

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS



Open Access, Refereed Journal Multi-Disciplinary
Peer Reviewed

www.ijlra.com

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Managing Editor of IJLRA. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of IJLRA.

Though every effort has been made to ensure that the information in Volume II Issue 7 is accurate and appropriately cited/referenced, neither the Editorial Board nor IJLRA shall be held liable or responsible in any manner whatsoever for any consequences for any action taken by anyone on the basis of information in the Journal.

Copyright © International Journal for Legal Research & Analysis

EDITORIAL TEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board



Dr. Namita Jain



Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India. India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020). Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi. Formerly Assistant professor of Law, Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration. 10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.



Avinash Kumar



Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship. He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi. Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi. He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS
ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

THE RIGHT TO BE FORGOTTEN: AN EVOLVING RIGHT

AUTHORED BY - DR. TANVEER KAUR

Assistant Professor, School of Law, UPES.

Abstract

The Right to be forgotten (RTBF) is a key legal principle in digital privacy and data protection. It balances individual rights with public interests. This paper explores the evolution of the Right to Be Forgotten (RTBF), focusing on the landmark Google Spain SL v. Agencia Española de Protección de Datos ruling. It examines how this right affects privacy, free speech, and public interest in the EU and abroad. Case studies and comparative analysis show the difficulties of implementing the RTBF in different legal systems, underlining the need for harmonization and clear instructions. This chapter recommends a balanced RTBF that adjusts to technology while protecting individual rights.

Keywords: *Right to be Forgotten (RTF), Court of Justice of the European Union (CJEU), data protection, General Data Protection Regulation (GDPR), European Union (EU) freedom of expression, public interest, legal frameworks, implementation challenges.*

Introduction

Digital information makes Right to be Forgotten (RTBF) important since personal data is easily accessible and spread online. Under certain conditions, individuals can petition search engines and online platforms to delete their personal data, reclaiming control over their digital identities¹. In May 2018, the General Data Protection Regulation (GDPR) formalized the Right to Be Forgotten (RTBF) in the EU. The law established the RTBF and stressed personal privacy in dynamic digital world². The 2014 case of Google Spain SL v. Agencia Española de Protección de Datos³ clarified the Right to be Forgotten and set a precedent for search engines to manage personal data⁴. The CJEU ruled that people can request that outdated or irrelevant

¹ Bennett, C. J., & Raab, C. D. (2017). *The governance of privacy: Policy instruments in global perspective*. Ashgate Publishing.

² European Commission. (2018). *Data protection and privacy in the EU: Your rights*.

³ (2014) 3 WLR 659

⁴ Cohen, J. E. (2019). What privacy is for. *Harvard Law Review*, 126(7), 1904-1936.

links be removed. This judgment prioritises privacy over information access⁵.

The RTBF presents significant challenges about how to reconcile privacy and free speech. The right may censor prominent figures' information, according to critics⁶. Dynamic internet characteristics and diverse international legal frameworks The Right to Be Forgotten statute requires overcoming many obstacles⁷.

Historical Context

The right to be forgotten and its historical roots

With technological advances and the digitalization of personal data, the RTBF evolved from secrecy and data protection issues. This privilege stems from legal and philosophical concerns about privacy and autonomy. RTBF philosophy values personal dignity and self-determination. As governments and corporations collected more data, European data protection regulations emerged in the 1970s to protect personal data⁸. Early talks on data protection established the framework for later discussions on personal data rights. The "Right to be Forgotten" became famous when social media sites collected massive amounts of personal data. The French Data Protection Authority (Commission Nationale Informatique & Libertes,) recommended that internet users might ask the deletion of their personal data in its 2010 report. This idea emphasized how important it is to manage digital footprints, since information that is out of date or not needed can hurt privacy and image.

The RTBF became law in May 2018 under the EU's GDPR. The European Commission (2016)⁹ states that Article 17 of the GDPR grants the "right to be forgotten," or the right to have personal data erased. The 2014 CJEU ruling in *Google Spain SL v. Agencia Española de Protección de Datos* recognized individuals' ability to request removal of outdated or irrelevant links, significantly impacting this law (Cohen, 2019). This case helped make the RTBF a legal right in the EU. However, the RTBF is not widely used. Privacy and free speech are handled differently in the US, which raises doubts about whether equivalent rights may be implemented

⁵ Margarit, A. (2018). The right to be forgotten: An analysis of its legal and practical implications. *European Journal of Law and Technology*, 9(1), 1-24.

