INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 4 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

THE RIGHT TO BE FORGOTTEN: A COMPARATIVE ANALYSIS OF EU AND INDIA'S APPROACH

AUTHOR – ROSHNI AGARWAL, STUDENT AT AMITY UNIVERSITY

BEST CITATION – ROSHNI AGARWAL, THE RIGHT TO BE FORGOTTEN: A COMPARATIVE ANALYSIS OF EU AND INDIA'S APPROACH**,** *INDIAN JOURNAL OF LEGAL REVIEW (IJLR),* 6 (4) OF 2026, PG. 949-959, APIS – 3920 – 0001 & ISSN - 2583-2344

ABSTRACT

The rapid expansion of digital technologies and the internet has fundamentally transformed the way personal information is created, stored, and disseminated. In this evolving digital ecosystem, the concept of the RTBF has emerged as a critical component of informational privacy, enabling individuals to seek erasure or restriction of access to personal data that is no longer necessary, relevant, or accurate. This dissertation examines the legal foundations, scope, and challenges associated with the RTBF, with a particular focus on the Indian legal framework in comparison with international developments.

The study traces the evolution of the right to privacy in India, culminating in its recognition as a fundamental right under Article 21 of the Constitution by the Supreme Court in the landmark judgment of Justice K.S. Puttaswamy v. Union of India. Building upon this constitutional foundation, the research explores how Indian courts have gradually engaged with RTBF claims, particularly in cases involving digital records, reputational harm, and the accessibility of judicial decisions through online platforms.

A comparative analysis is undertaken with the European Union's robust data protection regime, especially the General Data Protection Regulation, which explicitly recognizes the right to erasure. The dissertation critically evaluates the applicability of such a framework in India, considering the enactment of the Digital Personal Data Protection Act, 2023, and its implications for balancing individual privacy with competing interests such as freedom of expression, public access to information, and judicial transparency.

Furthermore, the study highlights the technological and practical challenges in implementing RTBF, including issues of data replication, search engine indexing, and jurisdictional limitations. It also examines the tension between the permanence of judicial records and the need to protect individual dignity and autonomy in the digital age.

The dissertation concludes that while India has made significant strides in recognizing privacy rights, the operationalization of RTBF remains fragmented and evolving. It underscores the need for a coherent legal framework, clear judicial guidelines, and technological accountability to ensure an effective balance between privacy rights and the broader public interest.

Keywords: *Right to Be Forgotten, Right to Privacy, Data Protection, General Data Protection Regulation, Article 21, Data Erasure, European Union*

Introduction

The digital age has fundamentally altered how information about individuals is created, stored, and accessed. Today, data is no longer temporary; it is permanently recorded, replicated, and made globally accessible

through search engines, social media platforms, and online databases. While this has enhanced transparency and access to information, it has also created a serious challenge to individual privacy, dignity, and autonomy. The persistence of digital records means that personal information once made public often remains accessible indefinitely, regardless of its relevance over time.

This issue becomes particularly critical in the context of criminal justice. Information relating to arrests, investigations, and trials is frequently available online, even when an individual is later acquitted or cleared of all charges. As a result, individuals continue to face social stigma, reputational harm, and professional exclusion based on outdated or incomplete information. This phenomenon has been described as a form of "digital life imprisonment," where the consequences of past allegations extend far beyond the legal process.

In response to these concerns, the RTBF gas emerged as an important legal concept. Rather than erasing history, RTBF seeks to allow individuals to limit access to personal data that is no longer relevant or necessary, thereby restoring a degree of control over their digital identity. It is rooted in the broader right to privacy and reflects the idea that individuals should have the opportunity to move beyond their past without being perpetually judged by it.

Globally, the RTBF has gained recognition through developments such as the General Data Protection Regulation[1846], which provides a structured framework for balancing privacy with competing interests like freedom of expression and public interest. In India, the right has evolved through constitutional interpretation, particularly following Justice K.S. Puttaswamy v. Union of India[1847], with courts gradually acknowledging its relevance in cases involving digital records and reputational harm.

However, the application of RTBF raises complex questions about transparency, open justice, and the public's right to know. This tension highlights the need for a balanced legal framework that protects individual dignity while preserving democratic values. This study, therefore, examines RTBF through a comparative and criminal justice–centric lens, emphasizing its role in safeguarding privacy in the digital era.

