

## ERASING THE ARCHIVES: RIGHT TO BE FORGOTTEN IN CYBER WORLD

MS. HIMANSHI BHATIA<sup>1</sup>, DR. DEEPTI KHUBALKAR<sup>2</sup>, MR. PRATEEK SIKCHI<sup>3</sup>

<sup>1, 2, 3</sup>Assistant Professor, Symbiosis Law School Nagpur, Symbiosis International (Deemed University), Pune - India.

\*Email: himanshibhatia@slnagpur.edu.in

### Abstract

*The complexity of human memory can be traced to the ‘Internet of things’ as well. The evolving digital space has witnessed & recorded the life of humans across the timeline of their usage. Due to the eternal memory of the internet along with its wide accessibility, the threat of the digital past is a contemporary issue for internet users globally. This implication of remembering everything, while deleting nothing has raised a recent discourse on the “Right to be Forgotten” (RTBF hereinafter) digitally. Thus, RTBF empowers an individual to control the accessibility of his information available online. However, in India, the recent regulation of the Information/data by the legislation is quite limited wherein RTBF is still an alien concept. Henceforth, this paper hypothesizes the essentiality of the RTBF in Indian domestic law. The paper will attempt to establish the necessity & consequences of recognition of such social forgetfulness rights in cyberspace.*

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

### Table of Contents

1. DEMYSTIFYING THE TERM – “THE RIGHT TO BE FORGOTTEN Objectives
2. EVOLUTION OF RTBF – A COMPARATIVE STUDY
3. RTBF & LAWS – AN INDIAN CONTEXT
  - 3.1 RTBF & I.T. Law
  - 3.2 RTBF & Data Protection Bill, 2019
  - 3.3 RTBF & Other Fundamental Rights
4. BUFFERING OF RTBF IN CYBER-SPACE – A WAY FORWARD
- Conclusion

### 1. DEMYSTIFYING THE TERM - “THE RIGHT TO BE FORGOTTEN”

The remembrance powers are often associated with the positive attribute whilst the forgetting is considered as something unfavorable to the memory aptitude. However, what if the same etching in the memory - remembrance turns out to be fatal for human sustenance? The technological advancement is woven with unaccountable transactional data, which is being stored for eternity. Thus, the infamously debatable privacy issue raises the concern on what level of accessibility & till what time such repository of information can be safe for an individual. The issue of data retention, revolves around these conundrums on why the data was collected? and for how long the data will serve the purpose? And lastly, if the purpose is being served then why it can’t be removed permanently from the digital space?

The attainment of the optimal level of social forgetfulness is a challenging endeavor, a balancing act between the need to hold people accountable and the desire to protect them to provide a "fresh start"<sup>12</sup>.

Thus, the Right to be Forgotten is inherently connected with data retention by technology. The dynamic development of the Internet & technology since 1995, has provided various problem content risks to which RTBF is one of the solutions. The level of sensitivity to personal data like sexual preferences, illnesses, family history, or past criminal records increases with the worldwide accessibility of tech apps & surveillance. The justification for the removal of such content by an individual can be due to the inaccuracy of data, malicious posting, cyber abuse, social stigmatization, outdated information, or just another personal threat to the well-being<sup>3</sup>. Unfortunately, the knowledge & research gap just exacerbates the increasing risks & threats to privacy, personality confidentiality, personal data & information.

The premise of data vulnerability led to the adoption of the "EU Data Protection Directive (DPD 95/46)" back in 1995 before the advent of the present advanced cyberspace. Whilst, it was before its time initiative but in the last two decades, the digital age has come far away. The severity & complexity of cybercrimes like bullying, stalking, revenge porn, sexual history, digitally induced suicides, and cyber frauds has grown out.

