

Protection of personal data by exercising the right to digital oblivion

حماية المعطيات الشخصية بممارسة الحق في النسيان الرقمي

Bourtal Amina¹

¹ University of Ain Temouchent, Faculty of Law (Algeria),
amina.bourtal@univ-temouchent.edu.dz

Received: 14/10 /2025

Accepted: 19/03 /2026

Published: March /2026

المخلص:

حق النسيان في العالم الرقمي من حقوق الإنسان الشخصية المستجدة ظهر نتيجة للثورة التكنولوجية الرقمية، تأثر شأنه شأن الحقوق الأخرى، بظهور الإنترنت والمواقع الإلكترونية، وأفرزته المخاطر التي تواجه حياة الأفراد، أين تنتهك حرياتهم الشخصية أو خصوصيتهم، لاسيما معطياتهم الشخصية التي أصبحت مهددة بتطور تكنولوجيا المعلومات والاتصالات بعدما ترسخت في مختلف الفضاءات الافتراضية، ويرتبط ارتباطا أساسيا بحق المستخدم الذي لا يرغب في بقاء معلوماته الشخصية لفترة طويلة، تحت سيطرة الشخص المسؤول عن معالجة البيانات ما لم يتوافر سبب مشروع للاحتفاظ بها، وحماية للبيانات والمعطيات الشخصية للأشخاص الطبيعيين التي نظم أحكامها بموجب القانون رقم 18-07 المؤرخ في 10 يونيو 2018 اعترف المشرع الجزائري ضمينا بحق النسيان الرقمي تأثرا ببعض التشريعات المقارنة.

الكلمات المفتاحية: معطيات شخصية، حماية، حق النسيان، رقمنة، جريمة.

Abstract:

The right to be forgotten in the digital world is one of the emerging personal human rights that emerged as a result of the digital technological revolution, which, like other rights, was affected by the emergence of the Internet and websites, and was produced by the risks facing the lives of individuals, where their personal freedoms or privacy are violated, especially their personal data, which has become threatened by the development of information and communication technology after it has taken root in various virtual spaces, and is fundamentally linked to the right of the user who does not want his personal information to remain for a long time, under the control of the person responsible for processing it. Data unless there is a legitimate reason for its retention, and in order to protect the personal data and data of natural persons, the provisions of which are regulated by Law No. 18-07 of June 10, 2018, the Algerian legislature has tacitly recognized the right to digital Oblivion as a result of some comparative legislation.

Key words: Personal data, protection, the right to be forgotten, digitization, crime.

Introduction:

Since the mid-twentieth century, the digital revolution has brought about fundamental changes in various concepts, resulting in the emergence of new rights that individuals exercise easily and effortlessly, and at the same time pose a clear threat to personal rights and freedoms, especially the preservation of personal data of each individual within modern devices or any modern technological means.

The information network has facilitated the ways of accessing personal data, other than the means of preserving data within the traditional environment, where the oblivion in the human element has become a natural process that occurs automatically over a period of time, which has enabled individuals to achieve the psychological balance necessary to harmonize with their external environment, and has allowed the page to be turned on the past. This is in contrast to the Internet, which contains absolute memory, where stored information cannot be easily erased, as a result of users' activities through websites, the collection of their old and incorrect data and information, and their indefinite storage, which entails great risks of their continued availability.

As a result, new forms of protection of the right to privacy have emerged, and to counter the increasing violations practiced by digital service providers, where the important mechanisms that protect personal data comes the right to digital oblivion,¹ which strikes at its historical roots of an ancient European origin applied in the European Union (EU), recognized by the European Court of Justice of the European Union in 2014,² This unavoidable right keeps pace with social and technological development and keeps pace with digital life, enabling individuals to have full control over their privacy.³

On this basis, this topic is considered one of the most important topics in the legal field, which imposes the need to recognize the right to digital oblivion as a stand-alone right related to the right of the individual to erase his personal data in respect of the right to privacy of life, as it is clear to us how important to ensure the right to be forgotten within the digital environment, given the desire of Internet users to document their privacy and personal lives without being aware of the potential risks they face in the near future.

The research problem lies in the legislative gap regarding ensuring the necessary protection of individuals' right to digital oblivion in respect of their privacy. What is meant by the right to digital oblivion? What is its legal nature? Does the Algerian legislator implicitly recognize the right to digital oblivion? What are the cases of infringement on the right to digital oblivion? Has the right to digital oblivion become like any other right and can it be invoked to demand measures for the deletion and removal of personal digital data?

