Original Article
ISSN (Online): 2582-7472

ShodhKosh: Journal of Visual and Performing Arts
February 2024 5(2), 1256–1265

THE RIGHT TO BE FORGOTTEN IN INDIA: COMPATIBILITY WITH PART-III OF THE CONSTITUTION

Parth Upadhyay [1], Dr. Rajesh Kumar Verma [2]

[1] Ph.D. Scholar, School of Legal Studies, Babu Banarasi Das University, Lucknow, Uttar Pradesh
[2] Associate Professor, School of Legal Studies, Babu Banarasi Das University, Lucknow, Uttar Pradesh

DOI
10.29121/shodhkosh.v5.i2.2024.5014

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

ABSTRACT

This research paper examines the evolving concept of the "Right to be Forgotten" (RTBF) in India, analysing its legal basis and its maintainability within the framework of Part III of the Indian Constitution. While not explicitly recognized as a standalone right, the RTBF finds its roots in the right to privacy, declared a fundamental right under Article 21 through the Puttaswamy judgment. This right to informational privacy forms the cornerstone of the RTBF, empowering individuals to control their online narrative by limiting the accessibility of outdated or irrelevant personal information. However, the RTBF presents a complex constitutional challenge, as it must be balanced against the freedom of speech and expression guaranteed by Article 19(1)(a), as well as the public's right to information.

This paper explores the inherent tension between these competing rights, analysing how Indian courts have navigated this delicate balance in various RTBF cases. It examines the role of the Digital Personal Data Protection Act, 2023, in providing a legal framework for data protection and incorporating elements of the RTBF. The research delves into the challenges of implementing the RTBF in India, considering the vastness of the digital space, the role of intermediaries, and the need for clear guidelines regarding data erasure. Furthermore, the paper analyses the criteria for balancing individual privacy with freedom of expression and the public interest, emphasizing the importance of judicial interpretation and evolving jurisprudence in shaping the future of the RTBF in India. It concludes by offering suggestions for strengthening the RTBF framework, emphasizing the need for clearer legislation, standardized procedures, enhanced judicial guidance, and public awareness campaigns to ensure its effective implementation while safeguarding fundamental freedoms.

Keywords: Right to be Forgotten, Informational Privacy, Article 21, Article 19(1)(a), Digital Personal Data Protection Act

1. INTRODUCTION

In today's hyper-connected world, our lives are increasingly lived online. Every click, every post, every search leaves a digital trace, forming a comprehensive profile that can be accessed and analysed by anyone with the right tools. While this interconnectedness offers numerous benefits, it also raises concerns about privacy and control over personal information. This is where the "Right to be Forgotten" comes into play[1] .

The Right to be Forgotten, also known as the Right to Erasure, is a concept that allows individuals to request the removal of their personal information from the internet under certain circumstances.[2] This right is not absolute and is

[1] Azur Mendi, A., Etayo Pérez, C. & Torrell del Pozo, A., The right to be forgotten on the Internet for children and teenagers. A survey in Spain. Communication & Society, 35(4), 19-36 (2022).

[2] Haley, K. Sharenting and the (potential) right to be Forgotten. Indiana Law Journal, 95(3), 1005-1020 (2020). Retrieved from https://www.repository.law.indiana.edu/ilj/vol95/iss3/9

often balanced against other fundamental rights, such as freedom of expression and the public's right to access information.

2. HISTORICAL CONTEXT AND LEGAL BASIS

The concept of a right to be forgotten has its roots in European legal traditions, where it was initially linked to the idea of rehabilitation for past offenders. The rationale was that individuals should not be perpetually stigmatized by their past mistakes, especially after they have served their time and reintegrated into society.

In the digital age, this concept has gained new relevance due to the pervasive nature of online information. The internet has a long memory, and information that was once public can remain accessible for years, even decades, potentially harming an individual's reputation, career prospects, and personal life.

Credit goes to European Union for being the forerunner in developing legal status of RTBF.[3] The Right to be Forgotten was formally recognized in 2014 by the Court of Justice of the European Union (CJEU) in the landmark *"Google Spain"* case. The CJEU ruled that search engines, such as Google, can be required to remove links to search results containing personal information that is "inadequate, irrelevant, or no longer relevant."