The current paper will study the nuances of why the demand for the erasure of online content should be entertained? Additionally, the responsibility of the service providers on which the content is available. Therefore, the research problem of the paper is based on: **How the RTBF is recognized as a distinct concept in the current IT Law regime of India?** The fact that privacy is being considered within the ambit of article 21 of the Constitution<sup>4</sup> also paves the way for RTBF implementation across data-sensitive legislation. Subsequently, the reasoning behind its applicability will be covered in the question, **Why RTBF is significant in the evolving digital advancement?** The explicit right of the individuals or an entity to delete or prohibit the retention of their personal information when it's of no use legally can be justified in the upcoming chapters.

## 2. EVOLUTION OF RTBF - A COMPARATIVE STUDY

The backdrop of the current RTBF discourse is due to the initial recognition & directives by the EU for the data protection & processing of such data. Therefore, the specifics of the RTBF are built upon the EU laws which were the first to grant it as a statutory right. However, the origin of the RTBF can be unearthed from the French term *Droit à l'oubli*, which means that a convicted criminal has the right to demand the erasure of his criminal records after serving the sentence.

<sup>1</sup>Assistant Professor of Law, Symbiosis Law School, Nagpur

<sup>2</sup>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

<sup>3</sup>Paul Lambert, *The Right to be Forgotten* (Bloomsbury Professional, 1<sup>st</sup> edn., 2019)

<sup>4</sup>*Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors.*, AIR 2017 SC 4161.



The vigilance of the western world led to the conflict between the “right to privacy” & “freedom of expression” of an individual with technological advancement. However, the court of the EU had tried to equate the values of both rights at the same pedestal, but it was not the case in the U.S., where free speech has extensively been paired with a weaker amount of privacy protection. Indeed, the United States has adopted an attitude to privacy that is virtually diametrically contrary to that of Europe, referring to it as the “right to inform”, while others refer to it as the “right to remember”<sup>5</sup>. Although this is not a formal phrase, it incorporates eloquently numerous privacy measures. While Europe has safeguarded privacy to the point of creating a new right to be forgotten, the United States has safeguarded free speech to the point where it is essentially a right to recall and not to forget precisely.

On 12<sup>th</sup> October 2015, the “Court of Justice of the European Union (CJEU)” rendered a decision in “**Maximilian Schrems v. Data Protection Commissioner**”<sup>6</sup>, putting an end to the transatlantic privacy conflict. The Schrems case has nothing to do with freedom of expression or privacy, but it does demonstrate the disparity in privacy treatment between the European Union and the United States, which might have severe financial repercussions. It also explains the widely divergent sentiments about the establishment of the right to be forgotten.

Henceforth, the European Data Protection Directive created a mandate concerning sharing of European citizens' data with the third country to have an acceptable degree of data protection. The adequacy level is determined by “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”.

When it became evident that the US would not adhere to the law, and a massive amount of data was being carried across the Atlantic, a solution had to be found. The “Safe Harbor” mechanism was devised by European institutions to allow personal information to be transported to the United States without certification that US laws protect personal information. The 2000 agreement enabled data to be shared with organizations in the United States who agreed to the “Safe Harbor Privacy Principles,” which are a simplified version of the Data Protection Directive's regulations<sup>7</sup>. The corporations also agreed that if they break these guidelines, the US Federal Trade Commission (FTC) or other regulatory agencies would hold them responsible.

The system had worked flawlessly for 15 years, but after the Edward Snowden surveillance scandal revealed that US IT corporations were complicit in the mass surveillance scheme, Schrems determined that data protection regulations had been violated. Because of this, Schrems requested

---

<sup>5</sup> Melanie Dulong de Rosnay and Andres Guadamuz, “Memory Hole or Right to Delist? Implications of the Right to be Forgotten for Web Archiving” <sup>6</sup> *Recherches en sciences sociales sur Internet (RESET)* (2017) available at <https://journals.openedition.org/reset/807> (last visited on May. 27, 2022).

<sup>6</sup> C-362/14, Judgment of the Court (Grand Chamber), (2015) available at <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62014CJ0362> (last visited on May. 27, 2022).

