Page 778 - 794 **DOI:** *https://doij.org/10.10000/IJLMH.118529*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 7 | Issue 6

2024

Comparative Study on The Protection of Personal Dignity in Tanzania Mainland: Focusing on The Need of The Right of Being Forgotten

JOHN JUMANNE JAMES[1]

ABSTRACT

Human memory's intricacy can also be linked to the "Internet of things." Human life has been seen and documented by the developing digital realm throughout its history. The peril of the digital past is a current concern for internet users worldwide because of the internet's vast accessibility and perpetual memory. The idea that everything should be remembered but nothing should be erased has sparked a contemporary discussion about the "Right to be Forgotten" (RTBF) in digital space. As a result, RTBF gives a person the ability to manage who can access his information on the internet. However, the laws that have just been passed in India have very little control over information and data, and the RTBF concept is still foreign. The RTBF's importance in Indian domestic law is thus hypothesized in this study. The purpose of the paper is to demonstrate the need for and implications of acknowledging these social forgetfulness rights in cyberspace.

***Keywords**: Right to be Forgotten, Cyberspace, Privacy, IT Laws, Digital Past.*

I. INTRODUCTION

Recall skills are usually associated with positive qualities, but forgetting is seen as a negative aspect of memory. But what if the same etching in the memory recollection turned out to be fatal to human existence? Technological innovation is entwined with unaccountable transactional data that is kept indefinitely. As a result, the infamously controversial privacy issue begs the question of how safe and accessible such a collection of data might be for an individual. The debate about data retention revolves around these questions regarding the purpose of data collection. How long will the data be helpful, too? Lastly, if the objective is being achieved, why is it not possible to remove it from the digital world forever?

(A) Statement of the problem

The Tanzanian Constitution guarantees privacy rights under Article 16 (1) and freedom of

[1] Author is a LL.M. Student at University of Iringa, Iringa, Tanzania.

 [ISSN 2581-5369]

communication under Article 18(c), ensuring respect and protection for individuals' privacy and private communications.

“Every person has the freedom to communicate and a freedom with protection from interference from his communication;”

Tanzania has ratified the International Covenant on Civil and Political Rights (ICCPR), ensuring no one is subjected to arbitrary or unlawful interference with their privacy, family, home, or correspondence, and has a positive obligation to adopt legislative measures.

Privacy is a crucial societal pillar, yet it is not widely addressed in Tanzania, despite its constitution and international conventions guaranteeing privacy rights. Cyberspace publications can last for decades, and it is suggested that victims' rights to dignity and privacy should be forgotten by the public to ensure their constitutional right to privacy and dignity.

Furthermore, due to the lack of the right of being forgotten as the legal remedy for the protection of one’s privacy and dignity leady to the availability and accessibility of information which was affecting someone’s privacy and dignity into cyber space.

Achieving the ideal degree of social forgetting is a difficult task that requires striking a balance between the need to hold individuals accountable and the need to give them a "new start" by protecting them[2].

Therefore, technology's retention of data is intrinsically linked to the Right to be Forgotten. Since 1995, the Internet and technology have developed rapidly, posing a variety of content dangers. RTBF is one way to mitigate these threats. With the widespread availability of digital apps and surveillance, the level of sensitivity to personal information such as sexual preferences, medical conditions, family histories, or prior criminal records rises. An individual may remove such stuff for a variety of reasons, including obsolete information, malicious posting, cyber abuse, societal stigmatization, inaccurate data, or just another personal hazard to their wellbeing[3]. Regretfully, the growing hazards and threats to privacy, personality secrecy, and personal data and information are only made worse by the knowledge and research gap.

Prior to the emergence of the current sophisticated cyberspace, in 1995, the "EU Data Protection Directive (DPD 95/46)" was adopted on the basis of data vulnerability. Although the project was ahead of its time, the digital age has advanced significantly over the past 20 years. Bullying, stalking, revenge porn, sexual history, digitally induced suicides, and cyber scams are examples

[2] ean-François Blanchette& Deborah G. Johnson, “Data Retention and the Panoptic Society: The Social Benefits of Forgetfulness”, 18(1) *The Information Society* 33-45 (2002) available *at*DOI: 10.1080/01972240252818216
[3] Paul Lambert, *The Right to be Forgotten* (Bloomsbury Professional, 1stedn., 2019)

of cybercrimes that have become more serious and complicated.