In order to uncover the various aspects of the research, we will rely in our study on the descriptive-analytical approach of various jurisprudential opinions and relevant legal texts, relying on the comparative method to determine the position of the legislation regulating this subject, and focusing on European guidelines and French law.

To address the subject of the study comprehensively, we will address it through two main topics as follows:

- 1- Conceptual Framework of the Right to Digital Oblivion of Personal Data
- 2- The Risks of Retention of Personal Data and the Scope of the Criminalization of the Violation of the Right to Digital Oblivion.

1- Conceptual Framework of the Right to Digital Oblivion of Personal Data:

The capabilities of information and communication technology, in addition to digital memory, entail the establishment of the right to protect individuals from risks arising from the disclosure of their personal data and all events affecting private life through the World Wide Web, which confirms the right to erase and delete such information, which consequently enshrines the right to digital oblivion. Let's try to take a comprehensive look at the right to digital oblivion through the following:

1.1- Definition of the Right to Digital Oblivion

The right to digital oblivion is a digital right that allows everyone to access, and use; create and publish digital content, and to use computers or other devices, software or communication networks without restrictions,⁴ but it is a multidimensional concept, which emerged as a new measure to protect personal data from the challenges it faces, as jurisprudence and law differ in the definition of the right to digital oblivion, This requires us to define the right to digital oblivion in jurisprudence and law, which we explain below:

A- Jurisprudential Definition of the Right to Digital Oblivion

The right to be forgotten⁵ in the electronic environment is just an extension of the right to erasure,⁶ it is a personal human right aimed at protecting against any infringement that expresses the right to privacy, which is of great importance compared to other rights or principles⁷ the right to be forgotten represents the greatest threat to freedom of expression online, and affects its practice, as personal data and information circulating over the Internet is re-controlled.⁸

The latter has turned into an endless path for the promotion of opinions,⁹ due to the fact that personal information has become available globally through the Internet indefinitely, where the jurist Morin proposes "the need to address the management of personal information in order to enable the user to control his digital destiny on the basis that "forgetting provides the "human mind" with peace of mind, mental growth and the building of positive human relationships that help to establish a personal identity, to know that it is a right that allows the individual to be able to "control his past" by omitting elements other than desirable.¹⁰

Accordingly, a person's right to digital oblivion has become a right that suggests the user's desire not to keep his personal information, and to store it by the person in charge of processing the data, by folding his electronic pages and erasing his electronic information and personal data from files and storage devices at those sites after a certain period or at the request of the data owner, so that it disappears from the websites after searching for them in various search engines on the Internet (such as the Google search engine) and social networking sites, which are likely to cause them harm in their social life.¹¹

From a jurisprudential perspective, the right to be forgotten is narrowly defined as "a right granted by law to individuals to obtain their right to be forgotten online by limiting and enabling their deletion of digital personal data."

However, it criticized the latter definition for failing to specify the period of time after which individuals can request to enter digital oblivion, and neglecting to indicate the extent to which data is retained through electronic storage systems outside the Internet.

In view of the criticism of the narrow definition of the right to digital oblivion, another jurisprudential perspective has emerged, which has come with a broad concept, defines it as

"the right of data subjects to erase their personal data and information, automatically or at the request of the data processor, after the expiration of its purpose, whether self-published or published by others, even if it is lawfully published to protect the user from his past."

Individuals have the right to control their personal data and determine when it is deleted from the Internet, including controlling and managing their digital memories at any time, whether by partially or completely erasing them or monitoring their data, which allows it to be accessed, modified or deleted.

In our view, it is advisable to adopt the broad concept of the right to digital oblivion as opposed to the narrow concept, since it is appropriate for the means used in the digital environment that have been described in the definitions, for example, the World Wide Web, the virtual medium in which this right is exercised where individuals lose control of their information once it is placed on the Internet, and the final deletion or objection to the processing of the information ensures the necessary legal protection of personal data from any risks.¹²

B- Legal Definition of the Right to Digital Oblivion

The legislative frameworks that paid clear attention to regulating the provisions of the right to digital oblivion varied in their approach, especially the European legislation that explicitly regulated this right, while other legislation implicitly referred to it by regulating the relevant aspects, including the Algerian legislation in the general rules and other miscellaneous legal texts:

- In French Legislation:

The broad concept of the right to digital oblivion was adopted by the French Data Protection Act No. 78-17 of January 6, 1978 and amended by Decree No. 2018-1125 of December 12, 2018¹³ under the provisions of Article 4, which emphasized the need to collect data in a lawful and lawful manner and preserve it in a way that preserves individual identity. The processing must take place for a period not exceeding the period necessary to achieve the purpose of processing the personal data and data, and every natural person has the right to request the processor to update or erase his personal data when the required period has expired.¹⁴

Based on the European Commission's communication that the right to be forgotten within the electronic environment is "the right of individuals to delete their data if they withdraw their consent unless there are other legitimate reasons for retaining the data",¹⁵ The European legislature affirmed in Article 20/1 of the new European General Data Protection Regulation (EU) No. 967/2016, which came into force on 28 May 2018, which aims to protect natural persons during the processing of their personal data and to ensure the free flow of information,¹⁶ and affirms the right of the data concerned to the transfer of his data and his explicit consent.¹⁷ This definition enables a person to exercise their right to be forgotten online and to limit the retention and revocable use of personal digital data".¹⁸

It should be noted that this right was previously affirmed in the European Court of Justice Decision C-131/12, which is based on the provisions of the European Directive on the Regulation of the Protection and Transfer of Personal Data Processing No. 46/95 of 1995, which establishes a legal basis for regulating the right to be forgotten throughout European countries in various aspects related to the protection of individuals and the processing of personal data, where Internet service providers are required not to store IP addresses for more than one year, and giving individuals the right to request the deletion of their personal data

available on the Internet, and failure to comply with these obligations constitutes a violation of the right to be forgotten, exposing the violator to civil and criminal liability.¹⁹

In addition to the 1950 European Convention on Human Rights, which requires internet users to ask search engines to remove search results for outdated or inaccurate personal data for as long as a person wishes to forget it even if the content is published legally.

On this basis, we see the extent to which the European legislator expressly recognizes the right to digital oblivion by the data subject, who has the right to delete his personal data that has been processed without justifiable delay by the processor, and the processing officer is obliged to take reasonable steps to inform a third party of the user's intention to delete his data, and this right may not be invoked if there are restrictions that justify the retention of personal data, such as the exercise of freedom of expression.²⁰

- In National Legislation:

Article 47 of the 2020 constitutional amendment enshrines²¹ the sanctity of private life and provides special protection for personal data of natural persons, which confirms the constitutional founder's implicit recognition of the existence of the right to "digital forgetting".

Similar to the general rules contained in French legislation,²² the Algerian legislature has affirmed, under the provisions of article 47 of the Algerian Civil Code,²³ the right of a person who has infringed on one of his inherent rights to claim compensation for the damages caused to him at the time of the attack; In other words, the continuous availability of personal data on the Internet constitutes an attack on the right and freedoms of the person, so that we can see that this article forms the basis of the right to be forgotten in the digital field, based on the nature of the right and its connection to private life.

We note through the provisions of the text of articles 42 and 43 of Law No. 15-04, which establishes the general rules related to electronic signature and authentication,²⁴ that the Algerian legislator did not explicitly refer to the right to digital oblivion, so it recognized that the process of collecting personal data by the provider of electronic certification services is subject to the explicit consent of the holder, and obliging them to collect the necessary data from the electronic certification certificates, which are prohibited from being used for purposes other than the purposes for which they were collected, without neglecting to maintain the confidentiality of the data and relevant information with electronic certification certificates.

In order to ensure the legal protection of the data of a natural person, the Algerian legislature enacted Law No. 18-07,²⁵ the provisions of which implicitly suggest the establishment of the right to digital oblivion, stipulating that personal data "shall be stored in a manner that allows the identification of the persons concerned within a period not exceeding the period necessary to accomplish the purposes for which they were collected and processed", in accordance with Article 09, and considered the "period of retention of information" as one of the basic data that must be included in the prior authorization, which includes the obligation to carry out the processing in accordance with Article 14 of the same law.

The obligation of the processor to retain personal data for a period of time not exceeding the period necessary to achieve the purpose of its collection and processing implies its obligation to erase or erase the data when the purpose of the collection and processing is achieved; A penalty shall be imposed on any processor who retains personal data beyond the

period stipulated in the legislation in force or in the permit or license, without prejudice to the harsher penalties provided for in the legislation in force.²⁶

In addition, the person concerned has the right to enable a request from the person responsible for processing to erase or close personal data,²⁷ due to the incomplete or incorrect nature of which is not in accordance with the requirements of Law No. 18-07, or because its processing is prohibited by law, as if the processing is illegal due to exceeding the time required to achieve the purposes of processing. Its members shall carry out all necessary investigations, work to make the necessary correction as soon as possible, and inform the person concerned in accordance with Article 35 of Law No. 18-07.

