THE RIGHT TO BE FORGOTTEN IN THE DIGITAL AGE: EXAMINING THE SCOPE, LIMITS, AND EVOLVING JURISPRUDENCE

Durgesh Kumar Chaudhary[*]

Adarsh Tiwari[**]

ABSTRACT

The right to be forgotten (hereinafter RTBF) has become a critical issue in the digital age because of the permanence of online information. In this article, we have discussed India's current legislation and the measures other countries have taken. How the RTBF evolved and its philosophical, ethical and jurisprudential aspects are also being evaluated. The Article delves into specific legislation, such as the European Union's General Data Protection Regulation (hereinafter GDPR) and India's Digital Personal Data Protection Act 2023 (hereinafter DPDP Act), how far they have incorporated the RTBF Principle, and their limitations. The judiciary's role is also worth noting in developing privacy rights cases, such as Justice K S Puttaswamy, India's cornerstone for privacy rights. The article also focuses on challenges such as balancing the RTBF with the right to information and border enforcement challenges.

Keywords: Right to be forgotten, digital platform, data protection, privacy.

[*] Research Scholar (PhD Student), Faculty of Law, University of Lucknow)

[**] Advocate, Enrolled with the Bar Council of Uttar Pradesh; Member, Kanpur Bar Association

INTRODUCTION

The right to be forgotten has become a very buzzword topic. In today's time, every moment, whether joyful, embarrassing, or sorrowful, is being recorded by the camera, and its ultimate destination becomes Facebook, WhatsApp, or other social media applications. Nowadays, people's embarrassing moments are converted into memes by some memers. It might be fun for some, but no one will understand the mental state of the person whose embarrassing moment was captured and converted into a meme.

Many times in sexual violence cases the perpetrators have been found intimidating the victim that they will circulate their nude, sexually explicit images or videos on adult website or other social media website and in many cases it is being committed by the perpetrators and the victim of sexual offences under pressure what people will say to her or how she is going to face the society, these thoughts ultimately compelled her to end her life. But how she is going to face the society is not the only reason of this but also in the back of the mind of the victim of sexual offences remains that these explicit images or videos is not going to removed or entirely erased from the internet sources and in extreme cases this overwhelming sense of helplessness leads her to believe that ending the life is easier than facing lifelong trauma of societal and digital humiliation and stigma.

Besides this, if any person is supposedly charged with certain offences but later on in court it is proved that the charges were wrong or found false, the person is acquitted. The negative news always spreads like a fire in the jungle, but when it comes to positive news, that is the news about acquittal, it does not spread as fast. Here, the person, although found innocent in the eyes of the court or other concerned authorities, is still guilty in the eyes of society. Society does not hesitate to ridicule that person for the offence that he did not commit, the court has acquitted him of that, or that has not been proved in court.

Further, the philosophical aspect is that if a person is convicted of any offence and incarcerated. After finishing the terms of the punishment it is believed that he is emancipated from his past deeds because he has suffered his punishment and now the time of reintroduction of that person in the society, but the online presence of records of his past deeds on digital platform or availability on the internet is not going to spare him. In most cases, society will not let him live or give him another chance to live an everyday life.

Today, all information is available on the Internet, and whenever anyone wants to know about anything, they Google it. Thus, Google has also become a synonym for searching on the Internet.[1] However, it also has drawbacks. For example, if anything is uploaded or written on the Internet, it becomes challenging to remove all its traces.

During COVID-19, the internet and other digital platforms increased unprecedentedly, and people generally relied on the internet for education, work, and other daily tasks.[2] While using digital resources becomes the need of the hour, the permanent nature of online data raises concerns about its misuse. Whether it's personal information or any embarrassing moment recorded on a camera and can be circulated online, which causes mental trauma to the person whose data is on the internet. Whenever the information comes to mind, this permanent online footprint haunts the person for several years. When an old mistake or any controversial incident remains accessible, it causes long-term repercussions on a person's psychological well-being and at the same time also harms a person's reputation. Nowadays, as Internet penetration reaches every corner of society, the issue of the permanent footprint of any event over the Internet has been discussed very vehemently in recent days.[3]

The RTBF principle stems from the argument that individuals should control their personal information, whether on the Internet or in any other form, and protect themselves from unwarranted public exposure. It is the natural extension of privacy rights, encompassing intangible personal dignity.[4] Technological advancements such as videography and the Internet intensify privacy invasions, and there is a need for legal recognition of the right to be left alone, as Judge Cooley called for.[5]

This modern extension of privacy law addresses similar challenges posed by the digital age, which Warren and Brandeis raised over a century ago. According to them, a person cannot be

