The Right to be Forgotten in Digital Media: A Study within the Framework of the European Union and Algerian Law

Received: 21/04/2025; **Accepted:** 01/06/2025

Dr. Hadja OUAFI*

Lecturer A
Laboratory of land and Environment law, Faculty of Law and Political Science, University of Mostaganem, Algeria
hadja.ouafi@univ-mosta.dz

Abstract

The right to privacy is a fundamental human right, protected by international and national legislation. It safeguards an individual's personal space, secrets, and identity from intrusion. However, technological advancements, especially in artificial intelligence, have eroded this private sphere. As society shifts toward a predominantly digital environment, the excessive exchange of personal data emphasizes the need for digital privacy rights. This includes the right to be forgotten, enabling individuals to control the erasure of their data and limit its manipulation. Efforts at both international and national levels aim to enshrine and implement this essential right in practice.

Keywords

Privacy;
Right to Be Digitally ;
Forgotten;
Personal Data;
Artificial Intelligence;
Applications;
Digital Media.

الحق في النسيان في الوسائط الرقمية ـ دراسة في إطار الاتحاد الأوروبي والقانون الجزائري-

ملخص

يعد الحق في الخصوصية من بين أهم الحقوق الأساسية للإنسان التي أولتها التشريعات الدولية والوطنية حماية قصوى، ويترتب عن هذا الحق حماية عناصره ومظاهره كحق الشخص في الاحتفاظ بأسرار حياته بمعزل عن أي إطلاع أو اختراق، وهذا الحيز له قداسة عند الفرد وملتصق بذاته وبشخصيته. غير أن التطور التكنولوجي وخاصة نظم الذكاء الاصطناعي، قوضت من تلك المساحة السرية لديه، وخاصة بعد انخراط الإنسان بوصفه فاعل أساسي في مجتمع تحول الى مجتمع رقمي بامتياز، حيث أنه مع التداول المفرط للبيانات الشخصية وخاصة منها الرقمية، فإن لكل منا رغبة في الحق في الخصوصية الرقمية، والتي تقتضي حقا تابعاً لها، وهو الحق في الدخول في طي النسيان وتمكنه من الحصول على حقه في محو ما يريد محوه، والحد من قدرة الوسائط الرقمية من الاحتفاظ بالبيانات الشخصية والتلاعب بها، ومن هنا تضافرت الجهود الدولية والوطنية في سبيل تكريس هذا الحق وتجسيده على أرض الواقع.

الكلمات المفتاحية

الخصوصية؛
النسيان الرقمي؛
البيانات الشخصية؛
تطبيقات الذكاء؛
الاصطناعي؛
الوسائط الرقمية.

* *Corresponding author. E-mail:* hadja.ouafi@univ-mosta.dz
Doi: https://doi.org/10.34174/0079-036-002-029

Introduction :

The contemporary era has seen widespread adoption of information and communication technology, leading to a huge increase in the quantity of personal data available across numerous digital platforms. As a consequence, this information is often used by companies that store and process it. While such circulation necessitates a robust legal framework to preserve and govern it, it also emphasizes the individual's right to be digitally forgotten, which gives them control over their data and the ability to erase stored or published content at anytime.

Technological and digital advancements have posed various challenges to rights that are fundamental, including the privacy rights and the safeguarding of personal data. Given these challenges, enforcing the right to be digitally forgotten concept has become vital for deleting data traces and protecting individual privacy.

The prevalent adage in the digital world, "the internet never forgets," has caused many people to regret putting anything online, uploading a video or image, or publishing personal information, only to learn later that it is embarrassing or inappropriate. In such instances, people often desire for these items to disappear. Furthermore, organizations, for example, are increasingly evaluating job applications based on their online presence and behavior, creating fresh anxieties about the lasting availability of personal data.

The right to be forgotten is a core right that applicable to private information, that is defined as any information directly or indirectly relating to an identifiable natural person. Individuals may request the correction, modification, deletion, or augmentation of personal data without demonstrating the harm, describing the situation, or submitting a formal request, if the data has served its intended purpose and the stipulated retention duration has expired.

Despite the rigorous and sensitive aspect of one's right to be forgotten (also termed "the right to be forgotten on-line"), its significance rises with the development and expansion of digital networks, particularly social media platforms, as well as the huge amount of online personal information. Unjustified electronic storage of personal data endangers people by facilitating the publication and sharing of their personal information, sometimes without their knowledge.

Problem Statement:
The problem statement to be discussed concerns the sufficiency of juridical safeguards afforded to the right to be forgotten under global law, notably in the framework of the European Union. What is the stance of the Algerian legislator on this matter?

Methodology:
To address this problem statement, a descriptive approach is utilized to clarify essential ideas concerning the subject, such as the right to digital erasure and personal information. Furthermore, an analytical approach is used to examine European provisions on this right while presenting the position of the Algerian legislator on this right, specifically through an examination of Law No. 18/07 on the protection of natural persons in the processing of personal data.

Study Importance:
This study addresses a significant modern issue, especially in light of the digital revolution, which has touched many countries throughout the world. It emphasizes a fundamental right that is strongly associated with individuals: the ability to safeguard and remove personal data as necessary. Given recent technological advancements, it is critical to study legal methods that enable internet users to delete their data from digital platforms, whether they published it themselves or it was shared by others.

First Section: The Theoretical Basis Framework of Personal Data and the Right to Erasure

Because of the relationship between the right to have one's personal data erased, it is crucial to first clarify the idea of personal data before determining this right in digital media.

