



The Legal Dimensions and Challenges of the Right to Be Forgotten: A Critical Review

Bhushita Sharma

Research Scholar, Maharaj Vinayak Global University

Swet Raj Parek

Assistant Professor, Maharaj Vinayak Global University

Abstract

An important ethical and legal notion in the modern digital era is the "Right to be Forgotten" (RTBF), which allows people to have their personal information erased from websites and other online services upon request. This study takes a close look at the history of RTBF, from its roots in European law to its progressive adoption in other jurisdictions like India, and provides a critical analysis of its legal aspects and difficulties. It delves into how RTBF interacts with basic rights including free speech, privacy, and public interest. The study draws attention to competing understandings, problems with execution, questions of jurisdiction, and the need to strike a balance between personal privacy and public openness. This research seeks to offer a detailed knowledge of the scope, limitations, and prospective changes of RTBF within the framework of global digital governance by referencing case laws, legislative frameworks, and academic discussions.

Keywords: Right to be Forgotten, Privacy, Data Protection, Freedom of Expression, Digital Governance

Introduction

In the age of ubiquitous digital connection, personal data may be shared quickly and retained permanently, frequently beyond the control of the individual. This fact led to the Right to be Forgotten (RTBF), a legal right to remove or de-index personal data from search engines, websites, and online databases. The RTBF, based on major CJEU judgments, balances privacy and public access to information. While the General Data Protection Regulation (GDPR) has made it popular in Europe, its adoption and enforcement in other countries, such as India, are still debated on legal, constitutional, and technological grounds. This study analyzes the RTBF's evolution, problems, and ramifications in the context of data privacy and free speech.

In the following paragraphs, we will provide a concise overview of the history of the Right to be Forgotten (RTBF), as well as the current legal definition of this phenomenon. I would also want to comment on the Right to Erasure, which is presently specified in the General Data Protection Regulation (GDPR) that is being proposed for the European Union. Furthermore, in order to clarify how the idea of forgetting, also known as erasing, has been used in actual business situations, we will present two instances of case law. Our primary emphasis is only upon foundational European legislation and case

law owing to the fact that the laws of States differ from one another globally. We are able to establish the conditions that are necessary to transform the Right to be Forgotten into a technical framework with the assistance of the legal analysis outlined in this paper.

Stakeholders & Terminology

An overview of the terminology is utilised to make the legal analysis clear and easy to grasp. GDPR utilises the same wording as "Right to Erasure" (Article 17) since they are in the same language. Article 17(1) of GDPR reads, "The data subject has the right to get the controller to delete personal data about him or her without delay, and the controller has to delete personal data without delay if one of the following conditions applies..." (under certain criteria such consent revocation, unlawful processing, or obsolete data). In Article 4(1) of GDPR, "personal data" means "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." These words establish the legal framework for examining the Right to be Forgotten's scope, restrictions, and enforcement in the Information Age.

A "data subject" is defined as "an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person;" This definition is stated in Article 4 (1) of the General Data Protection Regulation. "Processor" is defined as "a natural or legal person, public authority, agency, or any other body which processes personal data on behalf of the controller," as stated in Article 4 (6) of the GDPR.

"Controller" is defined as "the natural or legal person, public authority, agency, or any other body which alone or jointly with others determines the purposes, conditions, and means of the processing of personal data; where the purposes, conditions, and means of processing are determined by Union law or Member State law, the controller or the specific criteria for his nomination may be designated by Union law or by Member State law;" This definition is stated in Article 4 (5) of the Constitution of the European Union. The term "public domain" refers to any data or information that is available to the general public and may be read by anybody. The World Wide Web (WWW) is often the medium via which one may get access to the information.

Objective

1. Identifying the technical challenges which could be faced in implementing the RTBF in India.
2. Ascertaining the mechanisms to comply with the RTBF, such as effective data deletion and search result removal.

