase derogatory information or information that is outdated and may infringe on their privacy, worthiness, or even professional credibility. The discourse in itself achieves new levels of complexity when thrown into the discussion of free speech, content moderation, and the responsibilities of tech platforms, for in view of the RTBF, a set of opposing values of individual privacy and the collective right to free expression come together, giving rise to complicated legal, ethical, and technological problems. In India, with the increase in digital literacy and internet use, it has thus become essential to carve out a nuanced legal position on RTBF respecting individual dignity while maintaining public interest and transparency. As courts, legislators, and social media platforms grapple with the issue, the necessity for a structured and contextually contextualized understanding of RTBF becomes grounded.[1]

The year 2025 witnessed an increased interfacing between social media and the right to be forgotten. As internet users produce huge quantities of personal data across many platforms, the issue of having control over those data has only gathered attention with time. With the increase in user-generated content, the issue of erasing information that they consider injurious or outdated and is compromising their privacy, dignity, or sometimes choices to go to a good college or in finding work is increasingly coming to the fore. This becomes a tough conversation once you bring freedom of speech, content moderation, and obligations of tech platforms into the mix. The RTBF bastion rests on the uneasy boundary between individual privacy and free expression rights of the collective, posing a host of legal, ethical, and technical challenges. Entering India, with the rise of digital literacy and internet penetration, tremendous pressure in favor of a nuanced approach to RTBF, one that can preserve at least some degree of human dignity without watery it down with considerations of public interest and transparency, can be seen. While courts, legislatures, and social media platforms are eying the resolution of RTBF problems, much more urgent is the need for establishing an organized and context-specific sociopolitical understanding of RTBF.

---

[*] Student, LL.M. (Master of Laws), SRM School of Law, SRM University, Sonepat, Haryana, India.

[**] Associate Professor, SRM School of Law, SRM University, Sonepat, Haryana, India.

[1] Astha Srivastava, "The Right to Be Forgotten in the Indian Digital Sphere: Navigating the Fine Line Between Privacy and Free Expression in 2025", *available at:* https://lawfullegal.in/the-right-to-be-forgotten-in-the-indian-digital-sphere-navigating-the-fine-line-between-privacy-and-free-expression-in-2025/ (Visited on March 14, 2025).

Definition and Origins

The Right to Be Forgotten (RTBF) enables individuals to request the deletion or de-indexing of their personal information from activities that take place in the cyberspace, under certain conditions such as when it no longer serves a purpose, has become irrelevant, outdated, excessive, or offensive. The right of erasure does not provide an absolute right to erase all digital traces. Instead, it inserts a test of proportionality weighing on private interest and public interest, along with the freedom of expression and journalistic freedom. The legal formulation of the right was first conceived in Europe through the 2014 judgment in "*Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González*[2] (Case C-131/12)". In that case, the Court of Justice of the European Union determined that search engines act as data controllers and have the obligation to disallow all links whose content is no longer relevant in terms of personal data or is necessary for the purpose for which it had been originally collected. Such a judgment therefore paved the way for the RTBF being co-opted into larger data-protection regimes, in particular, the "General Data Protection Regulation (GDPR)", through which it received a statutory basis under "Article 17" as the "right to erasure." The conceptual basis for the same was founded upon principles of human dignity and information self-determination. In the Indian legal regime, the principle is still germinating, primarily through the courts and the provisions under the "Digital Personal Data Protection Act, 2023", under "Section 12(2)(a)", which recognizes a data principal's right to request erasure of his/her personal data where the purpose of processing it no longer exists. Despite this, the internal jurisprudence of India is still sparse on RTBF, thereby casting uncertainty as to its application, especially with respect to digital archives and social media platforms.[3]

Importance in the Digital Age

The RPIG (Right of Persons Interested Groups) is legally granted to individuals to request deletion or deindexing of the personal data from the online space when the data in question is considered irrelevant, outdated, excessive, or damaging to the individual. So it cannot be legitimately cited as the right to erase every single trace one has ever left online; rather, it introduces a proportionality test in which the private interest is balanced against the unique public interest, freedom of speech, and journalistic freedom. Initially, the legal expression found through the European avenue was given in the 2014 judgment in Google's (Germany) "*Google Spain S.L., Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González*[4] (Case C-131/12)". The Court of Justice of the European Union, in that case, found that the search engine constituted a controller of data in a personal nature; thus, they had to comply with the removal of links to data deemed to be no longer relevant or necessary for the purpose for which it was originally collected. This laid the framework of the integration of RTBF within the larger data protection regimes such as the "General Data Protection Regulation (GDPR)" and in particular within "Article 17", which gave formal existence to this right as the "right to erasure". The conceptual justification was based on human dignity and informational self-determination. However, in the Indian legal system, this concept is still finding its way, primarily through the judiciary and provisions in the "Digital Personal Data Protection Act, 2023", especially under "Section 12(2)(a)", which recognises the right of a Data Principal to the erasure of personal data when the purpose of processing it ceases to exist. Yet, the lack of concrete jurisprudence on RTBF is a hindrance to its application in India at large, especially concerning digital archives and social media platforms.[5]

The Conflict Between Privacy and Free Expression

Today sets an ecosystem online where social media venues hold a vast digital history, often permanent, in its grasp. An airing of a single tweet or comment coming back after years may destroy careers while allowing relationships to go down the nail, and in certain cases, mental wellbeing alone. Such a permanence of the digital world only spells urgency for the RTBF. Platforms like X, Facebook, and Instagram do allow almost instantaneous sharing but have no mechanisms to take down once seeded into virality, nasty content. The year 2025 has made matters worse with AI-generated content, deepfakes, and algorithmic pushing blur the lines of control-shadows on false or harmful information-Losing sight of RTBF only affects a user's power to seed his or her online presence. While established grounds of privacy rights confined themselves to physical intrusions and intervals, nowadays, extensions to include informational privacy are called for. An informational privacy idea brokers when they can access one's personal information, for how long, and sit with it. The "Digital Personal Data Protection Act, 2023" is an attempt to address this by allowing data principals to request the erasure of their data. The RTBF of 2025 thus remains relevant for empowering the user to control their narrative in the public domain and to cultivate accountability among the platforms. Yet the question remains: how does one enforce it and reconcile it with freedom of speech under "Article 19(1)(a) of the Constitution of India", especially when the content is a matter of public interest, critique, or history?

