International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Erasing the Past the Right to be Forgotten in India Progress Pitfalls and Prospects

Poorvaja Subramanian[1], Anjali Viswanaathan[2]

[1,2]Student, BA LLB, SASTRA Deemed University, Thanjavur.

ABSTRACT

In the digital age, particularly with respect to the developing legal regime in India, the "Right to be Forgotten" has been fast emerging as an important concept in the broad related discourse on privacy. The paper explains how RTBF intersects with the principles of privacy and public interest in India. Founded in the GDPR[3], this concept has generated considerable debate in India, with privacy now being considered a fundamental right under the Constitution following Justice *K.S. Puttaswamy vs. Union of India*[4].

Thus, the fine line that this paper throngs is between the right of erasure of one's digital footprint and societal needs of transparency, freedom of expression, and access to information by the public. Critical analysis with respect to the Indian Data Protection Bill, now the Data Protection Act[5], attempting to incorporate provisions of the RTBF, and juxtaposing the same with judicial pronouncements as well as comparative legal perspectives available in other jurisdictions is what this paper is about.

From case law and statutory provisions to academic discourse, this paper tries to unpack the challenges and opportunities that the RTBF poses in the Indian legal system. More than anything else, it calls for a nuanced approach, aware of individual privacy but equally sensitive to public interest, to finally leave its imprint on the lingering debate about data protection in India.

Keywords: Right to be Forgotten, Privacy, Public Interest, Indian Legal Framework, Data Protection Act, Freedom of Expression, Digital Footprint, Indian Constitution, Data Privacy.

BACKGROUND

The "Right to be Forgotten" (RTBF) has emerged as a crucial aspect of privacy discourse in India,This paper explores the intersection of RTBF with public interest and freedom of expression, analyzing judicial pronouncements and the provisions of the Data Protection Act. By examining these elements, the research aims to highlight the challenges and opportunities presented by RTBF in shaping a balanced data protection regime that respects individual privacy while addressing societal needs.

[1] Student, BA LLB, SASTRA Deemed University, Thanjavur.
[2] Student, BA LLB, SASTRA Deemed University, Thanjavur.
[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance).
[4] K.S. Puttaswamy v. Union of India,(2017) 10 SCC 1, AIR 2017 SC 4161.
[5] Digital Personal Data Protection Act, 2023,No. 22 of 2023,Acts of Parliament, 1992 (India).

LITERATURE

REVIEW Second Chances and Digital Erasure: Do Former Convicts Have the Right to Be 'Forgotten' in India - Sonsie Khatri and Tasneem Fatma[6]

The paper "Second Chances and Digital Erasure: Do Former Convicts Have the Right to Be 'Forgotten' in India?" by Sonsie Khatri and Tasneem Fatma looks at how the Right to Be Forgotten (RTBF) applies to former convicts in India. RTBF comes from the K.S. Puttaswamy v. Union of India case, where it was recognized as part of the right to privacy under Article 21 of the Constitution. But when it comes to criminal cases, where court records are meant to stay public for transparency, the use of RTBF is still not well-developed.

The paper explains how there is a conflict between RTBF and the idea of open courts, where the public has access to court documents. RTBF aims to help people protect their dignity and reintegrate into society, but because India doesn't yet have strong laws for it, courts apply it inconsistently. Cases like *Zulfiqar Ahman Khan v. Quintillion Business Media Pvt. Ltd*. and *Jorawer Singh Mundy v. Union of India* show that judges struggle to find the right balance between protecting privacy and maintaining public interest.

Khatri and Fatma also compare India with places like the European Union, where laws like the General Data Protection Regulation (GDPR) have a more structured approach to RTBF. There, remedies like de-indexing can help people reduce their online visibility without erasing public records, which offers a middle ground between privacy and transparency.

The paper concludes that while India's Digital Personal Data Protection Act, 2023 includes RTBF in a limited way, clearer laws are needed—especially for former convicts. Without better legislation, it's hard for them to protect their privacy and move on with their lives. The authors call for legal reforms that balance privacy, public interest, and transparency in a way that allows former convicts fair opportunities for rehabilitation.

Outcome of the Paper: The paper concludes that former convicts in India are uncertain about using RTBF due to unclear laws.

Research Gap: The research points out that India lacks clear legal guidelines on how to balance privacy with public access to information, especially when it comes to RTBF for former convicts.

1. **An Appraisal of the Right to Erasure as a Part of the Right to Privacy with Special Reference to Data Protection in India and Sri Lanka - Jayamol Padivathukkal Sasidharan**[7]

The paper "An Appraisal of the Right to Erasure as a Part of the Right to Privacy with Special Reference to Data Protection in India and Sri Lanka" by Jayamol Padivathukkal Sasidharan looks at how the right to erasure is becoming more important as part of the right to privacy, especially in India and Sri Lanka. The rise of technology and the digital world has made privacy harder to protect, which is why the right to erasure—where people can request that their personal data be deleted—is increasingly relevant today.

The author explains that both India and Sri Lanka have laws to protect personal data: the Digital Personal Data Protection Act (DPDP), 2023 in India, and the Personal Data Protection Act (PDPA), 2022 in Sri Lanka. These laws allow people to ask for their personal data to be corrected, updated, or erased. However,

[6] Kahtri, S. and Fatma, T. (2023) 'Second Chances and Digital Erasure: Do Former Convicts Have the Right to Be" Forgotten" in India?', *CALJ*, 8(vii).

[7] J.P. Sasidharan, *An Appraisal of the Right to Erasure as a Part of the Right to Privacy with Special Reference to Data Protection in India and Sri Lanka.*, 4 KDU LJ, (2024).

even though these protections exist, the right to erasure is still limited and hard to enforce fully because of other legal obligations.

The paper compares this with the European Union's General Data Protection Regulation (GDPR), which has a much stronger right to erasure. The GDPR has influenced the way courts in India and Sri Lanka think about privacy, particularly in cases like Justice K.S. Puttaswamy v. Union of India. The paper mentions that courts in both countries have started to see the right to erasure as an important part of the right to privacy.