The Right to Be Forgotten

As a component of the legal analysis, a brief description of the history of RTBF as well as the current interpretation thereof is vital to be looked into. The RTBF is not a novel idea; in fact, it already stands inculcated into the existing data protection law, without being specifically designated as such. In point of fact, the RTBF is described in Article 12(b) of the European Data Protection Directive (DPD), which came into effect in 1995, as follows:

The Member State must ensure that individuals have the right to obtain from the controller “the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data” (Directive 95/46/EC, Article 12(b)). In *Google Spain v. AEPD and Mario Costeja González*, the Court of Justice of the European Union (CJEU) established that individuals may request the removal of personal data that is “inadequate, irrelevant, or no longer relevant, or excessive in relation to the purposes of the processing.” Section 2.4.1 analyses the judgment's effects on European data protection law's Right to be Forgotten.

The following statement is categorically stated in the information sheet that provides an explanation of this case about the Right to be Forgotten: "In acknowledging the existence of the right to be forgotten, the Court of Justice established a general principle." It is necessary to revise and elaborate on this idea in order to accommodate the digital era.

The General Data Protection Regulation and Article 17

The future General Data Protection Regulation (GDPR) will include a description of the revised and clarified version of the concept. This regulation will also be the one in which the Right to be Forgotten will be made officially available.

According to Article 17 of the General Data Protection Regulation (GDPR), individuals have the "Right to be forgotten and to erasure." The General Data Protection Regulation (GDPR) is, in fact, a modernisation of a great number of data protection laws that were already in place.

Article 3 of the General Data Protection Regulation (GDPR) states that "non-European companies, when offering services to European consumers, must apply European rules." This provision is likely to make the GDPR more effective than the law that is already in place. In addition, the person is not responsible for proving that the data cannot be destroyed because it is still required or relevant; rather, the firm is the one that fulfils this need. In addition, the data controller is expected to make certain that personal data is deleted by third parties, and the General Data Protection Regulation (GDPR) authorizes data protection authorities to levy penalties of up to two percent of the annual global sales.

Analysis Of Article 17

Article 17 of the General Data Protection Regulation (GDPR) was modified in March 2014, and the title of the article was changed from "Right to be forgotten and to erasure" to "Right to erasure." In accordance with the provisions of Article 17, the individual who is the subject of the data has the right to request that the data controller delete his or her personal information. To put it another way, if the subject makes a request for the data controller to delete their personal information, the controller is

obligated to comply. At this point, we will examine the Right to Erasure in order to determine the grounds on which the data subject is permitted to have its personal data wiped.

Erasure of personal data:

When the subject's data is no longer required for the purpose for which it was collected or processed, the data subject has the ability to request that the data be deleted. It was emphasized that permission from the person whose data is being collected is necessary for the data to be gathered and taken into consideration. Whenever the permission is revoked, the individual whose data is being collected has the right to have their data deleted. In a similar view, the Right to Erasure may be used after the storage time that the person agreed to has come to an end. In addition, the subject has the right to demand the Right to Erasure from the controller for the following grounds: there is no legal basis for processing, the subject objects to the processing, the data has been illegally processed, or the data has been made public without reason. Additionally, it is conceivable for a European Court or regulatory body to rule that data should be wiped, which also implies that the person has the Right to Erasure. This is a potential significant development.

Restriction of processing:

It is stated in paragraph 4 of Article 17 that limited processing of personal data should be implemented rather than the complete deletion of such data. It is not possible to access or process the data in the usual manner, and it is also not possible to make any modifications to the data.

In the event that the subject raises doubts about the correctness of the data, the processing should be restricted. This will give the controller some time to check the accuracy of the data. Furthermore, processing should be limited when the controller no longer requires the data in order to accomplish its work, but at the same time, the data must be retained for the goal of conducting proof. There is also the possibility that the limitation will be implemented in situations where the processing is deemed illegal, but the data subject does not want their data to be deleted. In a manner analogous to the deletion of personal data, processing should be limited if a European Court or regulatory body makes the decision to proceed in this manner. The same is true in situations where the individual in question wants to move their data to a new system or where the storage technology cannot be deleted and was in use prior to the implementation of the GDPR. Furthermore, the controller is not permitted to handle the data in any other way if it is necessary to delete the data.