It should be noted that the Algerian legislature recognizes the legal protection of personal data, which means that it does not deny the existence of the right to digital oblivion of personal data, but implicitly refers to this human right under the provisions of Law No. 18-07. Unlike the European General Data Protection Regulation, which organized the right to erasure of personal data in an independent article, the Algerian legislator included it among the rights of the concerned individuals, both for the person concerned and his heirs, especially personal data related to their resources, with the exception of personal data related to the public's right to access information, which they cannot demand to be erased or closed. It addresses the problem temporarily.

1.2- The Legal Nature of the Right to Digital Oblivion

Jurists differed in determining the nature of the right to digital oblivion on the extent to which it is considered a property right, privacy, or an independent right; This is what we will touch on as follows:

A- The Right to Digital Oblivion from Property Rights:

Every individual has a right to his life, and he is not allowed to be infringed on in any way, so the question arises as to whether the right to digital oblivion falls within the property rights or not, as a part of jurisprudence believes that the characteristics of the right to digital oblivion directly contradict the characteristics of property rights, but the latter assumes the existence of a pre-existing right holder and exercises his authority, and therefore it is not permissible to adopt property rights as the legal nature of the right to digital oblivion.²⁸

B- The Right to Digital Oblivion is a Right to Private Life:

According to the general rules, the right to digital oblivion is one of the rights that are rooted in personality and one of the correct elements of the human right to his private life that requires ensuring legal protection against any abuse of power by the State and its agents,²⁹ which is affirmed in the Universal Declaration of Human Rights of 1948 under the provisions of Article 12 of the Universal Declaration of Human Rights: "No one shall be subjected to arbitrary interference in his private life, family, residence, correspondence, or to campaigns against his honour of his dignity and reputation, and every person has the right to the protection of the law from Such an intervention or..."

Everyone also has the right to maintain the confidentiality of his private life and personal data away from the knowledge of others, which has been confirmed by an aspect of jurisprudence that includes all personal elements and public data, which will become future secrets of his private life, as the re-publication of old relationships on the Internet that have

previously been forgotten by their owner constitutes a violation of the right to digital oblivion as part of the right to private life.

In this regard, the European judiciary confirmed that the right to be forgotten is one of the rights included in the right to private life, and the Supreme Court in Paris ruled on February 15, 2012 that the complainant has the right to forget her past life and that the Google search engine has violated her privacy,³⁰ and there is no doubt that the disclosure of the facts that have been forgotten, It is like revealing the privacy of individuals.

C- The Right to Digital Oblivion is an Element of the Right to Privacy:

The right to be forgotten as a multidimensional concept, linked to the right to privacy, includes elements of a personal nature (name, photograph, address, place of residence, etc.),³¹ where publicly available data and known information from the past become part of the private life in the future, which turns into future secrets, and is subject to the right to be forgotten by the owner of such data personally, where privacy includes various aspects of an individual's life, whether in the present or in the past, and any disclosure of information sent towards oblivion is similar to the disclosure of aspects of the private life of individuals,³² This has been confirmed by the European Court of Human Rights, which has enshrined the right to the protection of personal data as an integral part of the right to private and family life, under Article 8 of the European Convention on Human Rights.

It should be noted that the right to digital oblivion, although it is rooted in personal rights, But it differs from it; in terms of its temporal dimension, it is limited to ancient facts, unlike the right to privacy, which includes ancient and modern facts, as for nature, the right to privacy does not include public events because their privacy is not available, As for the right to forget aims to protect human identity and includes public and private events and ensure confidentiality, Although, from our perspective in this regard, exercising the right to digital oblivion results in the individual relinquishing all rights to control the use of their personal data, which constitutes one of the threats posed by modern technological developments.

The right to digital oblivion is also independent of the right to private life, because its scope of application is wider than the scope of application of the right to the sanctity of private life,³³ as it reflects the idea of private life due to what the digital age imposes, such as the disclosure of personal data and its circulation in order to enjoy various services via the Internet, which cannot be deleted. However, the veil of oblivion may fall on facts in a person's life that may not be lifted without his permission, as any disclosure of the facts, or an attack on the right to be forgotten, is not an attack on the right to private life, but a violation of the right to be forgotten in the digital world.³⁴

However, from our perspective, we define the legal nature of the right to digital oblivion as a modern right independent of other rights used in the digital space, evolving with the advancement of modern technological technologies, despite its connection to some traditional rights related to humans, as affirmed by some legal scholars and legislative texts.