First Sub-section: Defining Personal Data and Principles of Its Protection

1. Definition of Personal Data
Notably, the following terms are used to refer to data related with individuals: "personal data," "nominative data," and "personal data." While there is overlap and equivalent between the words "data" and "information," the Algerian legislators used the expression "personal data[1]". In contrast, the French lawmaker relied heavily on "nominative data" in Law No. 78/17. Certain parts of this law used the word "personal data" as well. The term "personal data" was used in the 1981 European Convention for the Protection of persons against Automatic Processing of Personal Data, as well as Directive No. 95/46 of the European Union regarding the protection of individuals against the processing of private information and its free flow. This prompted the French lawmakers to replace "nominative data" with "personal data" in

response to the European Directive in order to standardize the usage of this word. The amendment was implemented by Law 2004/801, enacted on August 6, 2004, which amended and supplemented Law 78/17[2].

The Committee on Informatics and Freedoms justified the use of the term in its report to the French Parliament during the debate over amendments to the Freedom and Information Act. The expression "nominative data" was criticized for having the word "name," which indicates that a name is linked to data in order to identify or define a person's identity. On the other hand, the word "personal data" is seen as more abstract and specific, referring to data about persons rather than merely data about their identities or data including their names. This notion is more appropriate and in line with the European Directive. Clearly, the term "personal data" is more relevant than "nominative data," since limiting identification to a name alone is problematic; it leads to a restrictive vision that ignores the growth of indirect identifying techniques[3].

The legislator defined personal data in Article 03, Paragraph 01 of Law No. 18-07 as "any information, regardless of its medium, relating to an identified or identifiable individual, referred to hereinafter as 'the data subject,' directly or indirectly, especially through reference to an identification number or one or more specific components related to the physical, physiological, genetic, biometric, psychological, economic, cultural, or social identity of that individual."

Comparative legislation, especially European law, follows the same definition as described above. This is most likely due to the fact that these definitions are derived from the Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Information and EU Directive 95/46, both of which focus on safeguarding natural persons in relation with personal data processing and promoting the free flow of that data.

In light of the foregoing , it can be inferred that the protected data is specifically related to individuals who are known or identifiable. This identification may be performed using unique components of their physical, physiological, genetic, biometric, psychological, economic, cultural, or social identity, without limiting the elements that can be used to identify the data subject.

In the legislation passed on August 6, 2004, the French legislators followed the definition of personal data established by the European Directive. In the first paragraph of Article 2, it defines personal data as "any information or data that can directly or indirectly identify a specific, identifiable natural person."

The European Directive[4] clarifies that a person can be identified directly or indirectly, particularly by using an identification number or a combination of data or attributes associated with physical, physiological, genetic, psychological, social, economic, or cultural characteristics.

Notably, Article 1 of the EC/95/46 and EC/2002/58 directives state that the principal goal of these laws is to safeguard natural people' basic rights and freedoms while processing personal data, particularly those relating to their private lives. As a result, the protection extends not only to information that directly identifies a person, such as their name or address, but also to information that indirectly identifies a person, often linked to modern technologies, such as mobile phone numbers, email addresses, fingerprints, credit card numbers, DNA , personal data like voice, or even biometric data[5].

2. Principles and Fundamentals of Personal Data Protection

Any personal data protection regulation is founded on the premise that personal data must be gathered by "lawful means and generally by the circumstances of the case," as stated in the Hong Kong Personal Data (Privacy) Ordinance. Unless the data subject consents, the data may only be used disseminated for the reasons for which it was collected, or for those that are closely related to them. These laws are reinforced by the "Six Principles of Data Protection," which are, in reality, the primary legal mechanisms:

Any law safeguarding personal data is based on the premise that personal data must be gathered using 'legitimate and fair methods under the circumstances,' as stated in Hong Kong's Personal Data and Disclosure Act. Such data may be used or disclosed or the purposes for which it was initially obtained, or for purposes that have a direct relationship to those original goals.

These laws are supported by six 'data protection principles' which constitute the fundamental part of legislative mechanisms[6]:

First Principle: Data collection is prohibited unless it is done for a legal reason directly related to the function or activity of the data user, who will only use personal data in lawful and fair ways. This requires the information user to inform the individual providing the data of the reason for which the data will be employed.

Second Principle: Data users must ensure that stored data is accurate and up-to-date. If there is doubt, the user must immediately cease utilizing the data. Data should not be retained longer than necessary for the purpose for which it was gathered.

Third Principle: States that without the data subject's consent, personal data shall not be employed for any purpose other than the one for which it was collected.

Fourth Principle: Stipulates that the data user shall take appropriate security measures to protect personal data and ensure adequate protection against unauthorized access, processing, deletion, or use by others who lack the authority to do so.
Fifth Principle: About the data user's obligation to disclose the kind of personal data. A 'privacy statement' that covers data accuracy, retention duration, security and usage, and protocols for data access and correction requests serves this purpose.
Sixth and Final Principle: This relates to the data subject's right to see their data and ask for a copy of any personal information that the person in charge information gathering maintained in file. If the data is found to be wrong, the individual who provided it possesses the right to request that the user amend it.

Second Sub-section: Defining the Rights to Digital Erasure and Their Features

1. Understanding the Right to Digital Deletion
Comprehending of the right to digital deletion stemmed from French jurisprudence and is expressed in French as "le droit à l'oubli" ("the right to be forgotten"). However, in Arabic, the term is more consistently referred to as "al-haqq fi al-nisyan al-raqmi" ("the right to be digitally forgotten"). This precise expression emphasizes that "forgetfulness" relates explicitly to the internet as a digital environment[7].

