'Right to Be Forgotten': Crafting A Privacy Framework for India

Dr. Deepak Kumar Srivastava*

Ms. Shriya Badgaiyan**

Introduction

The RTBF (Right to be Forgotten) is a significant principle that was developed in the digital era, which stresses the need of giving people the ability to regulate the exposure of their personal data on internet platforms. This idea is based on the fact that people should have the power to delete their data when it is no longer needed, it is no longer relevant, or if it can cause harm. The philosophical bases of RTBF are basically the ones that are connected with the basic human values such as dignity, autonomy and the right to privacy. These ideals are proof of the fact that the more the digital footprints are growing and penetrating all areas of the life, the need for the people to be able to edit their own digital narratives, to correct the outdated information and to correct the information which does not represent their actual views or present circumstances.[1]

Globally, the interpretation and application of RTBF can be very different, which shows the difficulties in balancing individual privacy rights and the interests of a society. The most excellent of the frameworks demonstrating this concept is the EU's GDPR. The GDPR is an innovative regulation that gives the individual's right to ask for deletion of the personal data when data its initial use has been done or when the consent for its processing has been withdrawn. The mentioned move is proof of the great care taken for protection of personal data rights in Europe.

The RTBF has been also introduced in the countries outside Europe like Argentina and Russia, but these adaptations took into account the unique cultural and legal contexts of these countries. On the contrary, in the United States, the RTBF is applied less since the First Amendment of the Constitution is the basis of the most important principles of free expression and speech. This leads to a complicated situation where the vested rights to privacy and free speech are often at the same time in conflict, thus, a more cautious acceptance of RTBF principles is being shown.

---

* Associate Professor& Registrar(I/C), Hidayatullah National Law University, Raipur, Chhattisgarh, <dr.deepak@hnlu.ac.in>

** Assistant Professor, MATS Law School, MATS University, Raipur; Hidayatullah National Law University, Raipur, Chhattisgarh. <shriya2229@hnlu.ac.in, shriyabadgaiyan@gmail.com>

[1] ROBERT WALTERS, *Right to Be Forgotten [RTBF]: Erasure*, *in* CYBERSECURITY AND DATA LAWS OF THE COMMONWEALTH 193, (2023), https://doi.org/10.1007/978-981-99-3935-0_10.

One of the notable achievements in the field of data protection & privacy rights has been the creation of Digital Personal Data Protection Act, 2023 in India. This legislative action is the result of the aforementioned Supreme Court decision made in *Justice K. S. Puttaswamy (Retd.) v. Union of India*, which declared privacy as a constitutional right.[2] The new act seeks to establish a strong data protection framework that would govern data collection, processing, storage, & transfer of digital personal data. In this way, the RTBF is designed to be handled in a way which allows people to have control over their data while at the same time taking into account other important issues such as freedom of speech, public interest, and the necessity of data retention for the government.

The Digital Personal Data Protection Act, 2023 is a vital step in the process of making India's data protection standards in line with the international norms. Through the Act, the right to privacy is well protected; at the same time, it integrates the individual interest with the interest of the state and the society. Thus, the Act not only becomes the guardian of the right to privacy in India, but as well as the precedent for how the countries can deal with the matters of the data rights in the modern world.[3]

Background and Evolution of RTBF

The idea of the RTBF was born in European legal philosophy and started to grow in popularity as the digital footprints of individuals made a deeper impact on their privacy rights. The chief case that was the evidence of RTBF was *Google Spain SL v. AEPD and Mario Costeja González*, which was in the European Court of Justice in 2014. Mario Costeja González, in this blockbuster case, asked Google to remove the links in its search results that led to an auction notice for his repossessed home, which he considered as a violation of his privacy long after the financial issue had been dealt with.[4] The Court's decision to choose him was a vital event in the history of privacy law, which was the main component in the legal establishment of the precedent. It was the reason why it was decided that sometimes people could ask for the deletion of their personal data for the reason that the outdated or irrelevant information could not affect their privacy anymore. This was a confirmation of the importance of balance between public interests & individual right to privacy and data protection.