This ruling established a legal precedent for the right to be forgotten in Europe and has since been incorporated into data protection laws, such as the General Data Protection Regulation (GDPR).[4] The GDPR grants individuals the right to request the erasure of their personal data under certain conditions, including when the data is no longer necessary for the purpose it was collected, when the individual withdraws consent for processing, or when the data has been unlawfully processed. The recognition of RTBF as a right has provided opportunity to safeguard people from various vulnerabilities in the online world.[5]

2.1. SCOPE AND LIMITATIONS

The right to be forgotten is not a blanket right to erase all traces of one's online presence. It is subject to certain limitations and exceptions, which are designed to balance individual privacy rights with other competing interests.

One key limitation is that the right to be forgotten typically applies to search engine results, not the underlying content itself. This means that while a search engine may be required to remove a link to a webpage containing personal information, the webpage itself may remain online.

Another limitation is that the right to be forgotten does not apply to information that is considered to be in the public interest, such as information about public figures or matters of public concern. This exception is intended to protect freedom of expression and the public's right to know.

Furthermore, the right to be forgotten may not apply if the information is necessary for legal reasons, such as for the establishment, exercise, or defense of legal claims.

2.2. IMPLEMENTATION AND CHALLENGES

Implementing the right to be forgotten can be a complex and challenging task. Search engines and other data controllers must establish procedures for receiving and processing erasure requests, while also ensuring that they do not inadvertently infringe on other rights, such as freedom of expression. Protecting privacy of children is also crucial for which strict monitoring and care is required.[6]

---

[3] Kiriiak, O.S., The Right to Be Forgotten: Emerging Legal Issues. Review of European and Comparative Law, 46(3),27-42(2021). Retrieved from-https://www.researchgate.net/publication/354071921_The_Right_to_be_Forgotten_Emerging_Legal_Issues

[4] Regulation (EU) 2016/679".

[5] Guadamuz, Andrés, Developing a Right to be Forgotten. EU Internet Law: Regulation and Enforcement, 59-76 (2017). Retrieved from-http://dx.doi.org/10.1007/978-3-319-64955-9_3

[6] Ross, S., California enacts "Right to be Forgotten" for Minors. Compliance and risk management, General (2015). Retrieved from-https://www.dataprotectionreport.com/2015/01/california-enacts-right-to-be-forgotten-for-minors/

One of the main challenges is determining whether information is "inadequate, irrelevant, or no longer relevant." This assessment often requires a careful balancing of individual privacy rights with the public interest.

Another challenge is the global nature of the internet. Information that is removed from search results in one jurisdiction may still be accessible in other parts of the world. This can make it difficult to fully exercise the right to be forgotten in practice. Protecting the RTBF beyond borders is also a tough task.[7]

2.3. GLOBAL PERSPECTIVES

The right to be forgotten is primarily a European concept, and its legal status varies across different countries and regions. While some jurisdictions have embraced the right to be forgotten, others have taken a more cautious approach, emphasizing the importance of freedom of expression and the free flow of information.

In the United States, for example, there is no federal law explicitly recognizing a right to be forgotten. However, some states have enacted laws that provide individuals with certain rights regarding the removal of their personal information online.

The right to be forgotten is a complex and evolving concept that reflects the tension between individual privacy rights and other fundamental rights in the digital age. It is a balancing act that requires careful consideration of competing interests and values.

While the right to be forgotten is not absolute, it represents an important step towards empowering individuals to control their online presence and protect their personal information. As our lives become increasingly intertwined with the digital world, the right to be forgotten is likely to remain a topic of ongoing debate and development.

2.4. THE RIGHT TO BE FORGOTTEN IN INDIA: NAVIGATING PRIVACY IN A DIGITAL AGE

India, with its burgeoning digital landscape and increasing reliance on online platforms, faces unique challenges regarding data privacy. The concept of the "right to be forgotten" (RTBF), also known as the right to erasure, has emerged as a significant point of discussion in this context. It raises complex questions about individual autonomy, freedom of expression, and the balance between privacy and public interest. While not yet explicitly enshrined in a dedicated law, the RTBF is gradually finding its place within the Indian legal framework, primarily through judicial pronouncements and evolving data protection legislation.

2.5. THE EVOLVING LEGAL LANDSCAPE

India lacks a specific, comprehensive law solely dedicated to the RTBF. However, the right to privacy, declared a fundamental right under Article 21 of the Indian Constitution by the Supreme Court in the landmark *Puttaswamy* judgment, forms the bedrock for discussions surrounding the RTBF. This right to privacy encompasses the right to informational privacy, which is intrinsically linked to the control individuals have over their personal data.