***Jurisprudential Definition**
In jurisprudence, the right to be digitally forgotten is referred to as the individual's right to have their past remain confidential and not be disclosed to the public after a certain period[8].

It is also defined as the right of every individual to retain lifetime control over their digital memories, to manage them whenever they want, and to partly or entirely delete them[9].

In a similar vein, Etienne Quillet views this right as including the freedom to choose suitable actions for the processing, dissemination, or preservation of information. Like the right to "informational self-determination," it also gives them the power to choose which of their personal data should be hidden behind the veil of deletion[10]".

Analyzing these definitions reveals that they do not adequately capture the essence of the right to be electronically erased with regard to the Internet. Furthermore, they do not define the duration in which a person has to claim this right.

The purpose of the right to digital erasure is to safeguard individuals from the public view of previous events at their own discretion, enabling them to hide such incidents from other people. This right gives people the ability to choose how their personal information is processed online and safeguards parts of their public lives by keeping them hidden from the public eye. In actuality, this implies that any user can delete all of their personal data and information.

However, other legal scholars support a more expansive interpretation of the right to be removed from the internet. Depending on different sources, it is an individual's right to manage and control personal data. This definition states that people have the lifetime right to control their digital memories, make changes to them whenever they choose, and remove them fully or partially. Some describe the right to be removed from the internet as the ability to delete personal data or ask that it no longer be shared after a certain amount of time[11].

***Legislative Definition:**
It relates to the right of a person to remove his data as the only legitimate owner of such data for a duration that may surpass, in his opinion, the initial objective or reason for which the data was collected. Article 6, dated January 6, 1978, of the French Information and Freedoms Law provides an explicit interpretation of this idea. As per this concept, the right to be digitally forgotten gives people the ability to keep an eye on their data and manage their online persona by giving them the ability to access and modify it.

With reference to this law, Article 4, Paragraph 5 discusses the option that information should not be kept for longer than necessary for the purposes for which it was processed by the information processor. Except in cases where it is kept for archival, public, historical, scientific, or statistical study, the information must be forgotten and erased after this time. It further emphasizes that, in accordance with Article 6 of the same legislation, it is illegal to keep personal information that shows a person's race, religion, or philosophical views, or that demonstrates racial prejudice. This earlier provision prohibits the data processor from keeping such data and clearly outlines the time frame within which people may seek its erasure[12].

Internationally, there is a noticeable consensus in favour of laws safeguarding personal information, including the ability to erase or delete it, and regulating the right to be digitally forgotten. This is described in 1948's Universal Declaration of Human Rights, Article 12[13].

In addition, the European Union's General Data Protection Regulation, issued in 2018, reaffirmed the right to be digitally forgotten under Article 17, which aligns directly with the rules of the Universal Statement of the Rights of Humans[14].

2. The Legal Basis of the Right to Digital Erasure

The legality of the ability to be electronically erased has been the topic of judicial dispute. While some consider it a separate right, others view it as a component of the right to confidentiality.

Others argue that the right to online data erasure is a part of the right to confidentiality as it covers all personal elements, even if the material is public. They defend this by claiming that the inviolability of privacy applies to all topics and occurrences that a person has observed in the past or is presently experiencing. There should be a veil of confidentiality and secrecy over private topics and occurrences, especially as time passes. If these private data are divulged, it represents a breach of an individual's private life[15].

According to this opinion, this right is just a subset of confidentiality, grounded in the principle that the deletion request concerns features that are inherent to a person's identity, which is a crucial component of their personal existence. This private life comprises many facets of a person's personality. Private information and data, even if released as an exemption, should nonetheless be secured by the right to deletion to prevent subsequent republishing, particularly after a long period of time. The basic cornerstone of this protection is, above all, treating it as part of one's own life. Beyond that point, whether the legal foundation varies is insignificant[16].

Conversely, some assert that the right to deletion is not fundamentally a component of the privacy right and does not come within its purview. Instead, it is viewed as an autonomous right since it protects facts that have already become public. Because these facts do not apply to private life, they provide the foundation for a unique and independent right[17].

As a result of the significant technical changes taking place throughout the globe, the ability to this right may be regarded as an individual right in the digital age. Hence, it may be seen as a separate right in and of itself, sometimes intersecting along with rights like privacy and the protection of personal information.

Section Two: The Right to +Deletion in the European Union and the Stance of Algerian Legislator:

Digital data circulated on the internet, through social media networks, and across various sectors is critical because it aligns with technological advancements, particularly digital transformation, the artificial intelligence revolution, and cloud computing, all of which address the informational needs of individuals and society. This situation is both essential and reasonable. However, technology has also resulted in new types of data breaches, particularly personal data, emphasizing the need of investigating legal methods to secure it.

Numerous artificial intelligence applications have grown in popularity, resulting in an increase in the everyday interchange of data. Manual data entry is no longer the dominant method; it has been replaced by specialized areas driven by AI systems, not only for storage and preservation, but also for analysis using self-learning algorithms and prior experiences, referred to as "patterns", with the assistance of neural networks that the software analyses. Much of this data is personal, and people usually want to dispose of it after a given time. However, AI applications see this data as a significant resource for training and improvement. The problem stems from the fact that this data cannot be readily deleted owing to its relevance to huge corporations, who, in their opinion, are entitled to it in return for the free services provided. Even more alarming, there exist data gathering centres and specific facilities for keeping this data, protecting it from damage or loss[18], sometimes without the knowledge of many people and without assuring a secure environment for its storage on computers running AI algorithms. All of this creates a direct risk if the data is abused. Furthermore, maintaining such information is a violation of the right to erasure, in accordance with the laws in force.