The most important decision by the European Court of Justice was the establishment of a legal framework on the digital privacy that was followed by the European Union with the

[2] Justice K.S. Puttaswamy (Retd.) v. Union of India, AIR 2017 SC 4161.
[3] Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).
[4] Google Spain SL v. AEPD and Mario Costeja González, C-131/12.

introduction of the GDPR in 2018. The GDPR is a complete data protection law that has all the RTBFs even in Article 17, that is, the RTBFs are clearly provided. The law obliges that personal data must be deleted without unnecessary delay in the case of data being no longer needed to its original processing purpose, data subject has withdrawn consent, or data processing does not comply with GDPR provisions. Through GDPR, the RTBF has been greatly made more enforceable by the introduction of these restrictions, and thus it has developed a strong model for the handling of the problems of digital privacy and data control.[5]

Comparison with RTBF Laws in Other Jurisdictions

In the US, privacy laws do not currently include a federal statute providing a general RTBF as found in the EU's GDPR. Instead, privacy regulations in the U.S. are specific to sectors and are characterized by their fragmented nature. One of the sector-specific laws is Children's Online Privacy Protection Act (COPPA), which empowers parents to intervene and request deletion of their child's information from online platforms. On a broader scale, California Consumer Privacy Act (CCPA), which came into effect in 2020, represents significant movement towards enhanced data protection. The CCPA allows Californian consumers to request deletion of their personal data. Despite this, the act still lacks a comprehensive right to be forgotten as it is conceptualized under the GDPR, focusing instead on certain conditions under which data deletion can be requested without establishing a broad, overarching right.

In Canada, the privacy framework shows a tendency towards the European style, particularly with the Personal Information Protection and Electronic Documents Act (PIPEDA), which oversees data protection. PIPEDA includes measures that require the deletion of personal information once it is no longer necessary for its initially stated purposes. Despite these provisions, Canada does not yet have a law that explicitly grants a right to be forgotten akin to that of the GDPR. The country is currently experiencing ongoing discussions and legislative development regarding the potential incorporation of an explicit RTBF. A critical aspect of this development involves balancing such a right with other fundamental rights, such as freedom of expression, highlighting the complexities of implementing RTBF in a manner that respects other established freedoms.

Australia's approach to privacy and data protection has been evolving, notably with recent amendments to its Privacy Act. Similar to the United States, Australian legislation does not explicitly recognize a right to be forgotten. Australian law mandates that businesses handle

[5] General Data Protection Regulation, art. 17.

personal information responsibly, which includes obligations to destroy or de-identify personal information that is no longer needed. However, these laws do not grant individuals a broad right to demand that their data be deleted on request. This limitation reflects a more conservative approach to data deletion, focusing on the management and security of personal data rather than on providing expansive deletion rights to individuals. The legislative framework thus prioritizes data management practices over individual rights to erase personal data.[6]

Implications for India

The European model, especially the GDPR, provides us with clear information on the links between privacy laws, digital innovation and economic development. The GDPR offers a full legal scheme which not only safeguards the personal data of the people but also the public causes it to be handled. This regulation has proved that strong privacy safeguards are not only possible but also the very essence of technological progress and economic expansion. The GDPR, through the demand for transparency from companies in their data processing activities & empowerment of individuals to control their own personal information, establishes a model for privacy laws world over, thus showing that the strict regulations can be a support for rather than a constraint to digital innovation.

The instances from North America especially being the United States and Canada on the RTBF is an interesting one to take a look at since it shows the difficulties and the complicated issues that arise when this right is not balanced well with the freedom of speech and the public access to information. This is the reason for the problems that are caused by the legal and cultural framework which highly values the freedom of expression & free flow of information as the base of democracy. The United States, with its First Amendment protection, and Canada, with similar constitutional safeguards, have all been aware of these issues and have been trying to find a balance that will respect privacy but not restrict the information that is needed for the public interest or that is part of the public records.