The Personal Data Protection Bill, 2023, which is now an Act, is a key piece of legislation that addresses data protection and incorporates elements related to the RTBF. It grants individuals the right to request the erasure of their personal data under certain conditions, mirroring similar provisions in the European Union's General Data Protection Regulation (GDPR).[8]

2.6. JUDICIAL PRONOUNCEMENTS AND EMERGING JURISPRUDENCE

While legislation is still developing, Indian courts have played a crucial role in shaping the understanding and application of the RTBF. Several High Courts have addressed RTBF petitions, often dealing with cases involving outdated

[7] Fabbrini F. & Celeste E., The Right to Be Forgotten in the Digital Age: The Challenges of Data Protection Beyond Borders. German Law Journal 21(1), 55-65 (2020). Retrieved from- https://doi.org/10.1017/glj.2020.14

[8] Werro, F., The Right to Be Forgotten. In F. Werro (Ed.), The Right to Be Forgotten a Comparative Study of the Emergent Right's Evolution and Application in Europe, the Americas, and Asia (pp. 1-38). Cham: Springer. (2020). https://www.doi.org/10.1007/978-3-030-33512-0

or irrelevant information online, particularly in the context of matrimonial disputes, criminal records, and defamatory content.

These judgments highlight a nuanced approach. Courts typically consider factors like the nature of the information, its relevance to the individual's current life, the public interest in retaining the information, and the proportionality of the impact on the individual's privacy. They often balance the individual's right to privacy against the right to freedom of speech and expression, as well as the public's right to information.

For instance, courts have been more inclined to grant RTBF requests in cases involving spent convictions or where the information is clearly outdated and serves no legitimate public purpose. However, they have been hesitant to grant such requests when the information pertains to matters of public record, ongoing investigations, or involves public figures.

3. CHALLENGES AND CONSIDERATIONS

People must have control over their data.[9] Implementing the RTBF in India presents several challenges. The sheer volume of data generated by a massive population, coupled with the decentralized nature of the internet, makes it difficult to effectively enforce erasure requests. Furthermore, the lack of clear guidelines and standardized procedures can lead to inconsistencies in implementation.

Another critical challenge lies in defining the scope of "personal data" and determining what constitutes "sensitive personal data," which may warrant stronger protection. The balance between individual privacy and freedom of expression also necessitates careful consideration. Overly broad interpretations of the RTBF could potentially stifle legitimate journalistic activity and hinder access to information of public interest.

The role of intermediaries, such as search engines and social media platforms, in implementing RTBF requests is also crucial. Clear guidelines are needed to ensure that these platforms comply with erasure requests while also safeguarding against misuse and frivolous demands.

3.1. BALANCING ACT: PRIVACY VS. PUBLIC INTEREST

The RTBF is not an absolute right. It must be balanced against other fundamental rights and societal interests. Information related to public figures, matters of public concern, or historical events often falls outside the purview of the RTBF. The Right to Information, guaranteed under the Right to Information Act, 2005, also plays a crucial role in this balancing act.

Courts are tasked with carefully weighing these competing interests on a case-by-case basis. This requires a nuanced understanding of the specific facts and circumstances, as well as a clear articulation of the reasons for granting or denying an RTBF request.

4. THE FUTURE OF THE RTBF IN INDIA

The RTBF is still evolving in India. The enactment of the Digital Personal Data Protection Act, 2023,[10] is a significant step forward, providing a legal framework for data protection and incorporating provisions related to data erasure. However, further clarity is needed regarding the specific procedures for implementing RTBF requests, the role of intermediaries, and the criteria for balancing individual privacy with other competing interests.

Continued judicial engagement will also be crucial in shaping the jurisprudence surrounding the RTBF. Court decisions will provide valuable guidance on the interpretation and application of the relevant legal provisions, helping to establish a more robust and consistent framework for protecting individual privacy in the digital age.

[9] Erdos, D., The 'right to be forgotten' beyond the EU: an analysis of wider G20 regulatory action and potential next steps. Journal of Media Law, 13(1), 1–35. (2021). https://doi.org/10.1080/17577632.2021.1884947

[10] The Digital Personal Data Protection Act, 2023 (Act 22 of 2023).

As India's digital landscape continues to expand, the RTBF will undoubtedly remain a central point of discussion. Finding the right balance between individual privacy, freedom of expression, and the public's right to information will be essential for ensuring a healthy and democratic digital ecosystem.