Conceptual Foundations and Historical Roots of Privacy

Privacy, though often perceived as a modern legal construct, is deeply rooted in the evolution of human society. From the earliest stages of civilization, information has functioned as a critical tool for connection, cooperation, and the formation of social structures. Shared narratives whether in the form of myths, religious texts, or cultural traditions enabled large-scale human collaboration. However, the same information that fosters cohesion also carries the potential for misuse, manipulation, and intrusion into personal domains. This dual nature of information laid the groundwork for the emergence of privacy as a necessary counterbalance.

Historically, privacy existed in implicit forms rather than as a formally articulated right. Ancient civilizations, including Greek, Roman, and Anglo-Saxon societies, recognized distinctions between public and private life. Philosophical ideas, such as Aristotle's division between the *polis* (public sphere) and *oikos* (private sphere), reflect early conceptualizations of privacy. Similarly, practices like maintaining separate living spaces, silent prayer, and personal boundaries indicate an inherent human inclination toward seclusion and control over personal space.

Religious and ethical traditions across cultures also acknowledged the value of privacy. Texts and practices in Hindu, Islamic, and Biblical traditions emphasized modesty, personal boundaries, and the protection of intimate matters. Legal codes such as the Code of Hammurabi and ethical frameworks like the

[1846]Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection gulation), 2016
[1847]Justice K. S. Puttaswamy & Ors. v. Union of India, (2017) 10 SCC 1.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 4 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

Hippocratic Oath[1848] incorporated elements of confidentiality and responsibility, demonstrating that the protection of personal information has long been a societal concern.

With the advent of documentation and later technological innovations from the printing press to the internet the nature of information transformed significantly. While these advancements enhanced knowledge dissemination, they also amplified risks to individual privacy. The landmark 1890 article by Warren and Brandeis marked a turning point by explicitly articulating privacy as "the right to be let alone,"[1849] thereby initiating modern legal discourse on the subject.

Evolution of Privacy in the Indian Context

In India, the concept of privacy has evolved through cultural, philosophical, and legal developments. Contrary to the assumption that privacy is alien to Indian society, historical texts such as the Dharmashastras, Upanishads, and epics like the Ramayana and Mahabharata reveal an embedded respect for personal autonomy and dignity. The principle "*Sarvaswe Swe Grihe Raja*" (every man is a king in his own house) underscores the sanctity of the private sphere.[1850] Ancient governance frameworks, including Kautilya's Arthashastra, also recognized procedural safeguards that indirectly protected privacy.[1851]

During the colonial and pre-constitutional periods, privacy began to be associated with the inviolability of the home and property. Documents like the Constitution of India Bill, 1895, the Commonwealth of India Bill, 1925,[1852] and the Nehru Report, 1928[1853], reflected concerns about unlawful interference in personal spaces. However, despite these developments, the framers of the Indian Constitution ultimately chose not to explicitly include the right to privacy as a fundamental right. This omission was the result of significant debate within the Constituent Assembly, where concerns were raised about its potential impact on governance, law enforcement, and evidentiary processes.

Nevertheless, the absence of explicit recognition did not negate the existence of privacy as a social and moral value. Over time, the judiciary assumed a pivotal role in shaping the contours of privacy within the constitutional framework, gradually linking it to the broader guarantees of life and personal liberty under Article 21.

Judicial Expansion and Constitutional Recognition

The judicial journey of privacy in India reflects a gradual but profound transformation. Early decisions such as ***M.P. Sharma* (1954)** and ***Kharak Singh***[1854] adopted a restrictive approach, denying privacy the status of a fundamental right. However, dissenting opinions, particularly by Justice Subba Rao, planted the seeds for future expansion by recognizing privacy as intrinsic to personal liberty.

The turning point came with the progressive interpretation of Article 21 in subsequent cases. The decision in *Maneka Gandhi v. Union of India*[1855] broadened the scope of the right to life and personal liberty, incorporating elements of dignity, autonomy, and fairness. Later judgments, including *R. Rajagopal*[1856], *PUCL*[1857] and further expanded privacy to include informational control, communication, and protection against arbitrary state intrusion. The recognition of both physical and mental privacy in *Selvi v. State of Karnataka*[1858]marked another significant development, linking privacy with protection against self-incrimination.