Practically, the UN experience serves as a model for adopting successful legislation that is in line with technical advances in the digital and AI areas. This led to in the recognition of the right to digital erasure and the establishment of safeguards to preserve it, causing several laws to follow suit, either explicitly or implicitly.

First Sub-section: Safeguarding the Right to Digital Erasure under EU Law

Inspite of various worldwide attempts, the European regional strategy has gained popularity and proved successful as a result of its quick adaptability to digital transformation advancements in the context of the fourth technology revolution. The European Union's attempts to consolidate laws have proved to be critical in enhancing the safeguarding of private information for the citizens of Europe. Both the European Parliament and the EU Council help advance a unified legal structure, which resulted in the approval of European Parliament and Council Directive EC/9/96, issued March 1, 1996, on the legal protection of databases.

Notably, in 2012, the European Commission proposed a law granting internet users the "right to erase data," requiring search engines to make adjustments to some search results to align with EU rules on personal information safeguarding [19].

In May 2014, the EU Court acknowledged in the Google Spain case, the ability of individuals to demand the deletion of pages from Google search results that reference their personal data. Since then, Google has launched an online form where Europeans may make requests to erase their personal data. The corporation evaluates each request on an individual basis, but has established some restrictions. For example, a request is more likely to be granted if the material is obsolete or erroneous. Conversely, if the material is of public interest or concerns a prominent person, it will be more difficult to erase[20].

According to the court ruling, "the operator of a search engine is required to remove search results obtained by entering the name of a person, as well as referral links leading to web pages published by others that contain information about this person, particularly when the name or information has not been removed or deleted from those pages, even if the publication itself is lawful[21]."

Google found this ruling disappointing for search engines and other internet publishers in general, since it contradicted a previous year's suggestion by one of the court's top lawyers that search engines not be held liable for the material appearing on search results pages.

Google followed the decision and began creating a request form on its website, establishing processes for removal requests. Google received over 70,000 requests to erase links containing personal data in accordance with European data protection rules. It declared that each request would be evaluated and assessed separately to see if it meets judicially defined norms[22].

Following the Court of Justice of the European Union's 2014 verdict, which explicitly stated the right to be digitally forgotten, European countries recognized the flaws in their legal framework. As a consequence, they needed to rethink how to offer better protection for personal data. The European Union later established the General Data Protection Regulation[23].
The goal of this European rule is to better secure the private information of people from Europe.

- The privilege of deletion and inclusion in the digital right to be removed by erasing their information online.
- The ability to be notified in the case of a violation of data.
- The freedom to enter all stored data or the right to know what data companies use and for what purpose, in order to oppose it.

Referring to Article 17 of the aforementioned rule, we see that it contains the terms "right to be forgotten" and "right to erasure." After examining this article, we discovered that it gives every individual whose personal data is being processed the right to request removal from the information's controller as soon as possible. The personal information controller is bound to respond to this demand if one of the following conditions are met.[24]:

- If the personal information is no longer required for the reasons for which it was collected.
- If the subject whose information is being processed quits the permission on which the use of the data was carried out, pursuant to Articles 1/6 and 9/2 of the regulation., unless there is another legal basis for processing.
- If the person opposes to the processing under Article 21 of the rule, and there are no prevailing valid reasons for conducting the processing.
- When information is processed in a way that defies the legal reasons provided by the legislation.
- If there is a legal obligation requiring the controller to erase personal data under EU or member state laws.
- If the processing is based on paragraph 1 of Article 8 of the legislation, which governs the processing of children's information.

Additionally, certain legal protections existed to protect the right to be erased. Incriminating violations of this right in the age of technology. entails addressing unauthorized access or lengthy retention of personal data beyond the initial reason for which it was obtained. These measures jeopardies a user's identification and privacy on the network. Thus, when taking necessary steps to safeguard personal data, the primary attention should be on resolving the following points:

- Storing personal data for longer than necessary for its original purpose.

- There are insufficient safeguards in place to ensure security of information.
- Failure to reply to the objection lodged by the information subject[25].

According to the preceding, the huge amount of personal data shared across several digital platforms and social networking sites today has a prominent position in law aimed at protecting numerous rights, the most important of which pertains to confidentiality. Accordingly, another right arises: the right to deletion. Legislative documents, especially the advanced and successful European law, have created a set of requirements for parties that use personal data, whether persons, institutions, organizations, or businesses. A significant feature of these legislation involves the rights connected with the supervision and utilization of personal information, especially during automated processing of data. [26]. These rights involve:

- The right to have private information deleted and retired from repository systems at the data the individual's demand..
- The right to obtain legal consent, judicial oversight, and compensation for any damage caused by unlawful data processing.
- The ability to reject and rectify any inaccurate data.
- The capacity to gain entry and control personal information.
- The ability to maintain an adequate level of transparency concerning how personal data is processed.

