

Analyzing the Right to be Forgotten in the Information Age

Bhushita Sharma

Research Scholar, Maharaj Vinayak Global University

Swet Raj Parek

Assistant Professor, Maharaj Vinayak Global University

Abstract

The exponential expansion of digital technology and the durability of online data have changed 21st-century privacy rhetoric. With the "Right to be Forgotten" (RTBF) as a key legal and ethical idea, individuals can seek the removal of their personal data from digital sites. This study examines the legal, ethical, and technological implications of the RTBF as a vital aspect of digital privacy in the Information Age. The paper investigates how the RTBF affects freedom of speech, public interest, and digital memory using worldwide case studies, including the EU's General Data Protection Regulation (GDPR) and Indian discussions. The examination contrasts individual autonomy with collective rights and examines how technology corporations and regulatory institutions operationalise this right. In an age of unparalleled information flow, the RTBF provides both a potential and a problem for privacy protection, requiring a delicate balance between digital erasure and cultural memory.

Keywords: Right to Be Forgotten, Digital Era , Internet, General Data Protection Regulation

INTRODUCTION

One of the most important aspects of data protection and privacy rights in the digital era is the right to be forgotten, which has become more important. In this day and age, where people's personal information is regularly gathered, saved, and distributed across a variety of digital platforms, there is a growing trend among individuals to want control over their identities pertaining to the internet. Individuals have the ability to request the removal of personal data that is no longer relevant, outdated, or inaccurate from search engines and other digital repositories. This right to be forgotten was formally recognised by the European Court of Justice in the landmark case *Google Spain SL v. Agencia Española de Protección de Datos* (2014) when it was formally recognised. Specifically, this right is referred to as the "right to erasure" in Article 17 of the General Data Protection Regulation (GDPR), which is where it is codified. When specific conditions are met, such as when the data is no longer required for the purposes for which it was obtained, when permission is withdrawn, or when the data has been improperly handled, it gives individuals the right to demand that their personal information be deleted.

The implementation of the right to be forgotten in a digital context, on the other hand, is fraught with difficulties on the regulatory, ethical, and technological fronts. Keeping this right in check with other rights, such as the right to freedom of speech and the right to access information, is one of the most important concerns. Journalists, historians, and scholars may argue that such material has public value,

despite the fact that people may prefer to delete all evidence of their history. The responsibility of mediating between the individual's right to privacy and the public's right to know is often demanded of the courts and regulatory agencies. This is a task that becomes increasingly difficult to do in situations that get a lot of public attention. In addition, search engines such as Google play a gatekeeping function in the processing of these queries, which raises worries about the availability of private firms with the authority to decide what material is available online.

The worldwide application of the right to be forgotten does, however, offer obstacles owing to the fact that different legal frameworks and cultural norms about privacy exist in different countries. While the European Union has comprehensive data privacy regulations that support this right, other countries, such as the United States, place a higher priority on free expression and may not recognise the right to be forgotten to the same degree. Multinational corporations have challenges as a result of this legal difference since they are required to traverse a complicated web of compliance responsibilities that vary depending on the area. Furthermore, the technological limits of data erasure, which include the persistence of data backups, data mirroring, or the re-posting of information that has been deleted by third parties, make complete implementation almost difficult. The footprint of material that has been put on the internet is often widespread and difficult to eradicate entirely after it has been uploaded.

The Right to Be Forgotten

It is quite probable that the Right to be Forgotten will continue to be one of the most talked about, contentious, and significant data protection and privacy legislation of the decade, and it is also likely to continue to be so in the years to come. In addition to being an extension to Article 12 (b) and Article 14 (a) of the European Data Protection Directive 95/46 (Shankar, 2014:229; Calder, 2016:12-13; DPD 95/46), it is founded on the Right to Data Protection, which is a fundamental right that is enshrined in the EU Charta of Fundamental Rights. Its legal and theoretical foundations serve as the basis for contemporary privacy laws in Europe. Individuals are able to "determine the development of their life in an autonomous way, without being perpetually or periodically stigmatised as a consequence of a specific action performed in the past" (Nohe, 2018). This concept is founded on the premise that individuals have the capacity to make their own decisions about the course of their lives. In recent years, individuals who are the subject of data have gained the ability to demand that any data controller or processor delete any information that they have stored about them. In the event that permission is revoked, this must be carried out quickly. According to Nohe (2018) and Calder (2016):42, organisations will not be able to provide a comprehensive list of potential grounds for rejection, which is why they will be obliged to have their data shown in a clear and concise manner. According to Calder's argument, anyone who is familiar with the internet will assume that this will be extremely difficult to accomplish. However, the authorities in charge of data protection will want to ensure that all of the necessary steps have been taken and that all of the procedural measures have been implemented in order to delete any and all data that could potentially be accessible to the public, such as newspaper articles and databases (2016:42). This is another reason why the title of the book, "The Right to be Forgotten," is somewhat contentious, given that the concept of "forgetting" in this day and age is extremely difficult to achieve. Furthermore, the exception that organisations might use to deny such a demand is the Right to Freedom of Expression and the Right to