4.1. PART III AND THE RIGHT TO BE FORGOTTEN IN INDIA: A CONSTITUTIONAL CONUNDRUM

The Indian Constitution, through Part III,[11] guarantees fundamental rights that are essential for individual liberty and dignity. While the "right to be forgotten" (RTBF) isn't explicitly mentioned, its conceptual underpinnings intertwine with several enshrined rights, particularly Article 21 (right to life and personal liberty)[12] and potentially Article 19(1)(a) (freedom of speech and expression).[13] This interplay creates a complex constitutional conundrum, demanding a nuanced understanding of how these rights interact and where the RTBF fits within the existing framework.

4.2. ARTICLE 21: THE FOUNDATION OF INFORMATIONAL PRIVACY

The Supreme Court's landmark *Puttaswamy* judgment declared the right to privacy a fundamental right under Article 21.[14] This right encompasses various facets, including informational privacy, which is crucial for the RTBF. Informational privacy acknowledges an individual's control over their personal data and its dissemination. The RTBF, in essence, seeks to empower individuals to control the narrative surrounding their past by limiting the accessibility of outdated or irrelevant information.

The *Puttaswamy*[15] judgment established a three-pronged test for any encroachment on the right to privacy: (1) the existence of a legitimate state interest; (2) a proportionate relationship between the objective and the means employed; and (3) the existence of procedural guarantees against abuse of this encroachment. Any restriction on the RTBF, therefore, must satisfy this test.

4.3. ARTICLE 19(1)(A) FREEDOM OF SPEECH AND EXPRESSION – A COUNTERPOINT

Article 19(1)(a) guarantees the right to freedom of speech and expression. This right, while fundamental, is not absolute and is subject to reasonable restrictions. The RTBF can potentially clash with this right, especially when information sought to be forgotten relates to matters of public record or public interest. For instance, information about a public figure's past actions might be considered relevant to public discourse, even if the individual wishes to erase it.

The courts, when adjudicating RTBF claims, often face the delicate task of balancing the individual's right to privacy under Article 21 against the public's right to information and the freedom of expression under Article 19(1)(a). This balancing act necessitates a careful examination of the nature of the information, its relevance, its potential impact on the individual, and the public interest in its continued accessibility.

4.4. THE INTERPLAY AND THE CONUNDRUM

The constitutional conundrum arises from the inherent tension between these two fundamental rights. While Article 21 protects an individual's right to informational privacy, Article 19(1)(a) safeguards the freedom of speech and expression, which includes the right to disseminate information. The RTBF sits at the intersection of these rights, demanding a careful calibration to avoid undue infringement on either.

The courts must determine whether the information sought to be forgotten is truly outdated, irrelevant, or disproportionately harmful to the individual's privacy. They must also assess whether the information serves a legitimate public purpose. Information pertaining to criminal convictions, particularly spent convictions, presents a

[11] The Constitution of India, part. III.

[12]The Constitution of India, art. 21.

[13] The Constitution of India, art. 19(1)(a).

[14] The Constitution of India, art. 21.

[15] *K.S. Puttaswamy v Union of India* (2017) 10 SCC 1,

complex scenario. While rehabilitation is a societal goal, the public also has a right to know about an individual's past, especially if it might have implications for public safety.

4.5. THE ROLE OF THE LEGISLATURE

While the judiciary has played a crucial role in recognizing the right to privacy and its connection to the RTBF, legislative action is essential to provide a more structured and comprehensive framework. The Digital Personal Data Protection Act, 2023 is a positive step in this direction, offering a legal basis for data erasure. However, it must be carefully implemented and interpreted to ensure a balanced approach.

The legislature needs to address crucial questions:

- **Scope of Personal Data:** Defining "personal data" and "sensitive personal data" is crucial for determining the extent of RTBF applicability.
- **Criteria for Erasure:** Clear guidelines must be established for determining when information is considered outdated, irrelevant, or disproportionately harmful.
- **Role of Intermediaries:** The responsibilities of search engines, social media platforms, and other intermediaries in implementing RTBF requests need to be defined. Social media has become one of the vast platforms where privacy of people is rigorously violated.[16]
- **Exceptions and Limitations:** Clearly defining exceptions, such as information related to public figures or matters of public interest, is vital.
- **Procedural Safeguards:** Robust mechanisms for processing RTBF requests and ensuring transparency and accountability are necessary.