[1848]Fried C. (1968). Privacy. 77 Yale L.J. p. 478.
[1849]Samuel D. Warren & Louis D. Brandeis, "The Right to Privacy," (1890) 4 Harvard Law Review 193.
[1850]Hutton E. J. (1976). The Right of Privacy in the United States, Great Britain and India in Richard P. Claude (ed.). Comparative Human Rights. P. 151.
[1851]Ramanarayan Dutta Shastri Ram (translated by) Valmiki Ramayana, Yudha Kand, p.1412; Shreepad Damodar Satavalekar (ed.) Mahabharata, Adi Parva, p.1000; Hargovind Sastri (ed.) Manusmriti, p.276.
[1852]https://www.constitutionofindia.net/historical_constitutions/the_constitution_of_india_bill__unknown__1895 1st%20January%201895?paragraph_number=18#CIB.18.
[1853]Nehru Report. (1928) 1st January, NR 4.

[1854] M.P. Sharma v. Satish Chandra AIR 1954 SC 300
[1855] Maneka Gandhi vs Union of India, 1978 1 SCC 248
[1856] R. Rajagopal vs State of Tamil Nadu 1994 6 SCC 632
[1857] People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301.
[1858] Selvi v. State of Karnataka, (2010) 7 SCC 263.

This evolving jurisprudence culminated in the landmark judgment of *Justice K.S. Puttaswamy v. Union of India*[1859], where a nine-judge bench of the Supreme Court unanimously affirmed privacy as a fundamental right under Part III of the Constitution. The Court held that privacy is intrinsic to life, liberty, and dignity, and is protected under Articles 14[1860], 19[1861], and 21[1862]. Importantly, it overruled earlier precedents that denied constitutional recognition to privacy.

The judgment also introduced a structured framework to assess state interference with privacy, based on legality, legitimate aim, and proportionality. While affirming privacy as a fundamental right, the Court clarified that it is not absolute and may be subject to reasonable restrictions in the interest of public welfare. This decision marked a watershed moment, firmly embedding privacy within India's constitutional ethos.

Contemporary Relevance: Digital Age, Global Norms, and the Right to be Forgotten

In the contemporary era, privacy has assumed unprecedented significance due to rapid technological advancements and the digitization of personal data. The proliferation of social media, big data analytics, and artificial intelligence has transformed personal information into a valuable commodity, often collected, stored, and monetized without adequate user awareness or control. This shift has intensified concerns about surveillance, data misuse, and erosion of individual autonomy.

Globally, privacy is recognized as a fundamental human right through instruments such as the Universal Declaration of Human Rights[1863] and the International Covenant on Civil and Political Rights[1864]. Regional frameworks like the European Convention on Human Rights[1865] and regulatory regimes such as the General Data Protection Regulation (GDPR)[1866] have further strengthened data protection standards, influencing legal developments worldwide, including in India.

Within this evolving landscape, the concept of the RTBF has emerged as an extension of privacy and human dignity. Historically, societies have acknowledged the importance of forgetting through mechanisms such as expungement of criminal records and doctrines of rehabilitation. In the digital age, however, the permanence and accessibility of online information challenge this principle. The RTBF seeks to restore individual control by allowing the erasure or restriction of outdated or irrelevant personal data.

The need for such rights is underscored by the extensive data collection practices of modern technology platforms, where personal information is continuously tracked and stored. This reality necessitates robust legal frameworks that balance innovation with individual rights. In India, the recognition of privacy in *Puttaswamy* has paved the way for legislative initiatives like data protection laws, reflecting an ongoing effort to address these challenges.

Ultimately, privacy today is not merely a legal entitlement but a cornerstone of human dignity, autonomy, and democratic participation. Its evolution from implicit social norms to a constitutionally protected right underscores its enduring relevance for safeguarding individual freedom in an increasingly interconnected, data-driven world.

