Volume 35, October 2024 ISSN 2581-5504

"Escaping the Digital Abyss: The Right to Be Forgotten in India"

***Khubaib Rehman**
Student, Faculty of Law,
Integral University,
Lucknow, Uttar Pradesh

****Minhum Zaidi**
Student, Faculty of Law,
Integral University,
Lucknow, Uttar Pradesh

*****Sharik Husain**
Student, Faculty of Law,
Integral University,
Lucknow, Uttar Pradesh

ABSTRACT

The exponential growth of personal information online has exacerbated concerns about individual privacy and control over data. The Right to Be Forgotten (RTBF), a concept gaining traction globally, empowers individuals to request the removal of certain information from online platforms. This essay explores the RTBF's potential application in India, a nation lacking a specific law yet witnessing a growing recognition of data privacy rights. The research delves into the RTBF's European origins through GDPR and its subsequent rise as a global conversation. While the Right to Privacy enshrined in Article 21 forms the legal foundation, landmark court judgments reveal an increasing judicial trend acknowledging the right to control online information. These judgments, though not explicitly invoking the RTBF, map the way for a future legal framework of the right to erasure in the digital domain.

The Personal Data Protection Bill, 2019 (PDP Bill 2019) incorporated provisions for the "Right to be forgotten" under Section 27. Though PDP was withdrawn, the revised Digital Personal Data Protection Bill, 2023 (DPDP Bill 2023) retains this crucial right under Section 12 which talks about "right to rectification and erasure of personal data", potentially offering individuals legal avenues to challenge inaccurate or outdated personal data held by data fiduciaries. The essay also argues that dilemma between this principle and freedom of expression, including the public's right to information will remain a crucial consideration. Technical challenges in ensuring complete erasure of information and the potential for misuse by individuals seeking to suppress legitimate information also need to be addressed.

It offers a potential avenue for individuals to reclaim control over their digital footprint and fosters a more balanced information ecosystem. As India navigates the complexities of its evolving digital landscape, a nuanced approach to the RTBF that protects both individual privacy and the free flow of information essential for a democratic society is necessary.

Keywords: Digital Privacy, DPDP, Right to Be Forgotten, Data Privacy Rights in India, Information Erasure, GDPR.

Volume 35, October 2024 ISSN 2581-5504

A. INTRODUCTION

With the vast amount of personal information circulating online, concerns regarding its potential misuse have become more prominent. The digital age has ushered in an era of unprecedented personal data collection. Every click, like, and search query adds to our ever-expanding digital footprint. This data fuels personalized experiences and targeted advertising, but also raises concerns about misuse and exploitation. The concept of the **Right to be Forgotten (RTBF)** emerges as a potential solution that empowers individuals to control their online presence. This right originated from a 2014 European Court of Justice (CJEU) ruling and has since sparked global discussions about data privacy.

The RTBF grants individuals the legal right to request the removal of outdated, irrelevant, or otherwise harmful personal information from search engine results and online platforms. Imagine a world where past mistakes, embarrassing moments, or even outdated information linger on search engines and online platforms indefinitely, potentially hindering employment opportunities or perpetuating a distorted image. As per a survey, 72% of Americans believe they have very little or no control over the data collected about them online.[1] Similar sentiments likely resonate with many Indians as well.

In India, the RTBF is gaining traction through landmark court cases and the recently enacted Digital Personal Data Protection Act (DPDPA). We'll examine these developments, alongside research data on the RTBF's impact globally, to paint a comprehensive picture of its potential role in shaping India's digital future.

B. PRIVACY CONCERNS

The interconnected web of social media platforms, e-commerce websites, and digital services, individuals constantly produce vast amounts of personal information. Every click and keystroke, including browsing habits, location data, preferences, and social interactions, adds to this digital footprint. While this data is often gathered to enhance user experiences and customize services, it also opens the door to potential misuse, exploitation and other malicious purposes. [2] Recent analysis shows that search volume for the keyword "privacy" has increased over the last four years, reaching about 600,000 user requests per month in 2021.[3]

---

[1] Faverio, M. (2023) *Key findings about Americans and Data Privacy*, *Pew Research Canter*. Available at: https://www.pewresearch.org/short-reads/2023/10/18/key-findings-about-americans-and-data-privacy/ (Accessed: 19 April 2024).

[2] Clark, C. (2022) *Your Digital Footprints are more than a privacy risk – they could help hackers infiltrate computer networks*, *Texas A&M Today*. Available at: https://today.tamu.edu/2022/04/11/your-digital-footprints-are-more-than-a-privacy-risk-they-could-help-hackers-infiltrate-computer-networks/

[3] Andrienko, O. (2021) *The rise of data privacy concerns*, *TechRadar*.https://www.techradar.com/news/the-rise-of-data-privacy-concerns .