4.6. JUDICIAL INTERPRETATION AND EVOLVING JURISPRUDENCE

Evolution of the RTBF as a right is a great example of judicial interpretivism where judiciary has taken an active role in protecting the rights of individuals.[17] The judiciary's role in interpreting the constitutional provisions related to the RTBF will continue to be significant. Through its judgments, the courts will shape the evolving jurisprudence on this right, balancing individual privacy with other competing interests. The courts will need to develop clear principles for determining the proportionality of RTBF requests and ensuring that they do not unduly infringe on freedom of speech and expression.

The RTBF in India presents a fascinating constitutional puzzle. Its roots lie in the right to privacy under Article 21, but it must be carefully balanced against the freedom of speech and expression guaranteed by Article 19(1)(a). While the judiciary has laid the groundwork for recognizing the RTBF, legislative intervention is crucial for providing a comprehensive legal framework. As India's digital landscape continues to evolve, the interplay between Part III rights and the RTBF will remain a critical area of legal and societal discourse. Finding the right balance will be essential for protecting individual privacy while preserving the free flow of information and upholding democratic values.

In ***K.S.Puttaswamy v Union Of India***,[18] the Supreme Court of India is also set to examine whether the right can be enforced against judgments by courts that reveal the identity of the acquitted person, given the contradictory judgments of the various High Courts on this issue.

In ***Google Spain SL v Agencia Española de Protección de Datos***,[19] the Court of Justice of the European Union (CJEU) held that the right to be forgotten should over-ride the economic interests of search engine operators and internet users'

[16] Jin-Young, K., A study of social media users' perceptional typologies and relationships to self-identity and personality. Internet Research, 28(3), 767-784 (2018). Retrieved from www.emeraldinsight.com/1066-2243.htm

[17] Wulff C.M. The Right to be Forgotten in Post-Google Spain Case Law: an Example of Legal Interpretivism in Action. Comparative Law Review 26, 255–279 (2020).

[18] (2017) 10 SCC 1,

[19] (2014) 3 WLR 659,

freedom to information. It ordered the search engines to de-index links of secondary sources carrying court documents concerning the claimant's acquittal. This precedent highlighted the challenges in the enforcement of this right as it merely lowered the accessibility of information regarding the claimant on a general search; the information could easily be accessed through a more targeted search. The liability imposed by the CJEU on search engines was found unsound before the Argentinian court: in ***Da Cunha v Yahoo de Argentina SRL***,[20] the court held that search engines were merely intermediaries and not liable to shoulder the duty of monitoring third-party data.

In ***SK v Union of India***[21] and ***Jorawar Singh Mundy v Union of India,***[22] the Delhi High Court ordered the information publication sites to remove the accused's name from their search engines and legal databases. The rulings favoured the redaction of information on the reasoning that continuing to associate the claimant's names with criminal accusations despite their acquittal would harm their reputation and privacy. However, in ***Vysakh K.G. v Union of India,***[23] the Kerala High Court stated that the right to be forgotten cannot prevail over the principles of open justice and larger public interest, and declined to overstep judicial boundaries and infringe on the powers of the legislature.

In ***Zulfiqar Ahman Khan v Quintillion Business Media Pvt. Ltd.,***[24] the Delhi High Court supported an individual's 'Right to be forgotten'. In that instance, Plaintiff petitioned the Hon'ble Court for a permanent injunction against the Defendants, who had authored two articles against Plaintiff based on harassment accusations they claimed to have received, as part of the #MeToo campaign. Even though the Defendants agreed to remove the news stories, they were reprinted by other websites in the meantime. The Court noted the Plaintiff's Right to privacy, of which the ''Right to be forgotten'' and the 'Right to be Left Alone' are inbuilt aspects, and guided that any republishing of the content of the originally disputed articles, or any abstract therefrom, as well as altered forms thereof, on any print or digital/electronic platform be held back during the pendency of the current suit.

In ***Dharamraj Bhanushankar Dave v State of Gujarat and Ors***,[25] the Gujarat High Court held that the publishing of any judgment would not be "reportable" as understood in the context of judgments reported by a law reporter, and it cannot interfere with the online publication of the judgment against the petitioner.

