Central University of Kashmir Law Review
Vol. 5 (2025)
eISSN: 2583-6935
pp. 108-135

Digital Footprints and the Right to Be Forgotten: An Analysis in the Indian Context

Naveen Kumar*
Raajdwip Vardhan†

Abstract

The advent of the internet has brought forth a novel problem – information about individuals, including data that can be detrimental to personal interests, persists within the internet for perpetuity, and can be retrieved fairly easily, thus allowing this information to cause 'harm' even when the repercussions involving the same have been dealt with. To address this previously unappreciated issue, the "right to be forgotten," a derivative of the right to privacy, has been developed and has found footholds within European and Argentine jurisprudence. Under Indian law, the right has had an interesting development. While some High Courts recognised the right by tracing its scope from the right to privacy, the enactment of the "Digital Personal Data Protection Act, 2023" lent it legislative credibility under Section 15 within the phraseology of "the right to erasure". However, the twin sources of the right, coupled with the overarching framework of the right to free speech within Article 19(1)(a), which stands in dichotomous opposition to the right to be forgotten, complicate Indian applicability. In addition, constraints such as jurisdictional concerns due to the extra-territorial nature of data published on the internet, the development of Artificial Intelligence (AI), and the psychological phenomenon known as the 'Streisand Effect' pose further challenges to the development of this right within Indian jurisprudence. This necessitates a thorough analysis of the right and its scope and applicability within Indian law.

Keywords: *le droit à l'oubli, Right to be Forgotten, Right to Erasure, Data Protection, Right to Privacy*

1. Introduction

The 'right to be forgotten' (hereafter RTBF) is a right that has been formulated to address how digital footprints are treated in the era of the internet. Unlike previous eras, where the dissemination of

* Associate Professor, Department of Law, North-Eastern Hill University, Shillong, Meghalaya, India. email: naveenkr77@gmail.com
† Research Scholar, North-Eastern Hill University, Shillong, Meghalaya, India.

https://doi.org/10.66498/CUKLR.5.2025.108-135

information was limited by human memory or the extent to which printed data could traverse geographically, and was therefore subjected to the limitations posed by geographical constraints such as distance, the internet has revolutionised access to information by allowing digital footprints to persist perpetually and be accessible from any corner of the world. This implies that digitised versions of personal information continue to exist on the internet, unless removed, thereby leading to detrimental repercussions and implications to the personal interests of individuals. The RTBF seeks to address this 'apparent' infringement of individual privacy by hinging the existence of digital information on the 'consent' of the owner of that data, and balancing it with societal interests. It is a right that allows information to be 'forgotten', if the *'data principal'* does not consent to its presence on the internet, with the caveat that it serves no societal purpose.

Globally, this right has two bastions – Europe and Argentina, with each jurisdiction taking a different approach to the right's scope and ambit, and these have collectively and individually furthered the scope of this right across other jurisdictions. In India, the RTBF traces itself from two sources – traditionally, it was sourced by various High Courts within the country from different fountains, ranging from privacy and its facets to safeguarding a woman's modesty, however, since the enactment of the Digital Personal Data Protection Act, 2023, the recognition of the right to 'erasure' within Section 15, it also has a legislative basis. However, three questions persist within Indian jurisprudence *vis-à-vis* the applicability of the RTBF – first, are the legislative and judicial recognitions bestowed upon this right consonant or divergent with each other in their scope; second, how does the RTBF reconcile with the right to free speech encapsulated within Article 19(1)(a) which also contains within itself a right to know; and third, how does the RTBF's scope in Indian law deal with challenges stemming from queries related to jurisdictional challenges and the development of novel technologies such as Artificial Intelligence (hereafter AI). These three pressing questions need some analysis, and the scope of this paper shall be to examine them and draw relevant conclusions.

Against this backdrop, this paper shall be divided into six sections. The first section is a brief introduction to the theme and scope of the paper. The second section shall delve into the jurisprudential

developments of the RTBF in the two foremost bastions of Europe and Argentina. The third section will analyse the twin sources of the RTBF in the Indian context, as well as their scope and ambit, to explain their nature. The fourth section will examine the dichotomous position between the 'right to know' under Article 19(1)(a) and the RTBF, and attempt to understand whether a synergous legal position is possible under Indian law. The fifth section will address the challenges that the current legal framework has and offer relevant juristic solutions from global jurisprudence. Finally, the sixth section will summarise the arguments presented and conclude the paper.

2. Development of the Right to Be Forgotten in the Global Context: Reflections from Europe, Argentina and the USA

(a) Europe

The jurisprudential roots of the RTBF are traceable to the French concept of *"le droit à l'oubli",* which can be translated to "right to oblivion", and was utilized to protect the interests of both convicted criminals who had served their penal obligations and the accused who had been acquitted, from facing the loss of dignity due to materials surrounding their accusation, conviction or incarceration, thereby protecting their interests.[1] Therefore, the first bastion of this right is European jurisprudence. Associated with the right to privacy, which has been guaranteed to every individual under customary international law,[2] it is an important facet of extending protection to one's data and preventing it from being accessed and misused without consent.

Within European law, the RTBF is a part and parcel of the broader "right to data protection" and without it, the former cannot be implemented. This interconnection necessitates a discussion on the development of the RTBF from data protection norms. In Europe, data protection rights trace their roots to "Resolution 509(68) of the Council of Europe in 1968", which obligated the Council of Ministers to look at the "European Convention of Human Rights" (hereafter ECHR) and examine whether adequate protection was given to data in light of the emerging technological developments. This examination

[1] Jeffrey Rosen, "The Right to be Forgotten" 64 *Stanford Law Review Online* 90 (2012).

[2] Universal Declaration of Human Rights, 1946, Art. 12.

was further delegated by the Council of Ministers to the "Committee of Experts on Human Rights", which in turn recommended the establishment of a specialist "Committee of Experts on the Protection of Privacy", and through "Resolution 22 (1973) and 29 (1974)", the *"ground rules"* for data protection about the private and public sectors respectively were covered.[3] The next development took place in 1981 when the "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data", adopted in 1981 (hereafter 1981 Convention) was organised, with 43 out of a total of 47 members ratifying the Convention, with the Convention itself coming into force in October 1985.[4] This aligned with the ECHR declaration that - "the right of every individual to have his private and family life as well as his home and correspondence respected."[5] Within a decade of the 1981 Convention, the sacrosanctity of data protection was also recognised by the United Nations, and a set of norms known as the "Guidelines for the Regulation of Computerized Personal Data Files" were adopted by the UN Human Rights Commission in 1990.[6] Subsequently, the ideas of self-determination propounded by Niklas Luhmann,[7] which were also instrumental in implementing the "German Information Self-Determination Law", which created a space that shielded private individuals from interference on personal matters,[8] later paved the way for the "European Union's Data Protection Directive, 1995" (hereafter EUDPD, 1995).