For India, the process of becoming a country where people can request to have personal data erased is complicated and requires a deeper look into its unique legal, social, and technological background. India must talk to this right from two balanced sides; on one hand, it should protect the privacy of individuals and on the other hand, it should not in any way interfere with the

[6] Peter Kuylen, *The Forgotten Property Right*, 5 TEX. &M J. PROP. L. 501, (2019), https://doi.org/10.37419/jpl.v5.i3.5.

values which are public transparency and freedom of expression. The lessons acquired from the European, American, and Canadian experiences show that the necessity of the creation of clear and enforceable rules that not only support the privacy rights but also the free flow of information is essential. The equilibrium is very important in the democratic setting and is highly relevant for India as it continuously expands its digital infrastructure and faces the double problems of being committed to democratic values and exploiting the technological advances. Public discussion and participation of the general public in policymaking will be key to the development of a right to be forgotten that will be in accordance with India's particular constitutional ethos and the socio-technical landscape. This discussion should be the way of the formation of the common understanding on the boundaries of this right, to make sure that it is proper to the democratic structure and the technological goals of India.

Current State of Privacy and Data Protection in India

The IT Act, 2000 that India has passed to regulate digital privacy and data protection is the main thing that has influenced the country's approach in this issue, and it is the basis of the nation's legal framework in this field.[7] The IT Act which was originally created for the ease of electronic commerce and to stop cybercrimes includes important and relevant provisions that will protect personal data. The most important part of the law is Section 43A, which requires companies to take and use probable security practices and procedures to protect the personal data which is sensitive. Furthermore, Section 72A sets the fines that are levied in cases where a person's privacy is infringed. Although it has the future-oriented parts, the IT Act has been the target of criticism due to the fact that it is not adequate. The Act is said to have the emphasis too much on the rules of the corporations, which enables it to move away from the individual's rights and does not provide the detailed, rights-based framework for data protection.

The Supreme Court of India has been a major factor in shaping privacy debate in the country along with the legislative process. The termination of the Supreme Court's decision in *Justice K.S. Puttaswamy (Retd.) v. Union of India* was a turning point in the development of privacy rights in India. This decision was the turning point that unequivocally confirmed the right to privacy as a fundamental right mentioned in the Indian Constitution. The direction of the decision was a breaking point, thus causing the rethinking of the way the privacy violations are dealt with in Indian law. It was striking evidence of the need for a powerful legal system to safeguard personal data from the abuse. The Supreme Court has, since this ruling, always

[7] Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).

issued more opinions on the privacy right in different decisions and the government's duty to protect it. These judgments have also examined the intricacy of the balance between right to privacy & other societal & fundamental interests thus they have given more depth to the legal interpretations and applications of the right to privacy in the digital era of India.[8]

India's way of building a strong legal system for data protection has seen major progressive steps, but it also has a lot of weaknesses that prevent the full data privacy environment from being established. The IT Act, the main pillar of data protection laws in India, is often criticized for the way it deals with data privacy which is more of a reactive than a proactive way. The Act is primarily reactive because it does not provide the details of the type of data that is to be protected and also, the scope and scale of the protection is not clearly defined. Thus, the provisions lack the necessary and definitive provisions to prevent the problem of data breaches even before they occur.

The IT Act does not include RTBF which is one of the most significant oversights. This contemporary privacy theory is very important because it gives people the ability to get rid of their personal data in certain situations like when the data is not needed anymore or when the people withdraw their consent. The lack of RTBF in the Indian law of data protection, thus, points to a huge difference in the global norm of the protection of personal data, where such rights are now the rule and are being implemented.