Know, which, together with the Right to Privacy, form the basic rights of a person. In other words, these rights fall within the category of fundamental rights.

Data Protection in Europe until May, 2018

The Council of Europe created legislative norms in 1981 with the purpose of facilitating the free flow of information among all member states of the European Union (EU) without compromising individuals' right to privacy. In 1984, the United Kingdom passed a law called the Data Protection Act. In Germany, the Federal Data Protection Act was the law that controlled data protection. In France, the Loi Informatique et libertés (LIL) was passed in 1978. The law that was concerned with data protection, on the other hand, was too diverse across the member states for a firm to be able to comply with the regulations in all of the countries in which it operates, and not only in its home country (Calder, 2016:14-16).

On October 24, 1995, the European Parliament and Council passed Directive 95/46, which was titled "on the protection of individuals with regard to the processing of personal data and on the free movement of such data" (UNESCO, 200:123). Since that time, this directive has served as the cornerstone of data privacy in Europe. Due to the nature of the Directive, EU countries were facing a "legal minefield" of different interpretations when applying it to national law, which led to fragmentation within the Union and the perception that there were significant risks to the protection of natural persons (Tankard, 2016:5; Article 1 (9)). Furthermore, under Directive 95/46, the amount of penalties was quite little (The Economist, 2018). This reality, in conjunction with the continuously changing data-driven world, necessitates the establishment of a new data security framework that is more suitable.

The General Data Protection Regulation (GDPR)

While a Directive lays out minimum conditions, it allows for interpretation and application to the national laws of individual EU member states in order to accomplish a predetermined objective. On the other hand, a regulation is a legally binding act that must be implemented in its entirety by all member states (EU GDPR Portal: eugdpr.org, Calder, 2016:17). Although it takes longer to be adopted because of the weight of its legal implications, it also guarantees a higher degree of uniformity (Calder, 2016: 36). According to Sobolewski et al. (2017):208, the General Data Protection Regulation (GDPR) will ultimately enter into effect on May 25, 2018, with all of its 99 provisions and for all 28 member states simultaneously and from the very beginning. A final version was released in July 2016, after a two-year waiting period for organisations and enterprises to complete compliance requirements (Tankard, 2016:6). The agreement was reached in December 2015, and the final version was released in July 2016. The fundamental idea that privacy and the protection of personal data are essential human rights is the foundation upon which the General Data Protection Regulation (GDPR) is built. This fundamental view is now protected by the Charter of Fundamental Rights as a right of an individual (Sobolewski et al., 2017:208). Providing the people with a number of rights that allow them control and authority over their own data is the primary objective of this initiative, which aims to unify data protection law across all nations that are members of the European Union. The Right to be Forgotten (according to Article 17 of the General Data Protection Regulation) is one of them, and it is also the most contentious of all of them.

Objectives

1. Examining the legal foundations of RTBF, focusing on landmark court cases such as Google Spain v. AEPD and the GDPR's provisions including relevant laws, regulations, and court decisions.
2. Evaluating the interpretation and application of RTBF by courts and regulatory bodies worldwide.

Research Method

This qualitative study examines the difficulties and implications of the "Right to Be Forgotten" (RTBF) under the GDPR. To analyse primary and secondary legal sources, including EU legislation, case laws, official guidelines, and scholarly commentary, a doctrinal legal research technique is used. The paper critically examines the RTBF's evolution, implementation across jurisdictions, and issues in balancing privacy rights with free speech and public interest. Comparative analysis also helps understand how other data protection regimes, like the US and India, handle privacy issues. Instead of fieldwork, thorough literature evaluation and legal document analysis collect data. The study seeks to illuminate the legal and ethical aspects of the RTBF in the digital age.