2- Scope of Criminalization of the Violation of the Right to Digital Oblivion of Personal Data

The essence of the criminal law lies in the protection of fundamental interests by criminalizing acts that harm or endanger rights, and setting deterrent penalties in the light of the criminal policy adopted by the legislation, and the criminalization of violations of the right to digital oblivion arises from the breach of obligations imposed on service providers, specifically through the Algerian legislator's criminalization, like the rest of the comparative legislation, of several criminal behaviors, which violate personal data to ensure the necessary legal protection for the right to digital oblivion. The study entails first talking about personal data and the risks of retaining it, and then identifying the crimes against the right to digital oblivion As follows:

2.1- Personal Data and the Risks of Retention

Since the subject of the right to digital oblivion is related to personal data and the mechanism of dealing with it, it has become necessary to define this personal data or data and the risks that arise from it, which we will address Through the following:

A- Definition of Personal Data and its Relationship to the Right to Digital oblivion

We will learn about the topic of the right to digital oblivion, which is represented in personal data in the light of various legal texts, and explain the relationship between it and the right to digital oblivion as follows:

- Definition of Personal Data

UN General Assembly Guidelines 45/95 sought to combat the unlawful or unlawful processing of personal data within human rights, based on the principle of transparency and impartiality, which requires that information on persons not be collected, processed in dishonest or unlawful ways, or used for purposes contrary to the purposes and principles of the Charter of the United Nations.³⁵

European Convention No. 801 of the Council of Europe defined private data through Article 2/a by stipulating that personal data "all information relating to an identifiable or identifiable natural person", such as names, phone numbers, email addresses, age, sex... In the same sense, Article 2/A of the European Directive No. 41-95 of 24 October 1995 and Article 4/1 of the General Data Protection Regulation of the European Union under the new European Directive No. 679 of 2016 "Personal data is any information relating to an identified or identifiable natural person",³⁶ in the sense that it can be identifiable either directly or indirectly, in particular by reference to name, ID number, location data, online identifier, or one of the factors. Assisting in the identification of the genetic, mental, economic, cultural, or social identity of this ordinary person."

As defined by the French legislature in French Law No. 801-2004 of 6 August 2004, in article 2: "A personal statement is any information relating to the identity of a natural person or can be identified, whether by direct or indirect means, whether his identity is identified by reference to his number or by reference to anything belonging to him."³⁷

From the above, it is clear to us that unlike the European legislator, which narrowly defined personal data,³⁸ the French legislator has given a more flexible definition, where the phrase "by reference to anything related to a person" means all the data that will be included in the future to identify the user, even if the data is of a sensitive nature.

As for the Algerian legislature, personal data has been defined under the provisions of Article 3 of Law No. 18-07 of June 10, 2018 on the protection of natural persons in the field of personal data, as

"any information, regardless of its basis, relating directly or indirectly to an identifiable or identifiable person, in particular by reference to the identification number or one or more elements of his physical, physiological, genetic, biometric, psychological, economic or cultural identity or social".

We note that this definition aligns with the definition of the European Union Regulation, which clarifies all forms of personal data that can identify the person concerned, as the Algerian legislator considered personal information in the same sense as nominal data, which refers to all information related to a natural person, whether it is related to his private life, professional or orientation without the legal person.³⁹

- The Relationship between Personal Data and the Right to Digital Oblivion

The right to be forgotten represents a landmark advancement in the protection of personal data and digital privacy,⁴⁰ EU law recognizes⁴¹ the right of individuals to protect their personal data, with the aim of effective control over their data, to raise the question of whether this personal data is subject to the right to digital oblivion or not, so that it becomes clear that the personal information and data that a person does not know their fate is subject to forgetfulness if a period of time has passed, meaning that the right holder to personal data has actually forgotten it, including the posts made by people through social media and the statements of personal data they make Without their knowledge and will, in this context, the Supreme Court in Paris on February 10, 2017 rejected a doctor's request to remove links to articles published due to his recent conviction date, as he was sentenced to four years in prison in a fraud case against a health insurance company in 2015.⁴²

The right to be forgotten would be inconsistent with the right of the press to information and the right to freedom of expression enshrined in article 10 of the European Convention on Human Rights, but it should not be exercised at the expense of the right of individuals to respect their private lives, while ensuring the necessary legal protection of personal data.

