UNPACKING THE RIGHT TO BE FORGOTTEN: LEGAL IMPLICATIONS AND PRACTICAL CHALLANGES

by

Archita Mahlawat & Hima Prajitha Bandaru

ABSTRACT

This paper explores the Right to Be Forgotten (RTBF) which is a legal and ethical concept providing recourse to individuals to request for removal of personal information from public records, especially at online platforms, to safeguard their privacy and reputation. RTBF originated from the European Union's General Data Protection Regulation (GDPR) and has sparked debate as it often intersects with the various other rights like freedom of expression and public access to information. This paper analyzes RTBF's application across various jurisdictions, including the landmark *Google Spain case*, as well as legislative developments in India and the United States. It examines how RTBF conflicts with other fundamental rights, particularly freedom of expression, by comparing privacy norms in regions where RTBF has been recognized and enforced. Additionally, the paper discusses practical challenges in implementing RTBF, particularly the case-by-case balancing required to address conflicts between individual privacy and public information access. Recommendations include adopting RTBF frameworks tailored to specific regional contexts, proposing cataloging mechanisms to track judicial trends, and considering alternative solutions like content delisting to harmonize RTBF with the freedom of expression. This paper aims to provide a nuanced understanding of RTBF's complexities and propose pathways for its effective global implementation in balancing privacy and public interest.

A. Introduction

In Indian context the principles based on which this Right to Be Forgotten ("RTBF") has been created can be inferred from the following observations made by the Hon'ble Supreme Court's Justice Nariman in *K.S. Puttaswamy and Another v. Union of India and Others*[1]:

> "*Humans forget, but the internet does not forget and does not let humans forget" ... "It is thus, said that in the digital world preservation is the norm and forgetting a struggle."*

In our opinion, RTBF is an extension of the Right to Privacy since it is based on the rationale that information of an individual is 'private' which makes it eligible to be erased/forgotten and does not arise from a rationale that any information expressed comes with a bundle of rights having ownership to remove it if desired.

B. Origin and current application of RTBF

RTBF can be retraced to an early right to oblivion in France called "*Droit á l'oubli*" enacted in 2010 which is based on privacy in relation to one's reputation and human dignity. It is also linked not only to privacy but the right to identity and self-determination.[2] RTBF is a procedural right through which these substantive rights of privacy and identity are enforced.[3]

RTBF can be defined as an individual's right to remove or restrict the public's access to that individual's personal information on the internet.[4] The first attempt by the EU to enact data protection and privacy laws was in 1981 through the 'Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data'[5]. It guaranteed an individual's right to access their stored personal information under Article 8 but came with

---

[1] (2017) 10 S.C.C.1

[2] Robert Fellner, The Right to be Forgotten in the European Human Rights Regime, GRIN (2014), https://www.grin.com/document/277390

[3] DE ANDRADE, N.N.G. OBLIVION: THE RIGHT TO BE DIFFERENT … FROM ONESELF: RE-PROPOSING THE RIGHT TO BE FORGOTTEN 65-81 (Alessia Ghezzi, Ângela Guimarães Pereira & Lucia Vesnić-Alujević, Palgrave Macmillan, London, 2014)

[4] David Lindsay, The Right To Be Forgotten in European Data Protection Law, in Emerging Challenges In Privacy Law, CUP, 290 (2014).

[5] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe, Jan. 28, 1981, C.E.T.S. No. 108.

a set of exceptions. This was followed by the enactment of the 'Data Protection Directive' in 1995.[6] The objective was to harmonize the data protection and privacy laws within the Member States for seamless data transfers and to further safeguard individual's fundamental rights and freedoms. Article 12 of this directive states that every individual has a right to the erasure of data and provides them with a right to apply for such erasure. Article 14 also allows individuals to object to data processing and mandates that the controller of data in such situation comply with the same in case of valid objections made by the individual.