Volume 35, October 2024 ISSN 2581-5504

The Cambridge Analytica scandal OF 2014 exposed a critical vulnerability in data privacy. The firm harvested millions of Facebook profiles through an unauthorized app, potentially influencing voter behaviour with targeted messaging. This sparked outrage over data misuse and calls for stricter regulations on data collection and use, particularly for political purposes.[4]

While privacy advocates have serious concerns about other ways that biometric data can be used. For example, tech start-up Clearview AI has been targeted by investigations and lawsuits because of the creation of a facial recognition tool powered by billions of images it scraped from social media sites without consent. [5] Such technology raises several privacy and security concerns, including the lack of consent, unencrypted faces, lack of transparency, technical vulnerabilities, and the potential for identity theft, stalking, and harassment. [6]

C. THE EU AND THE RIGHT TO BE FORGOTTEN:

It originated from the 2014 the Court of Justice of the European Union (CJEU) in the case of Google Spain SL, Google Inc. v Agencia Española de Protección de Datos[7], Mario Costeja González, where it was first codified. The case involved a Spanish citizen, Mario Costeja González, who objected to the appearance of a newspaper article about a property auction related to his debts, which was still visible in search results when his name was entered into Google. The court ruled that Google was responsible for removing the search results, establishing the right to be forgotten as a legal precedent in the EU.

This right to be forgotten was a key feature reflected in the General Data Protection Regulation (GDPR) which allows individuals to request the removal of personal information from search engine results or online platforms.

D. IMPACT ON INDIA

The GDPR went through extensive rounds of consultations and finally came into force in 2018. This effort to create a comprehensive data protection regulation in the EU influenced the debate in India. In a move aimed at bolstering citizen privacy, the Indian government announced its intention to establish a comprehensive data protection framework by October 2017. This initiative arose from growing anxieties surrounding the vulnerability of personal

[4] *Revealed: 50 million facebook profiles harvested for Cambridge Analytica in major data breach* (2018) *The Guardian*. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

[5] Gazetteterrymurphy (2023) *How facial-recognition app poses threat to privacy, civil liberties*, *Harvard Gazette*. https://news.harvard.edu/gazette/story/2023/10/how-facial-recognition-app-poses-threat-to-privacy-civil-liberties/

[6] *Facial Recognition Technology and privacy concerns* (21 Dec 2022) *ISACA*. https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2022/volume-51/facial-recognition-technology-and-privacy-concerns

[7] 128 Harv. L. Rev. 735

Volume 35, October 2024 ISSN 2581-5504

information and the absence of effective regulations to address data breaches by widely used messaging services like WhatsApp, Facebook, and Skype.[8]

It was pointed out that it will be very late to keep sleeping on this concern. Following the pressing need for enhanced data protection measures, the Committee of Experts on Data Protection, led by Justice B. N. Srikrishna, was instituted in 2017 to delve into pertinent data protection issues within the country The European Union's General Data Protection Regulation (GDPR) emerged as a potential model for India to emulate. Experts advocated for incorporating best practices and principles from the GDPR while keeping in mind the unique cultural and social context of India.

It proposed that users will have the right to port their data for a fee, seek information on how their data has been used, and have the right to correct it under its section 17 retaining the Principle of Right to be Forgotten as a statutory right.

As India's data economy grows, it finds itself grappling with regulation to catch up with the rich data that Indians are sharing every day, as they log onto hundreds of platforms— Study conducted by Deloitte, reported by PTI, predicts that India will have 1 billion smartphone users by 2026[9]. PDPB was India's first attempt to create a comprehensive data privacy law, however, it was withdrawn and replaced with the DPDP Act in August 2023.

E. THE RIGHT TO PRIVACY AND THE RIGHT TO BE FORGOTTEN IN INDIA: CASES

The Supreme Court of India had recognized the Right to Privacy as a fundamental right in the case of *KS Puttuswamy v Union of India*.[10] The Court had observed that the 'right of an individual to exercise control over his personal data and to be able to control his/her own life would also encompass his right to control his existence on the Internet.' Emphasizing the evolving Landscape of right to privacy, court stated that

> *"An issue like privacy could never have been anticipated to acquire such a level of importance when the Constitution was being contemplated. Yet, today, the times we live in necessitate that it be recognised not only as a valuable right, but as a right Fundamental in Constitutional jurisprudence."*