[1] Sanjay Vashishtha, "*The Evolution of Right to be forgotten in India*", *SCC OnLine Blog*, January 27, 2022, available at https://www.scconline.com/blog/post/2022/01/27/the-evolution-of-right-to-be-forgotten-in-india/ (last visited on April 30, 2025).
[2] Rohith K., "*Right to be Forgotten: A Critical and Comparative Scrutiny Between India and European Union*", IV Indian Journal of Law and Legal Research 1 (2022).
[3] S*upra* note 1.
[4] Samuel D. Warren and Louis D. Brandeis, "*The Right to Privacy*", 4 Harvard Law Review 193-194 (1890), available at http://links.jstor.org/sici?sici=0017-811X%2818901215%294%3A5%3C193%3ATRTP%3E2.0.CO%3B2-C (last visited on April 30, 2025).
[5] *Id.* At 195.

defined by past mistakes or outdated records.[6] It only impacts his reputation and causes mental trauma, and nothing else.

Thus, the RTBF is defined as an individual's ability to erase, limit, delink, delete, or correct personal information available on the Internet that is misleading, embarrassing, irrelevant, or outdated.[7]

The EU enacted the GDPR and adopted it on 14 April 2016, which came into effect on May 25, 2018. Article 17 of the GDPR outlines the Right to Erasure, which is also known as the RTBF. The provision enables the person to delete the personal data under certain conditions such as when the purpose for which data was collected and being fulfilled and no longer needed the data, when the person who given consent for the storage of the Data withdrew their consent, the data kept unlawfully or other legal compliance where deletion of data is necessary.[8]

However, Article 17(3) of the GDPR states that RTBF is not an absolute right, and a balanced approach with the Right to Information should be adopted. At the same time, an individual can request the erasure of data necessary in the public interest for transparency, free speech, and historical record-keeping.[9]

Article 5[10] The GDPR focuses on the lawful and ethical processing of personal data. It mandates that individuals' data be processed lawfully, fairly, and transparently to protect their rights. According to this article, data should be collected only for legitimate purposes and should not contradict the initial purpose for which it was collected. Thus, it emphasises the purpose limitation.

Article 5 also emphasises the principle of Data Minimisation, meaning that only necessary data should be gathered. Reducing the amount of personal data collected does not eliminate the risk of security threats, but significantly limits potential data breaches.[11] Further, Data should not

[6] *Id.* at (193-220).
[7] Michael J. Kelly and David Satola, "*The Right To Be Forgotten*", 1 University of Illinois Law Review 1 (2017).
[8] GDPR Info, "*Art. 17 General Data Protection Regulation – Right to erasure ('Right to be Forgotten')*", *General Data Protection Regulation (GDPR)*, available at https://gdpr-info.eu/art-17-gdpr/ (last visited on April 30, 2025).
[9] Hiroshi Miyashita, *"The 'Right to Be Forgotten' and Search Engine Liability"*, Brussels Privacy Hub Working Paper, Vol. 2, No. 8, p. 13 (Dec. 2016).
[10] General Data Protection Regulation, 2016, "*Principles relating to processing of personal data*", art. 5, available at: https://gdpr.eu.org/art/5/ (last visited on Apr. 30, 2025).
[11] RISMA Systems, "*GDPR Data Minimization: Compliance & Risk Mitigation*", RISMA Systems, available at: https://www.rismasystems.com/en/resources/articles/gdpr-data-minimization (last visited on Apr. 30, 2025).

be stored for a long time unless archival or research purposes justify the storage, thus focusing on Storage limitations. As the RTBF stems from privacy law, it also emphasises that data should be handled carefully and protected from unauthorised access, loss and destruction through appropriate technical and organisational support. Finally, it also makes the data controller responsible for any security lapse or non-compliance with the provision.[12]

Thus, Articles 5 and 17 try to strike a balance between the RTBF and the right to have access to necessary information. Both Articles show the GDPR's approach of balancing rights and practical concerns, ensuring personal data is protected and allowing accessibility where necessary.

CONCEPTUAL FOUNDATIONS AND LEGAL SIGNIFICANCE

The RTBF emerged from the French jurisprudence under the Right to Oblivion (le droit à l'oubli).[13] This concept allowed the convicted people who have served their punishment to be obliterated and exonerated from the societal taunting, as the person has already served their punishment for what they had done. Now he is exonerated and should be reintegrated into society without any stigma imposed on him by society. Over time, this principle further evolved, specifically when women facing sexual offences, it becomes necessary to hide their identities as victims to ensure that they do not suffer additional harm due to public exposure and can be protected from the societal stigma, safeguarding their reputation and dignity.