In 2012, the GDPR[7] was enacted. RTBF was enshrined in Article 17 which states the following:

> *"The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay…"*

This can only be pursued in the following circumstances: (a) the data is not relevant or necessary with respect to the purpose for which it was collected (b) the individual was withdrawn their consent for such data processing or the period for which it was consented for has expired (c) the individual has objected to such data being processed under Article 19 (Right to Object) (d) the data processing does not comply with the GDPR. In furtherance, the commission in its explanatory memorandum has clarified that this article does provide the citizens of the EU with a 'Right to be Forgotten and a Right to Erasure'.[8] Additionally, the Recital 66 of the GDPR imposes an overarching duty on the controller which is making personal data public to inform the controller processing the said data to erase all/any links, copies of such personal data.

---

[6] Oct. 24, 1995, L 281/31.
[7] Regulation (EU) 2016/679 of the European Parliament and of the Council, April 27, 2016.
[8] Proposal for a regulation of the European parliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (2012)

a) The Google Spain Case

In 2010, an individual had requested Google to remove a Uniform Resource Locator (URL)which was linked to a news article providing details about an individual's bankruptcy which occurred in 1998. Google's formal complaint mechanism concluded that the request cannot be accepted and thus the issue arose.

In this case of *Google Spain SL v. Agencia Española de Protección de Datos*[9]*("Google Spain Case")*, the CJEU stated after interpreting the Data Protection Directives[10] that search engine operators are mandated to remove any links to webpages which are displayed after entering their name in the search bar if the information is "inadequate, irrelevant, or is longer relevant or is excessive in relation to the purpose of the processing at issue and the same would hold good even if the information was published lawfully while being factually accurate."[11] It is pertinent to note that this was before the enactment of the GDPR in 2012 and thus the CJEU read this right within the scope of the 1995 directives. The court held that google in this case would fall within the meaning of a 'controller' as defined under Article 2(b) and (d). It also concluded that Articles 12(b) and 14 can be read to state that search engines like google must comply with any such removal requests made by individuals. Lastly, it stated that this right to erasure is subject to limitations and that an individual for their request to accepted must firstly, must request for such removal of information meaning they have to be the data subject and secondly, prove that such removal would not affect the public's right to accessing information. "Right to be forgotten codified by the GDPR which can be considered as the second generation of this right as well as the second generation of balancing regime."[12]

b) India:

Within the Indian framework, this RTBF is enshrined under Section 1(t) of Digital Personal Data Protection Act, 2023 ("DPDP Act") which states that any data that is

[9] Google Spain SL v. Agencia Española de Protección de Datos C-131/12 (CJEU, May 13, 2014).
[10] Oct. 24, 1995, L 281/31.
[11] Google Spain SL v. Agencia Española de Protección de Datos C-131/12 (CJEU, May 13, 2014).
[12] Kamrul Faisal, Balancing between Right to Be Forgotten and Right to Freedom of Expression in Spent Criminal Convictions. Security and Privacy (March 16, 2021), https://doi.org/10.1002/spy2.157

identifiable to the respective individual is deemed to be under the purview of this Act as ‘personal data’. Section 8(7) of DPDP Act puts an obligation on data fiduciary to not retain any personal data of the data principal if consent to process the same is subsequently withdrawn or purpose of processing fulfilled, and it is no longer necessary to process and retain such data. The only exception to this duty is an obligation by law to retain or process the data. This obligation of the data fiduciary goes hand in hand with the right of data principal to erase any such data upon request to the same.

The dilemma arises when the RTBF infringes upon right to information and could be inferred to be necessary by law to be retained. Thus, there is no clear guidance on this aspect that if it is the obligation of the data fiduciary to decide whether it is necessary by law to retain such information.

Other provisions wherein this RTBF is recognized in Indian legal system can be seen under Section 43A of the Information Technology Act, 2000. Herein, an organization has a duty to pay damages when it stores/retains any sensitive personal data but is negligent in implementing appropriate safeguard of such data causing wrongful loss or wrongful gain. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 provide for a procedure to file complaints with the designated Grievance Officer to have content that exposes personal information about the complainant removed from the internet without the complainant's agreement.