This paper will examine the subtleties of why the request to remove content from the internet should be granted. Furthermore, the accountability of the service providers that offer the content. As a result, the paper's research challenge is centered on how the RTBF is acknowledged as a unique notion under Tanzania's existing IT law framework. The consideration of privacy within the framework of Article 16 (1)[4] of the Constitution[5]. Also opens the door for the application of RTBF to data-sensitive laws. The query, "Why RTBF is significant in the expanding digital advancement?" will next go over the rationale behind its application. In the next chapters, the express right of individuals or an entity to remove or forbid the keeping of their personal information when it is no longer legally useful will be defended.

II. EVOLUTION OF RTBF A COMPARATIVE STUDY

The EU's original recognition and rules for the handling and protection of such data serve as the backdrop for the present RTBF discussion. As a result, the EU regulations that were the first to establish the RTBF as a statutory right serve as the foundation for its specifics. However, the French phrase Droit à l'oubli, which states that a convicted criminal has the right to request that his criminal records be erased after serving his sentence, is where the RTBF got its start.

The contradiction between an individual's "right to privacy" and "freedom of expression" with regard to technological advances resulted from the western world's heightened awareness. Though the EU court attempted to elevate the importance of both rights to the same level, this was not the case in the United States, where free expression has long been associated with less protection for privacy. In fact, the United States has taken a stance on privacy that is almost entirely at odds with that of Europe. Some call it the "right to remember," while others call it the "right to inform"[6]. This is not a formal phrase, yet it encapsulates many privacy protections in an elegant way. The United States has protected free speech to the extent that it is effectively a right to remember and not to forget specifically, but Europe has protected privacy to the extent of establishing a new right to be forgotten.

The "Court of Justice of the European Union (CJEU)" issued a ruling in "Maximilian Schrems v. Data Protection Commissioner" on October 12, 2015. [7], ending the privacy dispute across the

[4] Ibid
[5] Justice K.S. Puttaswamy (Retd.) &Anr. vs. Union of India &Ors., *AIR 2017 SC 4161.*
[6] Melanie Dulong de Rosnay and Andres Guadamuz, "Memory Hole or Right to Delist? Implications of the Right to be Forgotten for Web Archiving" 6 *Recherchesen sciences sociales sur Internet (RESET)* (2017)https://journals.openedition.org/reset/807
[7] C-362/14, Judgment of the Court (Grand Chamber), (2015) https://eur-lex.europa.eu/legalcontent/en/TXT/?uri=CELEX:62014CJ0362

Atlantic. Although the Schrems case has nothing to do with privacy or freedom of expression, it does highlight the differences in privacy protection between the US and the EU, which could have serious financial ramifications. It also clarifies the wildly differing opinions regarding the creation of the right to be forgotten.

In order to maintain an appropriate level of data protection, the European Data Protection Directive established a requirement regarding the sharing of European individuals' data with third countries. "The nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and final destination, the general and sectoral rules of law in force in the third country in question, and the professional rules and security measures that are followed in that country" are the factors that will determine the adequacy level.

A solution had to be found when it became clear that the United States would not follow the law and that a vast volume of data was being transported over the Atlantic. European organizations created the "Safe Harbor" system to permit the transfer of personal data to the US without requiring proof that the data is protected by US law. Data sharing with US firms who embraced the "Safe Harbor Privacy Principles," a condensed version of the Data Protection Directive's rules, was made possible by the 2000 agreement[8]. The companies also committed to being held accountable by the US Federal Trade Commission (FTC) or other regulatory bodies if they violated these rules.

After the Edward Snowden surveillance incident exposed the involvement of US IT companies in the mass monitoring program, Schrems concluded that data protection laws had been broken, even if the system had operated without a hitch for 15 years. Schrems asked the courts to invalidate the Safe Harbor agreements as a result. The case made it all the way to the CJEU, which concurred with Schrems and declared that the existing Safe Harbor was unconstitutional because it did not sufficiently safeguard the rights of Europeans. The Court cited the DPD, which gave Member States the power to set up national authorities to oversee the use of personal data.

Since it established the normative rules for member states to enact the necessary requirements for data protection, the EU statute that included DPD 95/46 was directive in character. Consequently, the EU enacted new General Data Protection Regulations following the Safe Harbor verdict (GDPR)[9] with the DPD standards being repealed. Without the normative

[8] Melanie Dulong de Rosnay and Andres Guadamuz, "Memory Hole or Right to Delist? Implications of the Right to be Forgotten for Web Archiving" 6 *Recherchesen sciences sociales sur Internet (RESET)* (2017) https://journals.openedition.org/reset/807

[9] (EU) 2016/679, *THE EUROPEAN PARLIAMENT AND OF THE COUNCIL* (https://eurlex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

 [ISSN 2581-5369]

authority of national law acceptance by the member states, these regulations were applied consistently throughout the EU.