Moreover, the enforcement of data protection in India is hindered by the lack of a data protection authority country. The given sentence without specialized body turns the responsibility for overseeing data protection to various regulatory frameworks and institutions, hence, it results in a disjointed enforcement and inconsistencies in compliance. The fragmentation of the systems means that the data protection practices are hard to monitor and the laws that are designed to protect personal data become less effective.

Besides, there is a clear absence of data protection guidelines regarding data minimization and retention that are vital ones in the field of data protection. Information minimization is a method of restricting gathering of personal data to what is required and directly relevant to the achievement of a certain goal. Additionally, data retention policies are necessary to guarantee that personal data is not kept for a longer time than it is needed. The lack of clear directives on these subjects in the Indian data protection laws makes personal data vulnerable to risks of misuse and over retention which in turn make the privacy landscape complex and in turn erodes the public trust in digital infrastructure.

---

[8] *Supra* note 2.

The process of RTBF in India has come to a critical stage with enactment of Digital Personal Data Protection Act, 2023. Thus, this new law is a huge change in the way India deals with the data protection problem, because it has provisions that cover the right to be forgotten. The project responds to the growing concern about the privacy issues associated with mobile applications and, thus, allows people to request deletion of their personal data under certain circumstances, which is a vital step towards the compliance with the international data protection norms, especially GDPR. [9]

The addition of RTBF to Indian law of the land indicates general agreement of the necessity of strong privacy laws in a society that is highly dependent on technology. It allows people to have more power over their private information, which in turn helps them to deal with their online presence more efficiently and to reduce the possible problems that can be caused by the leaking of personal data or its misuse.

However, the Digital Personal Data Protection Act is supposed to protect the right to privacy and its effectiveness will depend on the way it is implemented and enforced. Thus, the act compels the creation of specific and unambiguous rules that specify the conditions under which people can use their right to delete their data. The guidelines must be designed in such a way that they will help the public and legal necessities in a way that will favour the right to privacy, while also being fair and efficient. Besides, the existence of solid and efficient methods to deal with such requests is crucial for the actualization of the right to be forgotten, which is a practical process that can handle the requests in a clean and simple way, without any delay or complication.

The Need for RTBF Laws in India

The present era, defined by the digital boom which is the epitome of the information age, has become a source of big data, which has raised the issue of privacy and personal information management. India is the pivotal country in this global trend, because of its huge and constantly and increasingly growing internet user base. In every minute that passes, a big amount of personal data is collected, stored, and frequently shared through various platforms, such as social media networks and governmental databases. Although this growth in data collection and the connection of people to the Internet create new services and better user experiences, at the same time it is a serious threat to privacy and security. The huge digital footprints of users

[9] 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.

made it easier to misuse personal information. This persistent issue of "Instagram is working for you not you" strengthens the position of the RTBF laws. Thus, the law would give power to the people to ask for the deletion of their data whenever it is considered unnecessary or dangerous.[10]

After the Supreme Court's verdict in 2017, which acknowledged privacy as a fundamental right under the Indian Constitution, the Indian public's attitude to privacy changed dramatically. This important decision turned out to be the reason behind the shift in the public opinion, with more and more people now demanding the protection of their personal data as a basic human right to individual autonomy. Society is changing and it is getting more and more obvious that people are to be able to control their digital selves. The statement covers the right of the people to dispose of the data which can be used for discrimination, bias, or privacy invasion. For this reason, the public is increasingly favouring legislative reforms that will ensure the protection of data. This joint recognition & fear of the dangers of the data that is not under the control are the causes of the call for the RTBF laws to be established in India. Such legal regulations are seen as necessary for the alignment of the Indian legal system with the modern standards and norms of privacy and the management of personal data; thus, the country is endowed with the capacity to adapt to these new digital realities.