The right to information where personal information disclosure is exempted under Section 8(1)(j) of Right to information Act (“RTI Act”) wherein there is no such obligation exists when any information which relates to personal information that has no relationship to any public activity or interest or would inadvertently cause unwarranted invasion of privacy of the individual. Except decided otherwise, upon satisfaction of central public information officer or the state public information officer or the appellate authority that it is in larger public interest for the information to be disclosed.

c) United States of America (USA):

In the United States of America, the fundamental aspect of RTBF that is dealt with, the distinction between public and private information, for example, any public

information once sealed becomes private and historical as time goes on and would not be covered by the First Amendment protections. But, any public information that is morbid and encroaches into an individual's private lives, exceeding bounds of a reasonable man's common decency can also be classified as a privacy violation. The Supreme Court and other Courts have primarily ruled upon cases which concerned media and are yet to explicitly address search engines etc.,

But some states do have laws to guarantee the RTBF from the internet such as California's 'Online Eraser Law' [13] which allows minors under the age of eighteen to "take down content or information that they posted themselves as registered users on a website, online service, online application or mobile application (collectively known as online service)." It mandates that the operator of a website or mobile application has to provide a mechanism for minors to remove the content or information that they have posted on their service." The 'California Delete Act'[14] gives Californians full control over their personal information collected by 'data brokers' and grants them a right to demand erasure of their personal information from their records and these demands can be filed through the mandated central platform managed by the California Privacy Protection Agency (CPPA) wherein individuals can request deletion and the same would be forwarded to all registered data brokers in the State. Any business registered in California and collects personal information should also comply with the 'California Privacy Rights Act' which regulates and rules. This Act provides a recourse for individuals to demand their right to delete personal information collected by a business and when such a request is received the business is obligated to inform all third-party service providers and contractors. The businesses are also mandated to provide a mechanism on their website wherein a consumer can submit such deletion requests. While the Supreme Court is yet to elaborate upon RTBF, about fifty media outlets created voluntary programs to 'erase an embarrassing moment, a long-ago minor crime, a past accusation later dropped or cleared, or a business circumstance such as bankruptcy later reversed from public view.' [15] This displays an overall shift in need of the hour wherein citizens have become more proactive in enforcing RTBF.

[13] Online Eraser Law (2015)
[14] California Delete Act (2023)
[15] Gene Policinski, *The Right to Be Forgotten: Everything to Know About Erasing Digital Footprints*, Freedom Forum (2024) https://www.freedomforum.org/right-to-be.

Overall, the USA is yet to formulate laws or have a judicial precedent to guarantee RTBF, while states like California have bridged this gap to certain extent; there exists no streamlined process or regulation to seek these rights as the Supreme Court is yet to explicitly acknowledge the same which would then open doors for nationwide adoption of regulations for these rights, until then, a private suit would have to be filed and same needs to convince the Court that the data sought for deletion is private and publishing the same would be a violation of privacy beyond protections guaranteed by the first amendment.

C. RTBF v Other Rights:

1) RTBF v Freedom of Expression

RTBF cannot be termed as a negative right to freedom of expression because this would imply that there exists no governmental interference but not a positive onus to retract one's information. Hence, the RTBF is neither an extension of freedom of expression and nor arising from it, it is argued that it is a limitation to the right of freedom of expression.

Following the European Convention on Human Right's (ECHR) model, validity of such a limitation on freedom of expression is checked through a 'three-part test' [16] as enumerated in Article 10 (2) wherein any such restriction should be prescribed by law, have a legitimate aim and should be a necessity for a democratic society.[17] RTBF is a valid limitation and within the scope of legal framework which is not infringing the right of freedom of expression. All the above stated essentials of the 'three-part' test are being fulfilled. The RTBF is prescribed by law under Article 17 of European Union General Data Protection Regulation (EU GDPR). The legitimate aim being fulfilled by RTBF is the protection of one's privacy and reputation. It is a necessity for a democratic

[16] DOMINIKA BYCHAWSKA-SINIARSKA, PROTECTING THE RIGHT TO FREEDOM OF EXPRESSION UNDER THE EUROPEAN CONVENTION ON HUMAN RIGHTS : A HANDBOOK FOR LEGAL PRACTITIONERS (2017).