B- Risks arising from the retention of personal data

The use of digital technology in processing and storing personal data in databases, and linking these databases to the internet search, has increased the risk of unauthorized access to this data over the internet across multiple platforms at any time. Therefore, the data processor is obliged to implement all necessary precautions to ensure the security of such data,⁴³ in particular to prevent unauthorized changes or damage by individuals who are not authorized to access it, which is an essential aspect of its legal protection, as the absence of such measures increases the risks associated with personal data, including unauthorized access, disclosure or modification.⁴⁴

The risk of the right to digital oblivion lies in the violation by the person processing the personal data of the obligation to retain it, since it remains in a backup copy with the service provider for an unknown period of time in the event of account suspension or completion of the service, under the pretext that the user may retract it, which makes it easier for him to reuse his personal data again, which applies in the case where the account is deactivated or the user dies under the pretext of linking with specialized advertising parties and specialists to improve the level of service, in addition to In order to ensure the security of the user to reduce cybercrimes, committed with the aim of accessing stored information, or deleting personal data as a form of electronic processing, service providers that are committed to processing personal data must comply to ensure that the right of persons to digital oblivion is respected by deleting or removing personal data as soon as it is processed in accordance with the time limit.

It is worth mentioning that the retention of personal data and the circulation of databases facilitates the tracking of users through the Internet by adopting the policy of service providers, even if illegally through hacking, in order to analyze their patterns and interests to send advertisements that suit their tendencies, which increases the possibility of publishing them in an undesirable way, as a result of the weakness of personal data insurance and protection programs, and neglecting its continuous development, which makes them vulnerable to cybercrimes, and thus the violation of the right to digital oblivion.⁴⁵

2.2- Crimes against the Right to Digital Oblivion

The right to be forgotten reflects an individual's desire to erase their past, and if mere access to private information is present, it is necessary to criminalize unauthorized access to information and disclose it, and on this basis it criminalizes any criminal conduct committed by service providers by breach of their duties, unlawful disclosure of personal data or failure to take the necessary precautions to protect the privacy of the person during the processing of personal data, and to ensure respect for the right to digital oblivion various comparative legislations have imposed obligations on Electronic service providers to protect the interests of users, where failure to comply with these obligations or violation of these provisions is subject to criminal penalties, and the crimes affecting the right to digital oblivion are as follows:

A- The Crime of Keeping Personal Data for a Period Beyond the Permissible Limit:

Electronic transactions are becoming increasingly disclosed through websites or applications that facilitate the process of personal identification, allowing the required service to be provided, but it raises concerns about the potential risks that may be inflicted on personal data, in terms of its collection, storage, and access over the Internet, especially in terms of data banks and their enormous storage capabilities, given the emergence of cloud storage services provided by companies with varying storage capacities.

The essence of the right to digital oblivion lies in adherence to the restrictions on the storage and retention of data, one of the basic principles governing the processing of personal data, which requires its deletion or removal once the processing is complete, as it criminalizes any criminal conduct aimed at the retention and storage of personal data by the controllers of personal data for a period exceeding the permissible limit, in the sense that any extension of this period beyond the legally prescribed deadlines is a criminal offence subject to legal sanctions, including non-compliance with the purposes for which it was collected. For example, personal data is stored for historical, statistical or scientific purposes, and the purpose behind this is only to protect the personal data of individuals from risks.

This concept of crime relates to any act by a data recipient, service provider, or data controller who oversees the disposition of the distributor and the data it contains, as the person responsible for processing or storage, causing harm to the data subject or his personal life. These acts may include accessing, transferring, and disclosing data, whether intentionally or negligently. Thus, these acts are criminalized even if the data is collected correctly and legally.

Examples of security measures that a data processor should implement include setting passwords on databases to restrict access to only authorized individuals and encrypting personal data when it is sent over a network that connects multiple computers or over the Internet, and these measures ensure that unauthorized persons do not have access to the data.⁴⁶

In this regard, the Algerian legislature affirms, under Article 9/e of Law No. 18-07 of 10 June 2018, the preservation of personal data in a way that allows the identification of the individuals concerned within

the necessary period of time,⁴⁷ to achieve the purposes for which they were collected and processed. Even if it is legitimate and regardless of the nature of the personal data is normal or sensitive.