⁶ Kuczynski, J. (2020). Censorship vs. privacy: The dilemma of the right to be forgotten. *Digital Privacy Journal*, 5(1), 45-67.

⁷ Purtova, N. (2018). The right to be forgotten: A European perspective. In *The Oxford handbook of data protection law* (pp. 345-367). Oxford University Press.

⁸ Bennett, C. J. (1992). *Regulating privacy: Data protection and public policy in Europe and the United States*. Cornell University Press.

⁹ European Commission. (2016). *General Data Protection Regulation*.

there¹⁰. The differences between jurisdictions show the difficulties of balancing privacy with public interest and free speech.

Global Responses

The EU

The EU responded most thoroughly to the RTBF. The 2014 CJEU ruling in *Google Spain SL v. Agencia Española de Protección de Datos* established the RTBF as a basic right allowing persons to request deletion of personal data connections under specific conditions. When a person's personal data is no longer needed or if their consent is withdrawn, they are able to request its erasure thanks to the RTBF in the GDPR, which was established by this ruling. Data protection laws worldwide are influenced by the GDPR's balance of private rights and public information.

United States

America has been against RTBF's formalization. The First Amendment's protection of free expression and other American legal standards make such a privilege difficult to exercise. RTBF is excluded from CCPA safeguards¹¹. Critics say the U.S. policy promotes free expression over privacy, calling for a more balanced approach¹². A federal data protection bill has been debated, reflecting the ongoing conflict between privacy and free speech activists.

Latin America

The RTBF has received mixed reviews in Latin America, with some governments recognizing it legally. Brazil's 2018 General Data Protection Law includes GDPR-like rights to data deletion and access (Brazilian Law No. 13,709/2018). The RTBF's effects on public interest and historical record-keeping are still debated¹³.

The Asia-Pacific

Asia-Pacific reactions vary widely. The Privacy Act 1988 of Australia grants data deletion rights but not RTBFs. With their RTBF study, the Australian Law Reform Commission shows

¹⁰ Bennett, C. J. (2017). The right to be forgotten: A comparative perspective. In *Privacy and data protection in the age of big data* (pp. 45-62). Palgrave Macmillan.

¹¹ California Legislative Information. (2018). *California Consumer Privacy Act (CCPA)*.

¹²Regan, P. M. (2017). Privacy, technology, and the right to be forgotten. *Harvard Journal of Law & Technology*, 31(1), 123-150.

¹³ González Fuster, G., et al. (2020). The right to be forgotten in the European Union: The current status and future perspectives. *Journal of Law and Cyber Warfare*, 9(1), 45-68.

a growing interest in worldwide patterns. In Japan, the Act on the Protection of Personal Information (APPI) has strengthened individual rights but does not establish an RTBF¹⁴. India, among other countries, is preparing data protection laws that may include RTBF features, reflecting a growing awareness of privacy rights due to technology advances.

Legal Framework

General Data Protection Regulation (GDPR) of the European Union

The RTBF is primarily based on the GDPR, which went into effect on May 25, 2018. According to the European Parliament and Council (2016), Article 17 of the GDPR concerns the "right to be forgotten" (right to erasure).

1. When personal data is no longer needed for its original purpose, an individual can request its deletion (Article 17).
2. Upon withdrawal of consent and no further legal basis for processing.
3. In cases of data processing that is unlawful.
4. When removal is mandated by law.

The GDPR carefully balances personal privacy rights with public interest by considering considerations such as freedom of expression and information (Article 17(3)). Judicial bodies and institutions have established an extensive body of case law and guidelines to interpret and implement the Act, achieving a nuanced equilibrium¹⁵.