The limitations of the Right to be Forgotten:

In addition, the General Data Protection Regulation (GDPR) details the restrictions that apply to the Right to be Forgotten. This indicates that the RTBF does not apply in certain aspects because of the significance of the data to the general public. For the goal of complying with a legal requirement, the preservation of the freedom of speech, interests in public health, research for historical/statistical and scientific objectives (Article 17(3)), and situations in which limitation rather than deletion should be the result (Article 17(4)) are some of the topics that fall under this category.

Examples Of Case Law:

Observing Article 17 on its own does not provide sufficient insight into the manner in which the deletion of personal data is pursued from a legal standpoint. The purpose of this part is to examine two different examples in order to obtain a deeper understanding of erasure-

The first example demonstrates that search engines may be used to retrieve private information that is available to the general public. Therefore, it is possible to find material that is not only old but also out of date, which might have a detrimental influence on a person at a later point in their life. As a consequence of showing that search engines are, in fact, data controllers, the data subject is granted the right to request that certain search results be removed from the search engine.

The second case does not go into analysis of RTBF but demonstrates a different approach for the deletion of data in comparison to the Google Case. As an alternative to wiping search results, the material is simply not shown any more, which results in the removal of it for those individuals who had access to it. This may include individuals who are in the public domain.

Google Spain v AEPD and Mario Costeja Gonz'alez:

According to the Data Protection Directive, the interpretation of the Right to be Forgotten (also known as the Right to Erasure) that is now in effect was used in the case of Google Spain vs AEPD and Mario Costeja Gonz'alez. A quick glance at the explanation of the case is as follows- after doing a search on Google using Mr. Gonz'alez's name, the results included articles that discussed the circumstances surrounding the forced sale of property owing to social security arrears. At the tail end of the nineties, the essays were published in the newspaper titled La Vanguardia as well as on the website of the newspaper. Following the resolution of the concerns that were stated in the articles, Mr. Gonz'alez filed a case against both the newspaper and Google Spain in the fiscal year 2010. In the complaint, it was stated that any further reference to the articles was irrelevant since the problems had been remedied. An individual named González made a request to the newspaper to delete the stories, and he also asked that Google remove the links that were related to him and the articles. According to the AEPD, the material that was published in La Vanguardia was published in accordance with the law, and as a result, they dismissed that portion of the complaint.

After some time, the Court of Justice of the European Union (CJEU) came to the conclusion that EU law applies to search engine operators if they have a branch or subsidiary in a Member State. This is the case even if the server that is responsible for processing data is located in a location that is geographically outside of Europe. "Search engines are controllers of personal data," which implies that the laws governing data protection are applicable in this circumstance. Individuals have the right to request that search engines delete links that include personal information from their websites. "where the information is inaccurate, inadequate, irrelevant, or excessive for the purposes of the data processing," applies to the situation in which the right is applicable.

A person does not have an absolute right to be forgotten. In other words, it is necessary for it to "be balanced against other fundamental rights," and each request for deletion must be reviewed on an individual basis. However, in his study of the case, Van Hoboken believes that the Court of Justice of the European Union (CJEU) did not acquire an equally profound knowledge and appreciation of the beneficial and crucial function that search engines play online. The function that is being alluded to is

that search engines make information more accessible to users and create an audience for those who are interested in having information to be available online. In light of this, the removal of links from search engines is an infringement on the right to freedom of speech.

Europe vs. Facebook:

The Right to be Forgotten is not being used in the lawsuit that Europe is bringing against Facebook. Nevertheless, we have chosen to investigate this particular instance because it exemplifies a distinct method of wiping data. This case explains the erasure of data by not showing it to anybody who the data was presented to in the past. This is in contrast to the Google case, which involves the removal of certain search results.