In conclusion, the author argues that there should be stronger legal protections for the right to erasure to help people avoid reputational harm and protect their privacy. While the current laws in India and Sri Lanka are a good start, more detailed laws are needed to deal with future privacy challenges.

Outcome: The paper concludes that although Indian courts recognize the Right to Be Forgotten (RTBF), it is still inconsistently applied. The author calls for clearer laws that balance privacy and public interest, particularly for former convicts who want to rebuild their lives.

Research Gap: The paper points out that India lacks a clear legal framework for the RTBF, especially for former convicts. This leaves courts to handle cases inconsistently because there are no clear rules to follow.

2. The Right to be Forgotten: Path Towards Efficacious Realization of Data Protection - Tanish Arora[8]

Tanish Arora's paper, "The Right to be Forgotten: Path Towards Efficacious Realization of Data Protection," looks at how the Right to Be Forgotten (RTBF) has developed in the European Union and India. The RTBF started in France as "le droit à l'oubli," which lets people ask for outdated or harmful information about them to be deleted or corrected. This concept became well-known after the Google Spain SL v. AEPD case, where the European Court of Justice ruled in favor of Mr. Gonzalez, allowing him to have old and irrelevant information removed from Google search results.

In India, the RTBF has been slowly recognized, but the legal approach has been inconsistent. For example, the Gujarat High Court in *Dharamraj Bhanushankar Dave v. State of Gujarat* and the Karnataka High Court in another case gave different rulings on the RTBF. The K.S. Puttaswamy v. Union of India judgment finally recognized the RTBF as part of the right to privacy under Article 21 of the Constitution, but with certain limits to protect public interest and legal obligations. The Digital Personal Data Protection Act, 2023, now formalizes the RTBF in India, allowing people to request the correction or deletion of their personal data. However, there are exceptions, like data needed for legal or judicial purposes.

Arora emphasizes the need to balance the RTBF with other rights, such as freedom of speech and access to information. The paper also looks at how the European Union's General Data Protection Regulation (GDPR) has strong protections for data erasure, but also sets limitations. Arora argues that India's legal framework needs reforms to make the RTBF more effective. For instance, there should be clear deadlines for removing data and broader application of the RTBF to all areas where personal data may be stored.

In conclusion, the RTBF is important for protecting privacy, but it has to be carefully balanced with public interest and transparency to ensure it works fairly.

Outcome: The paper points out that the RTBF is becoming more important in India, especially after the Digital Personal Data Protection Act, 2023. It calls for reforms to make the RTBF more effective.

[8]Arora, T.B. (2023) *The right to be forgotten: Path towards efficacious realization of data protection*, *NUALS Law Journal*. Available at: https://nualslawjournal.com/2023/08/29/the-right-to-be-forgotten-path-towards-efficacious-realization-of-data-protection/ (Accessed: 12 September 2024).

Research Gap: The paper identifies the need for clearer guidelines in the Digital Personal Data Protection Act. This includes addressing data erasure across different domains, balancing the RTBF with public interest, and handling bad-faith requests. It also notes that the law should account for how the relevance of data changes over time.

3. Erasing the Archives: Right to be Forgotten in Cyber World - Himanshi Bhatia, Deepti Khubalkar, and Prateek Sikchi[9]

The paper "Erasing the Archives: Right to be Forgotten in Cyber World" by Himanshi Bhatia, Deepti Khubalkar, and Prateek Sikchi looks at the challenges of the Right to Be Forgotten (RTBF) in the digital world. The internet keeps data accessible forever, which is helpful for information retention, but it also creates serious privacy concerns. The RTBF, recognized in the European Union through the General Data Protection Regulation (GDPR) and the well-known Google Spain case, allows people to ask for outdated or harmful personal information to be removed from the internet.

In India, the RTBF has been recognized slowly. The Justice K.S. Puttaswamy v. Union of India case declared privacy a fundamental right under Article 21 of the Constitution, but there are still no clear laws in India to fully enforce the RTBF. Existing laws like the Information Technology Act, 2000, and the Data Protection Bill, 2019, focus on data protection but don't explicitly provide for the right to erase personal information.

The authors compare how RTBF works in India and the European Union, where it is implemented more strongly. They discuss the difficulties of balancing the RTBF with other important rights, like freedom of expression and the public's right to information. Although some Indian courts, like the Delhi High Court and Karnataka High Court, have recognized the RTBF, its exact scope is still unclear.

The paper concludes that India needs stronger laws to properly enforce the RTBF. The authors recommend that the government pass more comprehensive data privacy laws and provide clearer definitions of RTBF to protect individuals from the potential harm caused by the permanent availability of their personal data online.

Outcome: The paper argues that the RTBF is important for protecting personal privacy in the digital world, especially in India, where the laws are still being developed. It suggests stronger data protection laws to balance privacy with freedom of expression and the right to information.

Research Gap: The paper highlights that India does not have a strong legal framework for the RTBF and calls for better laws to address privacy concerns, especially in the digital age where personal data is always accessible.

4. India's pace with the right to be forgotten - Dr. Jayashree Khandare and Rutuja Suryawanshi[10]

The paper titled "India's Pace with The Right to Be Forgotten" explores the evolving legal landscape surrounding the Right to Be Forgotten (RTBF) in India, examining the tension between individual privacy rights and public interest. It draws comparisons with international frameworks, such as the General Data Protection Regulation (GDPR) in Europe, and discusses how India has been slow in developing a clear legal framework for RTBF. The analysis also delves into the judicial interpretations in India, highlighting

[9] Himanshi Bhatia, Deepti Khubalkar, Prateek Sikchi, 'Erasing the archives: RIGHT TO BE FORGOTTEN in cyber world' (2022) *Russian Law Journal* [Preprint]. doi:10.52783/rlj.v10i2.284.