Google Spain SL and Google Inc. v. Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzalez is a seminal case that served as the foundation for this tool[10]. It is considered to be the first instance of the "Right to be Forgotten." In this instance, a Spanish national complained to Google Inc. & Newspaper about the sale of his home to cover the debts. Despite this, he paid off the obligations years ago. In this case, the European Court of Justice (ECJ) made a decision about the applicability of directives to search engines such as Google that gather "personal information" and "processing." Conversely, the Court was considering the EU citizen's right to erasure under the regulation. In the end, the court ruled that search engines were legally required to delete all content that violated the subject's privacy.

The right to be forgotten under the new GDPR is not absolute, but it may only be used if a person requests it from the controller, who has the discretion to remove them. Erasure is a kind of the right to be forgotten under Article 17 of the GDPR. Within the next 30 days, a data subject may, under this article, request the deletion of their personal data on one of the numerous listed grounds. However, the person must select one of the four grounds below in order to exercise this privilege: (i) the data subject no longer needs the information; (ii) the data subject has revoked consent for the purposes for which it was collected; (iii) the data subject objects to the processing of the data; and (iv) the processing of the data is unlawful under the GDPR. When someone makes such a request, the internet service provider or data controller must "carry out the erasure immediately" unless data retention is necessary, while also taking into account "the right to freedom of expression," as established by local laws in member states. There is also an exemption[11] from the requirement to remove data for "the only purpose of processing personal data" for journalistic, artistic, or literary expression under the Regulation .

Furthermore, the data subject has the right to ask the controller to limit the processing of their personal data in accordance with Article 18 of the GDPR[12]. Data controllers may preserve personally identifiable information but refrain from further processing it when processing power is restricted. In this case, the controller, in accordance with the right to be forgotten, instead makes the data inaccessible. This information pertains to, among other things, the following situations: "In the majority of instances, personal information is no longer necessary

[10] C-131/12, Judgment of the Court (Grand Chamber) https://eur-lex. europa.eu/ legalcontent/ EN/TXT/ ?uri =CELEX %3A62012CJ0131(
[11] General Data Protection Regulation, art. 17(3)
[12] Ibid art. 18.

or otherwise relevant to the reasons for which they were gathered remodeled." Erasure rights are granted in these situations[13]. The restriction right is subject to other limitations, though. In cases where "the data contradicts the data's authenticity subject," for example [14]".

III. IMPACT OF EU RTBF

The Google-Spain case and the implementation of GDPR have had a profound effect on EU member states and even the rest of the world. The historic ruling made it possible for EU residents to fully exercise their right to have their personal data erased. As a result, hundreds of requests from EU citizens to have their data and associated links removed were flooding search engines like Google[15]. The ECJ's decision, however, only had worldwide ramifications, notwithstanding its jurisdiction over the EU region. Another dispute between Google and the French Data Protection Agency resulted from the widespread removal requests (CNIL).

The CJEU clarified the reach of the right to be forgotten in relation to search engines in two rulings published in 2019. In "Google Inc. v. Commission nationale de l'informatique et des libertés (CNIL)," the Court had to make a decision[16]. The territorial scope of the right to be forgotten. It created a general rule that access to non-EU search results is severely restricted when de-referencing occurs throughout the EU in conjunction with preventative or at least mitigating actions. "GC &Ors. v. Commission nationale de l'informatique et des Libertés (CNIL)" is the second case[17]. discusses data de-referencing and how search engines handle sensitive data operators. Due to the sensitive nature of the data, interference with the data subject's right to privacy and personal data protection is a problem in this area. Google won the case as a result of the ECJ's decision to restrict its use to the EU and not the rest of the world. However, in the most recent development for the non-EU states, Google started a request to remove user personal data, such as financial information, address, phone number, etc., that is useless to the general public[18].

IV. RTBF & LAWS – AN INDIAN CONTEXT

Indian privacy and data protection laws are inadequate when compared to those of the European Union. Neither the constitution nor the legislation expressly guarantee the "right to privacy."