The Right to be Forgotten under the GDPR: Evolution, Scope and Limitations

Conceptual Foundations and Emergence of the RTBF

In the digital age, participation in online spaces necessitates the disclosure of personal information, resulting in an enduring digital footprint. The permanence, replicability, and

[1859] Supra
[1860] India Consti, art 14
[1861] India Consti, art 19
[1862] India Consti, art 21
[1863] Universal Declaration of Human Rights, 1948.
[1864] International Covenant on Civil and Political Rights, 1966.
[1865] European Convention on Human Rights, 1950.
[1866] General Data Protection Regulation, 2016.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 4 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

accessibility of such data have created a paradigm where individuals remain perpetually tied to their past actions. This phenomenon has intensified concerns regarding informational autonomy and reputational harm, leading to the emergence of the RTBF.

The RTBF is rooted in the broader framework of privacy and human dignity. International instruments such as the International Covenant on Civil and Political Rights and the European Convention on Human Rights recognise protection against arbitrary interference with privacy and reputation. Within the European Union, these principles evolved into a more structured regime through the recognition of data protection as a fundamental right under the Charter of Fundamental Rights.

The need for such a right is best understood in the context of digital permanence and "de-contextualisation" of information",[1867] where data, though once accurate, becomes outdated or misleading over time. The RTBF seeks to address this by enabling individuals to limit the continued accessibility of such information, thereby allowing them to redefine their identity and avoid perpetual stigmatization. It represents not merely a privacy safeguard but a mechanism for ensuring personal autonomy in shaping one's social narrative.

Judicial Evolution and European Jurisprudence

The modern articulation of the RTBF owes much to European jurisprudence, particularly the landmark decision in the Google Spain case[1868]. The Court of Justice of the European Union recognized that search engines act as data controllers and are responsible for processing personal data. It held that individuals may request the removal of links to information that is inadequate, irrelevant, or excessive in relation to the purposes for which it was processed, even if the original publication was lawful.

This judgment marked a shift from traditional notions of privacy to a more dynamic understanding of informational control. It emphasized that the economic interests of search engines cannot override fundamental rights, and introduced the principle that data must not be retained beyond its relevance.

Subsequent decisions further refined the scope of the RTBF. Courts have consistently underscored that the right is not absolute and must be balanced against competing interests such as freedom of expression and access to information. The territorial limitations of the RTBF were also clarified, with courts holding that while de-referencing must be effective within the European Union, it does not necessarily extend globally. This reflects the diversity in legal approaches to data protection across jurisdictions.

The GDPR Framework: Scope and Legal Architecture

The General Data Protection Regulation represents a comprehensive and binding framework governing data protection within the European Union. It codifies the RTBF under Article 17 as the "Right to Erasure," thereby transforming a judicially recognized principle into a statutory right.

Under the GDPR, individuals are entitled to request the erasure of personal data where it is no longer necessary for the purpose for which it was collected, where consent has been withdrawn, where processing is unlawful, or where there is a legal obligation to delete such data. The regulation also imposes obligations on data controllers to take reasonable steps to inform third parties to erase links or copies of such data, thereby extending the practical reach of the right in the digital ecosystem.

The GDPR further strengthens individual control through complementary provisions such as the

[1867]Helen nissenbaum, privacy in context: technology, policy, and the integrity of social life 193 (2010).

[1868]Google Spain SL and Google Inc. v Agencia Espanola de Proteccion de Datos (2014).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 4 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

right of access under Article 15, [1869]which ensures transparency in data processing. Recitals 65 and 66 elaborate on the rationale behind the RTBF, emphasizing timely erasure, especially in cases involving data shared without full awareness, such as by minors.

Importantly, the regulation introduces the concept of revocation of consent, allowing individuals to withdraw previously given consent and reclaim control over their data. This reflects a shift toward informational self-determination, where individuals are not bound indefinitely by past disclosures.

Limitations, Balancing of Rights, and Conceptual Expansion

Despite its expansive scope, the RTBF is not an absolute right. Article 17 explicitly provides exceptions where data retention is necessary for exercising freedom of expression and information, compliance with legal obligations, public interest considerations, public health, scientific or historical research, or the establishment and defence of legal claims.