[10] Khandare, Dr.J. and Suryawanshi, R. (2022) 'India's Pace with The Right to Be Forgotten', *Journal of Positive School Psychology*, 6(4).

inconsistencies in court decisions regarding RTBF. The role of the Digital Personal Data Protection Act is discussed, emphasizing the need for a balance between protecting personal data and ensuring access to public information.

Research Gap: There is a lack of clarity in Indian laws on how RTBF should be implemented, particularly in cases involving criminal records and public figures, compared to global standards like GDPR.

Research Outcome: The paper suggests that India's legal system needs to develop clearer guidelines and consistent judicial decisions to effectively balance the RTBF with other rights, such as freedom of expression and public interest.

RESEARCH PROBLEM

The ambiguity in the Indian legal framework with regard to the Right to Be Forgotten (RTBF), and its conflict with other fundamental rights, **creates inconsistencies** in judicial interpretation and enforcement especially in cases of **criminal records and reputational issues**.

RESEARCH OBJECTIVE

This research paper aims to critically examine the ambiguities in India's legal framework concerning the Right to Be Forgotten (RTBF), particularly under the Digital Personal Data Protection Act (DPDPA), and how these uncertainties affect judicial interpretations in cases involving criminal records and reputational issues. It also seeks to explore the conflicts between RTBF and other fundamental rights, such as freedom of expression and public access to information, with the goal of proposing legal reforms and policy recommendations to establish a more consistent and balanced RTBF framework in India.

RESEARCH QUESTIONS

1. What are the key legal ambiguities in the current Indian legal framework, particularly the Digital Personal Data Protection Act, regarding the Right to Be Forgotten (RTBF)? What is RTBF and RTE? - Delinking/delisting or complete anonymity?
2. How do Indian courts interpret and apply the RTBF in cases involving criminal records and online reputational issues, and what inconsistencies have emerged in judicial decisions?\
3. What are the conflicting interests between the RTBF and other fundamental rights, such as freedom of expression and public access to information, in the Indian context?(RTI, FREEDOM OF SPEECH, RIGHT TO PRIVACY, whether can be enforced against individuals?)
4. What legal reforms or policy changes are necessary to create a more effective balance between individual privacy rights and the public interest in the enforcement of the RTBF in India?

RESEARCH HYPOTHESIS

The current legal framework and policy provisions in India, particularly under the Digital Personal Data Protection Act and related judicial interpretations, inadequately address the enforcement of the Right to Be Forgotten (RTBF), leading to inconsistent application, especially in criminal records and reputational matters.

Legal reforms introducing clearer guidelines, balancing individual privacy rights with public interest, will enhance the efficacy of RTBF in India.

RESEARCH METHOD & METHODOLOGY

The research methodology for this legal paper involves a doctrinal analysis of existing laws and judicial precedents related to the Right to Be Forgotten (RTBF), utilizing secondary sources such as legal texts, case law, and scholarly articles. The research is qualitative in nature, focusing on an in-depth examination of legislative frameworks, court rulings, and the interplay of RTBF with fundamental rights.
This is an analytical research that focuses on analyzing and interpreting existing laws, judicial decisions, and legal principles related to the Right to Be Forgotten (RTBF).

SCOPE & LIMITATION

The scope of this research is to analyze the Right to Be Forgotten (RTBF) within India's legal framework, particularly focusing on the Digital Personal Data Protection Act (DPDPA), judicial interpretations, and the conflict with fundamental rights. The limitation lies in its reliance on secondary sources for a doctrinal analysis, without incorporating empirical data or practical implementation challenges on digital platforms.

1. Introduction

1.1 Background of the Right to Be Forgotten (RTBF)

The Right to Be Forgotten (RTBF) is a legal concept that empowers individuals to request the removal of personal information from the internet, particularly when such information is no longer relevant or necessary.[11] The origins of this right can be traced back to the 2014 ruling by the Court of Justice of the European Union (CJEU) in the case of *Google Spain SL v. Agencia Española de Protección de Datos*[12], which established that individuals could request search engines to dec-link information that is outdated or irrelevant, thereby protecting their privacy and dignity[13].
In India, while RTBF does not have explicit legislative backing, it has gained recognition through various judicial pronouncements. The landmark case of *K.S. Puttaswamy v. Union of India* (2017)[14] established that the right to privacy is a fundamental right under Article 21[15] of the Indian Constitution. The Supreme Court observed that this right encompasses an individual's ability to control their personal data and existence on the internet[16]. Subsequent cases, such as *Jorawar Singh Mundy v. Union of India* (2021)[17], have further reinforced this right by allowing individuals to seek removal of judgments and other sensitive information from online platforms.

1.2 Importance of RTBF in the Digital Age

In today's digital landscape, where information can be disseminated rapidly and persistently, the importance of RTBF cannot be overstated. The proliferation of social media and online platforms means that personal data can remain accessible indefinitely, often leading to reputational harm and social

[11] The Evolution of Right to be Forgotten in India.(https://www.scconline.com/blog/post/2022/01/27/the-evolution-of-right-to-be-forgotten-in-india/), Accessed 29th September 2024.
[12] *Google Spain SL v. Agencia Española de Protección de Datos*,C-131/12, ECLI:EU:C:2014:317
[13] Right to be Forgotten – Explained, Pointwise,(https://forumias.com/blog/right-to-be-forgotten/) Accessed 29 September 2024
[14] K.S. Puttaswamy v. Union of India (2017),(2017) 10 SCC 1.
[15] Article 21 of the Indian Constitution,1950.
[16] Right To Be Forgotten," (https://www.drishtiias.com/daily-news-editorials/right-to-be-forgotten-3) Drishti IAS. Accessed 29 September 2024
[17] Jorawar Singh Mundy v. Union of India,W.P.(C) 3918/2021 & CM APPL. 19941/2021.

stigmatization for individuals. The RTBF serves as a crucial mechanism for individuals seeking to reclaim their privacy and manage their online identities.