[13] Ibid art. 17(a).
[14] Ibid art. 18(a).
[15] Nikolaj Nielsen, "EU regulators want right-to-be forgotten to go global" *euobserver* (Nov. 26, 2014) https://euobserver.com/rule-of-law/126680
[16] Case C-507/17, Judgment of the Court (Grand Chamber) (Sep. 24, 2019) *t*https://eurlex.europa.eu/legal-content/en/TXT/?uri=CELEX:62017CJ0507
[17] ibid
[18] Veronica Irwin, "Google will now remove personal information from search by request", protocol https://www.protocol.com/bulletins/google-search-personal-information

However, in the historic ruling of "Justice K. S. Puttaswamy v. Union of India," the Indian Apex Court ruled in 2017 that the right to privacy is a fundamental right"[19]. In the opinion authored by Justice S. K. Kaul, the Court also addressed the right to be forgotten, characterizing the RTBF as part of the broader informational privacy umbrella. The Court pointed out that this right gives people the ability to request that data about them be deleted and control over the information they share. A person has the "right to exercise control over and access to his data," according to Justice Kaul, who also asserts that the right to govern one's own life encompasses the right to manage one's online persona.

Since people's digital life shouldn't be impacted by their past evidence, the court acknowledged that mistakes were made throughout the trial. They shouldn't be prevented from changing and adapting. The court also pointed out that the general public does not have a right to all correct information about other people. However, the lack of a data privacy law was inevitably going to prevent these difficulties from being properly implemented and resolved. The main problem is that it is still unclear how broad the right to be forgotten is, and legal authorities will ultimately bear this burden. The legal system must make a snap decision regarding a potential "right" whose exact nature is unclear[20].

As a result, "Zulfiqar Ahman Khan v. Quintillion Business Media Pvt. Ltd &Ors" established a number of precedents[21]. The Delhi High Court acknowledged the plaintiff's right to be forgotten. According to the responder, the problem started when stories were published that detailed the complainant's alleged harassment during the #MeToo campaign. Because articles found online could seriously affect the plaintiff, the court ordered the defendant to delete this materials. The court ruled that two essential components of the right to privacy are the "right to be forgotten" and the "right to be alone."

Similarly, in the case of "DharamrajBhanushankar Dave v. the State of Gujarat"[22], The Gujarat High Court rejected a plea erasure, ruling that the case was dismissed since the petitioner had not specified which law elements were in question. In this case, the petitioner filed a writ under Article 226 to restrict the investigation's scope by asking that a court ruling that was previously published on the website be taken down, despite the fact that the decision was not reportable. It was interfering with his personal and professional life, the petitioner claimed. The court, however, retorted by asking how downloading the pertinent ruling violated Article 21 of the

[19] Paul Lambert, *The Right to be Forgotten* (Bloomsbury Professional, 1stedn., 2019)
[20] Jyoti J. Mozika, *"*Integrating the Right to be Forgotten in the Indian Legal Framework in the Light of Experiences from the European" 12(1) *INDIAN JOURNAL OF LAW AND JUSTICE* (2021).
[21] 2019 (175) DRJ 660.
[22] 2015 SCC OnLineGuj 2019.

Constitution. The Gujarat High Court decided that any party may ask the Assistant Registrar for a copy of the High Court's ruling on the request, citing the current HC guidelines. As a result, the court rejected the right to be forgotten. The Information Technology (Reasonable Security Practice & Sensitive Personal Data or Information, 2011) Rules and Procedures are in force, even though Section 69A of the IT Act is the law of the land. Thus, with all the factors and restrictions included here, there is a lack of clarity about an individual's right to information and their right to be forgotten.

Subsequently, the Karnataka High Court held in "Sri Vasunathan v. The Registrar General &Ors.[23]" that only copies of the order obtained online were ordered to be erased by the High Court; certified copies of the order posted on the court's website were not included in the list of erasing remedies. In this instance, the petitioner requested that the order in the digital archives no longer include the name of the petitioner's daughter. However, the petitioner's daughter filed a formal complaint alleging that the aforementioned directive was given to a man for drug-related charges, including pushing her to marry and forgery. As a result, the parties came to an agreement, and the FIR was dropped after they did. The Karnataka High Court ordered the petitioner's daughter's name to be hidden in the ruling, acknowledging that it is a legitimate right to be forgotten. The court decided that:

"would be in step with the trend in Western countries where they uphold the Right to be Forgotten as a rule in sensitive instances involving women in general and very sensitive cases including rape or hurting the person's modesty and reputation."