The recognition of the RTBF as a right can be traced from the Case of Google Spain SL v. AEPD & Mario Costeja Gonzalez (2014)[14]. Mario Conzalez, a Spanish man who took a loan and defaulted on it; for this, his property was put up for Auction. However, before his property was auctioned, he paid the debt and resolved the issue. In 1998, he found that his debt and property auction records appeared whenever anyone searched his name online. He challenged it before the Spanish Data Protection Authority for the removal of the information, as it was

[12] General Data Protection Regulation, 2016, "*Principles relating to processing of personal data*", art. 5, available at: https://gdpr.eu.org/art/5/ (last visited on Apr. 30, 2025).
[13] Diksha Pundir, "*Right to Be Forgotten: A Journey from Principle to Legal Right in India*", V(4) Indian Journal of Law and Legal Research (ISSN: 2582-8878) (2023).
[14] Google Spain SL v. Agencia Española de Protección de Datos (AEPD) & Mario Costeja González (Judgment) [2014] ECHR C-131/12.

causing harm to his reputation. However, the Authority directed Google to remove the information, not the whole newspaper.

Google challenged this direction before the European Court, which also upheld the order and observed that although Google does not create information, it is responsible for the data shown on its search engine.

The court further said that people can be forgotten or let alone. If the available information on Google becomes outdated, irrelevant, or inaccurate, then the concerned person can request the deletion of the data. However, the court also highlighted the need to balance privacy rights and public interest, and removal requests should be considered case-by-case, ensuring that public interest and freedom of access to information cannot be hindered abruptly.

INDIAN LEGAL LANDSCAPE: SCOPE, EVOLUTION, AND CHALLENGES

In India, the RTBF is not directly mentioned under any statute; however, its core meaning is being applied on a case-by-case basis in cases related to victims of sexual offences. Specific provisions such as Section 228-A of the Indian Penal Code and Section 327 of the Criminal Procedure Code mandate that the identity of the victim of sexual offences cannot be disclosed except for the victim's interest.

In Justice K S Puttaswamy (Retd.) v. Union of India[15]The Supreme Court analysed privacy rights extensively. It also discusses the concerns about state and non-state actors' control over individuals' personal information. According to the Court, our increased reliance on the Internet actively and passively increases our digital footprint. Even the collected personal data can be used to influence one's behaviour. Also, it has a stifling effect, meaning that the people will freely express no new ideas or opinions.

Descent and differences will be heavily monitored by the state and non-state actors. In these circumstances, the right to be forgotten becomes very important for protecting individual freedom, not only in the virtual world but also in the real world. The court further held that

[15] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCR 569, available at: https://digiscr.sci.gov.in/admin/judgement_file/judgement_pdf/2017/volume%2010/Part%20I/justice%20k%20s%20putiaswamy%20(retd.),_union%20of%20india%20and%20ors._1700550294.pdf (last visited on May 1, 2025).

privacy promotes liberty and dignity. Privacy lets people think freely, and these thoughts ultimately translate into speech, and now it's a personal choice to whom these thoughts should be shared. For example, if anyone wants to criticise someone but doesn't want to share it with the whole world. Now, on the Internet, any information remains safe and secure, whether it is anybody's criticism, your personal information, or anything. In most cases, anyone can access it, which has real consequences. Therefore, at the current time, the inclusion of RTBF in legislation has become very important and a necessity of the hour.

The Supreme Court also expressed its concern that digital information is permanent, and once it is on any digital platform, it becomes challenging to obliterate its traces from the public domain. Therefore, individuals should have control over their details in whatever manner they want to use them. Thus, the court indirectly reinforces the need for the RTBF in India.[16] Thus, although Puttaswamy was the landmark court decision paving the way for RTBF in India, RTBF remains subject to limitations and has not been explicitly mentioned even under the Indian Data Protection law.[17]

On July 31, 2017, the government of India formed a 10-member committee under former Supreme Court judge Justice B N Srikrishna to examine the key data protection issues in India and the mechanism for resolving them.[18] The committee was tasked "to study various issues relating to data protection in India" and "to make specific suggestions for considerations of the Central Government on Principles to be considered for Data protection in India and suggest a draft data protection Bill."[19] The committee played a crucial role in developing India's Personal Data Protection Law and setting the foundation for its privacy laws.[20] The committee under the chairmanship of Justice Sri B N Srikrishna, to give recommendations on the Data Protection Law of India, marked the initial phase of data privacy law.[21]