In ***Karthick Theodre v Registrar General, Madras High Court & Ors***,[26] the Madras High Court held that the sanctity of an original record cannot be altered except in a manner prescribed by law, and refused to allow the claimant's request for the redaction of information from online published court records. The Supreme Court stayed this order in ***Special Leave to Appeal (C) No(s). 15311/2024*** vide order dated 24 July 2024, and drew parallels between the right to be forgotten and the redaction of specific information of the claimant. The Court considered the plea to be too "far-fetched" and restricted judicial appreciation to requests for the redaction of information or the masking of names of the victims and witnesses.

Digital Personal Data Protection Act, 2023

The relevant sections under the Digital Personal Data Protection Act, 2023,[27] are:

"12. Right to correction and erasure of personal data[28]

[20] *Da Cunha v Yahoo de Argentina SRL* AR/JUR/40066/2020

[21] 2023 SCC Online Del 3544

[22] 2021 SCC online Del 2306.

[23] 2022 SCC online Ker 7337.

[24] 2019 SCC online Del 8494.

[25] 2015 SCC online Guj 2019,

[26] 2021 SCC online Mad 2755.

[27] The Digital Personal Data Protection Act, 2023 (Act 22 of 2023).

[28] The Digital Personal Data Protection Act, 2023 (Act 22 of 2023), s. 12.

(1) A Data Principal shall have the right to correction, completion, updating and erasure of her personal data for the processing of which she has previously given consent, including consent as referred to in clause (a) of section 7, in accordance with any requirement or procedure under any law for the time being in force.

(2) A Data Fiduciary shall, upon receiving a request for correction, completion or updating from a Data Principal,—

(a) correct the inaccurate or misleading personal data;

(b) complete the incomplete personal data; and

(c) update the personal data.

(3) A Data Principal shall make a request in such manner as may be prescribed to the Data Fiduciary for erasure of her personal data, and upon receipt of such a request, the Data Fiduciary shall erase her personal data unless retention of the same is necessary for the specified purpose or for compliance with any law for the time being in force.

13. Right of grievance redressal.[29]

(1) A Data Principal shall have the right to have readily available means of grievance redressal provided by a Data Fiduciary or Consent Manager in respect of any act or omission of such Data Fiduciary or Consent Manager regarding the performance of its obligations in relation to the personal data of such Data Principal or the exercise of her rights under the provisions of this Act and the rules made thereunder.

(2) The Data Fiduciary or Consent Manager shall respond to any grievances referred to in sub-section (1) within such period as may be prescribed from the date of its receipt for all or any class of Data Fiduciaries.

(3) The Data Principal shall exhaust the opportunity of redressing her grievance under this section before approaching the Board."

5. PROTECTING RIGHT TO BE FORGOTTEN: NAVIGATING THE DIGITAL MAZE

In today's digital age, every online activity contributes to a growing digital footprint, raising concerns about privacy and control over personal data. The "right to be forgotten" (RTBF) allows individuals to request the removal of certain personal information, but exercising this right can be challenging. A key strategy for safeguarding RTBF is proactive information management. This includes minimizing the sharing of sensitive details, using privacy settings to control access, and thinking carefully before posting online. Using pseudonyms in online forums and regularly reviewing one's digital presence helps manage personal information effectively. By taking these steps, individuals can reduce their digital exposure and maintain greater control over their online narrative.

5.1. UNDERSTANDING AND UTILIZING RTBF MECHANISMS

Understanding and utilizing RTBF mechanisms requires familiarity with relevant legal frameworks. Laws like the GDPR in Europe and the Digital Personal Data Protection Act in India outline conditions for requesting data erasure. Search engines, such as Google, provide processes for removing links to personal information, requiring justification for requests. Directly contacting website administrators can also help in removing specific data. Additionally, identifying organizations that store personal information and understanding their data retention policies allows individuals to exercise their RTBF effectively.

5.2. UTILIZING PRIVACY-ENHANCING TECHNOLOGIES:

Utilizing privacy-enhancing technologies can help safeguard personal data and manage online presence. VPNs mask IP addresses and encrypt internet traffic, making tracking difficult. Privacy-focused browsers block trackers and ads, reducing data collection. Secure messaging apps with end-to-end encryption protect sensitive communications, while password managers generate and store strong, unique passwords, enhancing account security. These tools collectively strengthen digital privacy and minimize online vulnerabilities.

[29] The Digital Personal Data Protection Act, 2023 (Act 22 of 2023), s. 13.

5.3. MANAGING YOUR DIGITAL FOOTPRINT

Managing your digital footprint helps reduce the amount of personal information available online. Deleting unused accounts prevents old data from remaining accessible. Limiting social media presence and being mindful of shared content enhances privacy. Using temporary email addresses for online sign-ups minimizes exposure, while opting out of data collection and targeted advertising further protects personal information. These steps collectively strengthen online privacy and control over digital identity.