Overview of the Tension

As societies have become more dependent on digital infrastructure for communication, commerce, and civic engagement, the confrontations between privacy and free expression have been deepening. In the age of algorithm-driven platforms where the content consumption is put into auto-pilot through automated curation, these tensions become all the more aggravated. Right to be Forgotten (RTBF), which empowers individuals to initiate the removal of aged or harmed information, often conflicts with the constitutional guarantee of free speech and expression under "Article 19(1)(a) of the Constitution

[2] Case C-131/12.

[3] Hannah Perry, Sumaya Nur Adan, et.al., Advancing Digital Rights in 2025: Trends, Challenges, and Opportunities in the UK, *EU and Global Landscape* 233 (Demos, London, 1st edn., 2025).

[4] Supra note 2.

[5] Grant Lapping, "Social media is at the crossroads of free speech and regulation", *available at:* https://themediaonline.co.za/2025/03/social-media-is-at-the-crossroads-of-free-speech-and-regulation/#google_vignette (Visited on April 2, 2025).

of India." The longer the memory of the internet, the more contributing any user posting, image, or article would become toward the digital repository that is often accessible indefinitely. This basically becomes detrimental to one's need to rightfully forget an error in judgment, irrelevant details, or simply unwarranted digital oppression. In the meantime, when a complaint is made for removal, even when the affected data subject has requested it, the removal of such content can intervene with at least being in the right to gather such information from others-veritably, the journalists, research scholars, and even the general populace. Hence, RTBF ultimately does not stand alone but directly intersects with democratic principles of transparency, openness, and accountability. This sub-section seeks to explore some aspects of this double bind frame in shaping legal discourse, particularly so in the area of social media in India, wherein the implication of such rights stands to be immediate at the widest level.[6]

Why IT Matters on Social Media

The conflict between the RTBF and the freedom expression emanates precisely because of the nature of online content, which can be easily copied, stored, and transferred within time and space. Upon invoking the RTBF, the individual is basically attempting to limit the circulation of certain types of personal data, whether they be true, defamatory, or lawful but harmful. Sometimes, this could lead to removing content that is part of a greater public record or has relevance in a public dialogue. Herein is the legal paradox: for one person something is private; for many it is important. Reports of past criminal accusations, old blog posts about controversial opinions, or historical records of litigation would all be subject to removal requests, thus raising the issues of censorship and tampering with public narratives. This scenario, now, is further complicated by social media platforms. A social media platform is not a mere passive conduit but in fact moderates contents on a huge scale, and its policies, algorithm, and moderation practices massively impact on how online discourse proceeds. When the RTBF is invoked to delete posts or de-index links, all that the platform may want to balance against is its public responsibility of free speech and preservation of content. The judicial framework perceives the challenge of addressing such requests not just in terms of an individual's right to privacy under "Article 21 of the Constitution of India" but also under the broader rights of society to know. The "Digital Personal Data Protection Act, 2023" addresses this through qualified rights. A Data Principal may request deletion of personal data when it is no longer necessary for the purpose it was collected under "Section 12(2)(a)." However, "Section 7" of the same Act provides for exceptions to these, on grounds of legal obligations and public interests, thus setting out a framework by which these contradictions shall be weighed on a case-to-case basis.

Legal Framework of the Right to Be Forgotten

The social media interface versus the right to be forgotten gained prominence in 2025. With the massive production of personal data by internet users on various platforms, the control over such aspects of this data gained mass attention in the Indian context with the passage of time. With the growth of user bloggers, people are increasingly looking for some sort of remedy available to delete information that they consider private, harmful, or embarrassing, affecting their reputation or livelihood. The matter becomes all the more complicated when freedom of speech, content moderation, and responsibilities of tech platforms enter the fray. RTBF sits at the perilous junction of individual privacy and rights to free expression of a collective, raising legal, ethical, and technical challenges. With India poised to increase its digital literacy and internet penetration numbers, there emerges a strong need for a nuanced position on RTBF that safeguards personal dignity without sacrificing public interest and transparency. While courts, legislatures, and social media are all currently looking for solutions, the need for an organized and contextualized understanding of RTBF is ever dire.[7]

International Perspectives

The Right to Be Forgotten has slowly grown from a fresh idea of judicial interpretation into a dominant theme in data protection laws the world over. It derives from the common acceptance of informational privacy, through which people have the right to exercise partial control over the disclosure and handling of their private data, especially in cyberspace. Once controversial due to conflicts with freedom of expression and integrity of archives, now RTBF has entered mainstream debates in different jurisdictions. Legislators and judges are challenged to make laws and interpret existing provisions in such a way that the RTBF is supported without compromising democratic values or without providing a tool for censorship of information. These concerns render legislative clarity, procedural safeguards, and definitional standards necessary. Taking cues from global patterns, India must attempt forging its path on RTBF, especially under the ambit of the "Digital Personal Data Protection Act, 2023", as well as constitutional rights under "Articles 19 and 21 of the Constitution of India." Hence, it is imperative to look at how the right was shaped legislatively in other jurisdictions and the implications for the practical/litigation thrust on social-media platforms around the globe to get a corporate understanding of how the right would proceed forward.[8]