As stated above, the European legal system is based on strong foundations, beginning with the inaugural law that set the broad norms for this union. This has resulted in a strong unity founded on robust legal principles that have not overlooked the protection of people's fundamental rights, particularly the right to be removed as a component of the freedom to privacy. This regulatory system has evolved alongside technological advancements and has served as the foundation for other forms of legislation, including agreements that outline obligations and rights, as well as directives that provide guidance to actors and those handling the personal data of European citizens. Consequently, this legislation has become an exemplary model within the international system for safeguarding privacy and digital information.

Additionally, after the 2014 ruling by the EU Court, various court rulings have required search engines to erase search results. For example, on December 19, 2014, the High Court of Paris issued an urgent order requiring Google to remove a referral link leading to a website containing information about the claimant's 8-year-old conviction, which was no longer on their criminal record but had made it difficult to find employment. Furthermore, on May 12, 2017, the same court issued an immediate order requiring Google to delete a referral link to a website featuring sexually suggestive photos of a model who had not given approval for their publishing on the connected websites.

Further highlighting the judicial nature of the right to be removed from search results, the French Council of State issued 13 decisions on December 6, 2019, establishing guidelines for search engines to follow in order to protect this right, which is overseen by the National Commission on Informatics and Liberty. They included:

- The judge, when ruling on a request, shall do so in light of the circumstances and applicable law when considering the request.
- A request to remove a referral link leading to a website containing personal data of an individual is regarded as a right.
- The right to request the removal of search results is not absolute; it shall be balanced with the right to information. This balancing process considers the nature of the personal data, which often includes the following:
    - Sensitive data, such as information about sexual life, religious beliefs, or health status, which has a greater intrusion into an individual's private life.
    - Data associated with criminal status, like past convictions.
    - Sensitive data not directly related to private life[27].

In the same line, the EU Court has the opportunity to define the geographical extent of the right to digital deletion in its decision on September 24, 2019. The Court stated that the scope of this right is restricted to the European area, implying that the power to delete search results is not extended outside the European Union. As a result, Google is not compelled to remove links globally under the right to deletion.; the removal applies exclusively to European search engines in all their versions[28].

Second Sub-section: The Algerian Legislator's Stance on the Right to be Digitally Forgotten

Algerian legislators were somewhat reluctant to handle personal data privacy, passing special law on the issue only in 2018. This development arose from the constitutional norm provided by the 2016 amendment to the 1996 Constitution, Law 16-01, enacted on March 6, 2016. The first paragraph of Article 46 emphasized the need of protecting private life and communication confidentially, which are described in the second and third paragraphs, respectively. Furthermore, the Constitution recognized the protection of personal data as a basic right, requiring the government to maintain this right and penalize violators.

In accordance with this idea, Algerian legislators passed Law 18-07 on June 10, 2018, regarding individual protection in the handling of personal data. However, an examination of its provisions reveals that the legislation does not directly address the right to digital deletion. Nonetheless, like with previous comparable legislation, it included some rights that indirectly help to upholding this idea.

Thus, unlike the European Directive and the French law implementing it, Law 18-07 does not specifically state that the concept of erasure is the primary guarantee of the right to deletion. However, a closer examination of Article 35 of this law, which addresses the right to rectification, indicates that it permits an individual to obtain free updates, corrections, erasure, or closure of personal data that is processed in violation of the law. The term "erasure" is synonymous with "deletion" or "removal," as demonstrated by the French translation of Article 35, where the term used is "l'effacement," which corresponds to "Mahw" (erasure) in Arabic [29].

Notably, the Algerian legislators did not adhere to the European Directive, That had a particular chapter on the right to deletion. However, the Algeria's laws classified it among other rights that people might exercise, such as the right to correction and closure, all of which are included under the heading of the right to rectification. As stated in Article 35 of Law 18-07, comparable to the French legislators and the European Directive, The exercise of this legal right is limited to circumstances when the processing breaches legislation. owing to its incomplete or wrong character, or where the processing is legally forbidden. This might signal that the lawmakers does not formally acknowledge the right to deletion.

As a result, the Algerian lawmakers should complete Chapter Four of Law 18-07, headed "Rights of the Data Subject," by including an additional chapter on "The Right to Erasure." This section should contain procedures that allow persons to seek the deletion or closure of their personal data if its processing does not conform with Law 18-07. Naturally, this should specify the circumstances for exercising this privilege, as well as the exceptions to it. In this regard, the Algerian legislator might refer to the text of Article 17 of the aforementioned European law[30].

Furthermore, in order to strike a balance between protecting people' privacy from their digital history and the public interest in accessing this past, the Algerian lawmaker should provide exceptions to the right to be deleted in the suggested section. This would strike a balance between this right and other similarly important rights, like the right to legal remedy, the right to a court-appointed defence, and the right to media and press equality as well. This balance is crucial when accessing personal data subject to digital erasure is vital for exercising these rights, particularly when it comes to protecting society from those attempting to gain from the right to be forgotten[31].

It is worth noting that, in addition to the previous discussion of Algerian legislators' positions on the right of deletion, Article 47 of the Civil Code may also be referenced [32] . Persons whose data is being processed may utilize this provision to request that their data be deleted or to prohibit any action that they think breaches their data, with this article serving as the basis for preserving personal rights. The continuous availability of personal data on the internet is seen as a serious infringement of an individual's rights, including personal freedom as well as the freedom of family and close friends.

In contrast, The legislative authority clearly affirmed the right to be erased in Article 46 of the 2016 constitutional amendment[33], which corresponds to Article 47 of the 2020 constitutional amendment. This article defines the inviolability of private life in all of its manifestations and specifically protects personal data.