The next major development came in the European Court of Justice's decision in the landmark "*Google Spain v. AEPD Mario Costeja González*",[9] a judgment that can be deemed the *grundnorm* for the development of jurisprudence on the RTBF, and that ultimately paved

[3] Chris Reed, *Computer Law* 579 (OUP, 2012).

[4] *Id,* at 581.

[5] European Convention on Human Rights, 1950, Art. 08.

[6] Adopted by the UN Commission on Human Rights, Resolution 1990/42; subsequently by the UN Economic and Social Council, Resolution 1990/38; and UN General Assembly Resolution 45/95.

[7] Niklas Luhmann, *Social Systems* 09 (Stanford University Press, 1995).

[8] G Hornung & C. Schnabel, "Data Protection in Germany I: The Population Census Decisions and the Right to Informational Self-Determination" 25 *Computer Law & Security Review* 85 (2009).

[9] ECLI:EU:C:2014:317.

the way for the creation of the "General Data Protection Regulation, 2016" (hereafter GDPR, 2016). The case involved a request by the respondent to a newspaper *La Vanguardia,* to remove information that was detrimental to his interests, and following their nonchalance, he filed a complaint with the "Agencia Española de Protección de Datos", (the primary data protection regulatory authority of Spain, hereafter referred to as AEPD) which in a 2010 decision rejected the liability of the newspaper but placed search engines under intermediary liability.[10] Following this imposition of intermediary liability, an appeal was filed by Google Spain in the ECJ. The ECJ relied on Article 12 and Article 6 of the EUDPR, 1995. Article 6 places a responsibility on a 'data controller' to ensure that the data about an individual is accurate and up-to-date. The notion of a 'data controller' having obligations about the data being processed by it if said controller has any discretion over the processing of data has been accepted since the British decision of "*Data Protection Registrar v. Griffin*".[11] The ECJ ultimately gave its judgment in favour of the plaintiff and directed the search engines to remove and delist data about a data subject that was irrelevant or had no significance upon a request for such delisting by the data subject. The ECJ also, however, cautioned that each request's significance was to be determined on a case-by-case basis by the *data controller*, and directed that information may not be removed if an overriding public interest is present for the existence of such information.[12]

This was a notable development since this judgment spurned a legacy of requests for deletion or removal of information considered prejudicial within domestic jurisdictions of the EU member countries, and Google has tackled them on a case-by-case basis; for example, in Belgium, a person whose conviction was overturned on appeal had his name delinked from an article about the incident for which he was tried after requesting about the same;[13] a request by a French priest who was convicted for possession of underage sexual imagery had his request for deletion of information about the incident denied, since the presence of such information on the internet was in the larger

[10] *Ibid*, para. 17.

[11] Ian J. Lloyd, *Information Technology Law* 58 (OUP, 2014).

[12] *Supra Note* 09*,* para. 94.

[13] Andrew Neville, "Is it a Human Right to be Forgotten? Conceptualizing the World View" 15 *Santa Clara Journal of International law* 163 (2017).

interest of society;[14] and in the United Kingdom, upon the request by a doctor to remove almost 50 URL links about a botched procedure, Google acquiesced and removed three URL links which had personal information about the doctor unconnected to the procedure, but kept up the other links.[15]

These developments, *inter alia,* led to the creation of the GDPR, 2018, and this Regulation is based on the belief that privacy is an inalienable tenet of modern life, which extends to the protection of personal data within the internet as well.[16] Article 17 is most significant in the present discussion since it explicitly delineates the right and empowers the *"data subject"* to seek the erasure of any personal data that relates to them, and also provides for the abstention of further dissemination or circulation of such data, on the successful application of the following four criteria –

a) The data does not have any significance about the purpose for which it was collected;
b) The data subject, which under the GDPR regime refers to a natural person, consent on which processing of the information is based, or the spatial scope of such consent has expired;
c) If the data subject raises objections under Article 19 of the GDPR, 2018;
d) The mechanism for processing data is in contrariety to the provisions of the GDPR. [17]

Furthermore, Article 17(2) elucidates that the *data controller*[18] must, if the personal data of individuals has been made public, and a direction has been given to erase the information, inform third parties which are responsible for the processing of such data that a request for removal of such data has been made by the *data subject* for the delisting or erasure of such personal data and its replication.[19] This position is however rooted in controversy to some extent for it implies that the *data controller* must take all reasonable steps to identify and

[14] *Ibid,* at 164.
[15] *Id*.
[16] Thea Kunz, *Celebrating Privacy Day: The Right to be Forgotten and Individual Privacy in the Digital Age* (2018) (Unpublished Master's Dissertation, Uppsala Universitet).
[17] General Data Protection Regulation, 2016, Art. 17(1).
[18] *Ibid,* Art. 4(7).
[19] *Ibid*, Art. 17(2).

ensure that all third parties who possess replicated copies of such data comply with the desires of the *data subject*, and this becomes extremely difficult in a digital medium such as the internet. It must be noted that the regime and framework constituted by Article 17 of the GDPR, 2018 is an exponential development when compared to the erstwhile EUDPA, and this development is reminiscent of the definition of privacy propounded by Alan Westin, wherein he defined privacy as *"the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others"*.[20] It must also be noted that providing and ensuring a formal recognition to the RTBF also democratises personal data on the internet, and provides control to individuals over their data, while at the same time, protecting them from exploitation and enforcing a general regime of data privacy on the internet. [21]

(b) Argentina

After Europe, Argentina is perhaps the nation that has attempted to formulate the most robust framework on the RTBF because it has historically given recognition to the right to privacy.[22] During the 1990s, Argentina incorporated an explicit provision into the Constitution empowering private individuals concerning the personal information of individuals that in case of the data being false or discriminatory, the individuals retained the right to request the *"suppression, rectification, confidentiality or updating of said data",*[23] although an exception for news reporting by journalists has also been recognized therein.[24] Data privacy, including the RTBF, is today guided by the comprehensive treatise titled "Personal Data Protection Act, 2000", and like other Argentine efforts within this domain, it also

[20] Alan Westin, *Privacy and Freedom* 7 (Atheneum, 1967).

[21] Eduard Fosch Villaronga et.al., "Humans Forget, Machines Remember: Artificial Intelligence and the Right to Be Forgotten" 34 *Computer Law and Security Review* 05 (2017).

[22] Edward L. Carter, "Argentina's Right to be Forgotten" 27 *Emory International Law Review* 35 (2013).

[23] The Constitution of Argentina, 1853, Art. 43.