European Union (GDPR)

The most thorough legal system for RTBF, provided by the European Union, is found under the provisions of the "General Data Protection Regulation (GDPR)" and, more specifically, under "Article 17". This submission is referred to as the "Right to Erasure", and under it, an individual may request to have personal data of his erased when it no longer serves the purpose for which it was collected, when consent is withdrawn, or when it is processed unlawfully. Also, it protects the situation where the individual objects to processing and where erasing the data is necessary to fulfill a legal obligation. On its side, "Article 17(3)" clearly states that there exist some exceptions that protect freedom of expression and public interest, such as by not erasing

[6] Thiago Dias Oliva, "Content Moderation Technologies: Applying Human Rights Standards to Protect Freedom of Expression", 20 *HRLR* 615 (2020).

[7] Li Lin, Zhou Kai, "When Content Moderation is Not About Content: How Chinese Social Media Platforms Moderate Content and Why It Matters", 0 *NMS* 112 (2024).

[8] Valentina Grippo, *Regulating Content Moderation on Social Media to Safeguard Freedom of Expression* 203 (Council of Europe, Strasbourg, 1st edn., 2024).

data if the retention of such data is necessary for the exercise of the right of freedom of expression, to comply with a legal obligation, or for the performance of a task carried out in the public interest. This balancing act tries to reconcile the concept of private life with broader societal interests. Due to the extraterritorial nature of the GDPR and the weight it carries in shaping global platform compliance, there is a considerable influence of this act worldwide. Google, Meta, and X have all spearheaded the development of internal mechanisms to handle erasure requests from countries lacking their own laws. While there is a legal framework provided for within the GDPR for RTBF, the solution is actually to be found in its application in real life cases, especially those where competing rights like press freedom and public access to information are at stake.

United States

The European Union provides the most exhaustive legal framework for RTBF within the "General Data Protection Regulation (GDPR)", in particular, "Article 17." This provision, entitled "Right to Erasure", gives individuals the right to request the deletion of their personal data when it is no longer required for the purposes for which it was gathered, when withdrawal of consent occurs, or when the data is unlawfully processed. The law also governs situations in which the data subject objects to the processing or if the data must be erased in order to fulfil some kind of legal obligation. Of special note is "Article 17(3)", which provides a series of exceptions safeguarding freedom of expression and the public interest, where for example, data cannot be erased upon a claim of erosion if its retention is necessary for exercising the right of freedom of expression, for compliance with a legal obligation, or for the performance of a task carried out in the public interest. This underlines the balancing act the law has attempted in setting priorities between personal privacy and broader societal interests. The influence of the GDPR has transcended political boundaries, owing to the extraterritorial reach it commands and its ability to set standards upon which global compliance by platform companies occur. Companies such as Google, Meta, and X have designed their internal mechanisms to handle such erasure requests even in jurisdictions that do not offer similar legislations. While GDPR attempts to give an implementable legal framework for RTBF, the bill touches on thorny problems that challenge its application in practice, especially when competing rights such as those of press freedom and access to public information become an issue.[9]

Other Jurisdictions

At the federal level, the United States does not acknowledge RTBF mostly due to First Amendment federal constitutional provisions related to the protection of free speech. The American legal culture values open discourse and the free flow of information to an extent that any attempt to block access to truthful information becomes deeply contentious. There exists, indeed, a strong presumption in the legal sphere in favour of public access to information, particularly when it touches public figures, criminal records, or matters concerning the public. Nevertheless, some state statutes may afford limited rights to deletion of data. The CCPA, derived from the California Consumer Privacy Act, for example, affords to such consumers the right to request the deletion of personal information concerning them collected by a business under Section 1798.105(a)(1). This right is not absolute, as there are exceptions to it, such as where retaining the data is required by law, is necessary to detect security incidents, or there is a free speech claim. CCPA shows a cautious American jurisprudential interest in privacy rights that are still evolving. Nevertheless, these rights do not constitute a full RTBF and are, in fact, usually qualified as consumer rights rather than fundamental ones. Erasure requests made to social media companies, which operate in the U.S., are usually declined unless there is a clear statutory requirement or a breach of their platform policies. All of this makes it clear that the deep philosophical divide between the U.S. and jurisdictions like the EU has privacy mostly on one side and unregulated speech on the other.[10]

Key Provisions and Sections

Numerous countries have enacted legislations either mirroring or following the RTBF in a multitude of ways outside the European Union and the United States. In Canada, the Privacy Commissioner has recommended that a right to de-indexing should exist under current federal privacy law; however, this has not yet been codified into legislation. Some provinces have shown interest in improving protection of digital privacy, particularly in response to challenges posed by data retention on social media. In parts of Asia, which include Japan and South Korea, courts have ordered content removal in cases involving serious damage to a person's reputation, especially where the information has no public interest. These decisions, however, are applied on a case-by-case basis and lack broad application akin to the EU. One interesting example is the California Minor Erabler Law, which allows minors to request the deletion of content they have posted on any website or app, essentially granting them a limited RTBF. This law intends to keep minors from negative consequences of reckless digital behavior and acknowledges the changing nature of identity and maturity. The patchy legal development thus indicates that while RTBF is developing traction, its enforcement remains uneven. Without harmonization between jurisdictions, global social media platforms are confronted with legal ambiguity as they have to process data subject requests pursuant to diverging legal standards, and yet at the same time guarantee consistency, transparency, and trust from users.[11]

Social Media Platforms and Content Moderation

Right up to 2025, the intersection of the RTBF and content moderation over social media will be one of the big, lingering digital governance issues. Platform designs of the likes of X, Facebook, and Instagram allow for the ceaseless user interaction and data sharing but also store large quantities of personal content that users might want to remove some day. The RTBF aims at giving a user some control over their digital identity. However, the social

[9] Asad Abbas, Antonio Torralba, Content Moderation in the Age of AI: Navigating the Trade-offs Between Free Speech and Privacy 144 (ResearchGate, 1st edn., 2024).