[8] Goswami, S., Haran, V. and Ross, R. (no date) *Analysis: Data protection in India - getting it right*, *Bank Information Security*. Available at: https://www.bankinfosecurity.asia/analysis-data-protection-in-india-getting-right-a-9866

[9] *India to have 1 billion smartphone users by 2026: Deloitte, The Economic Times*. https://economictimes.indiatimes.com/industry/cons-products/electronics/india-to-have-1-billion-smartphone-users-by-2026-deloitte/articleshow/89750324.cms

[10] AIR 2018 SC (SUPP) 1841, 2019 (1) SCC 1

Volume 35, October 2024 ISSN 2581-5504

This case formed a foundation for recognition of the Right to be forgotten as a person is entitled to their privacy and can choose the information available in public.[11]

In the case of Jitendra Meena vs The State of Rajasthan[12], the court asserted that the 'right to be forgotten,' particularly concerning juveniles under Section 24 of the Act of 2015, remains an unequivocal entitlement. Juveniles benefiting from Section 24 are granted the right to have their juvenile delinquency expunged from records, as perpetuating such records could lead to significant embarrassment and adverse consequences, especially in future endeavours like public employment selection processes. This stance aligns with the legislative intent behind juvenile laws, which prioritize rehabilitation and a fresh start for young offenders.

Likewise, in the case of Karthick Theodore vs. The Registrar General & Ors.[13], the court reaffirmed that the 'principle of fresh start' enshrined in the Juvenile Justice Act applies equally to adults. It emphasized that the 'Right to be Forgotten,' or rather the 'Right to be remembered well,' should not be denied to individuals if the circumstances warrant it. In this case the appellant was acquitted of criminal charges (Sections 417 and 376 of the Indian Penal Code) by the High Court in 2011[14]. The judgment, however, contained his personal details and was publicly available online. He argues that this information is a privacy violation, especially since his life has moved on and he has a new family. He unsuccessfully requested the redaction of his personal details from the judgment and its removal from a legal website. The appeal challenged the rejection of those requests.

The court clarified that the right to be forgotten cannot be invoked in ongoing or recent legal proceedings. The determination of grounds for invoking this right, falls within the purview of the legislature. Nonetheless, the court retains the discretion to permit parties to invoke this right based on the specific facts and duration involved in a particular case. In some instances, the court may order the de-indexing and removal of personal information from search engines or even the erasure and deletion of online personal data, invoking principles related to the right to erasure.

Early cases, like the Kerala High Court's verdict in WP(Civil) 9478/2016, set a strong precedent. Here, the court acted as a shield for a rape victim's privacy by allowing her to erase her name from a website. This judgment underscored the criticality of safeguarding privacy, especially in situations fraught with sensitivity. The Delhi High Court, in Zulfiqar Ahman Khan v Quintillion Businessman Media Pvt. Ltd[15], took a commendable step forward

[11] Dalmia, V.P. (2022) *Right to be forgotten: An analysis of the Indian position - Data Protection - India*, *Right To Be Forgotten: An Analysis Of The Indian Position - Data Protection - India*. https://www.mondaq.com/india/data-protection/1257164/right-to-be-forgotten-an-analysis-of-the-indian-position

[12] Writ Petition No. 9143/2021

[13] W.A.(MD)No.1901 of 2021.

[14] Crl.A.(MD)No.321 of 2011

[15] CS (OS) 642/2018

by providing a comprehensive definition of the RTBF. This definition served as a much-needed lens for understanding the scope of this right and its potential applications.

The Orissa High Court, in Subhranshu Rout v State of Odisha[16], further cemented the connection between the RTBF and the right to privacy. By exploring the RTBF within the context of a bail application, this case highlighted its growing acceptance as an intrinsic aspect of the fundamental right to privacy.

A landmark judgment in the Mundy vs. Union of India[17] case further bolstered the RTBF's foothold in India. Here, Justice Singh explicitly acknowledged the RTBF and the "Right to be Left Alone" as offshoots of the right to privacy. This recognition translated into a powerful order mandating the respondents to remove judgments of acquittal from online platforms and instructing Google to block search results for these judgments.

This trend of upholding the right to erasure personal data kept continuing in recent cases. Similarly, the Karnataka High Court, in Sri Vasunathan v. Registrar General[18], aligned with the global trend of safeguarding women's privacy, particularly in sensitive cases. This judgment highlights the growing awareness of the RTBF's role in shielding the reputation and dignity of individuals, especially women, in the digital age.