Data Analytical Framework

In this particular study, the interpretation of legal texts, judicial decisions, and scholarly publications that are associated with the "Right to Be Forgotten" under the General Data Protection Regulation (GDPR) is the primary emphasis of the data analysis that is mostly based on qualitative approaches. As part of the analysis, we will investigate the ways in which this right has been implemented in a variety of legal settings and assess the influence that it has had on the rights of persons with regard to their privacy, freedom of expression, and digital rights. The content analysis of historic court opinions and regulatory recommendations allows for the identification of key themes and patterns. It is possible to gain a thorough grasp of how the Right to Be Forgotten (RTBF) is being managed in the digital era by using this approach, which highlights both the legal foundation and the practical ramifications of the policy.

Analytical Framework for Studying the Right to Be Forgotten

“If the product is free, you’re the product.”

One of the objectives of this chapter is to offer a simple response to the first and second research questions. Based on a textual analysis of the blog entries, the first research question is to determine the primary concerns that are at stake in relation to the Right to be forgotten. The second research question is to investigate the ways in which the Right to be forgotten contributes to the (re-)shaping of the discourse around data protection and privacy in the future, taking into consideration the perspectives that were stated in the postings. In order to improve the reader's comprehension of the situation, a concise examination of the identities of the writers about their respective responsibilities is presented before the event.

By revealing what was previously concealed, critical discourse analysis enables us to acquire a thorough knowledge of an issue by providing us with a bird's eye perspective of the situation. The first research question is associated with the textual and discursive aspects, and it attempts to identify linguistic features

in the texts that convey the authors' beliefs and attitudes towards the Right to be forgotten. This research question is based on Norman Fairclough's CDA framework (2003). The second research topic is situated within the realm of societal analysis, and its primary emphasis is on providing explanations for the results within the context of a more general social setting.

It is essential to recognise the many players in order to have an understanding of the environment in which the writers' arguments emerge. Individuals, organisations, and legislative institutions are the three categories of actor groups that are being discussed here. In principle, there are three types of actor groups. Individuals are the data subjects that the General Data Protection Regulation (GDPR) applies to, empowers, and protects. More precisely, the Right to be forgotten applies to individuals. Data controllers and processors are organisations, such as Google or Facebook, who primarily operate their operations by processing personal data. Examples of such organisations are Facebook and Google. Not only companies who are heavily involved in internet marketing, but also organisations that are not-for-profit or public, as well as enterprises that are controlled by the state, are required to acknowledge the fact that they collect personal data. On the other hand, the processing may pose a greater or lesser threat to the individual's privacy, depending on the nature of each. Hospitals, for example, collect enormous quantities of data via patient records, which are not utilised for the purpose of earning a profit but rather for the sake of research, the advancement of medical treatment, and therapy. Despite the fact that these sorts of organisations will still be required to become more transparent and comply with GDPR, they are under a great deal less pressure than platforms such as Facebook and Google, which are only available online. Considering that these two corporations are the most dominating data controllers and processors in the world, it is interesting to see that practically all blog postings make reference to them respectively. Legislative actors are responsible for formulating policies and are specialists in the legal field who possess legislative knowledge and competence.

RTBF - Unidentifiable threat or silver lining? – A textual analysis

Posts on blogs, in contrast to articles published in newspapers or academic journals, often permit a far more expansive use of language. A particular attitude or viewpoint may be communicated via the use of a variety of language features, including colloquialisms, slang, and other varieties. According to the statistics, the majority of the articles that were chosen make use of such elements; nevertheless, some of the posts are written in language that is quite straightforward and impartial. In the next section, we will provide an overview of the topics that are at stake, as discussed by the writers, as well as how these concerns are represented in the texts.

An interesting observation is that two writers utilise metaphors and analogies that are rather powerful to explain the Right to be forgotten, and these metaphors and analogies exhibit a negative connotation. In the field of information technology security, Ellen Tannam anticipates a "deluge of requests" that businesses and organisations will have to deal with. In most cases, a "deluge" is something that one drowns in if they are not fast enough or do not have the means necessary to protect oneself from it. As an example, Christopher Knight, a lawyer, cited the story of The Lion King from Disney. He predicted that there would be a "approaching dust-cloud of a migrating horde of right to be forgotten litigating wildebeest," which would cause "like Mufasa, you be crushed underneath an unexpected flurry of developments." When compared to the other texts, this is the most imaginative language element, and it

demonstrates very clearly how Knight thinks about the future changes in legislation. In the same manner as Tannam does, he likewise anticipates a "unknown something" that seems to be rather menacing and that, both in terms of its appearance and its repercussions, is quite unexpected from his vantage point, which is located at a safe distance away.