National Implementations and Variations

The GDPR offers a framework, but member states must pass laws to clarify or broaden the RTBF. The CNIL now requires French search engines to examine requests individually (CNIL, 2020). France considers data requester age, sensitivity, and public interest. In contrast, the RTBF's future is uncertain in light of the UK's post-Brexit strategy. Data privacy talks have changed, and there are proposals for a more business-friendly framework that could restrict the RTBF's reach, even though the UK kept the GDPR in domestic law via the EU (Withdrawal) Act 2018. (UK Government, 2021).¹⁶

¹⁴ Kawashima, K. (2021). Data privacy in Japan: Recent developments and future directions. *Privacy Law & Business International Report*, (164), 10-12.

¹⁵ Bygrave, L. A. (2018). *Data protection law: Approaching its rationale, logic and limits*. Kluwer Law International.

¹⁶ UK Government. (2021). *Data protection and privacy after Brexit*.

Global Perspectives

The RTBF is slowly but surely becoming popular outside of the European Union. While the CCPA did establish certain deletion rights in 2019, it does not explicitly acknowledge the RTBF as is the case in the EU. The CCPA does away with customer data deletion requests, but it doesn't cover as much ground as the RTBF did, especially when it came to public records and search engines (California Legislative Information, 2018). In 2020, Japan amended its Act on the Protection of Personal Information (APPI) to improve individual rights such data erasure. Nevertheless, similar to the CCPA, it does not directly include an RTBF, which reflects the fact that different cultural contexts have varied perspectives on privacy rights.

Legal Framework in India

Present Situation

India does not yet have a complete legal system that respects the Right to be Forgotten. But in the 2017 decision of *Justice K.S. Puttaswamy (Retd.) v. Union of India*¹⁷, the Supreme Court ruled that the right to privacy is an inalienable fundamental right. This decision establishes a standard for acknowledging rights to data protection, which may include RTBF. Recognizing the right to be forgotten, the Court made it clear in the Puttaswamy case that it should not be absolute. Under certain circumstances, such as those involving matters of public interest, public health, archiving, research, or legal claims, this right may not be applicable. Claimed that if this right were to be recognized, it would only apply in cases where an individual's personal data is no longer needed or relevant. The right to "erasure" is recognized under the Digital Personal Data Protection Act of 2023, but how this law applies to publicly available data and court records is still up for debate, with different courts reaching different conclusions. Intermediaries are required to remove or limit access to any content that violates privacy within 24 hours of receiving a complaint, according to the Information Technology Rules, 2021. In relation to the Right to Be Forgotten, what are the relevant judicial precedents?

Case of *Rajagopal v. State of Tamil Nadu, 1994*¹⁸: This significant case distinguished the "right to be let alone" from public opinions on documents such as court decisions, which remain accessible for public discourse. . The Gujarat High Court rejected a motion to seal an acquittal from public record, stating that court orders must be available (*Dharamraj Bhanushankar Dave*

¹⁷ Writ Petition (Civil) No 494 of 2012; (2017) 10 SCC 1; AIR 2017 SC 4161

¹⁸ AIR 1995 SC 264 or (1994) 6 SCC 632.

*vs. State of Gujarat, 2017*¹⁹). In a criminal case involving "revenge porn," the Orissa High Court (2020) stressed the importance of a thorough discussion of the right to be forgotten. The execution of this right raises difficult issues that necessitate well-defined legal limitations and means for remedy, as pointed out by the Court.

A criminal case's right to be forgotten was expanded by the Delhi High Court (2021), enabling the removal of facts from search results to safeguard the petitioner's social life and professional opportunities. A system to remove the personal details of a couple embroiled in a difficult marital dispute from search engines was directed to be created by the Supreme Court's registry in a July 2022 order. Because of this, the right to be forgotten could be interpreted in several ways. Concerned about transparent justice and public interest, the Kerala High judicial ruled in December 2023 that the right to be forgotten cannot be applied to ongoing judicial proceedings. The court noted that the right might be considered depending on the precise characteristics of the case and the amount of time that has passed, but it also suggested that legislative clarity is needed. In a rape case that came before the Himachal Pradesh High Court in July 2024, the court ordered the removal of the identities of the victim and the accused, stating that a person should not have to live with the shame of being accused and then exonerated.