5.6. STAYING INFORMED AND VIGILANT

Staying informed and vigilant is crucial in protecting digital privacy. Keeping up with privacy news and developments ensures awareness of emerging threats and RTBF updates. Educating yourself about online tracking and surveillance techniques enhances digital security. Additionally, recognizing and avoiding phishing scams helps prevent unauthorized access to personal information. Staying proactive in these areas strengthens overall online safety.

5.7. SEEKING PROFESSIONAL HELP

If managing your online presence or exercising your RTBF becomes challenging, seeking professional help can be beneficial. Privacy consultants assist in protecting personal information and managing online reputation, while legal counsel can provide guidance if RTBF rights are violated.

Protecting RTBF requires a comprehensive approach, including proactive information management, legal awareness, privacy-enhancing technologies, and vigilance. While RTBF is not absolute, it empowers individuals to control their digital presence. As technology evolves, staying informed and adaptable is key to safeguarding privacy in an increasingly interconnected world.

6. CONCLUSION AND SUGGESTIONS

The Right to be Forgotten (RTBF) in India presents a complex interplay between Individual privacy, Freedom of Expression, and the ever-evolving digital landscape. While not explicitly enshrined as a standalone fundamental right, its roots lie in the right to privacy under Article 21, as affirmed by the *Puttaswamy* Judgment. This right to informational privacy forms the foundation for individuals to control their online narrative, particularly concerning outdated or irrelevant personal information. However, this right is not absolute and must be carefully balanced against the freedom of speech and expression guaranteed by Article 19(1)(a), as well as the public's right to information.

The constitutional conundrum arises from this inherent tension. The RTBF seeks to empower individuals to manage their digital footprint, while Article 19(1)(a) protects the dissemination of information, even if it pertains to an individual's past. The courts, therefore, play a crucial role in adjudicating RTBF claims, weighing the individual's privacy concerns against the public interest in retaining the information. This balancing act necessitates a nuanced understanding of the specific facts and circumstances of each case, considering factors like the nature of the information, its relevance, and its potential impact.

The Digital Personal Data Protection Act, 2023, is a significant step towards providing a legal framework for data protection and incorporating elements of the RTBF. However, its effective implementation and interpretation will be crucial. Further clarity is needed regarding the scope of "personal data," the criteria for erasure, the role of intermediaries, and the exceptions and limitations to the RTBF.

7. SUGGESTIONS FOR STRENGTHENING THE RTBF IN INDIA

1) **Clearer Legislative Framework:** While the DPDP Act provides a foundation, more specific guidelines are needed regarding the implementation of RTBF requests. This includes defining the roles and responsibilities of data controllers, intermediaries (like search engines), and regulatory bodies.
2) **Standardized Procedures:** Establishing standardized procedures for submitting and processing RTBF requests will ensure consistency and efficiency. This could involve creating a centralized portal or standardized forms for requests.
3) **Balancing Competing Interests:** Developing clear criteria for balancing individual privacy with freedom of expression and the public's right to information is essential. This requires a nuanced approach that considers the context and nature of the information.
4) **Enhanced Judicial Guidance:** Continued judicial engagement is crucial for shaping the jurisprudence surrounding the RTBF. Court decisions should articulate clear principles for determining the proportionality of RTBF requests and safeguarding against undue infringement on other rights.
5) **Public Awareness and Education:** Raising public awareness about the RTBF and how to exercise it is vital. This can be achieved through educational campaigns and resources provided by government agencies and civil society organizations.
6) **Technological Solutions:** Exploring technological solutions, such as privacy-enhancing tools and data anonymization techniques, can empower individuals to manage their digital footprint more effectively.
7) **International Cooperation:** Given the global nature of the internet, international cooperation is essential for addressing cross-border RTBF issues and ensuring effective enforcement.
8) **Regular Review and Updates:** The legal and technological landscape is constantly evolving. Regularly reviewing and updating the legal framework and guidelines related to the RTBF will ensure its continued relevance and effectiveness.

By addressing these suggestions, India can move towards a more robust and balanced approach to the RTBF, protecting individual privacy while upholding fundamental freedoms and ensuring access to information of public interest. The RTBF is not simply about erasing the past; it is about empowering individuals to shape their present and future in the digital age.