The above-mentioned legislative texts demonstrate that the notion of limiting data retention time is important in maintaining respect for personal data in general. It also plays an important role in enforcing and protecting the right to digital erasure. Retaining personal data, particularly that pertaining to the core of an individual's private life, for a limited and non-permanent duration results in its ultimate destruction or erasure. This prohibits its continued usage, irrespective of the reason, it contributes significantly to the advancement of the right to be deleted.

To conclude, in line with the standards set by the Algerian legislator in Law No. 18-07, the texts do not clearly specify the right to be forgotten by name, as does the European regulation. However, as with other laws, it contains provisions that support the safeguarding and practical implementation of the right to deletion, whether by means of the standards guiding the information controller's actions regarding the passive right to be erased or the affirmative rights provided for the recipients of the data, such as the right to erasure, objection, and restriction of processing.

Conclusion:

Despite legislative efforts to protect individuals' data and personal information, particularly within the European framework, which serves as a model for recognizing the right to be forgotten as a right reserved for European citizens, this approach should be expanded and adopted by other regional and national laws. However, this collection of law is inadequate unless it takes a global and inclusive perspective inside larger legal frameworks, such as international treaties. To properly defend this right, efforts must be undertaken in conjunction with stakeholders and contributors in the digital technology area.

Finally, the broad principles established by the European system, as adopted by numerous legislative bodies, including the Algerian legislator, undoubtedly contribute to nurturing and supporting the right to digital erasure, whether directly or indirectly. The principle of limited duration, which ensures that processed data is deleted after a set period of time, and the principle of purpose limitation, as previously mentioned, are critical in ensuring that stored data is not distorted from its original purpose, for which the data subject provided consent. Meanwhile, the concept of data relevance guarantees that data gathering is not excessive and only contains information required for processing purposes. Undoubtedly, if data controllers follow these rules, they will make a substantial contribution to protecting the right to digital erasure.

However, notwithstanding the above, it is clear that the right to digital erasure, despite its importance, has not gotten the attention it requires, particularly in terms of official acknowledgement via specific legal texts. It continues to depend on the regulations controlling personal data. As a result, it is critical to give this right the respect it deserves by establishing legislation particularly designed to regulate it and define the privacy it involves.

Thus, we recommend the following:

• Defining a clear concept of the right to digital delete and addressing the legal issues associated with it, such as the legal liability of users who store individuals' data.

• Continuing efforts to unify international and regional legislation to create a reference point from which national laws can draw effective provisions for protecting the right to be forgotten, while reinforcing criminal policies in this regard.

• Engaging those who share control and oversight of technology to reach a balance between safeguarding individuals and their data on the one hand, and ensuring the legitimacy of companies, workers, and users in this domain, so that their interests do not undermine individuals' right to eliminate their digital past and protect their personal data from exploitation.

• Any national or international legal system, no matter how positive, cannot be considered final or static; it is subject to evolution, additions, and innovation in line with the dynamics of digital technology.

• Fulfilling international commitments to implement the resolutions of conferences and drawing from them to benefit national legislation in safeguarding digital rights.

• Benefiting from successful models, such as the European model, particularly the General Data Protection Regulation (GDPR), and keeping up with digital advancements.

• Paying attention to the partners and stakeholders in the technological domain, as they have real authority over this digital space.

• Fostering international cooperation in the protection of private life in the digital space and ensuring that the right to digital erasure is guaranteed for all, regardless of their regional affiliation.

• Urging the Algerian legislator to organize the right to digital erasure in a dedicated section within Law No. 18-07, clearly defining all exceptions as outlined in European Regulation No. 679/2016, particularly in Article 17.

• Intensifying awareness campaigns to emphasize the importance of respecting personal data and avoiding the publication of harmful or embarrassing information about individuals on social media platforms.-

Referrals and References:

Books:

- Raymond Wax, *Privacy*, Hindawi Foundation for Education and Culture, First Edition, Egypt, 2013.
- Claudine Guerrier, *Protection of Personal Data and Biometric Applications in Europe*, Electronic Commerce Communication, July 1, 2003.

Theses:

- Ibrahim Coulibaly, *The Protection of Personal Data in Scientific Research*, PhD Thesis, University of Grenoble, 2011.
- Etienne Quillet, *The Right to be Digitally Forgotten on Social Networks*, Master's Thesis in Human Rights and Humanitarian Law, Panthéon-Assas University, 2011.

Scientific Articles:

- Boukhlout El-Zine, *The Right to be Digitally Forgotten*, *Journal of Thought*, Faculty of Law and Political Science, Issue 14, Biskra University.
- Bouzidi Ahmed Tidjani, *The Right to Access the Right to be Digitally Forgotten as a Mechanism to Protect the Right to Privacy*, *Voice of Law Journal*, Volume 6, Issue 2, November 2015, Algeria.
- Kazem Hamdan Sadkhan, Shorouk Abbas Fadel, *Applications of Infringement on Personal Rights Through Social Media*, *Journal of the Faculty of Law*, University of Al-Nahrain, Issue (2B), Volume 19, 2017.
- Sidra Wassila, *The Right to be Digitally Forgotten in French and Algerian Laws: Between Acknowledgment and Implementation*, *Al-Nibras Journal of Legal Studies*, Volume 7, Issue 1, June 2023.