Socio-Legal Implications

Privacy vs. Freedom of Expression

The RTBF highlights a crucial issue between privacy and free speech. This tension becomes more apparent when some people want to have dangerous information removed from the internet, while others want to make the point that everyone should be able to access the same information. This section delves into the relationship between these rights, the laws that control them, and pertinent court decisions. This tension is heightened in India due to its diverse population and cultural values of collective memory and individual dignity.

The Right to Privacy

Many legal systems recognize the right to privacy, which allows persons to control the disclosure of their personal information. Article 17 of the General Data Protection Regulation (GDPR) emphasizes the right to erase personal data under certain conditions (European

¹⁹ <https://www.sconline.com/blog/post/2017/02/04/websites-cant-be-restrained-from-publishing-non-reportable-judgments/>

Parliament and Council, 2016). This provision supports the idea that people should be able to maintain their online identities and reputations in an age with lasting digital footprints.

In the Google Spain SL, *Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González* (2014) case, the CJEU ruled that individuals can request to remove outdated personal information from search engine results. The decision emphasises privacy in the digital age and confirms that people can block access to outdated information (CJEU, 2014). After Supreme Court declaration for the privacy a fundamental right, India's recognition of privacy has grown. A nation with a rising online presence is becoming more cognizant of digital rights, and this legislative affirmation encourages citizens to govern their personal data. Without a comprehensive data protection law, exercising this right is difficult.

Freedom of Expression

On the other side, it is impossible to have public discourse, hold individuals accountable, or disseminate knowledge without the freedom of expression, which is fundamental to democratic nations. Those who oppose the RTBF point out that the ability to remove content can limit free speech, especially when it pertains to publicly-interested material²⁰. This conflict becomes apparent when people try to hide embarrassing details about themselves from public view. The Google Spain case highlighted this argument. CJEU: Finding a balance between privacy and free speech is crucial. The Court's 2014 opinion (CJEU) states that while people have the right to erase sensitive information, the public interest in retaining access must be weighed. There will be some removal requests that cannot be granted without conditions, and this judgment recognizes that. Free speech and expression are important rights under the Indian Constitution, underpinning democratic governance. When people remove public-interest content, this legal framework raises questions about governance accountability and transparency. Prolonged concentration on RTBF could limit public discourse, especially in a vibrant democracy like India, say critics.

Balancing Interests

Creating a law that balances privacy and free speech is the true challenge. Jurisdictions handle this balancing differently. The GDPR allows EU removal requests to be assessed individually to balance these interests. To evaluate requests, the European Data Protection Board (EDPB)

²⁰ Sullivan, M. (2017). Public interest and the right to be forgotten: Balancing privacy and freedom of expression. *Media Law Review*, 25(2), 45-65.

adopted rules based on public interest (EDPB, 2020). In contrast, the US supports free speech. The First Amendment protects free speech even when reputation is at danger. This mismatch shows cultural and legal differences in privacy and free speech.

Establishing a legal framework that balances privacy and free speech in India remains a significant challenge. Unlike the structured approach of the GDPR, India lacks clear guidelines for assessing RTBF requests, leaving individuals and authorities uncertain. This legal ambiguity necessitates a careful approach to drafting legislation that respects both rights while considering India's unique socio-cultural landscape.

Public Interest Considerations

The RTBF conflicts with privacy and free speech. While free speech is essential to democracies, privacy permits individuals to manage their data and online identities. In the Google Spain ruling, the CJEU affirmed the right of individuals to remove unnecessary or outdated personal information from search engine results. Critics say erasing data limits free expression, especially if the public needs it. Conflicting interests must be balanced when creating a legal system. In the EU, the GDPR balances these interests, but in countries like the US, the First Amendment protects free speech even if it harms someone's reputation.

Technological Implications

Search Engines and Data Management

The RTBF must manage data while ensuring privacy and accessibility. Google's massive data access drives this dynamic. Search engines must consider regional legal interpretations and sensitivities while processing RTBF requests in India due to varied linguistic and cultural contexts. Similar issues arise in the EU, where the GDPR requires rigorous data erasure (European Parliament and Council, 2016). As people become more conscious of digital rights, India needs dedicated personnel to analyze RTBF demands²¹. In Europe, search engines constantly adjust their algorithms to balance privacy and information access²².