[17] Toby Mendel, A Guide to the Interpretation and Meaning of Article 10 of the European Convention on Human Rights, Centre for Law and Democracy. https://rm.coe.int/16806f5bb3

society since it has become a "pressing social need"[18] that has arisen after public's contemplation on subject matters like digital privacy, data subject autonomy and control over one's data in European Union in the past decade, leading to the enactment of EU GDPR. To further support our argument of co-existence of both these rights, it can be inferred from the framework of the EU GDPR which has formally recognized the RTBF has separately recognized the freedom of expression under Article 85 and if it was the intent for it to be arising from it, there would not have been a need to balance both such rights under Recital 4 of the GDPR.

Therefore, upon establishing RTBF as a limitation of freedom of expression, it can be inferred that there will always be some conflict between both these rights as they limit each other necessitating balancing of these rights.

The ideological issue within the conflict between the RTBF and freedom of expression is that it is perceived to be a 'neither-nor' situation wherein freedom of expression proponents believe that the right to erasure (used interchangeably with RTBF in this paper) to be a threat based on the presumption that the digital space/internet is absolute free space and a cyberutopia while even delisting of data due to right to erasure/RTBF will turn this utopia to dystopia by being shackled to unnecessary control and manipulation of content.[19]

On the other hand, proponents of the RTBF believes that having such a right will make it equivalent to how human memory works wherein there is some data that we are bound to forget which will be an accurate representation of us because at present, remembering has become the norm and forgetting the exception which seems unnatural.[20] By forgetting information it can help in reducing the disadvantages of always remembering everything resulting in making one a prisoner of one's past without any second chances and not being able to make unencumbered sound decisions.[21]

---

[18] Observer and Guardian v. the United Kingdom, (1991) 14 EHRR 153

[19] Binoy Kampmark, To Find or be Forgotten: Global Tensions on the Right to Erasure and Internet Governance, 2(2), JGF 1 (2015)

[20] Maja Ovčak Kos, The Right to be Forgotten and the Media, 11 (2), LEXONOMICA (2019)

[21] Mayer-Schönberger V, Delete: The Virtue of Forgetting in the Digital Age, PUP (2009)

Although, this utopian view is emphasised by the proponents of freedom of expression, there is lack of evidence that substantiates this claim of a free and open space, since even before privacy concerns arose, there has been internet content restriction due to defamation, hate speech and other matters enshrined in the respective State legislation as an exception to freedom of speech. Governments have tried manipulating and censoring a lot of content by overreaching vague claims of threat to national security, public order, etc. Apart from the government, the digital players providing their services are also guilty of its manipulation employing dark patterns and social dilemma of only showing what you want to see and not the truth. This to an extent can be seen as an act of de-ranking information using their algorithms. Hence although the internet is a vast source of information, its manipulation of content and what data subjects see has been done for years. Therefore, the claim of the RTBF corrupting the freedom of the internet is wrong as it only now that users have control or some autonomy over their data rather than being a passive participant or product of it and is exercising their freedom of expression by choosing what they want to express and retract what they do not want.

2) Types of conflicts

Freedom of expression includes the expression of opinions and the freedom to receive and impart information.[22] RTBF is not an absolute right and has to be balanced out with other charter rights. Due to the vague statutes, precedents and their subjective nature, both these rights tend to conflict with each other while enacting the RTBF creating a chilling effect over freedom of expression.[23] Here are some specific areas of conflict with various other rights:

(a) *Right of the Public to Access Information v. Individual's Privacy*:

While the Court of Justice of the European Union (CJEU) through precedents upheld the right to free access of information especially for journalism, the

[22] Tietosuojavaltuutettu v. Satakunnan Markkinapörssi (2008) ECR I- 9831
[23] Muge Fazlioglu, Forget me not: the clash of the right to be forgotten and freedom of expression on the Internet, 3 (3), IDPL (2013).

same is in contradiction with its stance for the RTBF where it places an individual's RTBF over the public's right to access the said information. This leads to erosion of freedom of expression and goes against the initial aim of holding a fact-sensitive balancing exercise instead of one overpowering the other.