<sup>7</sup> *Supra* note 5.

the courts to throw out the Safe Harbor agreements. The case reached the CJEU, which agreed with Schrems and concluded that the current Safe Harbor was unconstitutional since it did not adequately protect Europeans' rights. The Court relied on the DPD which granted the Member States the authority to establish national agencies to monitor how personal data is used.

The EU law embodied DPD 95/46 was directive in nature as it set up the normative guidelines for the member states to adopt the essential requisites for data protection. Therefore, post the Safe Harbor ruling, the EU adopted new **General Data Protection Regulations (GDPR)**<sup>8</sup> with the repeal of the DPD guidelines. These regulations had uniform application across EU member states without the normative force of adoption by the member states in their national law.

The premise of this instrument is based on the landmark case of “**Google Spain SL and Google Inc. v Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzalez**”<sup>9</sup> which is regarded as the first case on the “Right to be Forgotten”. In this particular case, a Spanish citizen filed a complaint against Google Inc. & Newspaper relating to the auction of his house to pay the debts. Even though, the debts were paid by him years ago. Herein, the ECJ decided on the issue of directives' applicability the search engine like Google which collects “personal information” & “processing”. On the other hand, the EU citizen's right to erasure under the directive was under the consideration by the Court. Ultimately, the court held search engines legally liable to remove all the information as being violative of the privacy of the subject.

Though the new GDPR is not absolute, the right to be forgotten can be exercised only via the request of an individual to the controller with a discretionary power of removal. Under **Article 17 of the GDPR**, there is a right to be forgotten in the form of erasure. A data subject has the right to request the deletion of personal data as stated above, under this clause on one of many specified grounds within the next 30 days. To use this privilege, however, the individual needs to choose one of the four grounds listed below: (i) the information is no longer required (ii) The data subject has withdrawn consent for the purposes for which it was gathered (iii) the data subject objects to the data processing; and (iv) the data processing is in violation of the GDPR. When such a request is made, the internet service provider/data controller is required by an individual to unless data retention is required, “carry out the erasure immediately” balancing “the right to freedom of expression,” as defined by member states' local legislation. There is also an exemption<sup>10</sup> in the Regulation from the obligation to delete data for “the only purpose of processing personal data” for journalistic purposes, or artistic or literary expression.

Moreover, according to **Article 18 of the GDPR**, the data subject has the right to request the restriction of the processing of personal data from the controller<sup>11</sup>. When processing capability is

<sup>8</sup> (EU) 2016/679, *THE EUROPEAN PARLIAMENT AND OF THE COUNCIL* (Apr. 27, 2016) available at <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>

<sup>9</sup> C-131/12, Judgment of the Court (Grand Chamber) (May, 2014) available at <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131> (last visited on May. 27, 2022).

<sup>10</sup> General Data Protection Regulation, art. 17(3).

<sup>11</sup> *Id.*, art. 18.

limited, data controllers may store but not process personally identifiable information further. Instead, the controller renders the data unreachable in this circumstance as with the compliance of the right to be forgotten. This data relates to among other instances, erasure rights are granted when the following conditions are met: "In the majority of instances, personal information is no longer required or otherwise relevant to the purposes for which they were collected remodeled"<sup>12</sup> However, the restriction right has greater restrictions. For instance, in situations where "the data contradicts the data's authenticity subject"<sup>13</sup>.

### Impact of EU RTBF

The significant impact of the Google-Spain case & the adoption of GDPR can be felt in the EU member states & even globally. The landmark judgment led to the realization of the full-fledged right of erasure of personal information by EU citizens. Resultantly, search engines like google were afloat with thousands of requests from EU people to delist their data & related links<sup>14</sup>. However, even though ECJ's ruling had jurisdiction over the EU region only the global implications were there across the world. The mass request for removal led to another battle between Google & French Data Protection Agency (CNIL).