[10] Social Media Marketing, available at: https://www.gwi.com/blog/social-media-marketing (Visited on March 12, 2025).

[11] Freedom of Expression, available at: https://dig.watch/topics/freedom-expression (Visited on March 6, 2025).

media platform landscape, with its decentralized, peer-to-peer, and cross-jurisdictional nature, makes enforcement problematic. These very platforms may have provided a platform for public discourse but are also capable of perpetuating outdated and damaging narratives, thus impairing users' ability to sever ties from compromised past actions or irrelevant information. To get things done with RTBF enforcement on social media platforms, there needs to be a delicate balance of policy expertise, intermediary compliance, and ethical reasoning. There have been some patchy attempts of adaptation enforced with obligations arising out of data protection legislations such as the Digital Personal Data Protection Act, 2023, and the European Union's GDPR. There also needs to be a continuous balancing act during content moderation activities-whether in the intervention by human teams or back in the systems themselves: one that does not undermine personal privacy on one side and public discourse on the other. We will now look at how the platforms have dealt with RTBF requests, and observe the key issues that they face in the process.[12]

How Social Media Handles the Right to Be Forgotten

In 2025, an intersection between right to be forgotten and social media content moderation stands as one of the most pressing digital governance issues. Taking into consideration the platform-side infrastructure, both the likes of X, Facebook, and Instagram serve foremost with continuous user engagement and data sharing but at the same time create enormous storage for personal content that might translate into user desire for erasure. While the RTBF seeks to provide some degree of control over one's digital identity, social media platforms emphasize the enforcement convolutions with their decentralized, user-driven, and transnational nature. The same spaces that allow public dialogue can also be used to keep alive narratives that some might consider outdated or unfair; a factor that hinders one's power to dissociate from the acts or data that have now become irrelevant. Enforcement of the RTBF on these platforms, thus, calls for complex regulatory, legal, and ethical insights. Certainly, data protection laws have given these platforms little choice but to evolve, yet, adapting has come in fits and starts, and even much yet to be desired. Content moderation, if carried out through human or computer-based systems, must be forever readjusted inside complex competing requirements so as not to devastate either private space or public discourse. In this section, we will see how social media platforms have handled the claims of RTBF and the peculiar challenges thereof.

Policies of Major Platforms

Platform-specific policies reveal the disparate measures taken to accommodate RTBF-esque functions. X, formerly Twitter, offers deletion tools for accounts and content removal, permitting users to unpublish posts from the timeline or limit their visibility. However, no formal RTBF mechanism exists on X allowing data erasure beyond that which the user may activate through personal control measures. This transfers the responsibility completely onto the user, overlooking the situation wherein the content has been reshared, quoted, or preserved elsewhere. Facebook and Instagram, on the other hand, under Meta corporate, provide a greater magnitude of controls through their "Access Your Information" portals, enabling users to view, download, and delete data in batches. The Meta privacy policy speaks of data deletion but rather as a user right within their service framework than as a legal obligation under RTBF. Requests specific to RTBF are usually handled under the general data protection policies of Meta, wherein a legal review may be required depending on jurisdiction. Although, since the passing of the more stringent data protection laws, these systems have, to an extent, become more receptive to requesters of data erasure, their responses are still fragmented and sporadic. Users experience automated denials, notices without any timeline, or undetailed or ununiformed policy reasoning applied citing that it is in "public interest" to reject privacy rights. This patchiness represents the larger problem of implementing universal privacy rights on platforms that operate globally and yet, have patchy legal and cultural standards in each region.[13]

Challenges in Implementation

International legal frameworks around RTBF span a constellation of approaches-from wide-ranging guarantees of personal privacy in the European Union (EU) to speech-centric regimes in the United States. Very different approaches mirror existential cultural-constitutional commitments, placing the EU on the side of human dignity and protection of data and the U.S. on the side of free speech through the First Amendment. Canada and various Asian countries take a different road in this respect, making the landscape of such laws fragmented. This disparity creates huge barriers to social media companies interlinked on a global scale but carving them with local, possessing laws. Also, the enforcement mechanism and the procedure of invoking RTBF may differ, thereby creating conflicts of law in requests involving cross-border data. With such divergences at the global level, the call-fashioned to adapt India's RTBF not only through local constitutional values but also in a manner that responds to international legal developments and technological capabilities stands out. It is the appreciation of these considerations that is crucial in sighting the limitations and strengths of RTBF in the digital age.

The Role of Algorithms and AI in Content Moderation

Human moderation becomes insufficient when real-time consideration is given in RTBF cases, as social media content among others increases exponentially. Some AI and ML solutions were sought by platforms to automate removal requests and delisting. These AI algorithms define content as legal, relevant, or harmful, often acting autonomously to initiate removal processes, including flagging for content removal. From here, automation inherently offers speed and coverage extended. However, the interesting question of fairness, accuracy, and explanations arises for debate on how automation is being carried out. An algorithm gets trained on past data, which could be rife with institutional biases or cultural presuppositions. These algorithmic systems, especially in India with many layers of social, linguistic, and political intricacies, should be conceived keeping local contexts in

[12] Wozayer Kabir, "Regulating Social Media: The Balance Between Freedom and Responsibility", *available at:* https://thelegalquorum.com/regulating-social-media-the-balance-between-freedom-and-responsibility-10/ (Visited on March 22, 2025).