---

[16] *Ibid.*
[17] *Ibid.*
[18] The Hindu Centre, "*Official Documents: Justice B.N. Srikrishna Committee Report and Personal Data Protection Bill, 2018*" (July 31, 2018), available at: https://www.thehinducentre.com/resources/article24561713.ece (last visited on May 1, 2025).
[19] *Ibid.*
[20] Committee of Experts on Data Protection, "*A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians"* (Government of India, July 27, 2018), available at: https://prsindia.org/files/bills_acts/bills_parliament/2019/Committee%20Report%20on%20Draft%20Personal%20Data%20Protection%20Bill,%202018_0.pdf (last visited on May 1, 2025).
[21] Jane Lalnunsiami, "*Rights to be Forgotten: A Necessary Implication of Right to Health: India's Privacy Prospects Vis-A-Vis Europe's GDPR Policy*", 2(10) The Academic 338-346 (ISSN: 2583-973X) (2024).

However, the committee's recommendations were only partially incorporated under the Personal Data Protection Bill 2019 and even later on the 2023 Bill. Unlike the EU's GDPR, India's framework does not allow for an easy opt-out and removal mechanism for the data. The Indian data protection law also allows personal data to be used on the pretext of legitimate uses even without the consent of the concerned persons. The lack of a precise opt-out mechanism makes it very difficult to erase their data.

PERSONAL DATA PROTECTION BILL, 2019

In 2017, the Supreme Court stated privacy as a fundamental right. A ten-member committee was formed to prepare a draft on data protection. The committee presented the draft of the Personal Data Protection 2018 along with its report to the Ministry of Electronics and Information Technology. On this report and draft basis, a bill named Personal Data Protection Bill, 2019, was introduced in the Parliament.[22] The Bill's purpose was to give individuals the right to access, correct, delete and transfer their data. The organisation must obtain informed consent before taking any person's data. The Bill also creates the Data Protection Authority, which will keep an eye on any violation of any person's Personal Data. Also, he decides disputes related to it, and any decision given by it can be appealed to the Supreme Court. In an emergency, legal matters or for government benefits, personal data can be processed even without the concerned person's consent.[23]

Later, the Bill was sent to the Joint Committee of Parliament (JPC), which proposed several amendments to the Original Bill. Various Stakeholders, such as big tech companies, raised concerns about data localisation and government powers to access personal data. Because of this, the government decided to roll back the current Bill and prepare a new Draft.[24]

[22] Anurag Vaishnav, "*The Personal Data Protection Bill, 2019: All You Need to Know*", *PRS Legislative Research Blog*, Dec. 23, 2019, available at: https://prsindia.org/theprsblog/personal-data-protection-bill-2019-all-you-need-know (last visited on May 1, 2025).
[23] *Ibid.*
[24] "*Union government rolls back Data Protection Bill*", The Hindu, Aug. 3, 2022, available at: https://www.thehindu.com/news/national/union-government-rolls-back-data-protection-bill/article65721160.ece (last visited on May 1, 2025).

DIGITAL PERSONAL DATA PROTECTION BILL, 2023

The DPDP Bill was introduced in parliament on August 3, 2023. It aimed to balance individual privacy rights and the government and businesses' need for legitimate data use.[25] The bill covers data collected online or offline, which is later digitised. It also covers the data a foreign government or company collects about Indian users. The consent requirement was the same as in the earlier bill, with the same legitimate use exemption. Under this Bill, people can access, correct, and erase their data and seek grievance redressal. Finally, the DPDP Bill was passed by both houses, signed by the president, and became an Act.

Thus, the DPDP Act was made to protect individuals' data, but it does not explicitly use the term "right to forget." Instead, it provides the right to erasure under Section 12(1), which allows a data principal to request that a data fiduciary delete their Data.[26] Knowing the difference between the RTBF and the right to erasure becomes essential here. The right to erasure ensures the deletion of data from the server of the data fiduciary, meaning the entity handling the data. The RTBF goes a step further and enables individuals to prevent the continued availability of their data, including search engine results and other public records.

Essential Features of the DPDP Act, 2023[27]

1. The Act applies to Digital Personal data, whether processed in India or outside India, if it relates to Indian users.
2. The business organisation must obtain informed consent before collecting the personal data.
3. People can access their data, make necessary corrections, and delete it.
4. The government reserves the right to process personal data without the users' consent if it involves national security, public order, or legal investigation.

[25] PRS Legislative Research, "*Legislative Brief: The Digital Personal Data Protection Bill, 2023*" (2023), available at:https://prsindia.org/files/bills_acts/bills_parliament/2023/Legislative_Brief_Digital_Personal_Data_Protection_Bill_2023.pdf (last visited on May 1, 2025).