Challenges and Concerns with Implementing RTBF in India

Balancing Freedom of Expression and the Right to Privacy

In India, the challenge of integrating RTBF within the legal framework involves a delicate interplay between right to privacy & freedom of expression, both of which are fundamental under the Indian Constitution. While privacy is crucial to personal dignity and autonomy, freedom of expression is the cornerstone of a democratic society, facilitating open discussion and dissent. The introduction of RTBF laws must therefore be meticulously crafted to balance these rights effectively. It requires a regulatory framework that acknowledges and protects individual's right to privacy without undermining the public's right to information. Concerns arise from the potential for RTBF to be misapplied, possibly leading to the suppression of journalistic freedoms and free speech. Legislation must therefore delineate clear parameters that define what constitutes legitimately privacy-infringing information. These definitions and

[10] Ivneet Walia & Dinesh Kumar, *Need for Revamping Information Technology Laws in India*, 8 BRAWIJAYA L.J. 202, (2021), https://doi.org/10.21776/ub.blj.2021.008.02.03.

limitations are crucial to prevent the overreach of RTBF, ensuring it does not impinge upon the fundamental democratic value of freedom of expression.[11]

Technical Challenges in Enforcing RTBF

The enforcement of RTBF in the digital age encounters formidable technical obstacles due to the inherently decentralized and global nature of the internet. Once data is published online, it can be replicated and stored across an intricate network of servers worldwide, complicating any efforts to erase it completely. The technical difficulty lies not only in locating all instances of the data but also in executing its removal without impacting other data inadvertently. This process demands advanced technological solutions and considerable resources, which poses a particular challenge in resource-constrained settings, such as those often found in developing economies like India. As a result, enforcing RTBF requires significant investments in both technology and skilled personnel to manage these complex data landscapes efficiently and effectively.

Potential for Misuse and Overreach

The RTBF also raises concerns regarding potential misuse and regulatory overreach. The vagueness of what exactly qualifies as one's 'right' to be forgotten could lead to a broad spectrum of interpretations, allowing individuals to request deletions of records that are historically significant or contextually important. Such applications of RTBF could serve to not only sanitize personal history but could also distort public perception and rewrite public history. It is imperative that RTBF legislation include strict criteria to clearly define valid cases and establish robust oversight mechanisms to prevent abuse. These measures will help ensure that RTBF is employed judiciously and only where genuinely justified, thereby protecting against arbitrary or excessive application.

Impact on Journalism and the Media

Implementing RTBF carries substantial consequences for journalism and the media. Journalists and media entities often depend on access to archived information to perform investigative reporting and provide comprehensive coverage of ongoing issues, offering essential historical perspectives. The RTBF could potentially restrict access to such resources, hindering journalists' ability to conduct in-depth analyses or expose past misconduct. Thus, it is crucial

[11] *Id*.

for any RTBF legislation in India to consider exceptions that allow journalistic and public interest content to remain accessible. Safeguarding these exemptions is vital to uphold the media's role in scrutinizing power and informing the public, thereby supporting the pillars of democratic governance and societal accountability.[12]

Potential Benefits of the RTBF Laws

Protection of Personal Dignity and Privacy

The RTBF serves as a fundamental mechanism to uphold individual dignity and privacy in an increasingly digital world. This right empowers individuals to request the erasure of personal data that is either no longer relevant or is outdated, effectively allowing them to mitigate the risk of enduring reputational harm that could arise from previous behaviours or actions that do not resonate with their current standing or belief systems. In today's digital age, where information is permanently archived on the internet, such a provision is vital. It ensures that individuals have the capability to distance themselves from their past actions, which can be crucial for personal development and social rehabilitation. This aspect of RTBF is especially important in helping individuals move beyond their past mistakes, thus fostering a society that values growth and change over perpetual historical judgment.