The action was started by Max Schrems, who requested that Facebook supply him with all of the personal information that Facebook possessed on him. This information included information that Schrems believed had been erased from Facebook's database. The decision was made by Mr. Schrems to contact the Irish Data Protection Commissioner in order to lodge complaints against Facebook Ireland. The first 22 complaints were sent in August of 2011, and they addressed a variety of topics, including shadow profiling, facial recognition, excessive processing, and the failure to delete specific data.

Additional complaints were sent in September 2011, and they included a variety of topics, including the deletion of links to photographs, the monitoring of users via the use of the like button, and the frequent modification of policy. The fact that Facebook did not remove data, such as pokes, posts, friends, and chat messages, despite the fact that the user had clicked the "delete" button was one of the most significant problems. The user was made to assume that the data had been deleted when, in reality, Facebook had changed the data to a "not-to-be-displayed" setting rather than destroying it. The links to the photographs were the only ones that were removed; the pictures themselves were not altered in any way. According to the complaint, the photographs that had been removed were still accessible for a number of hours after the user indicated that they had "deleted" them. The Max Schrems team made the decision in July 2014 to drop the first 22 complaints, which brought a stop to the process that had been going on for years and included legal battles. The fact that the Irish District Prosecutor's Office has, for years, failed to make a formal judgement and has not even provided the most fundamental process rights (access to files, evidence, or the counterarguments) was the motivating factor for this decision. In point of fact, the DPC has ceased all means of contact and has disregarded all of the submissions that have been submitted. It was speculated by a number of analysts that this may be due to political and economic factors in Ireland.

Following the withdrawal of the complaints, a class action lawsuit was initiated against Facebook in August of 2014. The purpose of the case was to "make Facebook finally operate lawfully in the area of data protection." On the other hand, the criticisms in this particular instance are less detailed and instead concentrate on the following:

"A data use policy that violates EU law;"

"The lack of valid consent for numerous forms of data use;"

"The NSA's PRISM surveillance program is supported;"

"Internet user tracking on external websites (e.g., via "Like buttons");"

"using 'big data' systems to monitor and analyse users;"

The introduction of "Graph Search"¹⁷ is illegal.

"Unauthorised transfer of user information to third-party apps."

Max Schrems was accused of using Facebook "for commercial promotions of his publications," which led to the court in Vienna dismissing the case on the first of July, 2015. The reason for this decision was procedural in nature. Max Schrems said that he will file an appeal against the judgement that was made by the Court, which in turn advanced the matter to a higher tribunal. From brief appraisal of the situation involving Facebook and Google, observations can be made that are of interest from a technological point of view. The two methods that Facebook demonstrates for erasing data are distinct from the one that Google demonstrates. These methods include not showing data and removing connections to a file, which is an example of a picture.

Initial concept of the legal perspective

A perusal of the material available indicates that an intervention may take place, so that personal data can be wiped or forgotten by using the analysis of the Facebook and Google case. This basic notion is expanded upon in subsequent paragraphs with other concepts, and it is used in the construction of a model that may be utilized.

Model of the initial concept:

Various forms of data is shown in the form of an illustration of the loss of control that the data subject has over their personal data by the arrow on the right, which is labelled "Decreasing amount of control." In proportion to the distance that data travels away from the subject, the individual's ability to exercise control over their personal data decreases. There is no longer any control over personal information if it is available to the general public (that is, if it is in the public domain). It is not difficult to understand why this is the case: if information can be accessed by anyone or anything, then it can be copied, altered, and republished; the data subject supplies volunteered and observed data¹⁹ (top of Figure 1) directly to the public domain; or it can end up in the public domain via any of the other stakeholders, such as the controller, the processor, or a third party. It is also possible for these three stakeholders and the public domain to share personal information with one another. As an example, a data controller has the ability to retrieve information that is available in the public domain, then transfer that information to a processor. The processor then extracts additional or different information from the data before giving it back to the controller.