[13] Content Moderation, *available at:* https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2023/06/GFoE_Content-Moderation.pdf (Visited on March 25, 2025).

mind. The danger lies in putting too much trust in these systems without strong human intervention- more so in the legally sensitive area of RTBF, wherein a decision has to be weighed with privacy, legal claims, and freedom of expression.[14]

Automated Delisting Requests

When viewed from a Real-Time Basis (RTBF) perspective, human moderation becomes limited due to exponential growth in content being uploaded on social media platforms. Therefore, platforms have attacked to an array of AI and ML tools to automate requests for deletion and delisting. These AI systems classify content as legal, relevant, or harmful and would sometimes take action by marking that content for removal with no human intervention. Automation gives rise to efficiency and coverage on a large scale but is weighed against serious issues of fairness, accuracy, and explainability. An algorithm is most often trained on historical data that might carry institutional biases or cultural assumptions. Algorithmic systems within the Indian landscape must be defined with sensitivity toward local contexts, which unravel rich social, linguistic, and political nuances. The bigger danger lies in trusting these systems too much without strong human auditing, especially in the legally sensitive RTBF domain, where decisions bear regard to privacy, legal obligations, and freedom of expression.

Bias and Errors in AI Systems

With the ever-mounting content in social media, the swift execution of RTBF requests by human moderators has become practically impossible. The channels therefore had to turn to AI and ML for partial automation of the moderation process-a process that considers removal and delisting requests. Ideally, these systems shall look at user content for teratogenicity, relevance, and potential harmfulness to flag it, but sometimes the systems themselves may act upon such content without human review. Automatic methods also raise some pretty important issues like fairness, accuracy, and explainability. Most of the algorithms will be trained on the available historic data that usually carries institutional bias in culture or cultural presuppositions. Algorithmic systems in India have to be designed keeping in view local nuances, given there is a richness and diversity in social, linguistic, and political minutiae. The risk here is indeed an overreliance on such systems sans strong human oversight, especially in legally sensitive areas like RTBF, wherein decisions weigh balancing privacy, legal obligations, and freedom of expression.[15]

Case Studies and Judicial Interpretations

In the dynamic environment of data privacy and digital expression, the right to be forgotten (RTBF), especially as it applies to social media content, is sculpted by judicial interpretations. Courts in various jurisdictions have been confronted with cases where they have to decide if an individual's claim to privacy, control of his personhood, and data erasure takes precedence over other interests such as freedom of the press, access to information, and public interest discourse. Such cases lay down critical precedents and principles of interpretation that affect legislative drafting, administrative implementation, and platform-level policy making. Jurisprudence generally outlines the scope and limitations of the RTBF and addresses the legal balancing acts required in each specific scenario. In India, the Supreme Court has recognised the right to privacy under Article 21 of the Constitution of India, thus providing an afflux whereby RTBF claims may emerge. Though the Indian courts have not yet adjudicated an all-encompassing ruling codifying RTBF, a comparative legal scrutiny of prominent cases from other jurisdictions serves to set the stage for the increasingly relevant debates within Indian courts, regulators, and social media platforms. The case law review below commences with the cornerstone European Union case that ultimately laid down RTBF as a formal concept and then moves on to present more recent United States cases that explore the contrasting lines between regulation of platforms and constitutional freedoms.

Landmark Cases

Judicial interpretations hold central sway in determining the contours of the RTBF, particularly with respect to content generated by social media. Courts worldwide face the task of acting in such a manner that selections of privacy, identity control, and data erasure by individuals may or may not need to stand against competing interests such as freedom of the press, access to information, and discourse of public interest. These cases serve as precedent, provide interpretative guidance in the drafting of legislation, administrative implementation, and the making of decisions at the level of platform policy. Jurisprudence not only defines the bounds and limitations of RTBF but also points out the legal weighing of competing interests in every fact-specific context. The Indian Supreme Court has recognised the right to privacy under "Article 21 of the Constitution of India", which laid the foundation for claims under RTBF to rise. Even though the Indian courts have not yet pronounced on RTBF directly, comparative legal scrutiny of principal cases from other jurisdictions helps frame the argument that grows more relevant for Indian courts, regulators, and social media platforms. The ensuing review of case law begins with the landmark European Union judgment, which began the formal recognition of RTBF and then moves to recent cases in the United States that test the limits between platform regulation and constitutional freedoms.[16]

---

[14] Tackling Digital Safety Challenges to Create a Safer Online World in 2025, *available at:* https://www.weforum.org/stories/2025/01/tackling-emerging-harms-create-safer-digital-world-2025/ (Visited on March 4, 2025).

[15] Khalid Ali, Sandeep Arthur Kumar, *Navigating the Privacy-Freedom Dilemma: The Impact of AI on Content Moderation and Free Speech* 268 (ResearchGate, 1st edn., 2024).

[16] Hate Speech on Social Media: Global Comparisons, *available at:* https://www.cfr.org/backgrounder/hate-speech-social-media-global-comparisons (Visited on April 5, 2025).