The necessity of balancing competing rights lies at the heart of the RTBF's application. Courts and regulators must engage in a contextual assessment, weighing the individual's right to privacy and identity against the public's right to access information. This balancing exercise ensures that the RTBF does not become a tool for censorship or historical revisionism.[1870]

A significant conceptual development in the understanding of the RTBF is its linkage with the right to identity.[1871] While privacy concerns the control over information entering the public domain, identity relates to how that information represents an individual. The RTBF, therefore, extends beyond mere concealment of private information and addresses the problem of distorted or outdated representations of identity caused by persistent digital records.[1872]

In this sense, the RTBF enables individuals to renegotiate their relationship with the past, acknowledging that identity is dynamic rather than static. By addressing the issue of de-contextualised information, the right provides a framework for preserving dignity in an environment where technological systems tend to preserve information indefinitely.

Recognition of the RTBF in India

The recognition of the RTBF in India has emerged gradually through judicial interpretation, evolving statutory frameworks, and the growing influence of global data protection norms. While India does not yet have an explicit, standalone legal provision recognizing RTBF, its conceptual foundation lies in the broader right to privacy under Article 21 of the Constitution. The landmark judgment in *Justice K.S. Puttaswamy v. Union of India*[1873] marked a constitutional turning point by affirming privacy as a fundamental right, thereby opening the door for derivative rights such as RTBF.

Subsequent judicial decisions have cautiously acknowledged RTBF in specific contexts. Courts have allowed remedies such as anonymization, masking of identities, and limited removal of online content, particularly where continued digital exposure causes disproportionate harm to an individual's dignity or reputation. For instance, in cases where individuals were acquitted or proceedings were quashed, courts have recognized that indefinite online accessibility of such records may unjustly affect their personal and professional lives. Similarly, judicial directions to remove or restrict certain types of online content, including sensitive or unlawful material, demonstrate that Indian law

[1869]India Consti, art 15

[1870] Giorgio Pino, The right to personal identity in Italian private law: Constitutional interpretation and judge made rights, THE PRIVATIZATION OF PRIVATE LAW IN EUROPE, Hart Publishing, Oxford (2000). 79 Johann Neethling, The Concept of Privacy in South African Law, SOUTH AFRICAN LAW JOURNAL, 2005, 18, 22-24.

[1871] Norberto Nuno Gomes de Andrade, Oblivion: The Right to be Different… from Oneself: Reproposing the Right to be Forgotten, REVISTA DE LOS ESTUDIOS DE DERECHO Y CIENCIA POLITICA DE LA UOC, February, 2012, 122, 125.

[1872] Muge Fazlioglu, Forget me not: the clash of the right to be forgotten and freedom of expression on the internet, 3 INTERNATIONAL DATA PRIVACY LAW JOURNAL, 149, 154 (2013).

[1873]Supra

does accommodate content removal mechanisms, even if indirectly.

However, this recognition remains fragmented and case-specific. Courts have consistently avoided granting an absolute RTBF, emphasizing that it must operate within constitutional boundaries, particularly in relation to freedom of speech, judicial transparency, and public interest. Thus, RTBF in India currently exists more as an evolving judicial principle than as a clearly codified right.

Legislative Framework and the Digital Personal Data Protection Act, 2023

The enactment of the Digital Personal Data Protection Act, 2023[1874] (DPDP Act) represents a significant step in India's data protection regime. Although the Act does not explicitly recognize the RTBF, it incorporates related principles through the right to correction and erasure of personal data. Individuals are granted the ability to request deletion of their personal data when it is no longer necessary for the purpose for which it was collected, subject to legal and regulatory constraints.

The DPDP Act emphasizes consent-based data processing, requiring that consent be free, informed, and unambiguous. It also provides individuals with rights to access, update, and erase their data, along with mechanisms for grievance redressal.[1875] At the same time, the Act imposes obligations on data fiduciaries, including maintaining data accuracy, ensuring security safeguards, and notifying authorities in case of data breaches.[1876] These provisions strengthen informational autonomy and align India's framework with global data protection standards.

Despite these advancements, the Act has notable limitations. It does not establish a distinct RTBF comparable to frameworks such as the European Union's General Data Protection Regulation (GDPR). Additionally, broad exemptions granted to the State for reasons such as national security, public order, and legal enforcement raise concerns about potential overreach.[1877] The absence of a comprehensive regulatory authority with strong oversight powers further limits the Act's effectiveness. Consequently, while the DPDP Act enhances data protection, it leaves significant gaps in addressing the specific challenges posed by RTBF.[1878]

Balancing Privacy, Public Interest, and Freedom of Expression

A defining feature of RTBF jurisprudence in India is the continuous balancing of competing constitutional values. Courts have consistently held that the right to privacy, including RTBF, is not absolute and must be weighed against public interest, freedom of speech, and the principle of open justice. This balancing exercise is guided by the proportionality test, which requires that any restriction on privacy be lawful, pursue a legitimate aim, and be proportionate to that aim.