(A) RTBF & I.T. Law

The first law to address the usage of technology was the Information Technology (IT) Act of 2000, which was passed by the Indian parliament. The law was modified by the Information Technology (Amendment) Act of 2008 to enhance its use in the field of information technology. Although this Act successfully tackles the privacy issue, it is important to highlight how inadequate it is in terms of data protection. A thorough analysis of the clauses reveals a number of fundamental instruments that, with additional development, can guarantee that India has a strong data protection system. Some basic ideas in data protection are established under this regulation, such as data, data access, computer systems, information, and a breach of confidentiality[24].

As mentioned before, RTBF is not recognized by the Information Technology (IT) Act of 2000.

[23] Writ Petition No. 62038 of 2016.
[24] The Information Technology Act, 2000 (Act 21 of 2000), s. 2(1).

 [ISSN 2581-5369]

It does, however, cover a number of RTBF topics, including privacy and personal information. In accordance with Section 43A of the Information Technology (Amendment) Act (ITAA) of 2008, businesses are required to use sufficient security measures to safeguard confidentiality. Under this Act and its implementing regulations, corporations are responsible for protecting the privacy of data subjects. Certain S.43A rules pertaining to obstacles (restrictions) or privacy standards can be used to give "information providers" the authority to stop processing personal data, which is comparable to EU DPD standards.

Section 79, which offers various protections for "intermediaries," is one of the other provisions of the IT Act[25]. Because of the due diligence guidelines set forth in the IT Act of 2000, this clause exempts intermediaries from liability in specific situations. According to the IT Act, search engines are one of the intermediaries in this case. Examples of intermediaries that store and transfer the data as a third party include telecom service providers, system service providers, network access providers, web-enabling service providers, web indexes, search engines, online-commercial hubs, and cyber hubs.

In some situations, intermediaries are excluded from liability under Section 79 of the IT Act. According to this clause, an intermediary is not responsible for any third-party data, information, or communication link that he provides or helps create, even if it is unlawful. Even if the law is in force until further notice, this still holds true (3).

According to the S.79 principles, an intermediary must declare its rules and regulations, privacy policy, and user agreement before anyone can use or access its computer resource. Terms and conditions that prohibit hosting, displaying, uploading, editing, publishing, sending, updating, or disseminating content that violates the privacy of others should be mandatory for users of the computer resource.

Additionally, the guidelines state that without the user's consent, the intermediary cannot host or publish content that breaches the rules, such as information that infringes on the privacy of another individual. Crucially, the intermediary "must act within 36 hours after discovering on its own or after being informed in writing or via signed email by a person affected, and, if necessary, must work with the user or owner of the information to disable information that violates the rules, including information that invades privacy."

The right-to-be-forgotten ruling may be subject to limitations and challenges, such as defining what privacy infringement is. Nonetheless, a strong association seems to exist, which won't be

[25] Ibid s. 2(w).

 [ISSN 2581-5369]

confirmed until a comparable event takes place in India.

(B) RTBF & Data Protection Bill, 2019

The parliament passed the previous Data Protection Bill in 2006 with the goal of protecting personal information and data about individuals. However, the most recent Data Protection Bill, 2019 had to be amended due to the rapidly changing nature of technology[26]. The debate over data privacy laws in India gained prominence after the Puttuswamy ruling. In order to create a plan based on the Supreme Court's directives for an all-encompassing data protection strategy in India, the administration subsequently convened an expert panel. A study titled "A Free and Fair Digital Economy: Protecting Privacy and Empowering Indians," which included a proposal for the Personal Data Protection Act, was prepared by the committee's chairman, Justice BN Srikrishna (PDPA). The goal of the Data Protection Bill was to set the course for data protection going forward by building a comprehensive data governance structure and regulating the current geopolitical environment, which is growing more and more data-driven.

The right to be forgotten is not recognized by India's current data security framework, which consists of the Information Technology Act of 2000 and the Information Technology (Reasonable Security Practices and Procedures or Sensitive Personal Data) Act of 2011. Nonetheless, the recently proposed law seeks to create this entitlement[27]. According to section 20 of the law, each data principal has the authority to limit or forbid additional processing of any data fiduciary who has access to his data, provided that disclosure satisfies one of three criteria.

a. information has fulfilled its purpose, is no longer generally necessary or relevant, or
b. The data principal granted permission for the creation of this data, but that consent has now been revoked, or
c. It was issued against the terms and has since been canceled by the new Data Protection Act and any other applicable statute.