Taken together, these court cases paint an unambiguous picture: the RTBF is gaining significant momentum in India. While a specific law addressing this right hasn't been established yet, courts are increasingly recognizing it as a crucial extension of the right to privacy. This trend empowers individuals to exert greater control over their online presence and shields them from the persistence of outdated or irrelevant personal information. As the digital age marches forward, the RTBF is likely to play an increasingly vital role in safeguarding individual privacy and nurturing a responsible online environment in India.

The K.S. Puttaswamy judgment recognized the right to be forgotten as apart of right to privacy as a fundamental right, but it's not without limitations. The court acknowledged that the state could impose reasonable restrictions to protect important interests. These restrictions, however, aren't a free pass. The court will meticulously examine them based on specific provisions within the Constitution. For instance, if restrictions on privacy significantly restrict fundamental personal choices, individuals can challenge them under Article 21 alongside Article 14. This combined argument essentially claims that such limitations are both arbitrary and unreasonable. Similarly, restrictions based on freedom of speech (Article 19(1)(a)) can only be valid if they deal with topics mentioned in Article 19(2). Additionally, they must satisfy the legal tests established by the court for such restrictions to be considered constitutional. The judgment emphasizes the crucial role of the judiciary in

[16] Odisha HC- BLAPL No. 4592 of 2020

[17] W.P. (C) 3918/ 2020 & CM APPL. 11767/ 2021

[18] 2017 SCC OnLine Kar 424.

Volume 35, October 2024 ISSN 2581-5504

finding a balance between individual privacy, societal needs, and state interests. The court's experience and training position them well to make these complex judgments.

Based on the principle of open courts and justice, the ‘right to be forgotten’ is an exception to the principle of open justice that either must be statutorily provided for or specifically directed by the Supreme Court. The idea of the Right to be Forgotten (RTBF) is no longer a distant echo in the halls of Indian courts; it's gaining a powerful resonance.

F. THE ROAD AHEAD: THE DATA PROTECTION BILL AND THE FUTURE OF RTBF

Though, after its introduction, the PDPB bill was withdrawn from Parliament, leading to the unveiling of a Draft Bill for public consultation in November 2022; in August 2023, the Digital Personal Data Protection Bill, 2023 made its debut in Parliament, supplanting the earlier iterations and reflecting an updated and refined approach to data protection in India. The DPDPB endeavours to establish a comprehensive framework for digital privacy laws, with a keen focus on safeguarding individuals' privacy in relation to their personal data, regulating the flow and usage of such data, and nurturing trust between entities processing personal data and individuals.

Drawing inspiration from international benchmarks (GDPR), the DPDPBA the bill also acknowledges the global trend of the Right to Be Forgotten (RTBF), aligning with international standards for data privacy. The DPDPA under section 12 empowers data principals with the right of data access, rectification, and erasure under specific conditions, thus recognizing the importance of individuals' control over their personal information and so to get forgotten. Additionally, the bill mandates the appointment of Data Protection Officers (DPOs) to ensure adherence to the law and provides avenues for grievance redressal, further strengthening data protection measures in India.

G. POTENTIAL CHALLENGES OF DATA PRIVACY AND RIGHT TO BE FORGOTTEN

With the enactment of the Digital Personal data protection act, the various effects of this become a point to ponder and foresee to.

The question of whether information can be removed from various platforms requires a thorough examination of both the Right to Privacy of individuals and the Right to Information enshrined in the Right to Information Act of 2005. This legislation mandates governmental transparency by granting citizens access to public records, ensuring accountability and empowering informed decision-making. Balancing these rights requires careful consideration of individual privacy concerns alongside the public's entitlement to access information held by public authorities.

Volume 35, October 2024 ISSN 2581-5504

In case of **Mr. SJ vs Union Of India & Ors**[19]**,** the petitioner, a 33-year-old hotel management graduate, was involved in a criminal case resulting in FIR 293/2021, which was later settled and quashed. However, online articles about the incident led to the petitioner's suspension from their job at "Spyne.ai."

The court referred to previous cases regarding the right to privacy and the right to be forgotten and considering the potential harm to the petitioner's career due to the online articles, the court directed respondents to remove the articles and block access to them. The Ministry of Electronics and Information Technology (MeitY) was instructed to issue directives for blocking related articles within 48 hours. Specific URLs were provided for removal, with a deadline for compliance. The Indian Express was given one week to remove their articles.

Reading the section 12 of DPDPA, Section 12(3) provides that personal data may be erased unless retention of the same is necessary for specified purpose or for compliance with any law for the time being in force Court recognized that if aspects of their past that have become obsolete, i.e., the retention is no longer necessary, the judiciary must not turn a blind eye to privacy concerns and the entitlement individuals have, within legal proceedings, to move beyond.