²¹ Binns, R. (2018). Data privacy and the right to be forgotten: The social media challenge. *Computer Law & Security Review*, 34(6), 1247-1260.

²² Morrison, D. (2016). The challenges of implementing the right to be forgotten: A search engine perspective. *Internet Policy Review*, 5(2), 1-18.

Technologies for the Retention and Deletion of Data

There is an effect that the RTBF has on the retention and deletion of data within an organization. Companies in India are coming under growing pressure to build sophisticated data governance systems that are in accordance with both the RTBF and the proposed Personal Data Protection Bill (PDPB), which mandates the timely deletion of personal data upon request²³. This legal environment is comparable to that of the EU, where firms are required to meet severe data management procedures in order to comply with the GDPR (Shadbolt et al., 2016).

The efficient deletion processes are made more difficult by the sharing of data between platforms. In India, the difficulties are made even more difficult by the fact that organizations have different compliance standards and that they send data across international borders (Iyer, 2022). According to Jansen and Van der Meer (2018), this is a reflection of the challenges that are encountered in the United States, where fragmented data privacy legislation bring about complications in the process of maintaining the integrity of data during deletion.

Improving Technologies That Protect Privacy

The RTBF and other privacy restrictions have contributed to the rise in popularity of privacy-enhancing technologies (PETs). Customers in India are wanting greater control over their digital footprints, which is encouraging businesses to incorporate personal electronic signatures (PETs) into their services (Patel, 2021). This is because customers are becoming more conscious of their rights to data privacy. According to Culnan and Bies (2003), this tendency is also seen in nations such as Canada, where businesses are in the process of implementing similar technologies in order to increase consumer trust.

Consumers are able to exercise their right to be forthright (RTBF) through the use of PETs, which also aid businesses in meeting their legal requirements while respecting user privacy. Businesses in India who place a high priority on user privacy by implementing cutting-edge technologies have the potential to gain a competitive advantage. This is in line with worldwide trends, which indicate that privacy is becoming an important differentiator in digital services (Kaur, 2022).

²³ Jung, J., & Ahn, J. (2020). The right to be forgotten on social media: A case study of user privacy and content removal. *Journal of Information Policy*, 10, 80-99.

Managed Access for Users on Social Media

A unique set of RTBF challenges is presented by social media. Particularly in India, the interplay between private and public information presents a unique set of issues, particularly due to the fact that users may accidentally post content that is harmful, which results in an increase in the number of requests for removal (Reddy, 2021). This phenomena is witnessed all over the world, where the instantaneous nature of social media frequently makes it more difficult for users to control their identities when they are online (Rosen, 2012). Social media platforms such as Facebook and Twitter are investigating ways to improve user control over data in India. This would allow for improved monitoring of postings and comments throughout the platform.²⁴ However, the quick generation of content provides ongoing issues, as earlier posts may continue to circulate even after attempts to delete them. This is a reflection of similar concerns that are faced in other countries²⁵.

Case Studies

Case Study 1: Dispute between Google Spain SL and Spanish Data Protection Agency

Background: The Right to Be Forgotten is based on this 2014 CJEU ruling. Mario Costeja González requested the removal of links to his 1998 financial issues newspaper article. He said the material was old and useless, violating his privacy.

Results: Success for González at the CJEU meant that people can ask for search engines to delete links to their personal data if it's too much, irrelevant, or inadequate for the original purpose of processing. With this ruling, the RTBF was formed throughout Europe and the EU's data privacy standards were upheld with regard to search engines.

Significance: This case changed data privacy by forcing search engines to handle RTBF queries and changing online information access²⁶.

Case Study 2:-NT1&NT2 v. Google LLC

Background: This 2018 UK case involved two claimants seeking to erase their personal information from Google search results. NT1 had been convicted, but NT2 had reformed and wanted to move on. The High Court had to weigh privacy and public access.

²⁴ Shadbolt, N., et al. (2016). Big data and privacy: The challenge of the right to be forgotten. *International Journal of Information Management*, 36(4), 723-730.