The General Data Protection Regulation in the EU and the proposed right to be forgotten in India, however, differ significantly. Unlike the GDPR, the proposed Indian right does not include the right to fully erase the data. To prevent sensitive information from being published again, only one person, referred to as the data principal, removes acquired data. Additionally,

[26] Bill No. 373 of 2019

[27] " Data Protection Bill has provisions for 'right to be forgotten', Centre tells HC", The Hindu, (Dec. 17, 2021) available *at* https://www.thehindu.com/news/cities/Delhi/data-protection-bill-has-provisions-for-right-to-beforgotten-centre-tells-hc/article37973230.ece

the individual must request the Adjudicating Officer in order to exercise the right outlined in the Personal Data Protection Bill. The data principal does not have to do this in order to exercise any other rights granted by the Bill. In a similar vein, an individual, referred to as the data subject, may exercise his rights under the GDPR by asking the data controller to delete or remove any information pertaining to him.

(C) RTBF & Other Fundamental Rights

The CJEU's historic ruling acknowledging a right to be forgotten infuriated proponents of free speech. They claimed that giving people the option to ask for their personal data to be removed from Google searches amounted to blatant censorship and was incompatible with the right to free speech and expression. They justified their criticism by claiming that the right to free expression—which permits people to freely express their ideas, opinions, and thoughts as well as the right to receive information had been infringed[28]. According to some scholars, the Court "forgot" about free speech when it came to the outcome of the Google Spain case.

The United States Constitution and numerous international human rights accords, including the "Convention on the Rights of the Child, the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and the International Covenant on Economic, Social, and Cultural Rights," are examples of international treaties, and practically every nation recognizes the right to free expression. In General Comment No. 34, the UN Committee on Human Rights affirmed that Article 19 of the ICCPR safeguards all kinds of expression and the channels by which they are distributed, including electronic communication.

This demonstrates the importance of freedom of expression in both online and offline contexts. But the criticisms are baseless. First, research indicates that, based on aggregate data, Google has rejected 75% of erasure and right to be forgotten requests over the previous two years[29]. Theoretically, the interpretation of the decision refutes the claim that the right to free speech was entirely disregarded.

The Court holds that all rights are equal and that the only issue is which one should be given priority. Who won would depend on the specifics of the case. The Court believes that, generally speaking, the right to privacy outweighs the "not only economic aspects" interest of the search engine operator and the public in finding that information and looking up the name of the data subject. It put forth the idea that the limits of freedom of expression are set by privacy, not the

[28] Edward Lee, "The Right to Be Forgotten v. Free Speech", 12(1) *I/S: A Journal Of Law And Policy* (2015)
[29] Google Transparency Report, "Requests to delist content under European privacy law" available at https://transparencyreport.google.com/eu-privacy/overview

other way around. There is a vital connection between the right to privacy and the right to be forgotten.

In the case of "Olivier G v. Le Soir"[30] Regarding freedom of expression in 2008, when the Belgian weekly Le Soir made its complete archive freely accessible online. Consequently, the entire identity was revealed in a 1994 article about an automobile accident. The motorist in the collision asked for the picture or the driver's name to be removed. He had been properly convicted, the story went, and was "rehabilitated." The Belgian Court of Cassation ruled that Le Soir's freedom of expression may be protected by restricting the right to privacy under specific conditions. held that if a significant amount of time had passed, this might indicate a sincere desire to share the individual's name. After the crimes were revealed, the Court of Appeals determined that frequent website upgrades could seriously harm stakes over several years. Therefore, it came to the conclusion that the petitioner's right to privacy should take precedence over the newspaper's benefit from using its freedom of expression. Le Soir was forced to remove the applicant's name from the piece as a result.

The right of the public to know then expires like "milk," according to a 2016 Italian court ruling. In this instance, the petitioner had asked for an item to be taken down on the grounds that it would show up anytime someone searched for his or her firm name, causing records to surface that would ultimately hurt their stakes. However, due to its recentness, the article in question can have a greater impact than Google Spain. The court weighed the public interest in information and press freedom availability against the petitioner's right to privacy and determined that the latter had expired after two years. The publication was fined €10,000 for six months going forward for the delay in taking down the story from.

At the other end of the spectrum, where the protection of free speech and expression is crucial, are nations with more financial resources. The ruling in favor of RTBF against a journalistic group will undoubtedly be viewed as a First Amendment violation in the United States. In the US, there exist limitations on the right to free speech, although they are extremely onerous and only apply to [31] "the legal interests that the government can protect, or the imminent and serious danger." Given the seriousness of the matter, it seems doubtful that the United States of America will lose its right to free expression for the RTBF, albeit a thorough examination of this topic would depend on the particulars of each case.

As a result, there is always a clear balance between RTBF and claimed freedom of expression.