The significance of RTBF is particularly pronounced in cases involving former convicts or individuals who have been acquitted but still face public scrutiny due to their pasts. The ability to erase or de-link damaging information allows them to reintegrate into society without being perpetually defined by their past actions.[18] Moreover, RTBF aligns with broader human rights principles, emphasizing dignity, autonomy, and the right to lead a life free from unwarranted public interference.

As technology continues to evolve, so too does the need for legal frameworks that protect individual privacy rights while balancing them against public interests such as freedom of expression and access to information. Establishing a clear and comprehensive RTBF framework in India will not only enhance individual rights but also contribute to a more responsible digital ecosystem.

2. Theoretical Foundations

2.1 Conceptualizing the Right to be Forgotten

The Right to be Forgotten has emerged as a significant legal concept in the digital age, primarily aimed at empowering individuals to exercise control over their personal information online. This right allows individuals to request the removal of their personal data from search engines and online platforms, particularly when such data is deemed outdated, irrelevant, or excessive. The conceptualization of the RTBF is rooted in the European Union's General Data Protection Regulation (GDPR), which explicitly recognizes this right under Article 17.[19]

The RTBF is fundamentally anchored in several key principles. First and foremost, it emphasizes personal autonomy, granting individuals the authority to dictate how their personal information is utilized and disseminated. Additionally, it functions as a protective mechanism for privacy in an era where personal data is easily accessible and often misused. Furthermore, the RTBF acknowledges the importance of an individual's digital legacy by allowing them to erase past information that could negatively impact their future opportunities.

The theoretical foundations of the RTBF indicate a shift towards a more privacy-centric approach within data protection laws, highlighting the necessity for a balance between individual rights and public interest.

2.2 Intersection of RTBF with Privacy, Public Interest & Freedom of Expression

The intersection of the RTBF with privacy rights and public interest raises complex legal and ethical questions. On one hand, the RTBF aligns closely with privacy rights, reinforcing the concept that individuals should have control over their personal data and its dissemination. This alignment is particularly relevant in contexts where sensitive information may lead to reputational harm or emotional distress.

Conversely, public interest considerations often complicate the application of the RTBF. The public's right to access information can conflict with an individual's desire for privacy; for instance, when information pertains to public figures or issues of significant societal concern, there may be resistance to invoking the RTBF on grounds that such data contributes to societal knowledge. Moreover, arguments exist suggesting that erasing certain information could distort historical records, thereby impacting collective memory and accountability.

[18] Supra 9,11.
[19] Article 17 of the European Union General Data Protection Regulation (GDPR).

Justice Sri Krishna Committee[20] report observations highlighted that privacy rights must be assessed in relation to public officials' functions. This raises important questions about whether individuals accused of crimes can truly seek redemption through the right to be forgotten, especially when their cases have public implications.

In the case of *Karthick Theodre vs Registrar General*, [21]Madras High Court & Ors (2021)The Madras High Court ruled against allowing the redaction of names and identifiable information from online court records, emphasizing that altering original records must follow legal protocols. This decision was subsequently stayed by the Supreme Court in Special Leave to Appeal (C) No(s). 15311/2024 on July 24, 2024. The Supreme Court drew a distinction between the right to be forgotten and requests for redaction, labeling some claims as "far-fetched." It limited judicial intervention to protecting identities of victims and witnesses rather than erasing criminal records entirely.

The judgment clarified that while individuals may seek redaction concerning specific orders against them, acquitted individuals' names would still appear in FIRs and witness statements, preserving public access to judicial information.

Despite some acknowledgment of the 'right to be forgotten' within privacy rights and legislative frameworks, significant uncertainty remains. The Digital Personal Data Protection Act includes provisions for correcting and erasing personal data; however, these provisions have yet to be implemented. The interplay between this Act and recent Supreme Court judgments will play a crucial role in shaping future claims related to this right.[22]

This situation raises critical questions about whether remedies like redaction or de-indexing are adequate for achieving true "forgetting." Once information is online, can it ever be completely erased? Furthermore, how do principles of open justice, freedom of expression, and the right to information weigh against an individual's claim to be forgotten? These unresolved issues highlight the complexities of navigating privacy rights in an increasingly digital world.

Similarly, the conflict between the RTBF and freedom of expression[23] epitomizes a critical tension in contemporary legal discourse. While the RTBF seeks to protect individual privacy and dignity, freedom of expression serves as a cornerstone of democratic societies by promoting open discourse and access to information.

This conflict manifests in various ways. The application of the RTBF can restrict access to information deemed important for public discourse; for example, removing negative information about an individual may hinder journalistic endeavors or public scrutiny necessary for accountability. Legal precedents illustrate how courts have grappled with these issues across different jurisdictions. In Europe, case law from the European Court of Human Rights (ECHR) has established that while freedom of expression is a fundamental right, it is not absolute; it may be subject to limitations when balanced against other rights such as privacy.

Moreover, different countries approach this conflict through varying legal frameworks. Some jurisdictions

[20] Justice B.N Srikrishna Committe Report, (https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf)

[21] Karthick Theodre vs Registrar General,W.A.(MD)No.1901 of 2021.

[22] Balancing Privacy and Public Interest: The Evolving Jurisprudence of the Right to Be Forgotten in India(https://www.azbpartners.com/bank/balancing-privacy-and-public-interest-the-evolving-jurisprudence-of-the-right-to-be-forgotten-in-india/) Accessed 21 September 2024.

[23] INDIA CONST. art.19.

prioritize freedom of expression over privacy rights, while others adopt a more balanced approach that seeks to harmonize these two fundamental rights.

Ultimately, resolving this conflict requires ongoing dialogue among legislators, legal scholars, and civil society stakeholders to ensure that both individual dignity and societal interests are adequately protected.