Google Spain v. AEPD and Mario Costeja González

Judicial precedents act as the foundational pillars on which the juridical contours of the RTBF are laid. Courts have had to look into the complicated reconciliations between individual rights of privacy and collective rights to information, with outcomes formed differently according to the constitutions and statutory frameworks in force in each jurisdiction. In Nigeria and the European Union, for example, the right of privacy is fundamental; in America on the other hand, the First Amendment takes an upper hand whenever speech and information is involved. The manner of adjudging RTBF cases has formed either the national position or baulked the global corporate norms, specifically for transnational digital platforms. Such landmark cases also serve as conceptual reference points to burgeoning countries like India, where privacy rights enjoy constitutional protection under "Article 21" and digital governance is underpinned by the "Digital Personal Data Protection Act, 2023". The continued dinamism of digital life requires the translation of these judicial insights into Indian legal fora. Thus, the leading cases highlighted here are key in understanding how the courts have dealt with some of the thorny aspects arising at the nexus between data erasure rights and freedoms of expression, offering a pathway to future Indian jurisprudence.

Recent Cases (2024 −2025)

Recent case law, especially from the U.S., exemplifies the constant and agonizing friction between RTBF-like claims and free speech protections, with social media content moderation as a prime contemporary context. In "*Moody v. NetChoice, LLC*[17], the U.S. Supreme Court studied the constitutionality of two state social media laws, under which Florida and Texas purported to regulate the content moderation activities of platforms. While the Court did not treat the laws on their respective merits, it sent the cases back so that a proper First Amendment analysis could be made, thereby hinting at the importance of protecting speech in any form of regulatory regime vis-à-vis online platforms. This case reflects a broader resistance, within the U.S. legal system, to enforcement of RTBF-like measures since such measures are typically viewed as impermissible encroachments on editorial discretion and user speech. Such worries are particularly pronounced when state laws seek to coerce or forbid particular kinds of content-moderation behaviors. The refusal of the courts to uphold such laws suggests that any RTBF agenda in the U.S. would have extraordinary constitutional challenges stemming from the First Amendment's free speech and press freedoms.

Newer judicial developments, especially in the United States, show the ongoing tension between RTBF-like claims and free speech protections, particularly when it comes to content moderation on social media. In March 2024, the United States Supreme Court rendered a decision in" *Moody v. NetChoice*, *LLC*[18], upholding the legality of social media laws from Florida and Texas that aimed to regulate content moderation by platforms. The Court, however, did not decide the merits of the laws but remanded the cases for a proper First Amendment analysis, thus signaling that speech protections must occur at the very core of any regulatory approach to online platforms. The case epitomizes American legal resistance to enforce RTBF-like mechanisms because they are often considered as unconstitutional infringements on editorial discretion and user speech. This resistance is most starkly expressed when state laws seek to mandate or forbid particular practices of content moderation. Hence, the judicial reluctance to defend such laws spells an ominous future for any movement towards RTBF in the United States, mainly on constitutional grounds laying upon freedom of speech and press.

Analysis of Court Decisions

The judicial rationale in RTBF cases has majorly entered into the paradigm of right-interpretation and enforcement dramatic examples nationwide, particularly in the contexts of digital and social media. When a person wishes to delete or de-index personal data under conflicting scenarios posed by the rights of another person to access that information, the courts are compelled to address the legal, ethical, and technical conundrums. This balancing act has facilitated the appearance of a great array of legal adjustments dictated by the respective priorities in each jurisdiction, constitutional principles, or statutory safeguards. Indian courts are still in the early stages of honing their skills in dealing with RTBF claims while increasingly relying on international case law as persuasive authority. The judgments rendered by the Court of Justice of the European Union and various United States courts thus present opposing models of the debate, each compelling consideration of a different weight on fundamental rights. This divergence between the jurisdictions further illustrates the practical problems social media platforms are grappling with as they strive to put together a singularly compliant and ethically sound moderation policy. How the courts in the EU and the US weigh competing interests when deciding conflicts between privacy and expression gives pointers on the sort of doctrinal direction Indian courts will find themselves in need of when accounting for RTBF claims, most notably within the ambit of" Articles 19 and 21 of the Constitution of India" and the newly codified "Digital Personal Data Protection Act, 2023".

Balancing Tests

Judicial reasoning in the RTBF cases has contributed largely to how the right is constituted and enforced universally, also in respect to digital media and social media media. Courts, any time a request for erasure or de-indexing of personal data clashes with another's right to access such information, must resolve the various legal, ethical, and technological issues in the matter. This balancing act has led courts into an array of interpretations, often hinged on priorities within the jurisdiction, constitutional principles, and statute-based protections. Indian courts still being in the infancy of the RTBF claims trend now increasingly look toward foreign case laws as persuasive authority. The juxtaposition of decisions of the CJEU with those of different United States courts turn into two competing models, each emphasizing a different philosophy of fundamental rights. The split between jurisdictions highlights the conundrums encountered by social media platforms as they try to come up with the best consistent, legally, and ethically admissible moderation policy. Understanding how the courts in the EU and US apply balancing tests to privacy-expression conflicts shall enable one to predict the kind of doctrinal

[17] 603 U.S. ___ (2024).

[18] Supra note 17.

wiggle Indian courts might need to adjudicate RTBF claims under the auspices of Articles 19 and 21 of the Constitution of India and the newly codified Digital Personal Data Protection Act 2023.