[30] N° C.15.0052.F, Cour de Cassation Belgique, Apr. 29, 2016 (Belg.).
[31] Paul Lambert, *The Right to be Forgotten* (Bloomsbury Professional, 1stedn., 2019)

Privacy and freedom of expression would be issues. State laws and international norms both stress the value of freedom of expression and privacy, but they also place restrictions on both, such as the three requirements of need, proportionality, and legality.

V. BUFFERING OF RTBF IN CYBER-SPACE – A WAY FORWARD

The number of people using the internet has increased as a result of the expansion of the internet to every part of the world due to developments in communication technologies. Success in every sector depends on having access to and exchanging information. It is by far the most effective method for disseminating information globally. Internet usage has skyrocketed in the last several years. Every day, millions of people use the internet to the extent that they post all of their data, including private information. This online data exposes a person's life story to the world, which can be a serious privacy violation. It is evident that the internet has permeated every aspect of human growth. The widespread use of the internet has had a significant impact on our social lives. While some of the changes are good, others are concerning. A new threat to an individual's privacy has been brought about via the internet.

To stay up with the quickly evolving field of information technology, we need to change our regulations on a regular basis. One contemporary problem is the removal of content from the internet that is someone else's property. In Tanzania, there is no such thing as a right to request the removal of content since Tanzania law does not acknowledge such a negative right. Tracking every bit of information would be detrimental to society as a whole. Only knowledge essential to society's evolution, or at the very least information that is not damaging to society, should be remembered. If someone wants to move on from their past, society should help them. This is why embracing the concept of social forgetting is so crucial in our culture. RTBF will, without a doubt, perform admirably. The right to be forgotten will defend people's privacy in the modern internet era.

Because of the Internet and advances in storage technologies, data retention has become a worry. This right is intimately linked to the problem of data retention because it can only access data that has been stored. As a result, data retention needs to be regulated by the government. It is not advisable to allow information to be held indefinitely since data retention in information technology poses a threat to an individual's privacy. During the traditional paper-based communication phase of the 1970s and 1980s, collecting information was more vital than storing it. Because storage technology had not advanced far enough, this was the case. We have, however, made significant progress, and the situation has significantly changed. Because of the broad availability and advancement of storage technologies, data from the internet and other

 [ISSN 2581-5369]

sources is being collected at an exponential rate around the world.

A good example in the present era is that of India, our civilization must confront the idea of collective forgetfulness. In Juvenile Justice and Bankruptcy Law, there is some acceptance of the theory of social forgetfulness. Juveniles' previous records may be expunged upon their release under the Indian juvenile justice system. This is essentially an admission of one's ineptitude. The development of a strong data retention policy will aid in the expansion of this acceptance into new laws.

The creation of a Data Retention Policy that governs data-related activities such as data collection, handling, and storage is critical to resolving this problem. It's also necessary to develop fair information practices principles. The United States and the European Union came up with these guidelines. Other countries should follow suit for the advancement of the information age.

Legislation to protect social oblivion should be adopted. On the other hand, legislation will not sufficient on its own. The cyber world in Tanzania is rapidly expanding, and Tanzanian laws must be updated to reflect this. Tanzania has been one of the world's most prolific internet users in recent years, and the internet has had a significant impact on the country's economy. This is why the internet has become so crucial in Tanzania, and all internet-related concerns must be resolved as soon as possible. Tanzanian law does not recognize the RTBF on the internet explicitly. Every day, an increasing number of Tanzanians are posting their personal information online, raising fresh concerns about unauthorized data use, privacy invasion, and other issues. In today's reality, Tanzanian laws are unable to appropriately address this problem. The RTBF concept is a critical component in modernizing Indian law. As a result, an RTBF-based system of cyber-world control and privacy protection should be implemented in Tanzania society.

The right to privacy of an individual is well-established in Tanzanian law and is guaranteed by The Constitution. The Cyber Crime Act of 2016 and its following revisions have improved privacy protection in the cybersphere, although their breadth is still fairly limited. A step in the right direction for RTBF would be to improve the country's privacy regulations and give individuals more control over their personal information. The Tanzania Parliament, as well as any other legislative body, has refused to recognize it. The impact of RTBF on Tanzanian society is what we're focusing on. Tanzanians will surely benefit from this right, as their internet privacy will now be more secure. Furthermore, even if the data is stored by a third party, the data subject retains ownership and control over it. Finally, RTBF would benefit Tanzanian

 [ISSN 2581-5369]

society, despite its bad implications.