[24] *Supra Note* 21*,* at 37.

mirrors the European legislative treatise, which in this case is the EUDPD, 1995.[25]

Subsequently, the "*Virginia Da Cunha v. Yahoo de Argentina S.R.L. and Google*"[26] judgement influenced the development of the RTBF, and this case is undoubtedly the strongest indicator of the willingness of the Argentine judiciary to invoke this right in the interests of data privacy, on the one hand, and personal dignity on the other. The brief facts constituted an Argentine entertainer's assertion that search engines - Google and Yahoo, remove and delist specific results against her name, which were linked to sexual content and pornography. Herein, the *ratio decidendi* held that the search engines were liable for their failure to remove sensitive information from the search being made. This notion stemmed from the understanding that the algorithms employed are capable of preventing certain results from appearing by relying on sensitive keywords, thereby preventing injury, however, considering that although Google Inc. and Yahoo! were notified of the plaintiff's desire to have information about her delisted through the initiation of proceedings in this case in the year 2006, the data in question continued to persist until the decision by the appellate court in 2010. Because of the continued existence of this data, brought forth by the inaction of concerned search engines, it became possible that the plaintiff may suffer some injury.[27] The lackluster behaviour exhibited by the search engines *vis-à-vis* privacy rights and data protection rights was deemed intolerable.

This case furthered the norm because in *Google Spain,* the law on the RTBF was only concerned with removing information rooted in criminal antecedents that may be detrimental to the interests of an individual, within the tenets of *"le droit à l'oubli",* however, in *De-Cunha,* the yardstick of the right was increased to include any undesirably defamatory information, thus taking a significant step forward.

---

[25] John W. Dowdell, "An American Right to Be Forgotten" 52 *Tulsa Law Review* 324 (2017).

[26] AR/JUR/40066/2010.

[27] Julieta Andrea Grinffiel. "Don't Shoot the Messenger: Civil Liability for ISPs after Virginia da Cunha v. Yahoo - Argentina & Google Inc" 17 *Law and Business Review of the Americas* 118 (2011).

(c) United States of America

Within the United States of America, although certain state constitutions, such as the states of Alaska, Arizona, California, Florida, Hawaii, Illinois, and Washington, among others, have provisions about informational privacy, the American Constitution lacks any explicit provision regarding the same.[28] In the American context, Samuel Warren and Louis Brandeis (who later went on to become a Justice in the US Supreme Court) in their seminal thesis on privacy expressed it as the "*right to be left alone"* and asserted that it should stand on a different pedestal, independent from other rights.[29] The primary argument that these two scholars made was that there should be legal recognition of "*the right to an inviolate personality",*[30] and the idea for this came from the British common law case of "*Prince Albert v. Strange*".[31] The American Constitution, in the First Amendment, explicitly provides that "*the Congress shall make no law abridging the freedom of speech or of the press."*[32] Thus, the greatest obstacle to a framework centered around the RTBF comes forth in the form of the First Amendment which essentially makes any law that is in contrariety to the tenets of free speech unconstitutional.[33] Brandeis, after becoming Justice in the Supreme Court would go on to provide a dissenting opinion in favour of privacy over the constitutional First Amendment rights in "*Olmstead v. United States*"[34] wherein he famously quoted Chief Justice Marshall's opinion from "*McCulloch v. Maryland*"[35] that "*we must never forget that it is a Constitution that we are expounding,"* thus referring to the

[28] Meg Leta Ambrose & Jef Ausloos, "The Right to be Forgotten Across the Pond" 3 *Journal of Information Policy* 08 (2013).

[29] SD Warren, LD Brandeis, "The Right to Privacy" 4 *Harvard Law Review* 196 (1890).

[30] Dr. J.J. Mozika, "Integrating the Right to be Forgotten in the Indian Legal Framework in Light of Experiences from the European Union" 12(1) *Indian Journal of Law and Justice* 41 (2021).

[31] (1849) 47 ER 1302.

[32] Constitution of the United States of America, 1789, 1st Amendment.

[33] Chelsea E. Carbone, "To Be or Not to Be Forgotten: Balancing the Right to Know with the Right to Privacy in the Digital" 22 *Virginia Journal of Social Policy & the Law* 555 (2015).

[34] 277 U.S. 438 (1928).

[35] 17 U.S. 316, (1819).

fact that the Constitution must be interpreted in light of developments which were unfathomable at the time of its inception to ensure a balance between the constitutional provisions and present necessities.[36] Nonetheless, the forces of free press and freedom of expression have almost always triumphed against privacy rights, with the most evident example perhaps being the "*Florida Star v. BJF*"[37] case.

One roundabout to the limitations of the First Amendment can be derived from the observations made in "*Cohen v. Cowles Media*", wherein the American Apex Court held that contracts that promise to not reveal information of a certain kind are not violative of the First Amendment which guarantees the freedom of speech and expression in America.[38] If informational privacy is only bestowed a contractual nature though, and if the RTBF is traced from this position, then for securing protection under the right, the data subject must have uploaded the information himself or consented to the publication of the information,[39] since barring these two situations, no contractual obligation can be considered to exist.

3. Right to be Forgotten in the Indian Context

India has seen exponential growth in its digital infrastructure ever since the final decades of the 20th century, and today, it boasts the second-largest population of people who use the internet in the world.[40] Recently, the right to access the internet has been deemed a fundamental right within the context of Article 19(1)(a) of the Constitution, only subject to reasonable limitations supported by Article 19(2), according to the judgment of the Apex Court in

[36] *Supra Note* 26, at 328.

[37] 491 U.S. 524, (1989).

[38] 501 U.S. 663 (1991).

[39] Robert Kirk Walker, "Note - The Right to Be Forgotten" 64 *Hastings Law Journal* 272 (2012).

[40] Noyonika Baptista, "Koo's Multi-lingual Feature Empowers Indians to Express Themselves in Several Languages" *Republic World,* 06 October, 2021, *available at:* https://www.republicworld.com/initiatives/specials/koos-multi-lingual-feature-empowers-indians-to-express-themselves-in-several-languages.html (last visited on May 20, 2025).

"*Anuradha Bhasin v. UOI*",[41] albeit it only expounds the right in the context of Article 19(1)(a) and not as a standalone right.

However, the legal framework of cyber laws, particularly data protection and data privacy laws, has been insipid at best. The action of enacting laws for governing the internet falls within the exclusive dominion of the Union government[42] and the "Information Technology Act, 2000" (hereafter IT Act. 2000), supplemented by a comparatively recent body of rules, the "Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011" were the only the primary legislations dealing with this domain till the year 2023 when the "Digital Personal Data Protection Act, 2023" (hereafter the DPDP Act, 2023) was passed. The primary component dealing with data protection within the IT Act, 2000, was a later amendment, under Section 43A, which stated that "*a body corporate possessing, dealing or handling any personal information in a computer resource which it owns, operates or controls",* is liable, if on account of its negligence in maintaining reasonable security practices, any wrongful gain or loss is caused to some person. However, this was an extremely rudimentary and primitive safeguard, and also vague in its applicability due to the utilisation of unspecified terms such as *'wrongful gain or loss'* being components for triggering its application. Furthermore, although the IT Rules, 2011 place some responsibility on body corporates, such as consent and security while taking and storing information respectively, neither is adequate to address the privacy concerns of the modern world.