[26] Ajay Kumar, "*Exploring the Right to be Forgotten: Legal Perspectives and Challenges in India and Beyond*", VI(4) Indian Journal of Law and Legal Research 1391 (ISSN: 2582-8878) (2024).

[27] Ahuja and S. Kapadia, "*Digital Personal Data Protection Act, 2023 – A Brief Analysis*", Bar and Bench, available at: https://www.barandbench.com/law-firms/view-point/digital-personal-data-protection-act-2023-a-brief-analysis (last visited on May 1, 2025).

5. The Data Protection Board of India was set up to investigate complaints regarding data misuse and related disputes and to penalise wrongdoers. For serious violations, the penalty can be up to rupees 250 crores.
6. Data fiduciaries must obtain verifiable consent from the Guardian before accessing a Child's data, and the action must not negatively impact the child's well-being. Also, the organisation cannot monitor behaviour or target children with ads.[28]

Concerns and Criticism of the DPDP Act, 2023[29]

1. Government exemption in the national interest can lead to unchecked data collection, potentially violating privacy rights.
2. The Act does not address harm regulation due to identity theft, financial loss, or profiling.[30]
3. The RTBF is only partially included in the act and is not explicitly mentioned anywhere.
4. Personal Data can be transferred outside India, but there is no evaluation mechanism for data protection standards in recipient countries.
5. The term of Members of the Data Protection Board is 2 years, with reappointment eligibility, which will affect their independence.
6. The Act limits the scope of the Right to Information Act, making it harder for Journalists and Activists to access government-related Data.

ENFORCEMENT CHALLENGES

The enforcement of the RTBF in India faces considerable challenges due to the ambiguity in the DPDP Act and the absence of clear legislative guidelines. Due to ambiguity and the lack of clear guidelines, different courts interpret RTBF differently, resulting in inconsistency in judicial decisions. These legal vacuums and complexities exacerbate individuals' ability to assert their RTBF effectively, making the removal of personal data or online content challenging and unpredictable.[31]

[28] *The Digital Personal Data Protection Act, 2023*, s. 9, available at: https://indiankanoon.org/doc/98869575/ (last visited on May 1, 2025).
[29] *Supra* note 27.
[30] *Supra* note 25.
[31] Poorvaja Subramanian and Anjali Viswanaathan, "*Erasing the Past: The Right to be Forgotten in India – Progress, Pitfalls, and Prospects*", 6(6) International Journal for Multidisciplinary Research (E-ISSN: 2582-2160) (2024).

Another measure of challenges in enforcement is striking a balance between an individual's RTBF and the public's right to access information. Article 19 of the Indian Constitution gives persons the right to freedom of expression, enabling them to voice their opinion and at the same time have access to information freely. This creates a conflicting scenario when a person requests the removal of his records, and simultaneously, another person claims their right to know. Courts frequently face these conflicting interests where they have to weigh the protection of dignity and privacy of a person, and on the other hand, maintaining public access to significant information in broader societal interests.[32]

Cross-border Enforcement of RTBF becomes complicated because there is no harmonised global standard, and different countries have different laws and interpretations of the RTBF.

Different Countries have different data protection laws and have interpreted the RTBF differently. Because of this, it is challenging to apply the RTBF uniformly at the global level.[33]

RTBF V. RTI: TWO OPPOSING RIGHTS

The RTBF and RTI serve two opposing purposes. RTBF promotes privacy and allows individuals to remove their data from digital platforms. In contrast, RTI promotes transparency and public interest and mandates that people have the right to access information on the Internet. When an individual requests to remove data but the government prohibits it for public interest or national security, the conflict between these rights is visible.[34]

Thus, where RTBF promotes individual privacy by allowing users to delete outdated and irrelevant data, the RTI promotes transparency and good governance by keeping old records. Even the judiciary faces a dilemma regarding whether RTBF can supersede RTI. However, the courts have noted that RTBF is not an absolute right. A person can be prevented from exercising this right if the matter relates to national security, public order, criminal history or financial records.

---

[32] *Ibid.*

[33] Debaditya Das and Arti, "*A Study on Right to Forgotten with Right to Life under Article 21 of Indian Constitution*", 4(4) International Scientific Journal of Engineering and Management (ISSN: 2583-6129) (2025).

[34] Nandan D, "*Right to Be Forgotten and Right to Information: A Philosophical Analysis in the Indian Context*", IV(5) Indian Journal of Law and Legal Research (ISSN: 2582-8878), available at: https://www.ijllr.com/post/right-to-be-forgotten-and-right-to-information-a-philosophical-analysis-in-the-indian-context (last visited on May 3, 2025).