The social perspective

The regulation establishes more stringent restrictions and broadens the concept of personal data, geographical reach, and the definitions of data controllers and processors. Additionally, the legislation has become more comprehensive. On the other hand, the writers have brought out a number of problems that are not just relevant to the European Union but also universally applicable to the whole globe. This chapter combines the discursive practice with the social practice in relation to Fairclough's three-step model for discourse analysis. The social practice incorporates the discursive practice.

One of the most common concerns that can be seen throughout the data is the issue of maintaining equilibrium. The argument that the Right to be forgotten presents a substantial danger to the Right to Freedom of Expression and Information is one that is particularly valuable to the conversation and is particularly contributed to by legal professionals and authors. On the other hand, it is essential to take into account the fact that, as stated by the authors, the right to privacy is also recognised to be a basic human right. At the same time, it is necessary to strike a balance between the two rights in order to guarantee both of them simultaneously. This is the issue that has to be solved. When it comes to the 'economic' and 'security' logic that is mentioned in the theoretical framework, it is necessary to find a balance between safety and liberty. What is more important: the privacy and safety of the person, or the liberty of the individual, and by extension, the liberty of the free market? This is the issue that underpins the arguments that the writers provide. Because it is possible to argue that the liberty of the free market is just as vital, or perhaps more so, than the liberty of a person, yet both are essential for democracy, it is crucial to take a critical stance with regard to this duality. The solution to this issue cannot be given in and of itself since it is a question that will need to be addressed to each particular instance of the Right to be forgotten. Nevertheless, this question is a crucial component of the larger discussion over the Right to be forgotten.

The Technological Perspective of the Right to Be Forgotten

From the point of view of the law, we spoke about two examples that each demonstrated different ways in which confidential information might be forgotten. It should be emphasized, however, that these procedures do not delete data in a direct manner. A deeper investigation into what forgetting truly means, what variables lead to forgetting, and the fact that the location where forgetting takes place has a varied influence on various domains was conducted by the socio-philosophical viewpoint, as was previously mentioned.

we consider forgetting data to be the failure of a particular requester to access data at the time when the requester desires access to the data. This idea is refined for the technological viewpoint in this chapter, and we illustrate the areas in which accessing data might be impeded, to the point where it can be regarded forgotten or wiped.

Model of forgetting by denying access

In our explanation, we said that personal data may be accessed from a variety of domains, and thus forgetting might be considered a failure to obtain that personal data. It is necessary for us to provide a technical description of the process by which data is accessed and information is collected in order to successfully execute forgetting. Figure 3 illustrates this, for your perusal. The image illustrates the process by which a requester might get access to data, as well as the scenarios in which that requester's access can be restricted (which will be discussed in more detail later on in this chapter).