The moral element is only achieved when the offender learns that the period of retention of the data has exceeded the purpose for which it was carried out and that his will tends to continue to retain it, despite the end of the purpose of the electronic processing of personal data,⁴⁸ This offence is classified as a deliberate offence of general criminal intent, which includes knowledge and will, which means that the offender is aware that he or she is retaining the personal data and that the authorized retention period has exceeded the period in which the data was processed.

Anyone who retains personal data beyond the stipulated period or that mentioned in the permit or license shall be punished by a fine of 200,000 to 500,000 DZD as confirmed by Article 65 of Law No. 18-07 of June 10, 2018 and by imprisonment from six (6) months to three (3) years and a fine of 60,000 to 300,000 DZD or security measures in accordance with Article 68 of the same law.

It should be noted that unauthorized disclosure of personal data outside the legal deadlines and without consent constitutes a violation of the individual's private life, unless the necessary measures are taken to secure the personal data by the data processor, who must understand the information being processed and stored in the information system and his knowledge of the extent of the need for maintenance or updating the processing system, while neglecting to update or maintain encryption programs in the data processing system, with the aim of regulating the flow of data and maintaining the security of computing systems and networks, as well as Securing user accounts through digital identity verification systems.⁴⁹

B- Illegality of Collecting Personal Data

The Algerian legislature imposes a penalty of imprisonment from one (1) to three (3) years and a fine of 100,000 to 300,000 DZD for anyone who collects personal data in a fraudulent, dishonest or illegal manner, in accordance with Article 59 of Law No. 18-07 of 10 June 2018, which stipulates that the collection of personal data in such ways is piracy, as a result of copying and illegal use of operating systems and computer programs.⁵⁰ The system is breached due to the negligence or negligence of the personal data processor, which requires the protection of personal data from the risk of hacking due to poor network security and security programs, which should be developed and updated in order to secure users' accounts.⁵¹

Anyone who makes data of a personal nature available to ineligible persons shall be punished by imprisonment from two (2) to five (5) years and a fine of 200,000 to 500.00 DZD.⁵²

C- Failure to Respond to the Right of Objection of the Personal Data Subject

In accordance with Article 36/1 of Law No. 18-07, the Algerian legislature has granted the individual data subject the right to object to the processing of their personal data by the processor, where individuals have the right to object to the use of their data for purposes of public interest, advertising or direct marketing, which poses a significant risk to privacy in the digital age, or processing for scientific research purposes or for historical purposes, where the data controller must respond to objections and stop the processing.

To make it clear to us that the Algerian legislature allows the user to object to it at any stage of the process, provided that the danger of revealing personal data to his private life and other serious reasons,⁵³ and the essential element of this crime is the negative behavior that lies in the data processor's failure to respond to the legitimate user's objection, linked to old memories or private data, and therefore it is necessary to respond to the objection requests submitted.

In Article 55 of Law No. 18-07 of June 10, 2018, the Algerian legislature imposed a penalty of imprisonment from one (1) to (3) years and a fine of 100,000 to 300,000 DZD for anyone who commits to processing data of a personal nature despite the objection of the person concerned, which results in depriving him of the right to digital oblivion, and a fine of up to 500,000 DZD against any person responsible for processing who refuses the right to object without legal justification in accordance with Article 47 of the Law No. 18-07.

It is important to note that individuals cannot exercise the right to object if their data has been processed by a service provider that has previously waived this right or if the processing is consistent with a legal obligation, such as the processing of data by security or judicial authorities in the context of an investigation to uncover the circumstances of the commission of a crime.⁵⁴

Conclusion:

In conclusion, in the face of threats to information technology, and the widespread use of computers, the enforcement of the right to digital oblivion has become an urgent necessity to ensure the legal protection of personal data, and to preserve the right to privacy by granting legal authority to Internet users to control all previously published data and personal information, with the possibility of deleting and opposing its publication after a certain period, which has made it the focus of many national and international legislations.