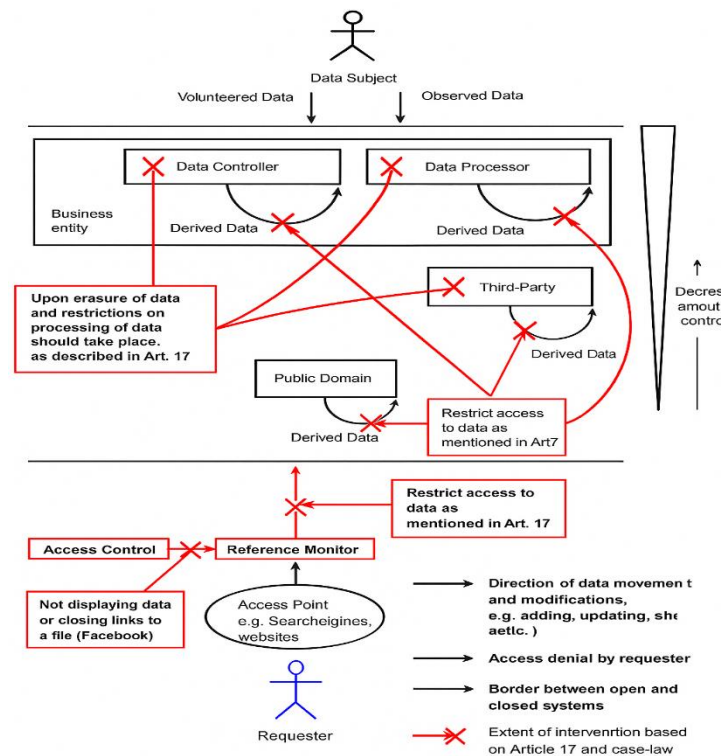


Figure 1: Initial concept with identification of discussed methods to erase or forget personal data

It is also possible for the data controller to process the data inside its own organisation, or to transfer it to a processor or a third party of their choosing. A further function of the data controller and processor is to analyse, aggregate, or mine the data that has been volunteered or seen. As an example, in order to develop a profile of the topic that is suitable for their business model, please refer to the circular arrow in the picture that is labelled "Derived Data." At times the same corporate organisation may serve the roles of controller and processor at the same time. Specifically, the dotted rectangle in Figure 1 illustrates this point. See Figure 1 for a visual representation of the 'Requester' entity, which may be anybody or anything that has access to the public domain or the corporate entity. For instance, a requester may be someone who is using a search engine to browse the World Wide Web, or it could be a search engine that is indexing content from the public domain, or it could be someone who is utilising a social network. For example, a search engine is an example of an object that has information that refers to the location of certain data. This information is known as the access pointer. It is the responsibility of the reference monitor, in conjunction with the access control system, to determine whether or not access to the personal data is permitted.

As a result of the study of Article 17, the observations made herein explain the fact that there is no indication on how to delete personal data. Only if a data subject chooses to exercise its Right to Erasure, which is shown by the red arrows pointing to the controller, processor, and third-party, it can be said that Article 17 has an impact. This is the only circumstance in which we are able to specify where Article 17 has an effect.

The Socio-philosophical Perspective On Forgetting

The observations made in the preceding paragraphs with respect to Article 17 demonstrate that the reasons provide an explanation as to why a data subject has the right to request that a controller delete its personal data; nevertheless, the article does not provide an explanation as to how the correction of personal data should be carried out. When it comes to the process of wiping personal information, the two legal cases discussed hereinabove provide two distinct approaches to the procedure. On the other hand, study of the legal cases indicates that personal information is not destroyed in a clear and unambiguous way; rather, it is simply "forgotten" by being unavailable or by being difficult to discover. This is shown by the fact that the cases were examined. When this is taken into consideration, the question that emerges is: at what point does information or data become forgotten or destroyed completely?