In two judgments issued in 2019, the CJEU clarified the scope of the right to be forgotten in the context of search engines. The Court had to decide in "**Google Inc. v. Commission nationale de l'informatique et des libertés (CNIL)**"<sup>15</sup> the right to be forgotten's territorial extent. It established a rule of thumb that de-referencing across the EU in connection with preventative or at least mitigating measures access to non-EU search results is severely limited. The second case "**GC & Ors. v. Commission nationale de l'informatique et des Libertés (CNIL)**"<sup>16</sup>, addresses how search engines handle sensitive data operators, as well as data de-referencing. Interference is a problem in this area with the data subject's right to privacy and personal data protection is responsible due to the sensitivity of such data. Consequently, Google won the battle with the ruling of ECJ to be limited to the EU region only and not globally. Howbeit, in the latest development for the non-EU states, google initiated a removal request for the personal data of the users like financial data, address, phone number, etc. which is of no use to the public at large<sup>17</sup>.

### 3. RTBF & LAWS - AN INDIAN CONTEXT

In comparison to the European Union, Indian privacy and data protection legislation are weak. The "right to privacy" is not explicitly guaranteed by law or through the constitution. However, in 2017, the Indian Apex Court declared the right to privacy to be a fundamental right in the landmark

<sup>12</sup>*Id.*, art. 17(a).

<sup>13</sup>*Id.*, art. 18(a).

<sup>14</sup>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> (last visited on May. 27, 2022).

<sup>15</sup>Case C-507/17, Judgment of the Court (Grand Chamber) (Sep. 24, 2019) available at <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62017CJ0507> (last visited on May. 27, 2022).

<sup>16</sup>*Ibid.*

<sup>17</sup>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> (last visited on May. 27, 2022).

judgment of **“Justice K. S. Puttaswamy v. Union of India”**<sup>18</sup>. The right to be forgotten was also discussed in the case in the ruling written by Justice S K Kaul, the Court described the RTBF as being composed of the larger informational privacy umbrella. The Court noted that this right confers control over the information disseminated by an individual, as well as the ability to request the removal of data about them. Justice Kaul claims that an individual has the “right to exercise control over and access to his data the right to rule one's own life includes the right to control one's physical existence on the Internet.”

The Court admitted that errors were made during the trial as people's digital lives should not be influenced by their history of a trail of evidence. Their ability to adapt and change should not be restricted. In addition, the court noted that the public does not have a right to all accurate information details about other persons. The absence of a data protection law then, on the other hand, was bound to deter the correct implementation and settlement of these issues. The fundamental issue is that the breadth of the right to be forgotten has yet to be determined, and this burden will eventually go to judicial authorities. The judicial system is tasked with making an impromptu decision on a prospective 'right' whose content is unknown and nebulous.<sup>19</sup>

Therefore, several precedents happened in **“Zulfiqar Ahman Khan v. Quintillion Business Media Pvt. Ltd & Ors.”**<sup>20</sup> The right of the plaintiff to be forgotten was recognized by the Delhi High Court. The issue arose as a result of the publication of articles containing the information regarding the complainant as an accused of harassment during the #MeToo campaign based on the respondent. The court ordered the respondent to remove these data as the plaintiff may be harmed significantly by articles obtained from the internet. **“The 'right to be forgotten and the 'right to be alone,' according to the court, are key elements of the right to privacy”.**

Similarly, in the case of **“DharamrajBhanushankar Dave v. the State of Gujarat”**<sup>21</sup>, the Gujarat High Court disagreed on a plea erasure, judgment noting that because the petitioner failed to indicate which legal provisions were at issue, the court dismissed the case. A writ was filed in this case by the petitioner to limit the scope of the investigation under Article 226 by requesting the removal of the publication of a court decision on the website even though the preceding decision was not reportable. The petitioner argued that it was interfering with his personal and professional life. However, the court countered it with the question of how downloading the relevant judgment constituted a violation of the law Article 21 of the Constitution. Citing the existing HC rules, the Gujarat High Court ruled that any party may request a copy of the High Court's decision on the request to the Assistant Registrar. Thus, the court refused to acknowledge the right to be forgotten. Although Section 69A of the IT Act, is the law of the land & the Information Technology (Reasonable Security Practice & Sensitive Personal Data or Information, 2011) Rules and Procedures

<sup>18</sup>*Supra* note 3.