In this backdrop, this chapter will attempt to analyse the applicability of the RTBF in the Indian context by tracing it from the right to privacy in the first part, and in the second part, it will try to assess the scope of the right in the DPDP Act, 2023.

(a) Tracing the right from the Right to Privacy under Article 21

The right to privacy within the Indian legal system has been a contentious issue. Neither the Constitution nor any legislation expressly recognises the right; nonetheless, after decades of

[41] 2020 3 SCC 637.

[42] Farzad Damania, "The Internet Equalizer of Freedom of Speech? A Discussion on Freedom of Speech on the Internet in the United States and India" 12 *Indiana International & Comparative Law Review* 248 (2002).

development, it was finally accepted as implicit in Article 21 in the landmark case of "*Retd. Justice K.S. Puttaswamy v. UOI"*[43] by revisiting the jurisprudence evolved in previous cases such as "*M.P. Sharma v. Satish Chandra*",[44] "*Kharak Singh v. State of Uttar Pradesh*"[45], "*Govind v. State of Madhya Pradesh*"[46] and "*R. Rajagopal v. Tamil Nadu*",[47] with the last case also being relevant as the first judgement, where the Hon'ble Apex Court finally recognised an individual's right to be left alone. These developments, also, interestingly, laid the groundwork for the recognition that unwarranted surveillance was not acceptable since it was an infringement against privacy in "*PUCL v. UOI*".[48] Expanding this, it has also been recognised by the Apex Court that the right to privacy prevents biometric information collected by the Unique Identification Authority of India (UIDAI) from being shared with other entities, including investigating agencies, without consent from the individual whose data is being shared.[49]

The formal recognition of the RTBF opened up a Pandora's Box of claims *vis-à-vis* digital data protection and privacy. Interestingly, in the *Puttaswamy case*, Justice S.K. Kaul explicitly considered the applicability of the RTBF in the Indian context and argued that it is a part and parcel of the wider ambit of 'informational privacy'.[50] In this regard, he said that the *"right of an individual to exercise control over his personal data and to be able to control his/her own life would also encompass his right to control his existence on the Internet."*[51] This is an appreciable observation because envisaging privacy without considering the significance of digital privacy and giving control over one's data, especially in an open domain such as the internet, would lead to conflicting positions.

In light of these developments, various High Courts have been active in recognising the RTBF. This is undoubtedly a welcome development because it presents the opportunity for individuals to exercise

[43] (2017) 10 SCC 1.
[44] AIR 1954 SC 300.
[45] AIR 1963 SC 1295.
[46] 1975 AIR 1375.
[47] (1994) 6 SCC 632.
[48] AIR 1997 SC 568.
[49] UIDAI V. CBI, (2014) SLP (Crl.) 2524.
[50] *Supra Note* 30, at 50.
[51] *Supra Note* 43.

meaningful control over their digital avatars and decide on the presence of information related to them on the internet. However, there persists great uncertainty over the extent of the right, primarily due to conflicting judgments by various High Courts within India, with some recognising and others refusing to grant recognition to the RTBF within the ambit of the constitutional right to privacy. Moreover, even in those cases wherein the Courts have granted recognition to the right and directed a remedy under the scope of the right, the roots of the right and the reasoning behind its application are contradictory.

In "*Dharmaraj Bhanushankar Dave v. Gujarat*"[52] the Gujarat High Court was approached by the petitioner, who wanted to remove a prior judgement given against him from online legal repositories. In the previous judgement, he had been acquitted by both the trial court as well as the appellate courts for culpable homicide amounting to murder. Nonetheless, the Court herein refused to entertain the request and dismissed the petition on two grounds, first, it said that the petitioner was unable to establish any threat to his life or liberty on account of the existence of that record; second, it argued that the publication of an online repository does not amount to 'reporting the judgement and that interpretation is only restricted to when the judgement has been recorded in law reports. Here, it can be considered that the interpretation adopted by the court depicts a narrow approach while expounding the right, since even in the absence of any harm caused at present, there is always the presence of some societal stigma and the potential of repercussions on the individual may become an instance of implicit double jeopardy.

In contrast, though, the Delhi High Court has upheld and recognised the applicability of the RTBF in similar situations where petitioners approached the Court for the removal of existing information about their prior legal records. In "*Jorawar Singh Mundy v. UOI*"[53], the petitioner had charges levied against him under the "Narcotics and Psychotropic Substances Act, 1985", albeit these charges were subsequently dropped; nonetheless, due to the existence of these charges as a record, the petitioner was having difficulty in finding employment. This prompted the petitioner to file a writ, following which, the Court decided in favour of the right to privacy (by citing the

[52] 2015 SCC Online Guj 2019.

[53] 2021 SCC Online Del. 2306.

RTBF) when weighed against the right to information (that is a public right) and ordered the removal of the objectionable information from the search engines that were hampering the interests of the petitioner since the information itself had lost its relevance. Finally, in "*S.K v. UOI*"[54] the Court passed an interim order directing online repository *Indian Kanoon* and to remove the name of the petitioner in this case, who had been acquitted of rape charges in 2018. Additionally, it also sought an affidavit from the portal wherein the portal was to highlight its policy *vis-à-vis* the right to be forgotten, and the steps that it would take to recognise this right by masking the names of similar individuals in cases and judgements of both High Courts as well as trial courts. The second part of the judgement is relevant because it takes initiative to concretise the RTBF by taking future challenges into consideration as well.

Interestingly, in another case where legal information pertaining to an individual was sought to be removed, the Madras High Court in 2024, in "*Karthick Theodore v. Registrar General, Madras High Court*"[55], also refused to entertain a petition seeking the removal of an original record, thus refusing to allow the redaction of content regarding the petitioner's published court records. This again created a conflicting legal position since the position of various High Courts concerning the applicability of the RTBF in requests regarding the removal of published legal information is in conflict. Notably, this judgement has been stayed after being appealed by the Hon'ble Apex Court, and it has decided to examine whether the RTBF is wide enough to allow the 'redaction of legal information' or if the right to redaction is a separate right when compared with the RTBF in the context of previously published legal information.[56] The issue is presently *sub-judice*.

The Karnataka High Court has also presented some interesting jurisprudence in "*Sri Vasunathan v. The Registrar General, High Court of Karnataka and Ors*",[57] wherein the father of a woman, who had

[54] 2023 LiveLaw (Del) 488.

[55] 2021 SCC OnLine Mad. 2755.

[56] "SC to Examine Right to Be Forgotten of Accused After Acquittal in Criminal Case" *Deccan Herald,* 24 July 2024 <*available at https://www.deccanherald.com/india/sc-to-examine-right-to-be-forgotten-of-accused-after-acquittal-in-criminal-case-3119628*> (last visited on 02 June, 2025).