Under Article 9 of Data Protection Directives exemption of processing of personal information is done for journalistic or literary purposes and Article 13 of Data Protection Directives allows states to adopt various statutes to restrict some provisions under the privacy directives to safeguard other freedoms granted to individuals. This conflict primarily arises due to the vague and lack of objective parameters for determining these cases. CJEU while upholding the right to erasure, also failed to guide the practical applicability of the same. Speaking of individual rights, it is pertinent to note that while privacy to an extent must be granted to citizens, the same must not be done at the cost of rights of public. Removing journalistic articles or information is essentially diluting the freedom of expression as this right does not cease to exist after some time unless explicitly mentioned or consented for. The journalists enjoy a pre-publication immunity (to avoid a chilling effect on the investigation, on-ground reports etc.,), the same must be extended post-publication to reduce the journalists from being censored by controllers. [24] The CJEU allows processing by publishing its judgements as press release and allows third party processing of the same in the interest of journalistic and public interest. Hence, a similar conflict is seen in EU as well where GDPR privacy rights are overridden by right to public information. [25]

In the Indian scenario, the debate on RTBF has recently arisen again when the Hon'ble Supreme Court in *Ikanoon Software Development Pvt. Ltd. Versus Karthick Theodore and Ors (Special Leave to Appeal (C) No.15311/2024)* commented on the need to examine enforceability RTBF with regard to

[24] Christopher Knight, Data Protection and Freedom of Expression: A balance or void, CIPIL (2021), https://www.youtube.com/watch?v=Z74icbYzMu4

[25] Kamrul Faisal, Balancing between Right to Be Forgotten and Right to Freedom of Expression in Spent Criminal Convictions. Security and Privacy (March 16, 2021), https://doi.org/10.1002/spy2.157

revelation of acquitted person's identity published in judgements passed by courts and further reported by various digital platforms like "Indian kanoon".[26] In the aforesaid case, the dispute arose against order issued by the Hon'ble Madras High Court wherein Ikanoon Software Development Private Limited was directed to take down the record of a judgement wherein the Respondent was granted acquittal in a sexual assault case under Section 417 and Section 386 of Indian Penal Code. The Respondent filed a writ in Madras High Court aggrieved by the record because subsequent to his acquittal, his visa application for Australia was denied by the authorities citing the aforesaid criminal case. The Hon'ble Supreme Court while issuing notice in the same had granted a stay on the directions of the Hon'ble Madras High Court's while observing the following [27]:

> *"Assuming you are being acquitted, how can the HC direct him (Indian Kanoon) to pull down the judgement...once the judgement is delivered it is part of the public record.*
>
> …
>
> *In a given case like child sexual abuse, we may say redact the names or mask the names of the victims or witnesses. That is the jurisdiction of the court, but to say the judgement will be pulled down is far-fetched."*

Indian Kanoon has stated the following as part of their privacy policy last updated on January 14, 2024[28]:

> *"Policy on Personal Data based on public documents: Court judgments are public records. If a case is heard by a court of India, no one can argue that the opinion should not be published and viewable*

[26] Anmol Kaur Bawa, Supreme Court to Settle Law On 'Right to Be Forgotten'; Stays HC Direction To 'Indian Kanoon' To Pull Down Judgment, LIVELAW (July 24, 2024)https://www.livelaw.in/top-stories/supreme-court-to-settle-law-on-right-to-be-forgotten-stays-hc-direction-to-indiankanoon-to-pull-down-judgment-264401

[27] supra

[28]Indian Kanoon, Privacy Policy, INDIAN KANOON (Feb 14, 2023) https://indiankanoon.org/privacy.html -:~:text=Policy on Personal Data based, says it cannot be displayed

by all, unless the court itself expressly says it cannot be published or a law says it cannot be displayed. We will not remove or modify any public documents without an order of the court competent to do so. Remember, there are many, many copies of these court decisions in existence, and Indian Kanoon has just one of those many copies."