<sup>19</sup>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).

<sup>20</sup>2019 (175) DRJ 660.

<sup>21</sup>2015 SCC OnLineGuj 2019.

are in effect. Thus, there is a dearth of clarity on the right to information of an individual with that right to be forgotten with all the considerations & the limitations attached herewith.

Subsequently, the Karnataka High Court held in “**Sri Vasunathan v. The Registrar General & Ors.**”<sup>22</sup> that the High Court ordered those only copies of the order received through the internet be deleted but did not include certified copies of the High Court order on the court’s webpage in the list of remedies of erasure. In this case, the petitioner wanted the petitioner’s daughter’s name to be removed from the order found in the digital archives. However, according to an FIR, the above instruction was issued against a man for drug-related offenses, brought by the petitioner’s daughter for offenses of forgeries, forcing her to marry, etc. Consequently, the parties have reached an understanding & the FIR was dismissed after the parties settled. Recognizing that it is a legal right to be forgotten the Karnataka High Court ordered the masking of the petitioner’s daughter’s name in the judgment. Court held that:

“would be in line with the trend in the Western countries where they follow this as a matter of rule **Right to be Forgotten** in sensitive cases involving women in general and highly sensitive cases involving rape or affecting the modesty and reputation of the person concerned.”

### 3.1 RTBF & I.T. Law

The Information Technology (IT) Act of 2000, passed by the Indian parliament, was the first law to address how technology is used. The Information Technology (Amendment) Act of 2008 amended the law to improve its application in the realm of information technology. This Act effectively addresses the issue of privacy; however, it is crucial to emphasize the inadequacy of this act on the issue of data protection. A detailed examination of the provisions exposes several basic tools that, if further improved, can ensure India has a good data protection framework. This law establishes some fundamental concepts in data protection, including data, data access, computer system, information, and a violation of confidentiality<sup>23</sup>.

As previously indicated, the Information Technology (IT) Act of 2000 does not recognize RTBF. However, it does discuss several aspects of RTBF, such as Personal Information and Privacy. **Companies must employ adequate security measures to protect sensitive personal information under Section 43A of the Information Technology (Amendment) Act (ITAA) of 2008.** Corporations are held accountable for data subjects’ privacy under this Act and its accompanying rules. There are some provisions with the barriers (restrictions) or the privacy standards under the S.43A that can be utilized in granting “information providers” the right to discontinue processing personal data which is similar to the EU DPD norms.

Other sections of the IT Act, include **Section 79**, which provides several safeguards for “intermediaries”<sup>24</sup>. This provision exempts intermediaries from liability in certain circumstances by

<sup>22</sup>Writ Petition No. 62038 of 2016.

<sup>23</sup>The Information Technology Act, 2000 (Act 21 of 2000), s. 2(1).

<sup>24</sup>*Id.*, s. 2(w).



the virtue of the rules for due diligence outlined in the IT Act of 2000. The intermediaries here include the search engines as per the description given in the IT Act. Telecom service providers, system service providers, network access providers, web-enabling service providers, web indexes, search engines, online-commercial hubs, and cyber hubs are examples of intermediaries that store & transmit the data as a third party.

Section 79 of the IT Act exempts intermediaries from liability in certain instances. This provision states that (1) an intermediary cannot be held liable for any third-party data, information, or communication link that he makes available or assists in the establishment of, even if it is illegal. This applies even if the law remains in effect until further notice (3).