[57] 2017 SCC Online Kar 424.

previously approached the Court to have her marriage certificate annulled, petitioned the High Court to have information about her legal endeavors relating to the annulment of the marriage certificate removed from online legal repositories which reflected her name, the High Court approved and accepted that the woman had a right to have the information removed. Interestingly, herein. The Court's decision, instead of tracing itself from the right to privacy, was centered on the understanding that the RTBF had to be used herein to safeguard the modesty and reputation of the woman in question.[58] This meant that the right was encapsulated with protecting information that was sensitive to the modesty of the women, and this change also contributed another significant jurisprudential layer to the right. The Orissa High Court has also relied upon this right to protect and safeguard the modesty of women in "*Subhrasnshu Rout v. State of Odisha*"[59]. When the Court was approached by the petitioner for the removal of private pictures and videos that had been published online, the Court cited the international position of the right and recognised its significance as an instrument for protecting the sanctity of women whose modesty and reputation had been hampered. By relying on the same, it directed the erasure of private pictures that had been published online. These two judgements, although they came prior to the enactment of the DPDP Act, 2023 where there was a lack of clarity on the source of the RTBF, it can be noted that these two pronouncements imply that the RTBF can be applied even for safeguarding something like the modesty of a woman without directly tracing it to the right to privacy or data protection.

Similarly, the Delhi High Court has also been at the forefront of applying the RTBF in the Indian context. Firstly, in "*Zulfiqar Ahman Khan v. Quintillion Business*"60 on an injunction order sought by the petitioner against the publication of information which was deemed to be damaging to his reputation, the Delhi High Court recognized the RTBF as a subset of the right to privacy and passed an order directing the defendant to take down the concerned information from its digital repository. This judgement, unlike the others, traced the right from the

[58] Ajay Pal Singh & Rahil Setia, "Right to Be Forgotten – Recognition, Legislation and Acceptance in International and Domestic Domain" 6 *Nirma University Law Journal* 49 (2018).

[59] BLAPL No.4592 of 2020,

[60]AIR 2019 Del. 132.

right to privacy. While the decisions of the Karnataka and Orissa High Courts were centered on the rights' international status, coupled with the paramount necessity to safeguard the sanctity and modesty of women, herein, the effects and implications of *Puttaswamy* were visible.

Finally, the Kerala High Court's observations in "*Google Inc v. XXXX & Ors*"[61] needs to be discussed. Herein, the petitioner had filed a request to review the Court's earlier judgment in judgment in *"Vysakh K.G v. UOI",*[62] and *inter alia*, the Court observed that notwithstanding the absence of legislation that formally recognizes the RTBF, a Court's order to remove information by the RTBF would inadvertently draw itself from Rule 3(d) of the IT Rules, 2011. This was significant because a legislative source is traced in this judgment by the judiciary to give validation to the judiciary's activist utilization of the right, and thus, this can be considered to be a precursor of the DPDP Act, 2023's right to erasure within a judicial context.

These developments present some interesting facets to the argument surrounding the applicability of the RTBF in India. The right itself is sacrosanct and this is exemplified by the recognition afforded to it even in the absence of a clear legislative source. The significance of data privacy cannot be underestimated and the activism that the judiciary has shown is commendable. Nevertheless, the varied sources and reasons for which the right has been given acceptance in the Indian legal system cause a degree of confusion, and the legal incoherence needs rectification. One way of addressing the same can be through a decision given by the Apex Court of the nation wherein it finalizes the source, extent, and ambit of the right, and declares it to be law by the constitutional powers embedded within it under Article 141. The European and Argentine jurisdictions have relied mainly upon the judiciary's activism to give concrete shape to the right. On the other hand, a second, and more commonly accepted means would be through legislative intervention, wherein the Parliament, *via* legislation, recognizes the right and elucidates its extent and ambit. The enactment of the DPDP Act, 2023 fulfilled this legislative requisite and the next part of this discussion will analyse the scope and ambit of the RTBF within the context of the DPDP Act, 2023.

---

[61] 2023 LiveLaw (Ker) 182.

[62] 2022 SCC Online Ker. 7337.

(b) Tracing the right from the Digital Personal Data Protection Act, 2023

The momentous *Puttaswamy judgement* changed the outlook on privacy rights in India and after the judgement, a committee under the chairmanship of Retd. Justice B.N Srikrishna was constituted to look into the nuances of the right to privacy within the digital sphere. This was followed by the Personal Data Protection Bills of 2019 and 2022. The latter received assent from the Parliament of India in 2023 and it led to the Digital Personal Data Protection Act, 2023 (hereafter DPDP Act, 2023). This legislation contains a reference to the "Right to Erasure"*,* which is a right synonymous with the RTBF.

In the DPDP Act, 2023, the *'data principal'* that is the person to whom the data or information in question refers to, or in case of the person being a child, the child's lawful guardians or parents, shall have the right to seek the "correction or erasure" of the data through a request to the *'data fiduciary'*.[63] The *fiduciary* is the entity responsible for ascertaining the means and purpose of the personal data, and upon receiving such a request, is bound to erase the personal data of the *principal* on the fulfillment of two grounds - "the retention of the personal data is no longer necessary"; and, "the purpose for which it was processed is not necessary anymore."[64] Contrarily, the *'data principal'* is also obligated to furnish only that information that is true and verifiable *via* authentication when exercising erasure rights afforded by the Act.[65] The government has been mandated to formulate the procedure to be followed by the *'data principal'* for making a request to the *'data fiduciary'*[66] and only this procedure can help the individual in exercising his right to erasure.

Furthermore, even in the absence of a request by the *principal,* the *fiduciary* is under the obligation to remove the personal data of *principals* on the fulfillment of two grounds – its retention firstly is no longer necessary since the purpose of retention is no longer being served; and secondly, the retention is not necessary anymore for either legal or business-related purposes.[67] Although this provision places an interesting obligation on *data fiduciaries,* the utilization and

[63] Digital Personal Data Protection Act, 2023, s. 2(j).
[64] *Ibid,* s. 12.
[65] *Ibid,* s. 15(e).
[66] *Ibid,* s. 40(2)(n).
[67] *Ibid,* s. 8(7).

reliance on ambiguous terms like "legal purpose" and "business purpose" are terms having a very wide interpretive ambit inadvertently defeats the purpose of the provision itself since the data in question can be construed to have a function within the ambit of these two terms, thus leading to arbitrary misuse of data under their shield.

Finally, for this discussion to be holistic, the DPDP Rules, 2025, which have been recently notified by the central government in pursuance of the powers given under Section 40(1) of the DPDP Act, 2023, in November, 2025 also need to be examined. Under Rule 8, an obligation has been placed on *data fiduciaries* falling under the Third Schedule of the Rules, which includes e-commerce entities with two crore registered users in India; social media intermediaries with two crore users registered in India; and, online gaming platforms with fifty lakh registered users in India, to erase personal data of users, after a period of three years from the date of last transaction between the *data principal* and the entity in question, unless there is a legal obligation to keep a record of the data. Additionally, the *data principal* must also be informed about the erasure of data 48 hours before the processing is completed to give the person an opportunity to keep his data intact. Beyond these, however, an additional caveat has also been placed, and it states that the data of individuals, including *"personal data, associated traffic data and other logs of the processing"* must be retained for a minimum period of one year after it has been processed if it is being used by any instrumentalities of the State in the *"interest of sovereignty and integrity of India or the security of the State"* or for the performance of any action under any law in force at that point of time.