In practice, this has led to a nuanced judicial approach. Courts have distinguished between different types of information, allowing greater protection in cases involving sensitive personal data, such as sexual offences or wrongful accusations, while preserving access to information that serves public interest or contributes to legal transparency. For example, courts have been reluctant to delete judicial records entirely, recognizing their importance in maintaining accountability and the development of legal precedent. Instead, they have adopted intermediate measures such as anonymization or de-indexing from search engines.

[1874]The Digital Personal Data Protection Act, 2023, No. 22, Act of Parliament, 2023

[1875]Karishma Sundara & Nikhil Narendran, The Digital Personal Data Protection Act, 2023: analysing India's dynamic approach to data protection, 24 Comput. L. Rev. Int'l 129, (2023), https://doi.org/10.9785/cri-2023240502.

[1876] Manjula Raghav & Sanjana Sharma Marwaha, Indian Legal Framework on the Right to Privacy in Cyberspace Issues and Challenges, 17 Fiat Justisia 1, XXXX (2023), https://doi.org/10.25041/fiatjustisia.v17no1.2667.

[1877] Douwe Korff, The Indian Digital Personal Data Protection Act, 2023, viewed from a European Perspective, 2023 SSRN Elec. J., https://doi.org/10.2139/ssrn.4614984

[1878]Charru Malhotra & Udbhav Malhotra, Putting Interests of Digital Nagriks First: Digital Personal Data Protection (DPDP) Act 2023 of India, 70 INDIAN J. PUB. ADMIN. 516 (2024), (https://doi.org/10.1177/00195561241271575) .

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 4 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

The tension between Article 21 (privacy) and Article 19(1)(a) (freedom of expression) remains central to this discourse. Judicial decisions have cautioned against overbroad censorship that could create "memory holes" and undermine democratic values. At the same time, they have acknowledged the need to protect individuals from perpetual digital harm. This evolving balance reflects an attempt to harmonize individual dignity with collective societal interests in the digital age.

Challenges, Institutional Gaps, and the Need for a Comprehensive RTBF Framework

Despite growing judicial and legislative recognition, the RTBF in India faces significant structural and practical challenges. One of the primary issues is the absence of a dedicated statutory framework governing RTBF claims. In its absence, individuals often rely on constitutional remedies or approach digital platforms directly for content removal. This has resulted in the increasing role of private intermediaries—such as search engines and social media platforms in adjudicating RTBF-related requests.

While platform-based mechanisms can offer quick and accessible remedies, they raise concerns regarding transparency, accountability, and consistency. Decisions are often governed by internal policies rather than uniform legal standards, leading to unpredictable outcomes. Moreover, the privatization of such decision-making processes raises normative concerns, as issues involving fundamental rights are effectively being resolved by corporate entities rather than judicial or statutory bodies.

Another significant limitation arises in relation to judicial records. Courts have emphasized that such records are part of the public domain and cannot ordinarily be erased. However, they have also recognized that unrestricted digital access may cause disproportionate harm, leading to selective remedies such as masking identities or restricting searchability. The absence of clear legal standards in this area has resulted in fragmented and evolving jurisprudence.

The need for RTBF is further underscored by the realities of the digital age, where personal data is extensively collected, stored, and disseminated. Individuals often lose control over their digital identities, with outdated or irrelevant information continuing to affect their lives indefinitely. RTBF provides a mechanism for reclaiming this control, enabling individuals to protect their dignity, reputation, and autonomy.

The recognition of RTBF in India reflects a gradual but incomplete transition towards stronger privacy protections. While judicial innovation and legislative developments have laid an important foundation, the absence of a comprehensive and coherent framework continues to limit its effectiveness. Moving forward, there is a pressing need for clear statutory recognition, well-defined standards, and robust institutional mechanisms to ensure that RTBF is implemented in a manner that balances individual rights with broader societal interests.