3. Legal Framework

3.1 Overview of Privacy Laws in India

The legal framework governing privacy in India has evolved significantly over the years, particularly with the recognition of privacy as a fundamental right by the Supreme Court in the 2017 landmark *Puttaswamy* judgment[24]. This landmark judgment established that the right to privacy is integral to the right to life and personal liberty under Article 21[25] of the Constitution of India. Prior to this, privacy was addressed primarily through various statutes, including the Indian Penal Code (IPC) and the Information Technology Act, 2000 (IT Act), which provided limited provisions for data protection and privacy rights.

The IT Act was initially focused on promoting e-commerce and e-governance but was amended in 2008 to include provisions for cybercrime and data protection.[26] However, the lack of comprehensive data protection legislation led to increasing concerns regarding personal data misuse and privacy violations in an era marked by rapid technological advancement and digitalization.[27]

In response to these challenges, the Indian government has been working on formulating a robust legal framework for data protection. This culminated in the introduction of the Digital Personal Data Protection Act (DPDPA) in 2023, which aims to provide a comprehensive structure for personal data protection, aligning with global standards while addressing local nuances[28] [29]

3.2 The Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, enacted on August 11, 2023, represents a significant step toward establishing a legal framework for data protection in India. The Act aims to safeguard individuals' personal data while facilitating the growth of digital services and technologies.[30]

The Act defines personal data broadly, encompassing any information that relates to an identified or identifiable individual. It creates a consent mechanism that mandates that consent must be obtained from individuals before processing their personal data. This consent must be informed, clear, and revocable.[31]

The DPDPA grants individuals several rights concerning their personal data, including the right to access, correction, erasure, and portability of their data. It establishes a Data Protection Authority (DPA) for overseeing compliance with the law, addressing grievances, and ensuring that individuals' rights are

[24] K.S. Puttaswamy v. Union of India,(2017) 10 SCC 1, AIR 2017 SC 4161.

[25] INDIA CONST. art.21

[26] Nagarathna, A. (2020) 'Cybercrime regulation through laws and strategies: A glimpse into the Indian experience', *International Journal of Digital Law*, 1(1), pp. 53–64. doi:10.47975/ijdl/1nagarathna.

[27] Singh, N. (2024) 'Data Protection and privacy as a fundamental right - an in-depth analysis of the European Union and India's Data Protection Legislation', International Journal For Multidisciplinary Research, 6(2). doi:10.36948/ijfmr.2024.v06i02.15869.

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

[29] Karishma Sundara & Nikhil Narendran, The Digital Personal Data Protection Act, 2023: analysing India's dynamic approach to data protection, 24 Comput. L. Rev. Int'l 129, (2023), https://doi.org/10.9785/cri-2023-240502.

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

[31] Karishma Sundara & Nikhil Narendran, The Digital Personal Data Protection Act, 2023: analysing India's dynamic approach to data protection, 24 Comput. L. Rev. Int'l 129, (2023), https://doi.org/10.9785/cri-2023-240502.

protected. The Act includes provisions for cross-border transfers of personal data, allowing such transfers only under specific conditions that ensure adequate protection for the data.[32]

While the DPDPA marks a significant advancement in India's approach to privacy and data protection, it also faces criticism regarding its enforcement mechanisms and potential conflicts with other laws governing technology and information security.[33]

3.3 Comparative Analysis with GDPR

The General Data Protection Regulation (GDPR), implemented by the European Union in May 2018, is often regarded as one of the most stringent frameworks for data protection globally. A comparative analysis between the GDPR and India's DPDPA reveals certain facts:

Under GDPR, individuals can request erasure if - Their data is no longer necessary for processing; They withdraw consent; They object to processing based on legitimate grounds; The data has been unlawfully processed; Compliance with a legal obligation necessitates erasure. While the DPDPA allows for similar requests, it does not provide a detailed list of conditions under which individuals can exercise this right. This vagueness may lead to challenges in enforcement and clarity regarding when individuals can request deletion.

The GDPR mandates that requests for erasure must be addressed without undue delay, typically within one month. If a request is denied, the individual must be informed of the reasons for refusal. The DPDPA outlines that individuals have rights similar to those under GDPR but lacks specific timelines for compliance with erasure requests. This could potentially lead to delays or inconsistencies in how requests are handled.

Under GDPR several exceptions where the right to erasure does not apply, are outlined. These include situations where processing is necessary for exercising the right to freedom of expression, compliance with a legal obligation, performing tasks carried out in the public interest, or for the establishment, exercise, or defense of legal claims. The GDPR emphasizes that these exceptions must be narrowly interpreted, requiring data controllers to demonstrate the necessity of retaining data under these circumstances.

In contrast, India’s Digital Personal Data Protection Act (DPDPA) does not explicitly define a Right to be Forgotten but allows for data erasure under certain conditions. DPDPA outlines that individuals can request deletion of their personal data when consent is withdrawn. However, this right does not apply if the data is necessary for compliance with legal obligations, prevention of crime, or public health functions. Additionally, data may be retained for statistical or archival purposes. This reflects a balancing act between individual rights and public interests but lacks the comprehensive detail found in GDPR regarding specific exceptions.[34]

While both frameworks emphasize individual rights and consent as foundational principles for processing personal data, there are notable differences in their enforcement mechanisms and penalties for non-compliance. However, India's Digital Personal Data Protection Act represents a significant leap towards robust privacy laws akin to those found in jurisdictions like the EU.

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

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

[34] Bhargav Chaganti, THE RIGHT TO BE FORGOTTEN: A COMPARATIVE ANALYSIS OF THE GDPR AND THE DPDPA, 12 IJCRT, (2024).

4. Case Studies and Judicial Precedents

4.1 Key Cases Influencing RTBF in India

4.1.1 Justice K.S. Puttaswamy v. Union of India (2017)

In the landmark case of *K.S. Puttaswamy v. Union of India*[35], the Supreme Court of India recognized the right to privacy as a fundamental right under Article 21[36] of the Indian Constitution. This ruling established that privacy is integral to various fundamental rights, including dignity and freedom of expression, thereby providing a robust foundation for the Right to Be Forgotten (RTBF) in India[37]. The Court emphasized that "*the right to be let alone*" is essential to individual privacy, which is pivotal for contemplating the significance of RTBF[38].