International and National Texts:

- Law No. 15-04 on General Rules Concerning Electronic Signatures and Certifications, Official Gazette No. 06, dated February 10, 2015.
- Law No. 18-07 on the Protection of Natural Persons in the Processing of Personal Data, Official Gazette No. 34, dated June 10, 2018.
- Order No. 75-58, dated 20 Ramadan 1395 (September 26, 1975), concerning the Civil Code, Official Gazette No. 78, dated September 30, 1975, amended and supplemented.
- Presidential Decree No. 20-442 on the Adoption of Constitutional Amendment, Official Gazette No. 82, dated December 30, 2020.
- Directive EC/9/96 of the European Parliament and Council, dated March 1, 1996, on the Legal Protection of Databases, adopted on March 11, 1996, and entered into force on January 1, 1998, amended by Directive No. 2019/790 of the European Parliament and the Council on April 17, 2019, concerning Copyright and Related Rights in the Digital Single Market.
- Law No. 78-17 of January 6, 1978, relating to Data Processing, Files, and Freedoms, modified by Order No. 2018-1125 of December 12, 2018.
- Law No. 2004-801 of August 6, 2004, concerning the Protection of Physical Persons with regard to the Processing of Personal Data, and amending Law No. 78-17 of January 6, 1978, relating to Data Processing, Files, and Freedoms, published in *JORF*, August 7, 2004, No. 182, available at: http://www.legifrance.
- Universal Declaration of Human Rights, 1948.

Websites:

- Ben Azza Mohamed Hamza, *Journal of Advanced Legal Research*, Issue 46, January 2021, article available at the following link: https://jilrc.com/archives/13569.
- Adel Abdel Sadek, *The Right to be Digitally Forgotten Between Knowledge and Privacy*, article available at the following link: https://accronline.com/article_detail.aspx?id=19502&srsltid=AfmBOoqUWC65SnJjNk2gsFX9o0QjL4CewBfQ9f7WoujyVi935C2INnS.
- *Tout sur le RGPD, Origine, Objectifs, Sanctions*, article available at the site: https://admaker.fr/blog/tout-sur-rgpd-origine-objectifs-sanctions.
- Anes Hadjadji, *The Right to be Digitally Forgotten: A Fundamental Support for Safeguarding the Right to Privacy*, article available at the following link: https://www.marocdroit.com/%D8%A7%D9%84%D8%AD%D9%82-%D9%81%D9%8A-%D8%A7%D9%84%D9%86%D8%B3%D9%8A%D8%A7%D9%86-%D8%A7%D9%84%D8%B1%D9%82%D9%85%D9%8A-%D8%AF%D8%B9%D8%A7%D9%85%D8%A9-%D8%A3%D8%B3%D8%A7%D8%B3%D9%8A%D8%A9-%D9%84%D8%AA%D8%AD%D8%B5%D9%8A%D9%86-%D8%A7%D9%84%D8%AD%D9%82-%D9%81%D9%8A-%D8%A7%D9%84%D8%AD%D9%8A%D8%A7%D8%A9-%D8%A7%D9%84%D8%AE%D8%A7%D8%B5%D8%A9_a8977.html.

1 The Algerian legislator used the term "personal data" in several laws, such as: Law No. 15-04 defining the general rules related to electronic signatures and authentication, Official Gazette No. 06, dated February 10, 2015. Law No. 18-07 related to the protection of natural persons in the field of personal data processing, Official Gazette No. 34, dated June 10, 2018. Article 47 of Presidential Decree No. 20 442 concerning the issuance of the constitutional amendment, Official Gazette No. 82, dated December 30, 2020.
2 Law No. 2004-801 of August 6, 2004, on the protection of individuals regarding the processing of personal data and amending Law No. 78-17 of January 6, 1978, relating to computers, files, and freedoms, Official Journal of the French Republic, August 7, 2004, No. 182, available at: http://www.legifrance.gouv.fr, accessed on December 25, 2024, at 23:00.

3 Ibrahim Coulibaly, "The Protection of Personal Data in the Field of Scientific Research," PhD thesis, University of Grenoble, 2011, p. 10.

4 The European Parliament and Council Directive EC/9/96 of March 1, 1996, regarding the legal protection of databases, adopted on March 11, 1996, and entered into force on January 1, 1998, amended by Directive No. 2019/790 issued by the European Parliament and the European Council on April 17, 2019, concerning copyright and related rights in the digital single market.

5 Claudine Guerrier, "Protection of Personal Data and Biometric Applications in Europe," *Communication and Electronic Commerce*, July 1, 2003, No. 7, pp. 17-22.

6 Raymond Wax, "Privacy," Hindawi Educational and Cultural Foundation, 1st edition, Egypt, 2013, p. 121.
7 Ben Azza Mohamed Hamza," the right to be digitally forgotten," "Jil Journal of Advanced Legal Research," No. 46, January 2021, available at: https://jilrc.com/archives/13569, accessed on December 25, 2024, at 23:25.
8 Boukhalout Azine, " the right to be digitally forgotten," Fikr Journal, Faculty of Law and Political Science, No. 14, University of Biskra, p. 581.
9 Kadem Hamdan Sadekhan, Shorouq Abbas Fadel, "Applications of Personal Rights Violations through Publication on Social Media Platforms," Journal of the Faculty of Law, University of Al-Nahrain, Issue (2B), Volume 19, 2017, p. 96.

10 Etienne Quillet, "The Right to Digital Forgetting on Social Networks," Master's thesis in Human Rights and Humanitarian Law, Panthéon-Assas University, 2011, p. 4.