Conceptual Foundations of RTBF and Comparative Legal Approaches

The RTBF has emerged as a critical legal response to the challenges posed by digital permanence, particularly within criminal justice contexts where reputational harm and public interest often collide. Different jurisdictions approach this right through distinct constitutional, regulatory, and cultural frameworks. The European Union represents the most comprehensive model, embedding RTBF within a structured legal regime under Article 17 of the General Data Protection Regulation (GDPR). This provision empowers individuals to seek erasure of personal data when it is no longer necessary, unlawfully processed, or when consent has been withdrawn. The jurisprudential basis of this right was firmly established in *Google Spain v. AEPD*, where search engines were recognized as data controllers, thereby imposing obligations on

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 4 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

intermediaries to regulate access to personal data.

The EU model operates through a carefully calibrated balancing framework. While individuals can request deletion or delisting, such requests are assessed against competing interests such as freedom of expression, public interest, and legal obligations. This proportionality-based approach ensures that RTBF does not become a tool for censorship but functions as a mechanism to protect dignity and informational autonomy. Procedurally, the system is supported by Data Protection Authorities (DPAs), which provide institutional oversight, enforce compliance, and ensure accountability. Thus, the EU's framework reflects a rights-based, structured, and enforceable model of digital erasure.

Speech-Centric Paradigm in the United States

In contrast, the United States adopts a fundamentally different approach rooted in the primacy of free speech under the First Amendment. The American legal system does not recognize a comprehensive RTBF. Instead, it prioritizes the protection of truthful information, even if such information causes reputational harm. Judicial precedents such as *Florida Star v. B.J.F.*[1879] and *Martin v. Hearst Corporation*[1880] reinforce this stance by holding that lawfully obtained and factually accurate information cannot be suppressed merely because it is embarrassing or outdated.

Rather than a unified erasure right, the U.S. relies on a fragmented framework of tort laws and limited statutory remedies. Individuals must resort to defamation, false light, or privacy torts, each requiring stringent evidentiary thresholds. These remedies are largely reactive, offering compensation after harm has occurred rather than enabling proactive control over personal data. Statutory measures such as expungement laws and the California Online Eraser Law provide limited relief, primarily restricted to government records or user-generated content.

A significant structural factor shaping this approach is Section 230 of the Communications Decency Act, which grants immunity to intermediaries for third-party content. This provision limits the liability of platforms and reduces incentives for proactive content removal. Consequently, the American framework conceptualizes digital memory as an extension of expressive freedom rather than a domain of personal data control. While public opinion increasingly supports greater control over digital identity, constitutional priorities continue to favour speech and historical preservation.

Global Diffusion and Regulatory Variations

Beyond the EU and the U.S., RTBF principles have gradually diffused across global jurisdictions, though with varying degrees of implementation. Many countries, including Canada, Australia, Turkey, and Russia, have incorporated elements of data erasure or delisting within their legal frameworks. However, these systems often lack the procedural clarity and enforcement strength of the EU model.

In Canada and Australia, regulators have explored extending existing privacy laws to include search engine delisting, particularly where reputational harm outweighs public interest. Turkey has explicitly recognized search engines as data controllers and adopted balancing criteria similar to European jurisprudence. Russia has enacted legislation enabling removal of outdated search results, though within a more state-centric regulatory environment. Despite these developments, enforcement remains inconsistent due to institutional limitations, constitutional constraints, and lack of harmonized standards.

A common challenge across jurisdictions is the absence of robust regulatory capacity and clear procedural mechanisms. Unlike the EU's coordinated enforcement through DPAs and the European Data Protection Board, many countries rely on fragmented or complaint-driven approaches. As a result, the practical realization of RTBF remains uneven, reflecting

[1879] The Florida Star v. B.J.F., 491 U.S. 524 (1989).
[1880] Martin v. Hearst Corp., 777 F.3d 546 (2d Cir. 2015).

broader differences in constitutional culture and governance models.