One welcome development, when compared to the erstwhile Bill of 2019, is the removal of the provision necessitating the payment of fees by the *principal* to the *fiduciary* for effectuating a request for the removal of information, which would have given a commercial aspect to the exercise of the right. The imposition of a fee was questionable on two grounds firstly, an ambiguous term "reasonable fee" has been used and there is no mechanism to understand what would determine the reasonableness of a fee charged under this provision; secondly, by bestowing a financial aspect into the exercise of the right, the provision severely limits its exercise since a person who is unable to afford the fee imposed by the data fiduciary may be unable to exercise the RTBF and therefore be forced to live with the stigma which the

information in question in that particular incident was causing him, thereby leading to a violation of his right to live with dignity as well. Therefore, the removal of this provision is a much-needed change. Secondly, while the earlier bill merely placed restrictions on the publication of information by placing restrictions on disclosing data,[68] the present legislation also includes data processing within its ambit, thereby increasing the scope of protection afforded.

It is also necessary that the shortcomings of the DPDP Act, 2023, be highlighted. Two major issues arise regarding the RTBF. Firstly, the legislation grants blanket immunity to the State and its agencies as far as coming under the ambit of the RTBF is concerned. The State (central government) or any of its instrumentalities can retain the personal data of individuals and not adhere to the requirements of the RTBF if certain grounds permit it.[69] This includes ambiguous terms such as "sovereignty and integrity of India", "security of the State" and "maintenance of public order" without defining the extent of these terms in the context of the DPDP Act, 2023. The impunity granted to the State is pernicious because it allows the State to collect and store the personal data of any *'data principal'* even when the individual is objecting against the same. It is an accepted position that the RTBF cannot be an absolute one, and certain exceptions are needed in the larger interests of society. Nevertheless, the immunity granted to the State presents a distressing scenario because it can easily allow the State to exploit the personal data of individuals.

The second shortcoming comes from its failure to address the challenges that are being faced in the digital domain by the advent of Artificial Intelligence (hereinafter AI) technology. AI has caused a paradigm shift, and it is being integrated and implemented in more and more areas with each passing day. AI liability is something that is often neglected within law because either it is considered a foreign concept for most jurisdictions or it is deemed to be harmless due to the nascent stage of the technology. Nonetheless, the challenges are real, and so are the implications stemming from it. One classic example is the aforementioned *Google case,* wherein the company

[68] Ashwinee Kumar, "The Right to Be Forgotten in the Digital Age: A Comparative Study of the Indian Personal Data Protection Bill, 2018 & the GDPR" *2 HPNLU Shimla Law Review* 87 (2019).

[69] *Supra Note* 63, s. 17(2).

had argued that it had no liability because the search engines were based on algorithms and it is the algorithm that brings forth certain results.[70] This is a very rudimentary example for furthering the arguments being made, however, they are by no means unimportant. This issue is further exacerbated by the fact that an AI does not "forget" in a way that a human does, and the deletion of information for removing it from the "mind" of an AI is especially difficult in the present data-driven regime.[71] Conversely, in the interest of AI development, machine learning primarily relies on data sets and the removal of 'data' from the data set without conditioning the algorithm to take care of the now "forgotten" information while making its calculations can have a detrimental effect on the conclusions formulated and the results presented. These issues could have been better addressed with a specific provision for dealing with the intersectionality of AI and the RTBF.

4. Freedom of Expression and Right to Be Forgotten – Search for a Balance

There exists a dichotomous relationship between RTBF and the right to free speech and expression. This is because the former seeks to limit the exercise of the latter, in the interests of privacy rights. Of course, no right is entirely absolute and an equilibrium must be formulated between these competing rights, in light of the tenets of *"le droit à l'oubli"*[72]

(a) Reasonable Restrictions

Within the European context, privacy rights have been given primacy within some domestic jurisdictions of the member states over the right to freedom of speech and expression. In a Belgian case, "*Olivier G v Le Soir*",[73] the Court of Cassation concluded that Article 8 of the ECHR, from which the RTBF draws itself, overruled the rights to free speech under Article 10, thereby implying that the RTBF would stand

[70] Lipsa Dash & Dr. Gyandendra Kumar Sahu, "Artificial Intelligence in Healthcare Sector: Ethics, Uses and Legalities" 13(2) *CPJ Law Journal* 384 (2023).

[71] *Supra Note* 21, at 06.

[72] Katarzyna Ciuckowska-Leszczewicz, "The Right to Be Forgotten, European Approach to Protection of Personal Data" 4 *University of Warmia and Marzury Law Review* 30 (2012).

[73] N° C.15.0052.F (29 April 2016).

on a higher pedestal than free speech.[74] Conversely, as the American scenario has shown, Courts have usually relied on the Constitutional First Amendment rights to tilt the balance in favour of the rights concerning freedom of expression, as against the RTBF, or any other right for that matter. This was explicitly recognised by the US Supreme Court in "*Schenck v. United States*"[75] when it postulated – "*freedom of speech as enshrined in the First Amendment, as the paramount right that prevails over all others in case of conflict.*" Similarly, in "*Bartnicki v. Vopper*"[76]*,* when weighing the applicability of privacy rights at the expense of free speech, the judiciary opined – *"privacy concerns give way when balanced against the interest in publishing matters of public importance."*

In the Indian context, the right to freedom of speech and expression has explicit protection under Article 19(1)(a) of the Indian Constitution, and its scope has also been increased to include within itself the dissemination of information in "*Secretary, Ministry of Information and Broadcasting, Government of India v. Cricket Association of Bengal*"[77], and freedom of the press with the Apex Court explicitly recognising in "*Printers (Mysore) Limited v. Assistant Tax Officer*"[78], that the freedom of the press, although not overtly represented as a fundamental right, is implicit under Article 19(1). This right to freedom of speech and expression has also been stated to be the most indispensable condition for guaranteeing almost every other freedom.[79] Furthermore, within the domain of the Internet, it has been recognized by the Apex Court in "*Shreya Singhal v. Union of India*"[80] that merely enhancing the degree of circulation, or the increase in impact which the dissemination of any information through such an enhanced mode of circulation can have, shall not be considered a ground for imposing any restriction on the right or justifying its denial.

---

[74] Marko Milosavljević et.al., "In the Name of the Right to Be Forgotten: New Legal and Policy Issues and Practices regarding Unpublishing Requests in Slovenian Online News Media" 8 *Digital Journalism* 05 (2020).