In their national legislation, European countries have talked about how important it is to defend an individual's privacy and right to a unique identity. Regulations governing information security have vastly improved since the second half of the twentieth century. Because of the European Union's Charter of Fundamental Rights, citizens in Europe were aware of their privacy rights.

It's no surprise that the Google-Spain ruling from the European Court of Justice caused a stir across the EU. Because they will gain an extra benefit, EU citizens will benefit more from this decision. By selecting this case, the ECJ made it clear that it wished to remain anonymous. In a court of law, this privilege might be enforced. The European Court of Justice's ruling has broad ramifications. The ECJ's ruling raised awareness of the problem of online security in other regions of the world, even though it only applied within the EU's borders. Other nations will seek advice from the European Court of Justice (ECJ) on how to improve their domestic defense procurements. India is affected by the European Court of Justice's decision.

VI. CONCLUSION

Finally, the discussion above suggests that, in comparison to the rapid advancements in the west, RTBF is still in its infancy in Tanzania. Consequently, the following suggestions can be applied to effectively implement the RTBF principle in India:

- Making sure that everyone has access to this benefit would be greatly aided by strict data privacy laws. To further safeguard people's privacy, the RTBF ought to be reorganized.
- Recent events highlight the significance of the Data Protection Bill becoming law. When using digital media, people must always be protected from cyberattacks. In order to prevent any possible conflict between the two fundamental rights of the ability to express oneself and the right to be free from discrimination, it is also essential to include a paragraph that describes different scenarios with specific consequences.
- Several courts have acknowledged the RTBF in their decisions, citing international precedent, despite the PDP Bill not yet been ratified. A methodical approach to successfully maintaining RTBF without violating the rights to information and freedom of speech and expression is still a long way off, even though the Delhi and Karnataka High Courts have acknowledged and judicially upheld the right. To defend their

 [ISSN 2581-5369]

constitutionally guaranteed right to private in the interim, individuals may file a defamation lawsuit.

Lastly, delinking gives search engines and online platforms the ability to modify their guidelines and determine when to delete personal information. Large companies like Google still own sensitive data even after being sued by a petitioner in the Kerala High Court. This makes it the least efficient way to put the law into practice. On the other hand, combining the three and applying them methodically could assist India in creating and implementing RTBF.

*****

 [ISSN 2581-5369]

VII. BIBLIOGRAPHY

- Jyoti J. Mozika, "Integrating the Right to be Forgotten in the Indian Legal Framework in the Light of Experiences from the European" 12(1) *INDIAN JOURNAL OF LAW AND JUSTICE* (2021).
- C-131/12, Judgment of the Court (Grand Chamber) (May, 2014) available *at*https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX%3A62012CJ0131
- Case C-507/17, Judgment of the Court (Grand Chamber) (Sep. 24, 2019) available *at*https://eurlex.europa.eu/legal-content/en/TXT/?uri=CELEX:62017CJ0507
- Edward Lee, "The Right to Be Forgotten v. Free Speech", 12(1) *I/S: A Journal Of Law And Policy* (2015)
- General Data Protection Regulation, art. 17(3)
- Google Transparency Report, "Requests to delist content under European privacy law" available at https://transparencyreport.google.com/eu-privacy/overviewN° C.15.0052.F, Cour de Cassation Belgique, Apr. 29, 2016 (Belg.).
- Jean-François Blanchette& Deborah G. Johnson, "Data Retention and the Panoptic Society: The Social Benefits of Forgetfulness", 18(1) *The Information Society* 33-45 (2002) available *at*DOI: 10.1080/01972240252818216
- Justice K.S. Puttaswamy (Retd.) &Anr. vs. Union of India &Ors., *AIR 2017 SC 4161.*
- Melanie Dulong de Rosnay and Andres Guadamuz, "Memory Hole or Right to Delist? Implications of the Right to be Forgotten for Web Archiving" 6 *Recherchesen sciences sociales sur Internet (RESET)* (2017)available *at* https://journals.openedition.org/reset/807
- Nikolaj Nielsen, "EU regulators want right-to-be forgotten to go global" *euobserver* (Nov. 26, 2014) available*at* https://euobserver.com/rule-of-law/126680
- Paul Lambert, *The Right to be Forgotten* (Bloomsbury Professional, 1stedn., 2019)
- The Information Technology Act, 2000 (Act 21 of 2000), s. 2(1).
- Veronica Irwin, "Google will now remove personal information from search by request", protocol (Apr. 28, 2022) available *at*https://www.protocol.com/bulletins/google-search-personal-information

*****