4.1.2 Sredharan T v. State of Kerala[39] (2016)

The Kerala High Court recognized the Petitioner's RTBF as a part of the Right to Privacy and passed an interim order requiring *Indian Kanoon* to remove the name of a rape victim which was published on its website along with the two judgments rendered by the Kerala High Court in the Writ Petitions filed by her in order to protect her identity.

4.1.3 Zulfiqar Ahman Khan v. Quintillion Business Media Pvt. Ltd (2019)

In *Zulfiqar Ahman Khan v. M/S Quintillion Business Media Pvt. Ltd.*[40], the Delhi High Court directed the removal of two defamatory articles concerning allegations against Khan, recognizing his right to privacy and RTBF. The petitioner argued that these articles violated his dignity and caused professional harm, leading the Court to affirm that individuals have a right to seek removal of harmful information from online platforms. This case aligns with international standards on RTBF and reinforces the necessity for legal frameworks protecting individuals from unwanted online exposure.

4.1.4 Jorawer Singh Mundy v. Union of India(2021)

The case of *Jorawer Singh Mundy v. Union of India*[41] involved a petition regarding the retention of personal data without consent, where the Delhi High Court decided in the favour of the petitioner and held that as the social and professional life of the petitioner is hampered and his reputation is getting affected despite the fact that he was acquitted from all the criminal charges, he is entitled to relief and directed the Respondents Google and Google LLC to block the access to the judgment using their search engine. This ruling further supports RTBF by asserting that unauthorized data retention infringes upon individual privacy rights.

4.1.5 Other Relevant Cases

- **Dharmaraj Bhanushankar Dave v. State of Gujarat(2017)**[42]:

The Gujarat High Court stated that, under Rule 151 of the Gujarat High Court Rules, 1993, the High Court was a Court of Record and thus its judgments could be made available. It noted that even third parties could make applications to the Court's Assistant Registrar to access copies of judgments and other

[35] K.S. Puttaswamy v. Union of India,(2017) 10 SCC 1, AIR 2017 SC 4161.
[36] INDIA CONST. art. 21.
[37] Indulia B and Ridhi, 'The Evolution of Right to Be Forgotten in India' (SCC Times, 14 February 2022) (https://www.scconline.com/blog/post/2022/01/27/the-evolution-of-right-to-be-forgotten-in-india/) accessed 10 October 2024.
[38] Prerna Shree,Oblivisci and the Right to Be Forgotten in India, DNLU-SLJ, (https://dnluslj.in/oblivisci-and-the-right-to-be-forgotten-in-india/) accessed 10 October 2024.
[39] Sredharan T v. State of Kerala, WP (CIVIL) NO. 9478 of 2016.
[40]Zulfiqar Ahman Khan v. Quintillion Business Media Pvt. Ltd, CS (OS) 642/2018.
[41] Jorawer Singh Mundy v. Union of India, W.P.(C) 3918/2021 & CM APPL. 19941/2021.
[42] Dharmaraj Bhanushankar Dave v. State of Gujarat, 2015 SCC OnLine Guj 2019.

documents. In addition, the Court highlighted that when a Court marks a judgment as "non-reportable", it does so in the context of the publication of the judgment in law reports, and that publishing a judgment on an online website does not amount to "reporting" a judgment [para. 7]

- **Vasunathan v. The Registrar General(2016)**[43]

The father (petitioner) filed a writ petition asking for directions for removal of her daughter's name from an order passed by this court as it has negative consequences on her daughter's repute and relationship with her husband. These orders are easily available on online platforms and just by typing her daughter's name, the order reflects in the search results. The Karnataka High court observed that

"This would be in line with the trend in western countries of the 'right to be forgotten' in sensitive cases involving woman in general and highly sensitive cases involving rape or affecting the modesty and reputation of that person concerned."

It held in favor of the petitioner and directed its registry to make sure that the name of the petitioner's daughter doesn't appear in the order anywhere wherever such order is available on the internet platforms.[44]

- **Subhranshu Rout v. State of Orissa(2020)**[45]:

The Orissa High Court rejected the bail application of an accused who was alleged to have uploaded victim's sexual assault personal data on social media platforms. The Court reiterated the importance of the right to be forgotten, noting that if it is

"*not recognized in matters like the present one, any accused will surreptitiously outrage the modesty of the woman and misuse the same in the cyber space unhindered"* [para. 13].

It added that it would be unreasonable to expect a victim to approach the court in every instance when she wanted inaccurate data/information to be removed by an online intermediary – especially as victims find the "justice system complex, confusing and intimidating"

4.2 Analysis of Inconsistencies in Judicial Application

The recognition of the Right to Be Forgotten (RTBF) in India has been marked by significant judicial advancements; however, the application of these principles remains inconsistent across various cases. One primary issue lies in the varying interpretations of privacy rights among different High Courts. For instance, while some courts have embraced a more expansive view of RTBF, others have adopted a more restrictive stance, particularly when balancing individual privacy against freedom of expression. This disparity results in a lack of uniformity in judicial outcomes, leaving individuals uncertain about their rights and the potential for redress. The Gujarat High Court's ruling in *Dharamraj Bhanushankar Dave v. State of Gujarat*[46] illustrates this inconsistency, as the court denied the existence of RTBF, emphasizing that public access to court judgments is essential for maintaining transparency and accountability within the judicial system[47].

Moreover, the challenge of balancing rights is further complicated by the courts' differing approaches to public interest considerations. In certain cases, courts have prioritized the right to information and public

[43] Vasanthan v. The Registrar General,W.P. No. 62038/2016.

[44] Pratyush Singh, *'Right to Be Forgotten: Applicable against Non-State Entities?'* (Law School Policy Review & Kautilya Society, 19 August 2021) accessed 14 October 2024.