Within the scope of this chapter, the concept of forgetting is deconstructed in order to provide us with a better understanding of the conditions under which data may be considered to have been lost or destroyed. Beginning with discussing the responses that have been adopted against the storing of digital information for an uncertain period of time, as well as the loss of power and control over the data. This will allow us to accomplish what we set out to achieve. Following this, let's first take a quick look at the process by which individuals lose information, and then proceed to delve deeper into depth on the factors that contribute to forgetting.

Responses:

It was claimed that technical advancements have made it feasible for a growing quantity of data to be saved in digital form for an endless length of time. Additionally, the data subject loses power and control over the data as a result of this. In the book that he wrote on the phenomenon of forgetting knowledge in the digital era, Viktor Mayer Schonberger offers six different possible alternatives. Due to the fact that they deal with the flow of data, the first three replies are relational. They operate on the assumption that the sender is the one who chooses whether or not the receiver should use the information and under what circumstances. As a result, there is a connection between the person who sends the personal data and the person who receives it. The latter three responses are more uncertain than the others.

The concept of forgetting:

To acquire a deeper comprehension of the topic of forgetting, we will quickly investigate the manner in which the human brain forgets knowledge and the methods used to assist us in remembering. Within the human brain, forgetting occurs. "Forgetting" is defined by Korenhof et al. as "a "fail[ure] to recall," a glitch somewhere in the memory process that either temporarily or permanently fails to retrieve specific information." This definition comes from a research that investigates the role that time plays in determining whether or not material should be maintained or forgotten.

When it comes to the human brain, there are three types of elements that contribute to the process of forgetting something: "the passage of time": new information is more likely to be retained in memory than older information; "the meaning of the information": information that is meaningful is more likely to be retained than information that is meaningless; "the regularity with which the information is used": information that is used frequently is more likely to be retained than information that is used infrequently.

Forgetting in an external transactive memory

An external transactive memory is a kind of external digital memory that allows anybody linked to it to contribute or retrieve data. This is something that we have established. In this part of the article, the process by which personal information might be lost from a transactive memory is being analysed. In order to do this, the idea of the transactive memory is converted into a technological model. System that is both open and closed For the purpose of making an initial difference between systems that entail a transactive memory, a paper that was compiled by ENISA was analyzed which discusses the technological methods that enable or enforce the Right to be Forgotten in information systems.

An open system and a closed system are broken down into their respective categories in the ENISA study. In a system that is open, it is possible for anybody to copy personal data, and there are no mechanisms in place to facilitate the monitoring of these copies. In an open system, it is not possible to enforce the Right to be Forgotten through the use of technical means, according to the report. This is due to the following reasons: in such an open system, it is not generally possible for a person to locate all personal data items (exact or derived) stored about them; it is difficult to determine whether a person has the right to request removal of a particular data item; moreover, no single person or entity has the authority or jurisdiction to effect the deletion of all copies.

Model of forgetting in an external transactive memory

In the next section, the idea that forgetting in a transactive memory is not distributed evenly across the parties involved is being discussed. This is due to the fact that a particular person or group is not granted access to the data. By using domains, which will be explained in more detail below, disparity was identified as depicted in Figure 2. Data that is considered to be personal is stored on a storage media, which is a component of a system. Personal data is protected by the system domain, which is the initial layer surrounding it and has access to it. This domain may include numerous systems belonging to the same organisation. Considering that the systems that are responsible for storing and processing personal data are a component of an organisation, the organisation itself is the second tier of access to the data. When it comes to the dividing line, organisations that operate in the (semi-)public domain are considered to be on the "Open system" side. There are organisations that do not function in the public domain that are considered to be part of the "closed system." In order to differentiate between companies that provide a service to the general public but need some kind of membership in order to utilise that service, it is required to divide the memory domain into two categories: semi-transactive and transactive. One example would be a free email service such as Gmail or a social networking site such as Facebook.