Before anyone can use or access an intermediary's computer resource, the intermediary must disclose its rules and regulations, privacy policy, and user agreement, according to the S.79 principles. Users of the computer resource should be required to agree to terms and conditions that state they will not host, display, upload, edit, publish, send, update, or spread material that breaches another person's privacy.

Furthermore, the guidelines provide that the intermediary may not host or publish content that violates the regulations, such as information that invades another person's privacy, without the user's permission. Importantly, 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".

There may be difficulties and constraints in the context of the right-to-be-forgotten decision, such as what constitutes an invasion of privacy. However, there appears to be a strong correlation, which will not be established until something similar occurs in India.

### **3.2 RTBF & Data Protection Bill, 2019**

The predecessor Data Protection Bill, 2006 was passed by the parliament aiming at the protection of individual personal data & information. However, the evolving technology demanded the amended version of the latest Data Protection Bill, 2019<sup>25</sup>. Post Puttuswamy judgment, the dispute over data privacy regulation in India came to the forefront. Henceforth, the administration organized an expert panel to develop a plan on the Supreme Court's directions for a comprehensive data protection strategy in India. The Chairman of the Committee Justice BN Srikrishna prepared a study titled "A Free and Fair Digital Economy: Protecting Privacy and Empowering Indians," a report that contained a proposal on Personal Data Protection Act (PDPA). The purpose of the Data Protection Bill was to establish the direction of data protection in the future by regulating today's geopolitical landscape, which is becoming increasingly data-driven by establishing an extensive data governance system.

---

<sup>25</sup> Bill No. 373 of 2019



The current data security framework in India, which includes the Information Technology Act, 2000 and the Information Technology (Reasonable Security Practices and Procedures or Sensitive Personal Data), 2011 does not recognize the right to be forgotten. However, the newly established proposed legislation aims to establish this right<sup>26</sup>. The bill's section 20 states, that each data principal has the power to restrict or prohibit further processing, of any data fiduciary who has access to his data if such disclosure fulfills one of three requirements:

- a. information has served the mission or is no longer relevant in general or needed, or
- b. Such data was created with the data principal's permission and such permission has been withdrawn, or
- c. It was issued in contravention of the conditions and has since been revoked any other applicable statute, including the new Data Protection Act

However, there is a substantial difference between the proposed right to be forgotten in India and the EU version of the General Data Protection Regulation. The proposed Indian right does not include a right to complete the erasure of the data, unlike the GDPR. Only the single individual known as the data principal deletes obtained data, only to keep sensitive information from being published again. Furthermore, to exercise the right envisioned by the Personal Data Protection Bill must be exercised by the individual by requesting the Adjudicating Officer. This is not necessary to be performed by the data principal in the course of exercising any other right given by the Bill. Similarly, a person, known as the data subject, can exercise their rights under the GDPR by requesting that the data controller erase or remove data or information about himself.

### 3.3 RTBF & Other Fundamental Rights

Proponents of free expression were outraged by the CJEU's unprecedented decision recognizing a right to be forgotten. According to them, providing people with the right to request that their personal information be deleted from Google searches amounted to flagrant censorship and was incompatible with free expression and speech. They defended their criticism by alleging that free expression had been violated which allows people to freely express their thoughts, opinions, and ideas & right to receive information as well<sup>27</sup>. Some academics suggested that when resolving the case, the Court "forgot" about free expression when the Google Spain decision conclusion was made.

Almost every country has recognized the right to free expression, the United States Constitution, as well as various international human rights accords, such as the "Convention on the Rights of the

<sup>26</sup> "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-be-forgotten-centre-tells-hc/article37973230.ece> (last visited on May. 27, 2022).

<sup>27</sup> Edward Lee, "The Right to Be Forgotten v. Free Speech", 12(1) *I/S: A Journal Of Law And Policy* (2015).