The Absence of clear-cut legislation on this issue in India results in judicial decisions acting as a light bearer and as a guide.[35]

The Delhi High Court in Jorawar Singh Mundy v. Union of India[36] Consider the Applicability of the RTBF. In this, the court acquitted the person of all criminal charges, and still, case-related information is available over the internet, which tarnished his image. Therefore, he requested the removal of information from the court. The court granted the interim protection by directing digital platforms to prevent a judgment from appearing in search engine results. The court also considers the dilemma of RTBF and the public's right to access the information**.]**

The court also stated that the RTBF is not an absolute right, and specific information must remain accessible to the general public if it serves a legitimate interest. Three-tier frameworks should be adopted to balance these two rights.

1. Search engine delisting,
2. Anonymisation in secondary sources,
3. Preservation of Primary court records.

The RTBF should not supersede RTI entirely but must be applied selectively. The court must protect privacy while maintaining judicial transparency to uphold good governance.[37]

AN INTERNATIONAL PERSPECTIVE OF RIGHT TO BE FORGOTTEN AND ITS EVOLUTION

EUROPEAN UNION: BALANCING RTBF AND PUBLIC ACCESS TO INFORMATION

[35] *Ibid.*
[36] Jorawar Singh Mundy v. Union of India, WP (Crl.) 391/2021 (Del HC, Aug. 13, 2021).
[37] V. Sreedharan, "*Transparency, Good Governance and the Right to be Forgotten*", National Law School of India University, Apr. 5, 2022, available at: https://ceerapub.nls.ac.in/transparency-good-governance-and-the-right-to-be-forgotten/ (last visited on May 3, 2025).

The RTBF is generally understood as a data protection right allowing individuals to request the removal of personal information that is inadequate, irrelevant, no longer relevant, or excessive.[38]

The EU is also facing the same fiasco as other countries over the ongoing challenge of balancing the RTBF with Public access to information. This legal and ethical debate revolves around individual privacy while maintaining freedom of expression, access to information, and historical accuracy.

In 1995, the European Council passed Directive 95/46[39] Protecting individuals regarding the processing of personal data and the free movement of such data. Art 12 of the directive allows data subjects to obtain from the controller, and Art 14 gives the data subjects the right to object.[40] Though the provisions of the directive don't explicitly label the RTBH, in a basic sense, a collectively formed RTBF, they empowered individuals to remove outdated or unlawfully obtained personal data. In the series of recognising personal data protection, in 2001, the EU Charter of Fundamental Rights came into effect, and Article 8 of the charter protects personal data. Under the Data Protection Directive, the RTBF was first recognised in the Google Spain Case.[41] The Court of Justice of the European Union held that Google must hide links related to personal information from search results when the request is made by the person to whom the data is related, unless a substantial public interest suggests otherwise. The core theme of the case is the tension between privacy and data protection and freedom of expression. In the tension of all the rights, the CJEU didn't create an absolute censor power; it assumed that a person's right to privacy is more important than the public's need to access outdated or unnecessary information.

[38] Eliska Pircova and Estelle Masse, "*EU Court Decides on Two Major Right to Be Forgotten Cases: There Are No Winners Here*", Access Now, Jan. 13, 2023, available at: https://www.accessnow.org/eu-court-decides-on-two-major-right-to-be-forgotten-cases-there-are-no-winners-here (last visited on May 4, 2025).

[39] Directive 95/46/EC of the European Parliament and the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995, available at: https://www.refworld.org/legal/reglegislation/eu/1995/en/13712 (last visited on May 4, 2025).

[40] Debbie Heywood, "*The Evolution of the EU's 'Right to Be Forgotten*", Taylor Wessing, 2019, available at: https://www.taylorwessing.com/en/interface/2019/privacy-theres-more-to-it-than-gdpr/the-evolution-of-the-eus-right-to-be-forgotten (last visited on May 4, 2025).

[41] Google Spain SL v. Agencia Española de Protección de Datos (AEPD) (Judgment) [2014], available at: https://globalfreedomofexpression.columbia.edu/cases/google-spain-sl-v-agencia-espanola-de-proteccion-de-datos-aepd/ (last visited on May 4, 2025).

Over time, the need for stronger, uniform rules grew, leading to the EU's GDPR. The directive was replaced by the GDPR in 2016, which became enforceable in 2018. [42]In GDPR Article 17, there is a promise in the form of the "right to erasure." Under articles 17 and 19 of the GDPR, individuals can be forgotten when their data is no longer necessary, processed unlawfully, or irrelevant to its original purpose. If their data were made public, the controller must take reasonable steps to ensure its removal. However, this right does not apply if the data is needed for legal compliance, public interest, or freedom of expression.[43]

The Google Spain Case 2014 made the world rethink how online privacy should work. The EU's RTBF is now an official, but it has limited rights in data protection. It balances personal privacy with the public's access to information. The EU's RTBF has opened a new chapter in privacy law that will shape policies in Europe and worldwide.