[75] 63 L.Ed. 470 (1918).

[76] 532 U.S. 514, 533 (2001).

[77] AIR 1995 SC 1236.

[78] (1994) 2 SCC 434.

[79] D.D Basu, *Introduction to the Constitution of India* 111 (Lexis Nexis, 2015).

[80] (2015) 5 SCC 1.

However, the scope of this right isn't unlimited, and it is subject to the reasonable limitations envisaged within Article 19(2). Concerning the notion of '*reasonable restrictions',* it has been observed in "*Papasanam Labour Union v. Madurai Coats*"[81] that the restrictions should not be arbitrary or excessive, and there must exist a direct and proximate relationship between the restriction imposed and the objective sought to be achieved. Considering that the RTBF falls within the principles contained within the right to individual privacy, any law enacted to enforce it shall be considered to be valid if it fulfils the test of reasonableness. Moreover, the "*DC Saxena v. UOI*" case is also relevant for this discussion wherein the Court opined - "*If maintenance of democracy is the foundation of free speech, the society is equally entitled to regulate freedom of speech or expression by democratic action. Nobody has a right to denigrate others right of person and reputation."*[82] Care must be taken however to ensure that a domestic jurisprudence that balances free speech that is in the interests of the public in favour of the RTBF since any other position would invariably be detrimental to the democratic setup of the nation. The concept of *'legitimate interests'* must be respected. Interestingly, the "Justice Srikrishna Committee" was also desirous of finding a balance between the two conflicting rights.[83]

(b) The Proportionality Test

The landmark "*Puttaswamy (II) v UOI*" judgment (Aadhar judgment)[84] provides an interesting outlook on how competing fundamental rights can be balanced. The test of *proportionality* was held to be one of the primary tenets, the *'lingua franca'* for judicial systems across the world, for discerning whether a limitation on one right was justified when weighed against another right. The court opined, by citing the Canadian case of "*R. v. Oakes*"[85] that competitive values must be weighed to understand whether the limitation of a particular right is *"reasonable and necessary in a democratic society";* and that it *"should be rooted in a legitimate aim which ensures that the goal is of sufficient importance to warrant overriding a constitutionally*

[81] AIR 1995 SC 2200.
[82] AIR 1996 SC 2481.
[83] *Supra Note* 68, at 85.
[84] (2019) 1 SCC 1.
[85] (1986) 1 SCR 103.

protected right or freedom."[86] The Court also cited the four requisites of proportionality as promulgated in "*Modern Dental College v. Madhya Pradesh*" – (a) there must be a legitimate goal for restricting a right; (b) the restriction must be a suitable means for furthering the legitimate goal; (c) there must not be any equally effective alternative that is also less restrictive; (d) there must be a balance and the restrictions should not have a disproportionate impact on the rights of the right holder.[87] The four axioms of the proportionality test, therefore, are – legitimate goal, suitable means, the presence of less restrictive alternatives, and, disproportionate impact. Comparing with the right to free speech, each of these tenets can be weighed against the RTBF, to examine when the latter can be a reasonable justification of the former.

First, the *legitimate goal* axiom necessitates that any RTBF claim which is silencing the right to free speech be rooted in a constitutionally cognizable interest, such as the protection of privacy, dignity, or from disproportionate reputational harm, thus allowing the RTBF to be invoked only when absolutely necessary, and preventing the suppression of public scrutiny or rewriting history through censorship.

Second, the *suitable means* axiom asks whether delisting or erasure actually furthers the goal to be achieved in the first part. This depends on the nature of the information being *'forgotten'* and the objective being sought to be fulfilled through its erasure. If the information is outdated, misleading, or no longer socially relevant, then its removal may meaningfully protect the individual, however, if the data is related to public functions where questions of accountability or public safety are raised, the RTBF may be compelled to bow against free speech and the dissemination of information.

Third, the *less restrictive means* axiom examines whether it is possible to achieve the same objective in the first axiom. Here, if it is possible to fulfill the objective envisaged through a comparative less restrictive means, such as contextualization, record updation, reduction in search visibility etc., instead of complete removal of information, then that may be the approach undertaken. However, if it is necessary that

[86] Aparna Chandra, "Proportionality in India: A Bridge to Nowhere?" 3 *University of Oxford Human Rights Hub Journal* 75 (2020).

[87] (2016) 7 SCC 353.

the entire information be removed and erased, in the interests of the RTBF, while also resulting in complete censorship of the information, then the right to free speech will have to be restricted.

Fourth, the *disproportionate impact* axiom looks at whether the restriction of a right shall have a disproportionate impact on society by weighing the societal value of the information against the individual's rights. If social relevance is higher, for example the information about someone's criminal past where the individual had engaged in a particularly heinous offence, or if serious allegations are present against a public figure, it might to necessary to ensure the presence of such information, thus restricting the RTBF. On the other hand, if the individual right is more affected than the social consequences of erasure, then the RTBF shall take precedence.

Thus, if proportionality is deemed the litmus test, the RTBF could be determined on a case-by-case basis, with the jurisprudence of the case evolving like what has been adopted by the ECJ. The social relevance of the data should be balanced against the individual right to reputation of an individual. If it is found that the existence of the data yields more value on a democratic and social level, the right to erasure should be curbed in favour of a right to the data's existence. Furthermore, there may be scenarios where even though considerable harm is caused to the reputation of an individual due to the published existence of some data on the internet, the nature of the data or the status or position of that person in society (for example, data about criminal antecedents of a politician) warrants its presence, with the right to information and the free speech rights gaining precedence over the RTBF, and in such scenarios, the proportionality test may give leeway to the former by silencing the latter.

Perhaps the most poignant argument towards a balance can be discerned from the British case of "*AMP v. Persons Unknown*"[88] whose judgment can be surmised to be a precursor to RTBF. The brief facts involve sexually explicit images of a girl retrieved from her stolen phone, which was uploaded as a torrent file on The Pirate Bay, and these were used to blackmail the victim. The victim filed an injunction to prevent the dissemination of this explicit information and also requested that Google remove the links to the torrent file in question

[88] [2011] EWHC 3454 (TCC).

from its search engines. The Court, relying on Article 8 of the ECHR, as well as the British Harassment Act,[89] accepted the plaintiff's request. The *ratio* relied upon by the Court was *"that application of privacy rights do not impact the freedom of expression"* in cases where the probable and possible damage caused to the enjoyment of the private life of an individual vastly outweighs all other considerations.

5. The Right to Be Forgotten: Challenges

The RTBF is in its nascent stages, and therefore, the following legal challenges exist in formulating a strong iteration of the right.