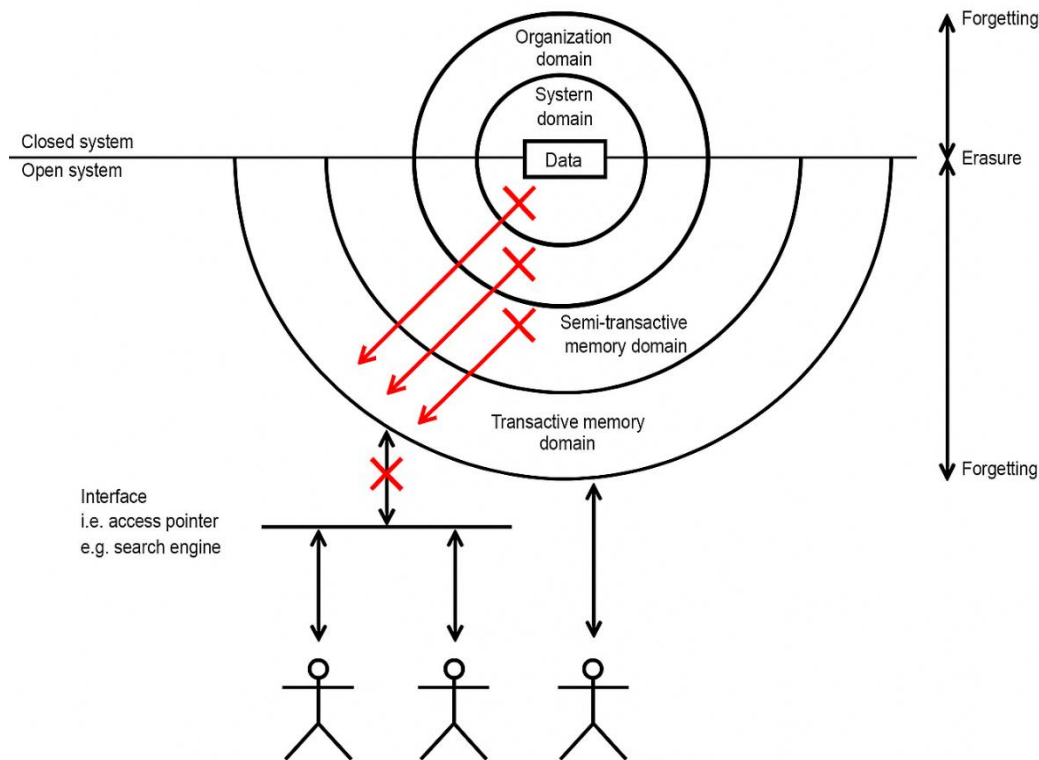


Figure 2: Effect of forgetting or erasing in a transactive memory across different domains.

The only people who are affected by a method that has an effect on the interface (also known as an access pointer), such as removing certain search results, are arbitrary requesters or requesters who have a limited awareness of the availability of specific data. Personal information may be accessed by arbitrary requesters in a random manner, for example, by means of an arbitrary search query. The person who made the request is only vaguely aware of the existence of the data since it was brought to its attention via a process.

Marginally, it is arbitrary. Interface may be aware of and avoid using a different channel, but it is necessary to utilise an interface in order to obtain access once again. As an example, think about the situation in which someone forgets a connection to a certain website and then utilizes a search engine to locate it again.

Difference between forgetting and erasing data

Greater the proximity of a way of forgetting the actual storage site of the data, greater the number of domains that would be impacted by the approach. Given the circumstances, we are of the opinion that the approach in question genuinely deletes data. Methods that are implemented on a domain that is farther away from the data really do not delete the data from a system; rather, they only prevent some individuals from accessing the data.

Factors that contribute to forgetting

The act of forgetting, or failing to recall anything, happens passively and naturally; humans can never forget something intentionally. The Internet and other forms of external transactive memory, on the other hand, remember information by default and do not passively remove or erase it. Data is only removed from this type of transactive memory when explicitly told to do so. There are a lot of factors that could be examined while trying to decide if it's essential to delete personal data from a transactive memory. Next, we'll take a look at these problems and see if we can put them in context with technological factors.