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 all examples of international treaties. The Human Rights Council of the United Nations Committee confirmed in General Comment No. 34 that Article 19 of the ICCPR protects all forms of expression, as well as the means through which they are disseminated including all forms of electronic communication.

This shows the significance of the freedom of expression which spans the online and offline worlds. However, the criticisms are unfounded. To begin, research claims that according to aggregate data, Google has denied 75 % of requests for the right to be forgotten & erasure requests received in the past two years<sup>28</sup>. On the theoretical side, the ruling’s construction does not support the contention that the right to free expression was completely neglected.


According to the Court, all rights are equal, and the question is which one should take precedence. The circumstances of the case would determine who would win. The Court considers in general, the right to privacy takes precedence over the “not just economic factors” interest of the search engine operator as well as the general public to find that information, and conduct a search for the data subject’s name. It presented the notion that privacy determines the boundaries of freedom of expression & not the other way around. The right to be forgotten and the right to privacy is linked crucially.

In the case of “*Olivier G v. Le Soir*”<sup>29</sup> on freedom of expression in the year 2008 wherein Le Soir, a Belgian weekly, has made its entire archive available for free online. As a result, a 1994 article reporting a car accident with the full identity was made public. The driver in the accident requested to erase the driver’s name or delete the photograph. According to the narrative, he had been legally convicted and deemed “rehabilitated.” The Belgians Court of Cassation determined that in certain circumstances, the right to privacy may be curtailed for warranting freedom of expression to Le Soir. Subsequently, held that if a considerable period has elapsed, this could be the case of a genuine interest in communicating the person’s name. The Court of appeal decided that the up-gradation of the website regularly can significantly damage several years of stakes after the acts were reported. Hence it concluded, that the petitioner’s right to privacy versus the newspaper’s profit in exercising its freedom of expression the privacy shall be given preference. Therefore, Le Soir had to delete the applicant’s name from the story.

Following that, an Italian court ruled in 2016 that the public’s right to know expires just like “milk”. In this case, the petitioner had requested that an article be removed on the premise that the site would appear whenever a search for his or his company’s name will be done then records will be surfaced eventually harming their stakes. However, unlike Google Spain, the article in question may have a stronger impact because of it being recent. The petitioner’s right to privacy was

<sup>28</sup>Google Transparency Report, “Requests to delist content under European privacy law” available at <https://transparencyreport.google.com/eu-privacy/overview>(last visited on May. 27, 2022).

<sup>29</sup>N° C.15.0052.F, Cour de Cassation Belgique, Apr. 29, 2016 (Belg.).



balanced against the public interest in information and press freedom availability by the court, holding that the latter had expired after two years. Henceforth, the newspaper was fined €10,000 for a six-month for the delay in the removal of the article from the site.

Countries with more resources are at the other extreme of the spectrum where the protection of free speech and expression is critical. In the United States, the order in favor of RTBF against a journalistic organization will certainly be looked down on as a violation of the First Amendment. There are restrictions on freedom of expression in the United States but severely restrictive, extending only to<sup>30</sup> “immediate and grave danger, or the legal interests that the government can protect”. An in-depth investigation of this question would be based on the specifics of each case, however considering the gravity of the issue, it appears unlikely that the United States of America will lose its right to free expression for the RTBF.

Consequently, in each case, a balance between asserted freedom of expression and RTBF is clear. There would be concerns about free expression and privacy. Both international standards and state rules emphasize the importance of both freedom of expression and freedom of privacy but subject both of them to certain limitations like the three criteria of legality, proportionality, and necessity.

#### 4. BUFFERING OF RTBF IN CYBER-SPACE - A WAY FORWARD

Due to the advancements in communication technology, the internet has expanded to every corner of the globe, increasing the number of online individuals. Access to and sharing information is critical to success in every field. It is by far the most potent medium for worldwide information dissemination. The use of the internet has risen dramatically in recent years. Millions of individuals utilize the internet every day to the point where they publish all of their data, including personal information. This internet information makes the timeline of an individual's life public, which can be a significant infringement of privacy. We can see how the internet has infiltrated every facet of human development. Our social life has changed dramatically as a result of the broad adoption of the internet. Some of the changes are beneficial, but others are worrisome. The internet has introduced a new danger to an individual's privacy.