UNITED STATES – FIRST AMENDMENT CONCERNS AND ABSENCE OF RTBF

In the US, the idea of legal protection for personal histories, particularly embarrassing and harmful past events, has long existed in American jurisprudence. One of the earliest privacy protections stemmed from property rights, specifically the principle that "a man's house is his castle," which was widely applied in the 19th century.[44] Courts recognised that a person has the right to exclude others from their private spaces, thus upholding the sanctity of the home. Later, trespass laws reinforced this notion, penalising unauthorised entry and intrusion. The Fourth Amendment of the US Constitution also gave crucial safeguards from unreasonable searches and seizures, upholding that individuals have the right to protect their personal belongings and private spaces even from government intrusion and interference.[45] Thus, while the RTBF was not explicitly mentioned anywhere in 19th century literature, its foundational idea gradually came from privacy, individual dignity, reputation and the right to be let alone. While the RTBF

[42] Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995, available at: https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:31995L0046 (last visited on May 4, 2025).
[43] Data Protection Commission, "*Right to Erasure: Articles 17-19 GDPR*", Data Protection Commission Ireland (n.d.), available at: https://dataprotection.ie/en/individuals/know-your-rights/right-erasure-articles-17-19-gdpr (last visited on May 4, 2025).
[44] David J. Seipp, "*The Right to Privacy in Nineteenth Century America*", 94 Harvard Law Review 1892 at 1894 (1981).
[45] *Id*. at 1896.

came in light in the cases like Google Spain v. AEPD and Mario Costeja Gonzalez (2014) but its early inception can be traced from the evolution of the privacy protection in the US which safeguarded personal autonomy, confidential communication and restrictions on public disclosure which indirectly contributed in the foundation of the RTBF. These principles later influenced modern debates on data protection over Digital platforms, giving rise to digital privacy, online reputation management, and the ability to remove outdated personal data.[46]

Another early reference to the RTBF can be inferred from the landmark Article "Right to Privacy" by Samuel Warren and Louis Brandeis, published by Harvard Law Review. This article emphasised an individual's right to be "let alone."[47] It criticised uncontrolled press intrusion into private lives, setting the stage for a future legal doctrine, the RTBF.

In the US, there have been differences of opinion in different cases by the courts over the RTBF, as some cases highlighted the importance of the RTBF. In contrast, there have been some cases in which courts emphasise the public's right to access truthful information, and the government can also keep the information if it finds it necessary for national security or in the public interest. Runkle v. Meyer (1803, Pennsylvania) A newspaper published an article alleging a clergyman's past dalliance. The Pennsylvania Supreme Court ruled that stating such personal information is improper for public examination, even if true.[48]

The US does not have any specific legislation that will give effect to the RTBF. The US Congress strengthened the freedom of speech and access to information by the Constitution's First Amendment. Thus, it provides more strength to the media to publish information fearlessly. The US courts also favour the public right to access information and the freedom to publish news in the media. However, specific laws such as the Health Insurance Portability and Accountability Act (HIPAA), 1996 prohibit healthcare providers from disclosing personal information without the consent of the patient or the patient's representative. Similarly, the Drivers' Privacy Protection Act of 1994 prevents the concerned authorities from disclosing vehicle information from the vehicle records. In certain exceptional cases, information is

[46] *Id.* at 1892.
[47] Amy Gajda, "*Privacy, Press, and the Right to Be Forgotten in the United States*", 93 Washington Law Review 201 at 206 (2018).
[48] *Id*. at 209.

allowed to be disclosed.[49] Thus, although the US does not have dedicated legislation to address the RTBF issue, it still tries to serve the purpose through various legislations.

TECHNOLOGICAL AND ETHICAL DIMENSIONS IN THE DIGITAL AGE

The Digital era has transformed how information is stored, retrieved, and erased, raising complex issues regarding privacy and accessibility. The purpose of RTBF was to remove outdated, irrelevant, and harmful information from the online public domain. Still, significant challenges are faced in implementing this, particularly in the context of search engines and artificial intelligence models.[50]

From a technological perspective, deindexing removes specific information from the search engine without erasing it from the source. This mechanism aims to reduce the information's accessibility rather than eliminate it from the source. Search engines use information retrieval models such as Boolean, Probabilistic, vector space, and embedding-based approaches to rank and retrieve data.[51] However, introducing large language models has increased the complexities, as these AI models can memorise and contextualise information. Because of this, erasing and removing data becomes more difficult.