Balancing Privacy and Free Expression

Balancing tests ensure, on the one hand, the existence of competing constitutional and statutory rights, and are the essential operation of RTBF adjudication. In the EU, the CJEU places great emphasis on privacy and data protection as fundamental rights under the EU Charter of Fundamental Rights. The courts use a balancing test, weighing the interest of an individual in the erasure of data versus the people's right to know. The considerations that usually guide this weighing include the type of data, the degree to which the data subject is a public figure, and the data's vitality to ongoing public discourse. Typically, when an individual is a private person and the information is no longer of public interest, the courts lean towards deletion. In contrast, the content may be kept when it relates to political activity or criminal accountability of the highest public interest. The 2019 CJEU judgment in *Google v. CNIL*[19] upheld the territorial limitation, whereby it was decided that while the RTBF was valid within the territory of the EU, it shall not per se extend to other territories. This territorial limitation stands in the way of automatic global de-indexing, thereby allowing platforms to localise compliance and to align with different statutory schemes. Whereas, in the US, courts have consistently placed a premium on the right to free expression, particularly under the First Amendment. Balancing tests used in US courts customarily start with a presumption in favor of speech and subject takedown requests based on privacy to rigorous scrutiny. The protections offered by the First Amendment are interpreted broadly to not only encompass direct speech, but also incorporate the right to receive and disseminate lawful information. Recent court proceedings, such as the ones dealing with state social media regulation laws, focus on editorial discretion by platforms as being protected speech. Such a well-established constitutional tradition reveals why a full-fledged Right to be Forgotten is legally impossible in the US. The difference in legal regimes marks these balancing tests as applied to RTBF[20]

Theoretical Frameworks

Historically, balancing rights in the sphere of law has tended to rest heavily on normative and theoretical bases that lay down the parameters of the stakes and scientifically opine why such rights are to be respected. There is a public concern that information disseminated both beneficially and harmfully, depending on how quickly and extensively it travels, can cause major effects. Therefore, lawyers or scholars tend to take an international human rights perspective or philosophical view that serves as a principled basis for weighing privacy against freedom of expression. These frameworks are not mere abstractions but, in reality, greatly influence how statutes are interpreted and public policies are formulated. Since both rights are constitutionally protected in India, such theoretical models become useful tools in judicial argumentation and provide further clarity to legislations whenever there is a need, especially in situations where the two rights come into conflict within the digital environment, such as on social media.

Human Rights Perspectives

Balancing rights in law usually begins with some normative and theoretical perspectives, grounded on the gist of interests under consideration and reasons for claiming something as a right. Without much interference from the digital world, however, because the speed and large scale of communication equally increase both the benefits and the harms of disseminating information. To counter this, legal academics and institutions resort to theoretical underpinnings from international human rights frameworks and arguments that justify the balancing of privacy and freedom of expression. These frameworks, in fact, are not purely abstract ideas that merely assist in the interpretation and application of other statutes, but in drafting public policy as well. In India, where both rights are constitutionally permitted, these theoretical frameworks assist in clarifying legislative and judicial intent, especially when conflicts come forth in digital contexts like social media.

Philosophical Arguments

International human rights are accepted as the fundamental rights through which the right to be forgotten is determined according to the dynamism of each incident involving balancing acts with free expression. Privacy and expression are recognized in the UDHR as fundamental rights. Article 12 of the UDHR rests that no one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence, while Article 19 grants the freedom of opinion and expression: including freedom to seek, receive, and impart information and ideas through any media and regardless of frontiers. These rights are also reiterated in the International Covenant on Civil and Political Rights, thus practically strengthening their implementation as equally essential rights in the international law domain. Several previous attempts of the United Nations to reconcile these rights at emerging circumstances include the Global Digital Compact of 2024, highlighting the need for digital spaces that are safe, inclusive, and respectful of privacy in tax for free expression. This finding insinuates that aside from the RTBF being an issue of dignity, it must not be degenerative into arbitrary censorship; rather, the weighing of erasing or retaining data shall rest upon necessity, proportionality, and accountability. It has strong implications in India, especially considering the Digital Personal Data Protection Act 2023, wherein the right to erasure granted under Section 12(2)(a) is subject to legitimate interest of state and public interest under Section 7. Henceforth, a flowing balance means not only individual assertions but also systemic protection against abuse to maintain democratic freedoms.[21]

---

[19] C-507/17.

[20] Joseph A. Cannataci, Bo Zhao, et.al., Privacy, *Free Expression and Transparency: Redefining Their New Boundaries in the Digital Age* 212 (UNESCO, Paris, 1st edn., 2016).

[21] Vishaka Suriyabandara, "Balancing the Conflict Between Right to Information and Right to Privacy Under Sri Lankan Fundamental Rights Perspective", 15 *SUJ* 173 (2016).

Practical Implications

From a conceptual perspective, RTBF acquires full significance only when conceived. The enforcement affects social media users, platform administrators, civil societies, and the state. If some types of injustices lead investors to RTBF protection, civil societies may be threatened that such deletions jeopardize transparency. However, social media platforms must weigh adverse domestic and international legal considerations that should be considered in an individual's request to maintain consistency in its operations and retain jurisdictional counsel. How stakeholders describe its successes or failures will, in turn, influence their perception of black-letter law in content moderation, AI decision-making, and jurisdictional fragmentation.

For Individuals

The theoretical foundation for RTBF attains complete significance only when it is actually conceived. Enforcement has differing consequences for the users on social media platforms, for platform administrators, for civil society, and for the state. Where there is injustice, investors seek RTBF protections, while civil society is threatened by such deletions as a threat to transparency. It is incumbent upon social media sites to balance considerations of both domestic and foreign law, so as to keep their own house in order, and thereby counsel the law. The manner in which the stakeholders have amalgamated the successes and failures will operate greatly upon their ability to see through the black-letter law to content-moderation, AI decision-making, and fragmentation of jurisdictions.[22]