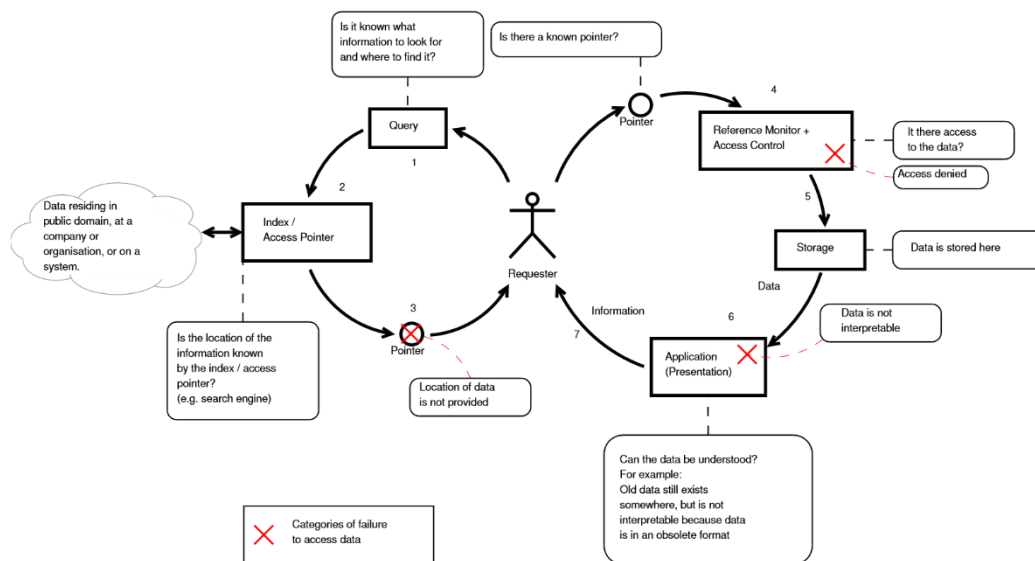


Figure 1: Forgetting or erasing personal data by denying access

The person who is making the request in the centre of Figure 3 has two choices: either it is interested in learning anything or it is already aware of where particular information may be found. If there is anything that the person making the request wants to know, then they need to be aware of what information they should seek for and where there is a likelihood that they may discover it. Take, for instance, the process of formulating a search query and using a search engine in order to locate the information. In response to the query (1) that is directed towards the index (2), a pointer will be generated that will give the location of the real data (3). In the event that the index does not know the answer to the query or if it is not permitted to deliver a particular result, it is not feasible to provide a reference.

Applicability of the model regarding a requester

This paradigm, which is seen in Figure 3, may be used in a variety of domains, depending on the domain in which the person making the request lives. For instance, the person making the request may be:

- an organisation that seeks information from sources other than itself;
- an organisation that seeks information from within itself;
- a system that receives an assignment to retrieve data from sources other than itself;

- a system that receives an assignment (for example, from software) to retrieve data from within itself;
- an individual seeking specific information.

In each and every one of the areas, the model might be used. For the sake of elucidation, we will provide an example: in order for a system to get information from inside itself, it must be aware of a pointer to the file that contains the data that is being sought. In the event that the data is corrupted or destroyed, the program will be unable to understand the data. As a consequence, the application will be unable to properly access the data, which will result in the information being lost.

Other network related storage methods

In the following part, we will provide a concise explanation of storage mechanisms that do not fall within the categories of encryption or DHTs that were discussed before.

EphPub

The ideas (such as Vanish) that depend on DHTs to store and remove keys or data are connected to Ephemeral Publishing (EphPub), which provides a similar service. EphPub, on the other hand, makes use of the DNS caching mechanism in order to store and revoke the encryption keys. This allows for the difficulties that are caused by a Sybil attack on a DHT to be overcome. Using the Sybil attack against Vanish, for instance, it is possible to recover keys for 99% of the messages sent by Vanish. This is accomplished by traversing the DHT and preserving each stored value before it fails. More information on the Sybil attack against Vanish may be found by referring to [1]. A DNS resolver caches the result to a recursive DNS query in order to service additional requests. This cached response is stored for a period of time, which is referred to as a Time To Live (TTL) value. EphPub depends on this aspect of DNS which allows it to function properly. After the time out period (TTL) has passed, the record is deleted. EphPub uses a key k to encrypt a message, much as it used to do with earlier notions. The key is not stored on a keyserver; rather, it is dispersed to distinct DNS cache resolvers, bit by bit, rather than being stored on a keyserver. Following the expiration of the DNS cache in accordance with the TTL, the encryption cannot be retrieved, which means that the data is lost. The operation is as follows:

A list of random DNS cache resolvers and a list of random valid domain names with a time-to-live (TTL) that is as near as possible to the storage duration are both generated by sender S . After then, sender S sends a non-recursive DNS request in order to conduct a random test to determine whether or not the various domains are already stored in the cache of a resolver. If the domains are already stored in the cache, they are deleted from the list accordingly.

Parasitic Data Storage

When it comes to storing data, there is an entirely different technique that comes in the shape of parasitic data storage. The fact that this method of storing data does not depend on storage media makes it more susceptible to data loss than any of the other solutions that were previously considered. It is true that it saves data by transmitting it between a server and a reflector node using Internet Control Message Protocol

(ICMP) packets. This process is repeated over and over again. Simply dropping the packets is all that is required on the server side when data has to be deleted.

On the other hand, in the event that there is a disturbance with the connection, the data that has been saved will also be lost. Because of this, Parasitic Data Storage (PDS) is more susceptible to unauthorised access than encrypted data in case the key is lost. If you have the latter, there is a possibility that you can still try to brute-force the key, but if you have PDS, the data is unquestionably gone.

Table Based on the implementations, or concepts described above, we can create the following table:

Methods	Changing permissions			P				
	Editing credentials			P				
	Modifying search results							
	Removal of pointers			X				X
	Moving data				X			
	Destruction of storage medium						X	
	Data is damaged				P		P	
	Data is transformed	X	X		X	X		X
Factors	Time	X	X	X		X	X	
	Meaning							
	Regularity			P	X			
	Space				X			
		Ephemerizer	Vanish	Comet	Freenet	EphPub	Volleystore	FoSgen
		Cryptography	DHT			Other network storage		Overwriting

Implementation / concepts

Each of the approaches and components that are used by the notion is denoted by the letter X. The letter P is used to identify which of the several approaches and aspects that the notion may potentially apply or consider. Comet, Freenet, and Volleystore are three ideas that are shown in the table. Each of these concepts utilises unique approaches to erase data from a system. In the next two chapters, we will focus on two of these ideas and provide a more in-depth explanation of each of them.