Hence, there is an existing tussle between right to public information and right to privacy that the Supreme Court of India is intending to clarify soon through this case.

But in the United States, especially laws in North Dakota, Minnesota, Montana, Alabama etc., requires strong protection of child criminal records, destruction of the records, fingerprints, pictures after they attain the age of majority and in some states its mandated that the authorities neither acknowledge these records nor publish them and must act like these records never existed.

On the other hand, a counter argument is made wherein right to privacy cannot be extended to personal information presented in an open court while proceedings are going on as held by Supreme Court and multiple High Courts in the below mentioned cases of India:

i. The Hon'ble Supreme Court in *Swapnil Tripathi V. Supreme Court of India*[29] wherein the underlying principle of justice is maintained by checks that an open court trial provides in contrast to maintenance of any claims of privacy.
ii. The Hon'ble Kerala High Court in *Vysakh K.G. V. Union of India and others*[30] inter alia dealing with a writ of habeas corpus seeking the production of a fiancée or minor children claiming alleged illegal detention is a private matter not involving public interest. The petitioner requested the court to protect their privacy by masking

[29] (2018) 10 SCC 639.
[30] (2022) SCC Online Ker 7337.

names and addresses in the judgment. This request is based on the right to privacy, or the "right to be let alone." Thus, it was held that any claim for protection of personal information based on the right to privacy and right to be let alone cannot co-exist in an open court justice system. On a similar line of thought, the Hon'ble Supreme Court in *R.Rajagopal V. State of Tamil Nadu*[31] has held that the right to privacy is subject to the exception that publication becomes unobjectionable if it is based upon public records including court records.

iii. The Hon'ble Karnataka High Court in *(Name Redacted) v. Registrar General, High Court of Karnataka & Ors.*[32] while dealing with a writ petition seeking a direction against the Respondent No.1 to remove the name of petitioner's daughter in the digital records maintained by the High Court to the extent of the same not being visible for the search engine including google or other search engines in a case of, inter alia, abduction of woman to compel her to marry which was later quashed upon mutual compromise. The court held that it should be the endeavour of the Registry to ensure that any internet search made in the public domain, ought not to reflect the petitioner's daughter's name. The underlying reasoning for such direction was held to be in line with western countries' ideology where they follow this as a matter of rule in sensitive cases involving women in general and highly sensitive cases involving rape or affecting the modesty and reputation of the person concerned. But the Court refused to mask the same in the High Court's records wherein any certified copy of the order will not be provided with a masked/ redacted the name of the petitioner's daughter.

(b) *Access to Information for Research v. Government's Power to Regulate Access*:

[31] (1994)6 SCC 632.
[32] (2017) SCC Online Kar 424

CJEU in the case of *Google Spain SL*[33] stated that the search engine operators upon request by an individual must remove 'unwanted' links and sites which appear upon searching an individual's name and held that if the removal request was 'legitimate' then the individual's right to erasure overrides the public's interest and right to access that information. This is in direct conflict with Article 9 of ECHR. While it does protect an individual's right, the same is not done by compromising on freedom of expression. Erasing all information about an individual previously accessible would deprive the public of a certain area from obtaining information. Given that information is only erased from the EU and not it's in entirety as different privacy laws govern different countries. While this information has been erased from EU states, the same could still be accessible in other countries. CJEU in practicality is adamant to apply standards imposed by other courts such as Strasburg etc., which is visible during its oral sessions or in its defeating silence concerning questions of balancing exercises creating problems for domestic courts. [34]

3) Case-to-Case balancing Issue

In enforcing the RTBF, freedom of expression is an exemption to it. The issue in exercise of this right is the ambiguity of how to deal with such an exemption since the power is vested with each member State to decide upon this exemption. Despite being prescriptive legislation, this conflict has not been elaborated upon leading to a lot of confusion and lack of any direction. The monumental case of *Google Spain SL*[35] on RTBF held it necessary for there to be a case-to-case assessment when erasure is deliberated upon because of the nature of information and its connection with one's privacy and private life at one hand and public interest in accessing that information on the other.[36] CJEU has recognised that neither of these fundamental rights are absolute nor superior to the other.