- Firstly, the spatial scope of judgements enacted by domestic courts must be ascertained. The internet does not have spatial limitations and data on the internet is not confined to borders. There is complete decentralisation of the internet and this implies that there cannot be any meaningful regulation of the internet or its contents by any singular legal jurisdiction.[90] Information protected by the right in one legal jurisdiction may be accessible in another legal jurisdiction,[91] and this is even more problematic in countries like America where laws differ from state to state. Virtual Private Networks (VPN) of country-specific URL extensions can also be used to access information rendered inaccessible domestically but available elsewhere. This issue occurred when two German convicts imprisoned for murder in 1990 and released on parole had their information removed from the German-language Wikipedia but the information persisted in the English version.92 The conundrum of non-transboundary application was also accepted by the ECJ in "*Google v. CNIL*".[93] Thus, a proper regime of the right needs not just domestic applicability but transboundary application for it to be properly enforceable. To address this issue, an attempt can be made to ensure the harmonization of standards across the board, through international or regional treaties that are bilateral or multilateral.

[89] Protection from Harassment Act, 1997, s. 3.

[90] *Supra Note* 30*,* at 43.

[91] *Supra Note* 13, at 166.

[92] John Scwartz, "Two German Killers Demanding Anonymity Sue Wikipedia's Parent", *NY Times,* 12 Nov, 2009, *available at:* nytimes.com/2009/11/13/us/13wiki.html (last visited on May 16, 2025).

[93] *Case C-507/17 (2019).*

These can be based on the protectionary regime envisaged by global leaders such as the GDPR, 2016, and can be used to extend the application of domestic RTBF standards to transboundary locations through a common legal framework.

- Secondly, the development of artificial intelligence (hereafter AI) poses a threat. Humans naturally forget information after some time due to natural limitations, and therefore, information delisted by using the RTBF may cease from human memory[94] but AI programs and entities do not have such limitations. One solution is putting automatic expiration dates on sensitive information, following which it is deleted entirely[95] but even that may not be a completely feasible solution since in a regime governed by laws such as the GDPR, the data subject decides when the information is to be purged by invoking the right. Perhaps the best way forward is to inculcate the right's nuances into technology during the developmental stage itself, albeit the nuanced extent to which the right would be applicable needs further analysis from a neutral standpoint.[96]
- Thirdly, the *Streisand Effect* can be a hindrance. The *Streisand Effect* is used to denote a phenomenon when censorship makes the intended information extremely popular, a popularity that would not have manifested without censorship.[97] This implies that censorship through the right could have an inevitable domino effect whereby the censored information increases in popularity. Since information on the internet behaves differently than traditional iterations of information and data,[98] it becomes very difficult to predict how the *Streisand Effect* will impact digital information censored by the right.

---

[94] *Supra Note* 21*,* at 03.

[95] Viktor Mayer-Schönberger*, Delete: The Virtue of Forgetting in the Digital Age* 45 (Princeton University Press, 2011).

[96] Urs Gassern, "Recoding Privacy Law: Reflections on the Future Relationship Among Law, Technology, and Privacy 130 *Harvard Law Review Forum* (2016).

[97] Sue Curry Jansen & Brian Martin, "The Streisand Effect and Censorship Backfire" 9 *International Journal of Communication* 658 (2015).

[98] Angelo Maietta, "The Right to Be Forgotten" 12 *Revista de Estudos Constitucionais Hermenêutica e Teoria do Direito* 221 (2020).

- Fourthly, if the RTBF is confined to the solution envisaged in *Mario Costeja González,* where the information was merely delisted from the internet's search engine database, publishers could exploit technological loopholes to re-publish the data.[99] This makes it important to revisit the drawing board and see whether merely delisting information is enough for the realisation of erasure under the RTBF. Since information uploaded on the internet is difficult to control, as it doesn't behave in the manner traditional information does,[100] estimating the implications of the *Streisand Effect* in this realm becomes very difficult.

6. Conclusion

The modern world is governed by data. American legal scholar Daniel J. Solove has contemplated that humanity is heading towards a world where information will forever persist within the internet, thus forcing humans to live with a detailed record of their lives, which is an impediment to their freedom.[101] *Forbes* echoed this sentiment when it stated, *"Data is the New Oil – And That's A Good Thing"*.[102] Data and the internet are also being extensively used to shape people's personal, social, and political consciousnesses, as the *Cambridge Analytica* incident has highlighted. 103

In light of these observations, data protection and a robust RTBF can be considered the *sine qua non* of the present society. In the Indian context, some of the High Courts have taken appreciable steps in recognizing the right, however, in the absence of a concrete framework, either represented by legislation or promulgated by the Supreme Court, the right will remain a 'paper tiger', subject to whims of the judicial bench before which the matter is placed. The DPDP Act, 2023 shows promise, nonetheless, to be more effective, it needs to envisage the right's ambit by analyzing its development within the

---

[99] *Supra Note* 25*,* at 333.

[100] *Supra Note* 98, at 221.

[101] Daniel J. Solove, *The Future of Reputation: Gossip, Rumour and Privacy on the Internet* 17 (Yale University Press, 2007).

[102] Christoph Stach, "Data is the New Oil - Sort of: A View on Why This Comparision is Misleading and Its Implications for Modern Data Administration" 15 *Future Internet* 71 (2023)

[103] Michael Fuller, "Big Data and the Facebook Scandal: Issues and Responses" 122 *Theology* 14 (2019).

aforementioned European and Argentinian legal systems, and applying it in a manner that is consonant with the Indian constitutional framework, with the foremost challenge in this regard being the balancing of free speech vis-à-vis the RTBF. The Argentinian model, where the right is not merely confined to cases where criminal antecedents are involved but also where the mere existence of the concerned information is a threat against the individual's well-being, including but not confined to an infringement of his reputation or dignity, should be given more primacy since it is broader in its ambit and scope. In a way, this wider understanding has already been utilized by the Karnataka, Orissa and Delhi High Courts in their judgements.

Finally, a comprehensive framework on the right should also have a clear lexicon, coupled with the appropriate taxonomical demarcation between conceptually similar, yet consequentially different terms, including but not limited to collection of data (surveillance, interrogation), processing of information (aggregation, identification) and information dissemination (disclosure, exposure, appropriation intrusion).[104] While a complete taxonomy would exceed the scope of this paper, it is argued that the scope and ambit of the terms used should be defined and elaborated without any ambiguity. For example, while data collection can refer to a passive approach through surveillance practices, and an active approach through interrogative practices, the scope of the term must clearly delineate how and what it sets out to accomplish. A system where this clarity is pursued across the entirety of the law shall have far-reaching consequences in ensuring that the legal provisions are not misused by any authority or entity. It will also allow the adoption of a user-centric approach where individuals retain primary control over data concerning their private lives, where the flexible connotations of the term 'property' also contain within themselves informational property,[105] will both augment and magnify the *"le droit à l'oubli"* being envisaged by the RTBF.

[104] Daniel J. Solove, "A Taxonomy of Privacy" 154 *University of Pennsylvania Law Review* 483 (2006).

[105] Paul M. Schwartz, "Property, Privacy and Personal Data" 117 *Harvard Law Review* 2067 (2004).