²⁵ González Fuster, G., et al. (2017). The emergence of privacy in social media: A study of Facebook and Twitter users. In *Privacy and identity management* (pp. 123-140). Springer.

²⁶ De Hert, P., & Papakonstantinou, V. (2016). The right to be forgotten: A comparative study of the legal frameworks in the EU and the US. In *Data protection and privacy: The age of the GDPR* (pp. 3-24). Hart Publishing.

Results: The court found in favor of NT2, allowing him to delete links to his past due to his rehabilitated status and the lack of public interest. The court denied NT1's motion since his criminal conviction was in the public interest (Google LLC v. NT1 & NT2, 2018).²⁷

Significance: Courts must balance individual rights and the public interest while deciding RTBF requests. It also shows how privacy rules change among jurisdictions²⁸.

Case Study 3: GC v. M. J.

Background: In 2019, the CJEU heard a case concerning people trying to remove links to critical news stories. The petitioners claimed the stories damaged their reputation and violated their right to be forgotten.

Results: The CJEU upheld the right to have links removed, confirming that persons can request the removal of irrelevant or unneeded information. The court stressed the relevance of facts and setting in upholding the RTBF (CJEU, 2019).

Significance: This decision clarified RTBF request evaluation criteria and demonstrated the court's dedication to balance privacy and information rights²⁹.

Case Study 4 Google-CNIL

Background: The CJEU considered whether the RTBF should apply globally or solely in the EU in 2019. Google challenged the French data protection body CNIL's global link removal order, claiming it infringed free speech rights in other states.

Results: The court determined that the RTBF applies only to EU search engines, not global ones. This verdict means that while EU people can have information removed from European searches, Google is not required to remove it from global searches (CJEU, 2019).

Significance: This case highlighted the challenges of enforcing privacy laws across jurisdictions, raising questions about the RTBF and global data management (Sweeney, 2019).

Case Study 5: Social Media "Right to Be Forgotten"

Background: Social media networks have struggled with RTBF requests, especially for user-generated content. One noteworthy 2020 case featured a user seeking Facebook to erase personal information and nasty remarks.

²⁷ Google LLC v. NT1 & NT2. (2018). High Court of Justice.

²⁸ Wright, D. (2019). The right to be forgotten: Balancing privacy and public interest in the UK. *European Data Protection Law Review*, 5(1), 17-29.

²⁹ González, M. C. (2020). Privacy in Brazil: The impact of data protection laws on freedom of expression. *Journal of Comparative Law*, 15(2), 123-145.

Outcome: Facebook's answer showed the difficulties of applying the RTBF to social media, where content is widely shared and incorporated. The platform removed the content but was criticized for privacy issues³⁰.

Significance: This case shows how social media businesses struggle with user privacy and the RTBF in fast-changing situations³¹.

Recommendations for Future Frameworks

Comprehensive Legislative Framework

Recommendation: Governments should develop comprehensive legislation that explicitly defines the RTBF, its scope, and its limitations. This legislation should incorporate the following elements:

- **Clear Definitions:** Define key terms, including "personal data," "irrelevant information," and "public interest," to reduce ambiguity.
- **Criteria for Request Approval:** Establish transparent criteria for evaluating RTBF requests, balancing individual rights against public interest and freedom of expression.

Framework Component: The legislative framework should be adaptable, allowing for periodic reviews and updates in response to technological and societal changes.

International Collaboration

Recommendation: Given the global nature of the internet, an international approach is necessary. Countries should collaborate to create harmonized standards for RTBF.

- **Bilateral and Multilateral Agreements:** Encourage countries to enter agreements that recognize and enforce RTBF across borders while respecting local laws and cultural contexts.

Framework Component: Establish an international body to oversee and facilitate discussions on RTBF, sharing best practices and addressing conflicts between jurisdictions.

Recommendation: Develop technological tools that can support RTBF applications and enforcement.

- **Automated Systems:** Create algorithms that assist in processing RTBF requests, ensuring efficiency while maintaining human oversight to address complex cases.

³⁰ Margarit, A. (2018). The right to be forgotten: An analysis of its legal and practical implications. *European Journal of Law and Technology*, 9(1), 1-24.