---

[33] Supra at 9
[34] Christopher Knight, Data Protection and Freedom of Expression: A balance or void, CIPIL (2021), https://www.youtube.com/watch?v=Z74icbYzMu4
[35] Supra at 9
[36] Google Spain SL v. Agencia Española de Protección de Datos C-131/12 (CJEU, May 13, 2014).

Even in India, Supreme court has recognised the sensitivity of such balancing as observed by Hon'ble Supreme Court in *Subhranshu Rout V State of Odisha*[37]wherein the following was stated prior to enactment of DPDP Act:

> *"It is also an undeniable fact that the implementation of right to be forgotten is a thorny issue in terms of practicality and technological nuances. In fact, it cries for a clear-cut demarcation of institutional boundaries and redressal of many delicate issues which hitherto remain unaddressed in Indian jurisdiction. The dynamics of hyper connectivity -the abundance, pervasiveness and accessibility of communication network have redefined the memory and the prescriptive mandate to include in the technological contours is of pressing importance..."*

We agree with the CJEU's approach because of the fundamental nature of both these rights as the EU has a right to privacy under Article 8 of ECHR and freedom of expression under Article 10 of ECHR. Since both are fundamental rights, it will be difficult to decide without looking into the context of each case. Any right is subject to a range of contingencies. An absolute implementation of such rights suggests the negation of its very purpose. [38]

But this approach has its problems with it. The first failure of a case-to-case basis approach is a lack thereof of any uniform guideline to help in determination of the scope of implementation, thereby creating confusion in appropriate balancing of these rights. There have been contradictory decisions even with similar fact situation across member states.[39] Such contradictions are a threat to uniformity that GDPR envisions since it was these non-uniform practices of the 1995 Directive that led to the birth of GDPR.[40]

---

[37] (2020) SCC Online Ori 878

[38] Binoy Kampmark, To Find or be Forgotten: Global Tensions on the Right to Erasure and Internet Governance, 2(2), JGF 1 (2015)

[39] Maja Ovčak Kos, The Right to be Forgotten and the Media, 11 (2), LEXONOMICA (2019)

[40] Muge Fazlioglu, Forget me not: the clash of the right to be forgotten and freedom of expression on the Internet, 3 (3), IDPL (2013).

The next failure is that this uncertainty gives rise to ambiguity for data controllers to act upon such requests of erasure with no clear framework to rely upon since the data controllers usually work globally. Even though GDPR makes them liable under it, it fails to state which Member States' legislative system to adhere to in case of contradictory opinions of different member states, when data subjects belong to multiple states. Hence the question of which State's policy regarding the conflict of right to erasure and freedom of expression to be followed remains. This vagueness will make it difficult for data controllers to comply appropriately with data protection laws and leading to inaccurate decisions and curtailment of data subjects' rights arbitrarily.

Since a similar approach is being adopted in India wherein section 8(7) of the DPDP Act puts the onus on data fiduciary/data controllers to decide. This will lead to a situation where a capitalistic entity will be balancing these fundamental rights as first instance authority. Although, obligation under Section 8(7) has not been extended to the courts by virtue of Section 17 of the DPDP Act. However, there is nothing that prevents the courts from providing recourse to RTBF for deserving individuals upon and it is left for the courts to decide applying case to case basis approach on such erasure/redaction. It is not against the principles of open court if such RTBF is enforced against such judgements/ proceedings since it is not veiling an open court proceeding rather safeguarding identity of an accused. Mere possibility of misuse is no excuse to not enforce such a right.