We go into more detail about Freenet. However, Freenet asserts that it is able to wipe data, in contrast to Vanish, which just deletes keys. When determining whether or not data should be destroyed, it additionally takes into account two factors—regularity and space—that are not taken into consideration by other ideas. describes the operation of the Volleystore. We have decided to go with this idea since it is the only one that deletes its storage media in an active manner. The ICMP packet that saves a portion of the data is actually dropped by it, and it does not depend on any physical storage device. We do not

include Comet since it is dependent only on the issue of time and does not adequately describe the process by which data is really erased.

Conclusion

Initially, this thesis provides an overview of the theoretical foundations of privacy, the existing state of affairs, and the forthcoming changes in Europe. Additionally, it provides a concise assessment of the changes that the new rule might potentially bring about. Norman Fairclough's three-dimensional model of discourse analysis serves as the foundation for the theoretical framework, which is a need for the CDA. Both the analysis and the results were analysed and interpreted via a critical lens. Following the establishment of the theoretical premises, the analysis was based on a selection of sixteen distinct blog entries on the Right to be forgotten. The purpose of the study was to discover discursive and sociological consequences, as well as to get a knowledge of the online discourse on privacy and data protection.

References

1. Fabbri, Federico & Celeste, Edoardo. (2020). The Right to Be Forgotten in the Digital Age: The Challenges of Data Protection Beyond Borders. *German Law Journal*. 21. 55-65. 10.1017/glj.2020.14.
2. Singh, Raminder. (2025). Right to be Forgotten: Navigating the Right to Privacy and Regulations in Digital India. *Communications on Applied Nonlinear Analysis*. 879-890. 10.52783/cana.v32.5114.
3. Bag, Akash & Khattri, Upasana & Agrawal, Aditya & Roy, Souvik. (2024). Navigating the Digital Dilemma: The Right to Be Forgotten, Privacy, and Freedom of Speech in the Age of GDPR. 10.4018/979-8-3693-0472-3.ch007.
4. Khan, Asma & Mushtaq, Shahzada & Siddique, Muhammad & Wadood, Muhammad. (2025). The Right to be forgotten in the Digital Age: A Pakistani Perspective on Balancing Data Protection & Privacy, Freedom of Expression, and Cyber Security. *Journal for Social Science Archives*. 3. 387-403. 10.59075/jssa.v3i1.126.
5. Allegri, Maria. (2022). The Right to be Forgotten in the Digital Age. 10.1007/978-3-031-11756-5_15.
6. Newman, Abraham. (2015). What the "right to be forgotten" means for privacy in a digital age. *Science (New York, N.Y.)*. 347. 507-8. 10.1126/science.aaa4603.
7. Mbah, Geraldine. (2022). Data Privacy and the Right to be Forgotten. *World Journal of Advanced Research and Reviews*. 16. 1216-1232. 10.30574/wjarr.2022.16.2.1079.
8. Upadhyay, Parth & Verma, Rajesh. (2024). THE RIGHT TO BE FORGOTTEN IN INDIA: COMPATIBILITY WITH PART-III OF THE CONSTITUTION. *ShodhKosh: Journal of Visual and Performing Arts*. 5. 10.29121/shodhkosh.v5.i6.2024.5014.

9. (2023). Right to Be Forgotten: Navigating Online Privacy and Public Interest.
10. Thilakarathna, K A A N. (2025). Identity privacy and the right to be forgotten.
11. Xue, Minhui & Magno, Gabriel & L. T. P. Cunha, Evandro & Almeida, Virgilio & Ross, Keith. (2016). The Right to be Forgotten in the Media: A Data-Driven Study. Proceedings on Privacy Enhancing Technologies. 2016. 10.1515/popets-2016-0046.
12. Atata, Bashirat. (2024). Artificial Intelligence and the Right to be Forgotten. International Journal of Research Publication and Reviews. 5. 4300-4310. 10.55248/gengpi.5.0824.2310.
13. Guadamuz, Andrés. (2017). Developing a Right to be Forgotten. 10.1007/978-3-319-64955-9_3.