For instance, journalists depend on freely available information to uncover wrongdoing. The RTBF could make it difficult to access past records of individuals involved in scandals, potentially hindering investigative journalism. Similarly, erasing negative information can distort the historical record, making it difficult to learn from past mistakes.

It has been found that GDPR and similar data privacy regulations have significant implications for fin-tech and consumer tech players, particularly in terms of compliance costs and the need for data protection policies and procedures. These regulations require companies to balance the use of data for personalized and hyper-targeted financial products and services with privacy concerns, and to adopt a customer-centric approach to data management.[20] The use of in-product data raises concerns about privacy, and companies must fully understand liability issues and take appropriate measures to mitigate them. The DPDPA places several obligations on e-commerce businesses with respect to processing and handling of personal data, including the appointment of a Data Protection Officer (DPO) for certain organizations, the implementation of a Consent Manager, and the ability for individuals to give, manage, review, or withdraw their consent to the Data Fiduciary through a Consent Manage.

[19] W.P.(C) 5608/2023

[20] Rosenberg, R. (2023) *The data conundrum: Finance & privacy*, *The Data Conundrum: Finance & Privacy | FinTech Magazine*. https://fintechmagazine.com/articles/the-data-conundrum-for-the-finance-industry

Volume 35, October 2024 ISSN 2581-5504

The GDPR, in particular, has had a global impact on companies, with some studies suggesting that companies exposed to the new regulation saw an 8% reduction in profits and a 2% decrease in sales.[21]

Additionally, The Right to be Forgotten (RTBF) can trigger a domino effect in financial markets, potentially leading to instability. Financial institutions rely heavily on a borrower's complete financial history to assess risk and make informed lending decisions. Imagine a scenario where a company with a history of reckless spending and near-bankruptcies utilizes the RTBF to scrub negative financial news and public records. This sanitized online presence could mislead banks into believing the company is a sound investment, enticing them to offer loans with favourable terms. However, the underlying financial instability of the company remains.

When negative information is selectively removed, it creates an "asymmetric information trap" where some market participants lack complete information. This can lead to distortions: riskier businesses might be more likely to operate online (adverse selection), and companies might engage in riskier behaviour knowing they can erase negative feedback (moral hazard). A report by the International Monetary Fund (IMF) highlighted potential risks associated with the RTBF in financial markets. The report suggests that the ability to erase negative financial news could lead to an increase in non-performing loans, impacting financial stability.[22]

Beyond these direct market impacts, the RTBF can erode trust in online interactions if negative information is easily removed. Additionally, companies might become less motivated to innovate if they can erase negative feedback, ultimately harming consumers.

H. CONCLUSION

Finding a balance is key. Clear legal frameworks defining what information can be removed can prevent abuse. Time limits on information removal can ensure transparency alongside privacy. Platforms can explore mechanisms for users to flag removed content for further review. A 2019 study in the Journal of Information Policy suggests that time-bound restrictions on the RTBF could be an effective approach. [23]

In summary, the Right to be Forgotten (RTBF) is carving a significant space in India's data privacy landscape. While not explicitly codified yet, the RTBF is gaining momentum through

[21] Presidente, G. and Frey, C.B. (2022) *The GDPR EFFECT: How data privacy regulation shaped firm performance globally*, *CEPR*. https://cepr.org/voxeu/columns/gdpr-effect-how-data-privacy-regulation-shaped-firm-performance-globally

[22] Adrian, T., Natalucci, F. and Wu, J. (2023) *Inflation remains risk confronting financial markets*, *IMF*. https://www.imf.org/en/Blogs/Articles/2023/07/27/inflation-remains-risk-confronting-financial-markets

[23] Qu, Y., Nosouhi, M.R., Cui, L. and Yu, S. (2019). Privacy Preservation in Smart Cities. *Smart Cities Cybersecurity and Privacy*, pp.75–88. doi:https://doi.org/10.1016/b978-0-12-815032-0.00006-8.

Volume 35, October 2024 ISSN 2581-5504

progressive court judgments and the recent enactment of the Digital Personal Data Protection Act (DPDPA). However, the RTBF also presents challenges. To create a balance between individual privacy and the public's right to information is of paramount consideration. Additionally, potential economic concerns, particularly in the fintech sector, necessitate careful consideration.

The future of the RTBF in India hinges on navigating these complexities. Clear guidelines within the DPDPA framework, coupled with ongoing discourse, will be crucial in shaping a future where privacy and transparency may be able to coexist in India.