For Society and Public Discourse

RTBF is crucial to guard individuals against the unwanted persistence of information online that serves no longer a lawful or beneficial purpose. For example, this can be the Internet version of revenge content, cyberbullying, misinformation, mistaken identity, or job search or election-related news reports resurfacing after more obvious events. Delisting or take down of such content may be the only course available for regaining control over one's digital identity. Legal jurisdictional variances however tend to affect the availability and efficacy of this right. In the E.U., through Article 17 of the GDPR, one may seek from platforms and regulators themselves the suppression (actually deletion) of data. On the contrary, the U.S. does not have any consolidated RTBF jurisprudence as such, and the few scattered protections may be found under state laws, e.g., California Consumer Privacy Act. The biggest leap so far in the U.S. has been the passage of the California Minor Eraser Law, which provides minors the ability to delete content that they have posted online, an important tool for digital-self-renewal. In India, RTBF has gained legal basis through Section 12(2)(a) of the Digital Personal Data Protection Act, 2023, giving data principals the remedy of requesting the erasure of personal data when it is no longer needed. It is promising, but where the real effectiveness of this right lies will be in administrative clarity, compliance by platforms, and user awareness. Without procedural mechanisms in place, without appeal mechanisms, and without a good measure of transparency in how decisions are made, the average individual may find the right to silence to be either empty or simply inaccessible, especially when having to encounter foreign platforms and uncooperative intermediaries.

Conclusion

The interface between social media and RTBF, as it evolves in 2025, underscores a fundamental reconstitution of digital rights in which privacy and free expression are constantly being negotiated between one another. In a country like India, this balancing act takes on an extremely constitutional hue, requiring the harmonisation of "Article 21 of the Constitution of India", which guarantees the right to privacy, and "Article 19(1)(a)", which guarantees freedom of speech and expression. Social media platforms, now considered quasi-public spaces, are rife with reputational harms-the past wrongdoings and irrelevant nonconsensual data security!--making RTBF a necessity rather than a privilege for digital sovereignty. However, it can never be its own end. The lust for content erasure should never stand in the way of the interests of public discourse, of the archival functions served by the internet, or of the democratic interest in transparency and accountability. Indian law must be able to distinguish between the personal harm that is worthy of erasure and the public interest that urges retention, employing a straightforward, principled, and reviewable test to evaluate claims under RTBF.

The changing relationship between social media and RTBF in 2025 exemplifies a fundamental recalibration of digital rights, where privacy and free expression are perpetually being renegotiated. In a country like India, this particular balancing exercise acquires a constitutionally-mandated character by demanding in some way that "Article 21 of the Constitution of India", which guarantees the right to privacy, be harmonised with "Article 19(1)(a)", which guarantees freedom of speech and expression. Today, social media platforms are considered in some way akin to public spaces where a person's past reputation, past misdeeds, and irrelevant information can reside forever, making RTBF a right, rather than a luxury, of digital autonomy. However, this safety net cannot be absolute. Eliminating any content should not diminish public discourse, the archival function of the internet, and the democratic interest in transparency and accountability. Indian law must distinguish between instances of personal harm that merit erasure and instances of public interest that merit retention, employing a clear, principled framework that is subject to review.

In fact, the entire construction of RTBF comes across as an empty subject unless actual applications and consequences are taken into consideration. Enforcing this nonprofit over social media platforms has varying implications with regard to the individual, the operator of the platform, civil society, and the state. On the one hand, an individual wants RTBF protection against disclosures that might cause him or her stigmatization or harm to his or her reputation; on the other hand, there is also a public interest in having such information made public for greater transparency. Social media platforms, therefore, face enormous pressures on the other side because of the competing claims of users forced against the operational consistency of the platform and their legal compliance as dictated by the laws, both national and international. Mostly will the real success or failure of RTBF depend on extra-distance actors perceive its applicability, especially with newer content-moderation types and AI-based decision-making that obviously falls under jurisdictional fragmentation?

[22] Supra note 21.

In the Indian legislature, statutory foundation of RTBF lies underneath the "Digital Personal Data Protection Act, 2023", especially the "Section 12(2)(a)". This enables the user to request deletion of his personal data when its purpose for which it was sought no longer subsists. However, socio-legal adjudication of this provision now factors beyond mere legislative construct into procedural precision, inspectorial mechanism, and independent auditing. The Act dwells upon several exceptions, notably under "Section 7" for purposes of statutory compliance, public interest, and fair use in journalism, thereby safeguarding RTBF against serving as a veil to repress legitimate content. Yet, these exceptions create numerous issues on jurisdictional applicability, user awareness, and algorithmic audit trails while interfacing with platform moderation policy. Rather than being a judicial forum, social media platforms are now beginning to sit in judgment directly affecting fundamental rights. Therefore, India must institute a safeguard system consisting of notice requirements; stating reasons for refusal; an internal appeals process; and access to data protection authorities if claims are still unresolved. Without procedural scaffolding, the right remains idealistic and threatened with arbitrary application.

Beyond legal and technological dimensions lie the far-reaching societal impacts of the RTBF. The public's support for the right is colored by visible harms: online harassment, revenge content, the reappearance of far-distant charges. The RTBF thus becomes secondary relief in such cases, especially for those outside public life. On the other hand, the legitimate fear remains that RTBF would be readily co-opted by powerful private actors to dismiss narrative, obstruct public record, or evade accountability. As with balancing anything, it requires formal regulation and a change in culture concerning the value of digital memory. Platform governance must entail transparency, due process, and independent scrutiny. Indian courts playing a pivotal role on the constitutional limits of RTBF while balancing fundamental rights, as exercised in the "*Kesavananda Bharati v. State of Kerala*[23], type landmark cases, can ensure that RTBF doesn't infringe upon the broader public's right to information and democratic participation.[24]

[23] AIR 1973 SC 1461.

[24] Social Media on Trial: Can the Law Keep Up with the Times, *available at:* https://depenning.com/blog/social-media-on-trial-can-the-law-keep-up-with-the-times/ (Visited on March 2, 2025).