Indian Framework: Constitutional Evolution and Criminal Justice Constraints

India presents a hybrid and evolving approach to RTBF, grounded in constitutional jurisprudence rather than explicit statutory recognition. The doctrinal foundation lies in the landmark judgment of *Justice K.S. Puttaswamy v. Union of India*, where the Supreme Court recognized privacy as a fundamental right under Article 21. This decision introduced the principle of informational self-determination, implicitly supporting RTBF claims. The proportionality test articulated in this case requiring legality, necessity, and proportionality serves as the central framework for balancing privacy against competing interests such as freedom of speech.

Subsequent judicial developments have cautiously operationalized RTBF. High Courts have permitted measures such as anonymization, masking of identities, and de-indexing of search results, particularly in cases involving acquitted individuals or sensitive personal matters. However, Indian courts have consistently resisted the complete erasure of judicial records, emphasizing the principle of open justice and the importance of transparency in legal proceedings. Judicial records are treated as public documents essential for accountability and the development of precedent.

The enactment of the Digital Personal Data Protection Act, 2023 (DPDP Act) marks a significant legislative step by recognizing the right to erasure. However, the Act stops short of explicitly codifying RTBF and includes broad exceptions for legal compliance, state functions, research, and public interest. As a result, India adopts a conditional erasure model rather than an absolute right.

In the criminal justice context, RTBF faces additional limitations. Preservation of evidence is essential for investigation, trial, and appellate processes, making data retention a legal necessity. Courts therefore, prefer limited remedies such as anonymization rather than complete deletion. This reflects a broader attempt to balance individual dignity with systemic integrity.

Overall, India's approach represents a nuanced and evolving model that seeks to harmonize privacy, rehabilitation, transparency, and free expression. Unlike the EU's structured regulatory regime or the U.S.'s speech-centric framework, India relies on constitutional balancing and judicial discretion. As regulatory mechanisms mature and jurisprudence develops, India's RTBF framework is likely to become more defined while retaining its core emphasis on proportionality and contextual adjudication.

Conclusion

The RTBF has emerged as one of the most compelling yet complex developments in the contemporary discourse on digital privacy, reflecting the broader transformation of how information is created, stored, and accessed in the digital age. The permanence and accessibility of online data have fundamentally altered the relationship between individuals and their personal histories, often subjecting them to prolonged reputational, social, and professional consequences for information that may have lost its relevance over time. In this context, the RTBF represents an essential attempt to restore balance by enabling individuals to exercise a degree of control over their digital identities and to protect their dignity and autonomy. Within the Indian legal framework, the recognition of privacy as a fundamental right under Article 21 has provided a strong constitutional foundation for the gradual development of RTBF principles.

Judicial decisions have played a crucial role in shaping this emerging right, often adopting a nuanced and case-specific approach that seeks to harmonize privacy interests with competing constitutional values such as freedom of expression, transparency, and the public's right to information. Legislative efforts, particularly the enactment of the DPDP Act,

2023, signify an important step toward institutionalizing data protection norms, although the absence of an explicit and comprehensive RTBF framework continues to create uncertainty in its application.

The Indian approach thus reflects a cautious and evolving model, one that prioritizes proportionality and contextual balancing rather than absolute erasure. At the same time, the comparative analysis with jurisdictions such as the European Union and the United States highlights the diversity of legal responses to digital memory, shaped by differing constitutional traditions and normative priorities. While the European model offers a structured and enforceable right to erasure grounded in dignity and informational self-determination, the American approach emphasizes freedom of speech and historical preservation, thereby resisting broad claims for digital deletion. India, situated between these paradigms, is developing a hybrid framework that integrates constitutional adjudication with emerging regulatory mechanisms. However, significant challenges remain. Technological realities such as data replication, algorithmic amplification, and the global nature of digital platforms complicate the practical enforcement of RTBF. Institutional limitations, including the evolving role of regulatory bodies and the absence of standardized procedures, further hinder consistent application.

Moreover, the normative tension between individual privacy and collective interests continues to demand careful judicial and legislative calibration. Ultimately, the future of RTBF in India will depend on the ability of legal and institutional frameworks to adapt to these complexities while remaining anchored in constitutional values. The objective is not to erase history but to ensure that the digital representation of individuals remains fair, proportionate, and contextually relevant. A well-developed RTBF regime can serve as a vital mechanism for promoting dignity, facilitating rehabilitation, and safeguarding informational autonomy, while simultaneously preserving the principles of transparency and democratic accountability.