Enhancing Trust in Digital Services

The implementation of RTBF laws significantly bolsters consumer confidence in digital platforms. When users understand that they can control the visibility and existence of their personal data online by requesting its deletion, they feel more secure and empowered. This enhanced trust is critical for the sustainability and expansion of the digital economy. It promotes greater user engagement with online services, encouraging more open and robust interactions across digital platforms. Moreover, when consumers trust the services they use, it creates a healthier, more competitive market that benefits both businesses and users. Thus, RTBF plays a crucial role in cultivating a safe & trusting online environment that is essential for digital innovation and consumer satisfaction.[13]

Aligning with International Data Protection Standards

---

[12] Saif Shahin, *Right to Be Forgotten*, 93 JOURNALISM & MASS COMMC'N Q. 360, (2016), https://doi.org/10.1177/1077699016638835.
[13] *Id*.

The adoption of RTBF laws is a significant step toward aligning national data protection policies with global standards, notably the GDPR. This alignment is not just a regulatory adjustment but a strategic move that enhances international data cooperation and trade. For countries like India, it reinforces the nation's commitment to safeguarding personal information, which is a critical aspect of international commerce today. Such alignment facilitates smoother cross-border data flows, essential for industries that rely on global data exchange. By adhering to internationally recognized data protection standards, a country can enhance its standing as a reliable participant in the global market, fostering partnerships and business opportunities that hinge on stringent data protection practices.[14]

Economic Benefits through Increased Consumer Confidence

RTBF laws not only protect individual privacy but also catalyse economic benefits by boosting consumer confidence. When individuals feel assured about the security and privacy of their online activities, they are more likely to utilize digital services. This increase in digital engagement drives growth in e-commerce and digital transactions, which are pivotal to the modern economy. Additionally, a strong data protection framework makes a market more attractive to foreign investors and global companies looking for reliable and secure data environments. Companies prioritize markets that demonstrate a commitment to protecting consumer data because it reduces their operational risks and aligns with global compliance standards. Consequently, the economic impact of RTBF extends beyond individual benefits to broader economic growth and innovation, making it a crucial policy for future-focused economic strategies.[15]

Conclusion and The Way Forward

The discourse surrounding the adoption of RTBF laws in India is not merely a legal debate but a crucial pivot around which revolves the future of individual privacy in the digital era. The sanctity of personal dignity in the online environment is paramount. In an age where digital footprints are indelible and personal histories are perennially retrievable, RTBF laws provide a necessary recourse for individuals to shield their past, particularly from incidents that no longer represent their current status or beliefs. Such legal provisions empower individuals to request deletion of data that might be outdated, irrelevant, or prejudicial, thereby safeguarding

[14] *Supra* note 4.
[15] Chenoy Ceil, *Right to be Forgotten Case*, 2018 SSRN ELEC. J., https://doi.org/10.2139/ssrn.3520390.

their public image against permanent stigmatization. This is crucial in a country like India, where social stigma can have profound and long-lasting impacts on an individual's life. The advent of RTBF laws would enhance trust in digital platforms. With increased digitalization of services, from finance to health, and education to employment, individuals are often compelled to share personal information online. The assurance that they can retract this information when it is no longer necessary builds trust. This trust, in turn, is vital for the healthy growth of the digital economy. As data breaches and misuse of personal information become more common, the RTBF stands as a bulwark that can mitigate these breaches by offering people a chance to erase their digital traces.

Furthermore, adopting RTBF laws would align India with international data protection standards. As global commerce becomes increasingly dependent on data flows, India's alignment with international privacy norms, such as those exemplified by the GDPR, becomes imperative. This alignment is not merely a fulfillment of international best practices but a strategic enhancement of India's attractiveness as a secure destination for technological investment and innovation. Moreover, the implementation of RTBF laws addresses a contemporary necessity in the legal landscape marked by the intersection of technology and human rights. The landmark decision by the Supreme Court of India in Justice K.S. Puttaswamy (Retd.) case explicitly recognized privacy as fundamental right under Indian Constitution. This judicial acknowledgment mandates legislative and policy measures to protect privacy in tangible forms, RTBF being a prime example.