D. Recommendations

Considering the issues and debates above, following recommendations can be made:

RTBF, in relation to judicial pronouncements in India, should in our perspective come under the ambit of unlawful retention only to the extent it applies to the information regarding acquitted individual who has already gone through the trial and tribulations of the law. This not only protects their right to life and privacy but also helps them live a life of dignity after suffering through a trial. An act of balancing in such a matter demands that there is delinking / pseudonymization of the personal details while other information of the case record remains in the public record in the interest of the public.

This approach will be in line with EU GDPR's method of pseudonymization under Recital 28.

In the USA, some States like North Dakota, Minnesota, Montana, Alabama etc. mandates the destruction of all criminal records, fingerprints, pictures etc., of children below the age of eighteen which reinforces the RTBF in the interest of the child. This is also followed in some States for blood reports and results for certain disorders. Other than these two instances, States like Alabama, mandate the sealing of the original birth certificate once a child is adopted and Kentucky also makes sure no details of adoption are shared with any personnel in proximate distance of the child during birth etc. California makes it possible for a new birth certificate to be issued in cases wherein an individual requests a change in name or gender. Mississippi allows for the destruction of abortion records and West Virginia allows doctors to erase information about their previous drug dependencies if any. All these laws allow individuals from all stages of life to hold some sort of right which gives them authority over their personal information and shields such information from being used with a malafide intention and even helps individuals exercise right over their own private lives.

From the data controller's perspective, we agree with Edward lee's suggestion of having a catalogue.[41] It will prove beneficial to not only track the existing developments but also to be updated with new developments in the judicial decisions on the RTBF. Since there cannot be a strict standard that can be applied as both rights' balancing is highly contextual and blanket rules will create more problems and this is in line with GDPR giving the member states discretion to make their own decisions on this. Following such discretion, the only plausible way to accept the diversity of application while also keeping it uniform and within the framework of GDPR is by having a catalogue wherein a list of facts on which decision was based as well as the ratio will be enumerated. This will not only help remove uncertainty for data controllers worried about compliance. But can act as a guide for the courts of these member states to refer to actions of other courts in similar circumstances although it cannot be made binding on such courts but can be a guide and any deference by any court can also be listed as

[41] Edward Lee, The Right to Be Forgotten v. Free Speech (August 26, 2015) (on file with A Journal of Law and Policy for the Information Society)

a subcategory. For data subjects as well, this can be a list which can be easily accessible and readable by these subjects who can get better acquainted with their rights in different fact situation. will help immensely in reducing the uncertainty.

Although we agree with the adoption of delisting as a legitimate option that is least invasive and least obstructive of freedom of expression. This is also maybe why it is an option that search engines can use since it merely breaks the chain of linking the information while searching without deleting the data maintaining freedom of expression by merely making it a bit difficult to search that specific information, not complete erasure from the actual source page. Similar to this, a solution to give more control and autonomy to the data subject is by letting them arrange the first page of the search result when their name is inputted into the search engine.[42] By only allowing to arrange the first and not the rest there is a balance of both the right to privacy and freedom of expression as it merely de-ranks the links rather than delist or erase it. Hence this could be a technical solution adopted to offer recourse at first instance. And in this framework, if not satisfied the data subject can then file of delisting the information and the last step could be the demand of erasure which can be adjudicated upon by courts of their respective member states.

Thus, it can be concluded that in the current legal scenario it is difficult to infer the right to erasure being freedom of expression although such interpretation will make it easier to balance both these rights by assuming it to be a part of one encompassing right. But since that is not possible, there is still a need to analyze the existing conflicts that the paper has addressed and recommendations for easier practical application of it. Although we do not completely negate the idea of the right to erasure being part of freedom of expression, it can only be possible shortly when the concept of privacy itself gets diluted wherein to keep anything personal becomes difficult/impossible in the future then maybe right to erasure can be seen freedom of expression as a choice that one exercises to pick what information about oneself shall be disclosed and what remains disclosed.

[42] Jonathan Zittrain, Don't Force Google to "Forget", N.Y. TIMES (May 14, 2014) https://www.nytimes.com/2014/05/15/opinion/dont-force-google-to-forget.html