The ethical implications of the RTBF are also very prominent, as unrestricted deindexing can disrupt the collective memory and public access to information. Maintaining a striking balance between individual privacy and societal transparency became a critical issue as unrestricted removal of content and information may hinder historical accountability and legal precedent. Thus, RTBF in the digital age must be approached with technological precision and ethical sensitivity, ensuring that privacy protection does not hamper the integrity of public knowledge.[52]

Another fear emerged from the rapid advancement of Artificial Intelligence, specifically in large language models (LLMS), which gave birth to complex ethical and technological challenges in digital privacy. Unlike traditional search engines such as Google, Yahoo, Bing,

[49] *Supra* note 26 at 1387.
[50] Salvatore Vilella and Giancarlo Ruffo, "*(De)-Indexing and the Right to be Forgotten*", arXiv, Jan. 8, 2025, available at: https://arxiv.org/pdf/2501.03989 (last visited on May 3, 2025).
[51] *Ibid.*
[52] *Ibid.*

etc., the LLMS stores and processes data differently, making RTBF compliance more difficult. Ethical concerns arise as the LLMS can memorise individuals' data, and technological limitations hinder the removal of the data.[53] Solutions such as differential privacy, machine unlearning, and model editing have been offered, but their effectiveness remains uncertain. This rapid development in AI has raised concerns and underscores the need for robust AI regulations to balance with individuals' rights.

RECOMMENDATIONS

There should be a balance between the two rights: the RTBF and the right to know. Therefore, instead of erasing all data from the Internet or other online sources, there should be an alternative option of anonymising personal information so that direct identity revelation can be curbed. Historical news archives should have limited accessibility.[54]

RTBF should be categorically mentioned in the Indian DPDP Act to establish a clear legal guideline to help individuals and organisations understand their rights and obligations.

The Data Protection Authority should also have judicial members to ensure independence and limit executive influence in appointments and operations.[55]

As the Srikrishna Committee did not pay any heed to the state's mass surveillance, this issue should be discussed, and clear guidelines should be laid out on when the state can monitor any person's online activity and personal information.

There should be a twofold test or assessment.[56] This determines what information can be made public and should be kept. The first test aligns with the European Court of Human Rights' Approach, which advocates protecting sensitive personal data such as Race, religion, caste, health status, contact information, etc. This ensures that deeply personal and potentially discriminatory data remains protected from unnecessary public disclosure.

---

[53] Dawen Zhang et al., "*Right to be Forgotten in the Era of Large Language Models: Implications, Challenges, and Solutions*", AI and Ethics, Sept. 10, 2024, available at: https://link.springer.com/article/10.1007/s43681-024-00573-9 (last visited on May 3, 2025).
[54] Simon Verschaeve, "*Going Dark or Living Forever: The Right to Be Forgotten, Search Engines and Press Archives*", (KU Leuven Faculty of Law, Leuven, 2020).
[55] Swati Pandita and Lovely Sharma, "*Right to be Forgotten: A Study with Special Reference to India*", Social Science Research Network (2023).
[56] *Ibid*.

The Second step should be assessing the Actual Harm or the real-world consequences if the data were leaked or certain information was publicised. Factors like reputation, safety or livelihood should be considered before reaching any conclusion. These considerations balance the privacy rights and freedom of information, ensuring that essential public records remain accessible. At the same time, individuals are also protected from undue harm.

CONCLUSION

The RTBF has emerged as an essential aspect of data protection in the digital era, addressing privacy, personal dignity, and people's right to access information on internet sources. While the European Union, through the GDPR, tries to incorporate the RTBF in the form of the Right to erase data from internet sources, its implementation remains a complex issue due to striking a balance between the individual's right to erase and public access to information.

The Google-Spain case reinforces that the individual to whom the personal data belongs should have complete control over it and how they want to use it, whether to remove it or keep it on the Internet. It also sets a legal precedent for search engines' liability. However, challenges persist, specifically in cross-border enforcement, as countries interpret privacy laws differently.

The Supreme Court in the Justice K S Puttaswamy Judgment highlighted the importance of the RTBF principle and privacy rights. However, in the DPDP Act, this right is not included explicitly. Thus, it limits the individual's right to remove outdated or irrelevant data from internet sources.

Technological Advancements have also exacerbated the concern regarding privacy rights on the Internet. Even if information is deindexed from the search engine, its traces will not be deleted entirely unless removed from its source. Therefore, legislators, legal professionals, and technical experts should intervene and find the most suitable way to maintain privacy rights while retaining the right to access information for the public.