[45] Subhranshu Rout v. State of Orissa, 2020 SCC OnLine Ori 878.

[46] *Supra 39*

[47] 'Does the Internet Ever Forget? An Analysis of "right to Be Forgotten" under Indian Law' (AZB, 14 September 2021)(https://www.azbpartners.com/bank/does-the-internet-ever-forget-an-analysis-of-right-to-be-forgotten-under-indian-law/) accessed 21 October 2024.

discourse over individual privacy claims, leading to decisions that may undermine the essence of RTBF. For example, in *K.S. Puttaswamy v. Union of India*, while the Supreme Court recognized privacy as a fundamental right, it also clarified that this right is not absolute and may be limited by public interest considerations. This inconsistency creates an environment where individuals may feel disempowered in seeking to remove harmful or outdated information from digital platforms.

Another significant factor contributing to the inconsistencies in judicial application is the legislative gap surrounding RTBF. Currently, there is no comprehensive legal framework governing this right in India, which forces courts to rely on existing privacy laws that may not adequately address the unique challenges posed by digital contexts. The absence of clear statutory guidelines leads to varied interpretations and applications of RTBF principles, as judges must navigate complex legal landscapes without a coherent set of rules. As noted by legal scholars, the lack of a specific statutory framework contributes significantly to these inconsistencies.[48]

Furthermore, judicial precedents play a pivotal role in shaping the landscape of RTBF claims. However, some precedents emphasize individual rights while others prioritize public interest or freedom of expression. This patchwork approach complicates the enforcement of RTBF and creates uncertainty for both individuals seeking relief and legal practitioners advising clients on potential outcomes. For instance, cases like *Zulfiqar Ahman Khan v. M/S Quintillion Business Media Pvt. Ltd.* demonstrate a willingness to protect individual privacy rights against defamatory content, other rulings have reinforced the idea that public records should remain accessible[5]. As a result, litigants may face unpredictable judicial responses based on the specific court or judge assigned to their case.

In conclusion, while key judicial decisions have laid important groundwork for recognizing RTBF in India, inconsistencies in application highlight broader challenges within the legal framework. These inconsistencies underscore the urgent need for comprehensive legislation that provides clarity and uniformity in addressing RTBF claims. Establishing a coherent legal structure would not only empower individuals to exercise their rights effectively but also promote greater consistency in judicial decision-making across different jurisdictions.

5. Challenges and Recommendations in Implementing RTBF

5.1 Challenges

The implementation of the Right to Be Forgotten (RTBF) in India presents several challenges due to ambiguities in the existing legal provisions. India currently lacks a specific legislation that clearly defines RTBF, leading to varied interpretations by courts across different jurisdictions. This legal uncertainty results in inconsistencies in judicial rulings, making it difficult for individuals to effectively invoke their rights to have personal data or online content removed.

A major challenge lies in balancing the individual's right to privacy with the public's right to access information. Article 19 of the Indian Constitution guarantees the freedom of expression, allowing citizens to express their opinions freely, but this can conflict with an individual's desire to have certain information erased from public view. Courts often struggle to reconcile these competing interests, as they must weigh the individual's right to privacy and dignity against the public's right to know, especially when the information in question is of public relevance. The absence of clear guidelines on how to evaluate RTBF

[48] Prerna Shree,Oblivisci and the Right to Be Forgotten in India, DNLU-SLJ, (https://dnluslj.in/oblivisci-and-the-right-to-be-forgotten-in-india/) accessed 15 October 2024.

requests complicates the task, with courts needing a robust public interest test to determine when privacy should prevail over public access.

Former convicts face particular difficulties under the RTBF framework due to the lasting stigma associated with their past offenses. While these individuals have a right to rehabilitation and reintegration into society, persistent media coverage and online records of their convictions can continue to harm them. The legal system does not provide clear guidance on how RTBF should apply in cases involving former convicts, creating uncertainty about their ability to protect their privacy. Courts may hesitate to grant RTBF requests in such cases due to concerns about public safety and the integrity of the justice system, leaving former convicts in a precarious position where they are subject to continued public scrutiny but lack sufficient recourse for protecting their rights. A more nuanced approach, taking into account the nature of the crime and its relevance to public interest, is essential for addressing these challenges, promoting the reintegration of former convicts while safeguarding public safety.

5.2 Recommendations

To address the gaps, it is essential to enact comprehensive legislation that clearly defines RTBF, its scope, and its limitations. Such legislation should incorporate principles from international standards, such as the General Data Protection Regulation (GDPR) in Europe, which provides a robust framework for data protection and individual rights. This would not only align Indian law with global practices but also ensure that individuals have a clear legal avenue to seek redress for violations of their privacy rights.[49]Balancing the right to privacy with competing interests such as freedom of expression and public interest is crucial for the effective implementation of RTBF.:

An RTBF law would cover several aspects that the Right to Erasure under the Digital Personal Data Protection Act (DPDPA) does not address. Here are the key areas where an RTBF law would extend beyond the existing provisions:

Define the terminology: Clearly define the different terms associated with the right to be forgotten such as “delisting”, “de-indexing”, “redaction”, “anonymisation” etc. to avoid broad or vague interpretations.

Criteria for Exercising RTBF

Nature of Information: Distinguish between personal information that affects an individual's dignity (like health data, past offenses, or intimate details) and information that serves a public interest (such as public figures' activities or matters of public safety).

Harm and Impact: Clearly outline that data subjects must demonstrate significant harm or risk to privacy, dignity, or mental well-being from the continued availability of the data.

Clarification on Types of Content: - Explicitly state that RTBF does not extend to public records (e.g., court judgments, government reports) unless specific circumstances demand it.

Delisting, Deindexing & Redaction of Information : An RTBF law would empower individuals to request delisting or deindexing of specific URLs that appear in search results or redaction of specific information from secondary sources thus preventing easy public access to harmful, outdated, or irrelevant information without necessarily deleting the data from its original source.