11 Boukhlout Azine, ibid., p. 551.
12 Article 4 of Law No. 78-17 of January 6, 1978, related to computers, files, and freedoms (Amended by Ordinance No. 2018-1125 of December 12, 2018 - art. 1/5): "Processing is necessary for the execution of a public interest mission or the exercise of public authority vested in the data controller." Article 6 of Law No. 78-17 of January 6, 1978, related to computers, files, and freedoms (Amended by Ordinance No. 2018-1125 of December 12, 2018 - art. 1): "It is prohibited to process personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or union membership, genetic data, biometric data for uniquely identifying a person, health data, or data concerning a person's sexual life or sexual orientation."
13 Article 12 of the Universal Declaration of Human Rights states: "No one shall be subject to arbitrary interference with his privacy, family, home, or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks."
14 Article 17 - Right to Erasure (Right to be Forgotten) of the General Data Protection Regulation (GDPR) of May 23, 2018: "The data subject has the right to obtain from the data controller the erasure, without undue delay, of personal data concerning him or her, and the data controller shall erase such personal data without undue delay when one of the following grounds applies…"
15 Boukhlout Azine, ibid., p. 586.
16 Ben Azza Mohamed Hamza, ibid.
17 Kadem Hamdan Sadekhan, Shorouq Abbas Fadel, ibid., p. 96.
18 Artificial Intelligence, Privacy, and Children's Privacy, Report of the Special Rapporteur on the Right to Privacy, Session 46, available at:
https://www.ohchr.org/ar/documents/thematic-reports/ahrc4637-artificial-intelligence-and-privacy-and-childrens-privacy , accessed on 25-12-2024 at 23:50.
19 Adel Abdelsadeq, "The Right to be Forgotten: Between Knowledge and Privacy," article available at:
https://accronline.com/article_detail.aspx?id=19502&srsltid=AfmBOoqUWC65SnJjNk2gsFX9o0QjL4CewBfQ9f7WoujyVi935C2INnS_, accessed on December 25, 2024, at 00:12.

20 **Anes Hadjadji**, " the right to be digitally forgotten: A Fundamental Support for Safeguarding the Right to Privacy," article available at the following link: https://www.marocdroit.com/%D8%A7%D9%84%D8%AD%D9%82-

%D9%81%D9%8A-%D8%A7%D9%84%D9%86%D8%B3%D9%8A%D8%A7%D9%86-
%D8%A7%D9%84%D8%B1%D9%82%D9%85%D9%8A-%D8%AF%D8%B9%D8%A7%D9%85%D8%A9-
%D8%A3%D8%B3%D8%A7%D8%B3%D9%8A%D8%A9-
%D9%84%D8%AA%D8%AD%D8%B5%D9%8A%D9%86-%D8%A7%D9%84%D8%AD%D9%82-
%D9%81%D9%8A-%D8%A7%D9%84%D8%AD%D9%8A%D8%A7%D8%A9-
%D8%A7%D9%84%D8%AE%D8%A7%D8%B5%D8%A9_a8977.html, accessed on 26-12-2024 at 22:45.

21 **Ben Azza Mohamed Hamza**, ibid.

22 **Adel Abdel Sadek**, ibid.

23 Everything About the GDPR: Origin, Objectives, Sanctions, article available on the website: https://admaker.fr/blog/tout-sur-rgpd-origine-objectifs-sanctions/, visited on 26-12-2024 at 23:55.

24 **Ben Azza Mohamed Hamza**, ibid.

25 **Bouzidi Ahmed Tidjani**, "The Right to Access the Right to be Digitally Forgotten as a Mechanism to Protect the Right to Privacy," *Journal of Law Voice*, Volume 6, Issue 2, November 2015, Algeria, p. 1252.

26 **Raymond Wax**, ibid., p. 133.

27 **Ben Azza Mohamed Hamza**, ibid.

28 **Sidra Wassila**, " the right to be digitally forgotten in French and Algerian Law : Between Acknowledgment and Implementation," *Al-Nibras Journal of Legal Studies*, Volume 7, Issue 1, June 2023, p. 44.

29 Article 35 of Law 18-07 in Arabic states:

"The concerned person has the right to obtain, free of charge, from the data controller the following: a) Update, correct, erase, or lock personal data that is being processed in violation of this law due to its incomplete or incorrect nature, or because its processing is prohibited by law. The data controller is obliged to make the necessary corrections free of charge, for the benefit of the applicant, within 10 days from the date of notification."
The same text of the article in French reads: "The concerned person has the right to obtain, free of charge, from the data controller: a) The update, correction, erasure, or locking of personal data whose processing does not comply with this law, especially due to the incomplete or inaccurate nature of such data, or because its processing is prohibited by law. The data controller is obliged to make the necessary corrections free of charge for the applicant within ten (10) days of his/her request."

30 **Sidra Wassila**, ibid., p. 47.

31 **Sidra Wassila**, ibid., p. 49.

32 Article 47 of Order No. 75-58, dated 20 Ramadan 1395, corresponding to September 26, 1975, regarding the Civil Code, Official Gazette No. 78, dated September 30, 1975, amended and supplemented, states : *"The civil rights of a person who has suffered an unlawful violation of their rights are protected, and they may request the cessation of such violations and compensation if damage has occurred."*

33 Article 47 of the 2020 Constitutional Amendment states :
"Everyone has the right to protect their private life and dignity. Everyone has the right to the confidentiality of their correspondence and private communications in any form. These rights cannot be infringed upon except by a justified order from the judicial authority. The protection of individuals when processing personal data is a fundamental right. The law punishes any violation of these rights."