Conclusion

As the landscape of privacy rights and digital governance continues to evolve, the Right to be Forgotten is a significant development that signals a key milestone. This paper highlights the critical need to find a way to harmonize the opposing ideals of openness, freedom of expression, and public interest with the sovereignty of individuals over their own personal data. In spite of the fact that the idea has garnered a considerable amount of legitimacy within European legal frameworks, its interpretation and implementation in other countries, such as India, continue to be confronted with constitutional, procedural, and technical obstacles. For the aim of ensuring that the Right to Be Forgotten accomplishes its intended purpose without damaging democratic ideals, it is vital to have a solid legal framework, along with clear rules for striking a balance between conflicting rights and privacy. With the expansion of the digital domain and the rising permanence of information, the Right to Be Forgotten will continue to be an instrument that is both essential and contentious in terms of molding the future of data protection and individual dignity.

References

1. De Hert, P. (2015). The right to protection of personal data: Incapable of autonomous standing in the basic EU constituting documents? *Utrecht Journal of International and European Law*, 31(80), 1–4. <https://doi.org/10.5334/ujiel.cz>
2. Erdos, D. (2021). The ‘right to be forgotten’ beyond the EU: An analysis of wider G20 regulatory action and potential next steps. *Journal of Media Law*, 13(1), 1–35. <https://doi.org/10.1080/17577632.2021.1896821>
3. Gesenhues, A. (2014). The inevitable happened: First company provides “Right to Be Forgotten” removal service. *Search Engine Land*. <https://searchengineland.com/reputation-vip-online-management-firm-launches-site-assist-googles-forget-form-194998>
4. Globocnik, J. (2020). The right to be forgotten is taking shape: CJEU judgments in *GC and Others (C-136/17)* and *Google v CNIL (C-507/17)*. *GRUR International – Journal of European and International IP Law*, 69(4), 380–388. <https://doi.org/10.1093/grurint/ikaa041>
5. Hoffman, D. (2016). Creating an internet obscurity center: Reducing the burden of Google Spain on businesses. *Lawfare*. <https://www.lawfareblog.com/creating-internet-obscurity-center-reducing-burden-google-spain-businesses>

6. Kulk, S., & Zuiderveen Borgesius, F. (2018). Privacy, freedom of expression, and the right to be forgotten in Europe. In E. Selinger, J. Polonetsky, & O. Tene (Eds.), *The Cambridge handbook of consumer privacy* (pp. 301–318). Cambridge University Press. <https://doi.org/10.1017/9781316831960.019>
7. Lee, D. (2014, May 14). Google ruling ‘astonishing’, says Wikipedia founder Wales. BBC News. <https://www.bbc.com/news/technology-27407017>
8. Lee, E. (2015). The right to be forgotten v. free speech. *I/S: A Journal of Law and Policy for the Information Society*, 12(1), 85–111. https://kb.osu.edu/bitstream/handle/1811/80043/ISJLP_V12N1_085.pdf
9. Marks, D. (2016). The internet doesn’t forget: Redefining privacy through an American right to be forgotten. *UCLA Entertainment Law Review*, 23, 41–64. <https://escholarship.org/uc/item/4n00j4j3>
10. Mayes, T. (2011, March 18). We have no right to be forgotten online. *The Guardian*. <https://www.theguardian.com/commentisfree/libertycentral/2011/mar/18/forgotten-online-european-union-law-internet>
11. McGoldrick, D. (2013). Developments in the right to be forgotten. *Human Rights Law Review*, 13(4), 761–776. <https://doi.org/10.1093/hrlr/ngt035>
12. Milosavljević, M., Poler, M., & Čeferin, R. (2020). In the name of the right to be forgotten: New legal and policy issues and practices regarding unpublishing requests in Slovenian online news media. *Digital Journalism*, 8(6), 780–796. <https://doi.org/10.1080/21670811.2020.1747942>