An eligibility criteria shall be laid down for each of these requests and upon failure to fulfil these conditions, information becomes ineligible for delisting, de-indexing or redaction.

[49] Sreedharan V, TRANSPARENCY, GOOD GOVERNANCE AND THE RIGHT TO BE FORGOTTEN NATIONAL LAW SCHOOL OF INDIA UNIVERSITY (2022), https://ceerapub.nls.ac.in/transparency-good-governance-and-the-right-to-be-forgotten/ (last accessed 2024).

Protection against Publicly Available Information/ Third Party Data sharing: While the Right to Erasure is effective for data provided directly by the user to a service, it does not cover personal information that is publicly available or shared by third parties, such as news websites, public records, or social media posts. RTBF legislation would allow individuals to request the removal of such data from public access, especially when it is no longer relevant, misleading, or harmful.

Third-party entities must comply with requests for removal, subject to exceptions concerning matters of **public interest, safety,** or **historical relevance, journalistic integrity and freedom**.

Criminal Records and Rehabilitation: RTBF laws can provide individuals with the ability to seek de-indexing or delisting about past criminal records, arrests, or charges from secondary sources

If acquitted, then he requests his personal details to be redacted from secondary sources.

For convicts who have served their sentence and a specific period of rehabilitation has passed, the option of delisting of secondary sources could be made available,

This is crucial for rehabilitation and reintegration, allowing individuals to move on without their past actions being continually resurfaced in online searches.

Balancing Privacy with Freedom of Expression and Public Interest: A specific RTBF law would define criteria to balance an individual's privacy with freedom of expression, public access to information, and the right to information.

Public Interest Clause: Incorporate a clause that explicitly states that the RTBF cannot be used to suppress information that is of genuine public interest, such as information about public figures, matters of public health, or historical events.

Freedom of speech exceptions: Explicitly exempt information processed for journalistic, artistic, or academic purposes to protect freedom of expression and avoid suppression of truthful and relevant information.

Requests for the removal of information involving journalistic content, public archives, and government records shall be assessed with heightened scrutiny. Authorities must ensure that removal does not unjustly limit freedom of expression, journalistic activities, or the right to information, except where privacy concerns clearly outweigh public interest.

Judicial Guidelines and Structured Implementation: RTBF legislation could provide more structured guidelines for courts and authorities, allowing consistent interpretation and application. It would establish clear procedures for individuals to request the removal of information and set out conditions under which such requests can be granted or denied, such as age of the information, public relevance, and the individual's role in public life.

Legal Recourse and Penalties: Failure to respond to legitimate RTBF requests will attract penalties and directives to ensure compliance and Individuals shall have the right to seek legal recourse and claim compensation for any damages resulting from the unauthorized processing of their data.

Standardized Procedures and Appeals: Legislation can introduce standardized procedures for filing RTBF requests and for appealing decisions, which currently vary significantly. By formalizing the process, individuals and organizations would have a clear understanding of how to proceed, including Timelines for making decisions on RTBF requests, Clear steps for appeal if a request is denied as well as defined penalties for non-compliance by data controllers.

This would streamline judicial processes by reducing procedural ambiguities, allowing courts to focus on the substantive aspects of the case rather than procedural issues.

Guidelines for Handling Sensitive Information: A well-crafted RTBF law could offer specific provis-

ions for cases involving sensitive information, such as criminal records, health data, or information about minors. Courts often face dilemmas when dealing with requests related to such information due to the lack of a clear framework.

Geographical and Jurisdictional Limits: Define how RTBF applies to Indian users, especially in cases where content is hosted on foreign servers or involves multinational platforms. Guidance on extraterritorial enforcement would help address jurisdictional issues.

Periodic Review and Updates: Establish a process for periodically reviewing and updating guidelines to keep pace with evolving technology, societal norms, and emerging privacy issues. This will help address new challenges, such as AI-driven profiling or data aggregation.

Proportional Approach: Ensure the RTBF law requires authorities to use the least restrictive means to achieve privacy protection. This can include delinking, de-indexing, or anonymizing information instead of outright deletion, especially when the information is of public interest.

Independent Review Board: Establish a Data Protection Authority (DPA) or an independent review board to oversee the requests and provide a transparent decision-making process, ensuring that each case is evaluated on its merits.However, safeguards shall be established to ensure fairness, impartiality and adherence to due process.

By implementing these recommendations, India can create a more coherent legal framework surrounding RTBF that respects individual privacy while balancing other fundamental rights.

7. Conclusion

This research has examined the challenges and ambiguities surrounding the Right to Be Forgotten (RTBF) within the Indian legal framework, with particular emphasis on the Digital Personal Data Protection Act (DPDPA), case law involving criminal records, and the balancing of privacy rights against public interests like freedom of expression and the Right to Information (RTI). The key findings of this study highlight several pressing issues that need resolution to make the RTBF effective in India.

Firstly, the research revealed that the Indian legal framework, particularly the DPDPA, lacks specific provisions that clearly define the scope of the RTBF. This has led to inconsistencies in judicial decisions, where courts apply varied standards in interpreting RTBF, especially in cases involving criminal records and online reputational harm. Moreover, the ambiguity in defining RTBF — whether it pertains to de-listing or complete erasure — creates further confusion for courts and individuals alike.

Secondly, the study found that Indian courts have struggled to balance the RTBF with competing fundamental rights, especially freedom of expression and the public's right to access information. This conflict is particularly pronounced in cases involving public figures, former convicts, or individuals involved in matters of public interest. While some courts have been willing to grant RTBF, others have emphasized the importance of public access to judicial records and historical information, leading to inconsistent outcomes.

Finally, this research identified a pressing need for comprehensive legal reforms. To create a more consistent and effective RTBF framework, Indian law must introduce clear guidelines for courts on how to evaluate RTBF claims, particularly through a public interest test. There must also be better clarity on how the RTBF should be applied to individuals with criminal records, balancing their right to reintegration with the public’s need for safety and information.