We must update our rules regularly if we are to keep up with the rapidly changing world of information technology. The wiping of material on the internet that belongs to someone else is a current issue. Because Indian law does not recognize such a negative right, there is no such thing as a right to seek the deletion of material in India. It would be harmful to society's overall good to keep track of every bit of information. 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.

---

<sup>30</sup>*Supra* note 18.



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

In the present era, 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 1principles. The United States and the European Union came up with these guidelines. Other countries should follow suit for the advancement of the information age.

In addition, legislation to protect social oblivion should be adopted. On the other hand, legislation will not sufficient on its own. The cyber world in India is rapidly expanding, and Indian laws must be updated to reflect this. India 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 India, and all internet-related concerns must be resolved as soon as possible. Indian law does not recognize the RTBF on the internet explicitly. Every day, an increasing number of Indians are posting their personal information online, raising fresh concerns about unauthorized data use, privacy invasion, and other issues. In today's reality, Indian 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 Indian society.

The right to privacy of an individual is well-established in Indian law and is guaranteed by the Indian Constitution. The IT Act of 2000 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 Indian Parliament, as well as any other legislative body, has refused to recognize it. The impact of RTBF on Indian society is what we're focusing on. Indians 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 Indian 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 wonder that the European Court of Justice's Google-Spain verdict reverberated throughout the EU. EU citizens will be better off as a result of this decision since they will receive an additional benefit. The ECJ made it apparent that it wanted to go unnoticed by choosing this case. This privilege might be enforceable in a court of law. The judgment of the European Court of Justice has far-reaching consequences. Although the ECJ's judgment only applied inside the EU's authority, it drew attention to the issue of online security in other parts of the world. Other countries throughout the world will turn to the European Court of Justice (ECJ) for guidance to strengthen their national defense procurements. The ruling of the European Court of Justice has repercussions in India.

Although Indian law recognizes some aspects of the RTBF, such as the concept of "Fresh Start" as defined by the Juvenile Justice Law, this is insufficient. In the online world, RTBF needs to be fully acknowledged. The rights to free expression and the public's right to know are recognized and protected by all democratic legal systems around the world. RTBF jeopardizes the right to free speech and factual information. The adoption of RTBF should not nullify these rights. As a result, a compromise between RTBF and other rights is required.

## CONCLUSION

Lastly, It can be inferred from the above discussion that RTBF is still in its infancy in India comparing it with the fast-pacing developments in the western world. Therefore, the following recommendations can be utilized to properly execute the concept of RTBF in India:

- A strong data privacy regulation would go a long way toward ensuring that everyone has access to this benefit. The RTBF should be restructured to better protect people's privacy.
- The importance of the Data Protection Bill becoming law is demonstrated by recent occurrences. People must always be protected from cyberattacks through the use of digital media. It is also vital to include a paragraph that defines various scenarios with detailed effects to avoid any potential contradiction between the two fundamental rights of the right to express & RTBF.
- Even though the PDP Bill has yet to be passed, several courts have recognized the RTBF in their rulings, citing international precedent. While the High Courts of Delhi and Karnataka have recognized and judicially enforced the right, a systematic strategy for effectively preserving RTBF without infringing the rights to information and freedom of speech and expression is still a



long way off. In the meanwhile, they can sue for defamation to protect their right to privacy under the Constitution.

Finally, delinking allows search engines and digital platforms to change their policies and decide when personal data should be destroyed. Despite being sued in the Kerala High Court by a petitioner, massive firms like Google continue to hold sensitive information. As a result, this is the least effective method of implementing the law. Combining the three and systematically using them, on the other hand, could help India build and implement RTBF.