³¹ Pfitzmann, A., & Hansen, M. (2010). Anonymity, unlinkability, undetectability, and unobservability: A consolidated proposal for terminology. In *Privacy enhancing technologies* (pp. 1-19). Springer.

- **Data Minimization Techniques** Adopt GDPR-compliant solutions that reduce data gathering and retention.
- **Framework Component:** Promote collaboration between technology companies and legal experts to innovate solutions that respect user privacy while maintaining transparency in data practices.

Public Awareness and Education

Recommendation: Increase public awareness and understanding of the RTBF.

- **Educational Programs:** Implement programs aimed at educating individuals about their rights under RTBF, the process of making requests, and the implications of sharing personal information online.

Framework Component: Develop resources and tools for individuals to navigate RTBF requests, making the process accessible and user-friendly.

Balancing Privacy with Freedom of Expression

Recommendation: Establish guidelines that adequately balance the RTBF with freedom of expression.³²

- **Public Interest Tests:** Implement systematic public interest tests for cases where RTBF requests conflict with journalistic or academic expression.

Framework Component: Create an independent review board to assess complex RTBF cases involving freedom of expression, ensuring impartiality in decision-making.³³

Monitoring and Compliance

Recommendation: Establish mechanisms to monitor compliance with RTBF regulations.

- **Regular Audits:** Conduct periodic audits of search engines and data processors to ensure compliance with RTBF requests and the effectiveness of processes in place.

Framework Component: Develop a reporting system where individuals can report non-compliance or grievances regarding the handling of RTBF requests.

Adaptability to Emerging Technologies

Recommendation: Make sure the RTBF framework can handle AI, blockchain, and IoT.

Proactive Assessments: Regularly examine how new technologies affect privacy rights and the RTBF and update legislation to mitigate threats.

³² Sweeney, L. (2019). Privacy, technology, and the global right to be forgotten: Challenges and opportunities. *Internet Policy Review*, 8(2), 1-19.

³³ Rosen, J. (2012). The right to be forgotten. *Stanford Law Review*, 64(1), 88-137.

Framework Component: Create a task force of legal experts, technologists, and ethicists to evaluate and propose amendments to RTBF legislation as technologies evolve.

Conclusion

The RTBF revolutionizes digital privacy, data protection, and freedom of expression. Subsequent to the 2010 study by the French Data Protection Authority and the 2018 General Data Protection Regulation, the RTBF emphasizes individual freedom over personal data in the digital age. The RTBF possesses robust legal support within the EU; yet, its global implementation presents challenges. Non-EU nations, such as the United States and those in the Asia-Pacific region, value freedom of expression above privacy safeguards. This disparity underscores the necessity for a comprehensive legislative framework to harmonize these interests across jurisdictions. The GDPR's equilibrium between private and public interests may serve as a model for other countries implementing similar protections.³⁴

The RTBF has significant socio-legal ramifications as it reconciles privacy and free speech within democratic societies. Cases such as *Google Spain SL v. Agencia Española de Protección de Datos* illustrate the significance of the Right to Be Forgotten in data management and discussions over individual rights. Technological advancements complicate the Right to be Forgotten (RTBF). In a rapidly evolving digital landscape, data retention and deletion necessitate innovative solutions, encompassing privacy-enhancing technologies and robust governance frameworks. Social media platforms have challenges related to user-generated content and the enforcement of the RTBF.

The RTBF must adjust to technical and societal transformations. Thorough legislation must delineate the right, establish clear criteria for its implementation, and accommodate emerging technologies. Establish a global standard for the recognition and enforcement of the RTBF through international cooperation. India faces opportunities and difficulties from the developing Right to be Forgotten. RTBF implementation requires a comprehensive and nuanced strategy, despite the Supreme Court and Personal Data Protection act auspicious start. India must balance individual privacy rights with community goals as it navigates 21st-century digital privacy. Future legislation must incorporate global best practices while respecting India's distinct culture and society.

³⁴ Culnan, M. J., & Bies, R. J. (2003). Managing privacy: The challenge of information technology. *California Management Review*, 45(3), 24-46.