Among the most important findings were:

- The Algerian legislature has strengthened the idea of the tacit recognition of the right to digital oblivion under various legal texts and the provisions of Law No. 18-07 on the protection of natural persons in the field of the processing of personal data, influenced by the European Directive No. 46/95 on the protection of personal data and the new European Directive No. 679/2016.
- The network for the circulation of data and personal information of a digital nature requires everyone to exercise the right to digital oblivion and to guarantee the right to private life.
- The right to digital oblivion resulting from the deletion of personal data is a personal right that falls into the category of intangible rights.
- The difference in jurisprudence on the nature of the right to digital oblivion between considering it as an independent right or under the elements of the right to privacy and the protection of private life enshrined in national constitutions and legislations.
- The right to digital oblivion is linked to a certain period of time on personal data to demand its deletion and oppose its publication.
- The violation of the right to digital oblivion is not limited to exceeding the retention period of personal data, but also includes breaching the guarantee of personal data protection, failure to respond to the user's right to object to the processing of their personal data, unlawful disclosure of personal data and failure to take the necessary measures to secure and preserve it.
- Imposing severe penalties on any violator of the right to digital oblivion in order to protect personal data.

Among our recommendations are:

- The Algerian legislator must explicitly recognize the right to digital oblivion due to the absence of legal texts regulating this right in Algerian law.
- We hope that the Algerian legislator will regulate all legal aspects of the right to digital oblivion under explicit legal texts due to its importance in the modern era.
- Establishing a dedicated body for the protection of personal data instead of digital search through electronic platforms.
- Secure the personal data of the users, and their explicit consent to its publication through the website.
- Holding conferences and workshops on mastering the protection of personal data and related rights with the aim of improving the ways of dealing with experienced electronic environments.
- Educate individuals on how to respond to attacks that violate the Privacy Policy.

Citations:

- 1- Saadoun Engeman Jamil Muhanna, Penal Protection of The Right to Digital Oblivion, ZAC Conference Series: Social Sciences and Humanities, 3rd International Humanitarian Conference, Baghdad, Volume 1, Issue 1, 2024, p. 338.
- 2- Judgment No. (12/C/131) issued by this Court on 13/May 20 referred to: Abdulkarim Abdulkarim/ Aland Tamer, The Right to Forget and the Tortious Liability Resulting from its Violation, A Comparative Analytical Study, Journal of Law, Kuwait University, No. 3, September, 2024, pp. 368, 369.
- 3- Fadia Hafez Jassim / Hadeel Ali Mohan, Criminal Responsibility for Assault by Closing the Digital Right to Forget Down, International Journal of Legal Studies, Al-Raya International Electronic Network, Jordan, Volume 2, Issue 1, 2020, pp. 86, 88.
- 4- Belaroussi Amin / Khaled Serbah, The Impact of Cybersecurity and Administrative Control on Rights and Freedoms in the Digital Age, Journal of Law, Society and Authority, University of Oran 2, Volume 14, Issue 1, March 2025, pp. 202, 203.
- 5- It is worth noting that we call the right to forget the right to erasure and the right to cancel return, forgetting is a language derived from the verb forgetting and forgetting someone forgets an idea or something that they remembered, and in English to forget means to forget, while digitization is the transformation of paper, written or printed documents, into digital documents, which can only be read through electronic devices.
Referenced by: Mahmoud Zaki Zaki Zeidan, Objective Criminal Protection of the Right to Digital Oblivion 'A Comparative Study', Faculty of Law, Journal of the Spirit of Laws, Tanta University, Egypt, Issue 101, Part 1, January 2023, pp. 359, 366, 382.
- 6- Napoleon Xanthoulis, Conceptualising a Right to Oblivion in the Digital World A human rights-based approach, Privacy and Surveillance 2013, Social Science Electronic Publishing, 2012, p. 16.
- 7- We give examples of these rights and principles: the right to freedom of expression, the principle of security and data integrity.
- 8- Carlos Cortés and Luisa Fernanda Isaza, Implementing “Digital Oblivion”: Forgetting Details, faculty of law freedom of expression and access to information study centre, university of palermo, February 2019, p. 9.
- 9 - Sami Jerbi, Civil Liability in Tunisian and Comparative Law, Tasfir Artistic Press, Tunis, 1st edition, 2011, p. 126.
- 10- Napoleon Xanthoulis, art. p. cit, p. 2, 3, 4.
- 11- Fadia Hafez Jassim / Hadeel Ali Mohan, op. cit., pp. 88, 89.
- 12- Saadoun Engeman Jamil Muhanna, art. p. cit, p. 339
- 13- Law No. 78-17 of 6 January 1978 on information technology, files and freedoms and various provisions concerning the protection of personal data, amended by Ordinance No. 2018-1125 of 12 December 2018, JORF No. 0288 of 13 December 2018, and Law No. 2018-439 of 20 June 2018 on the protection of personal data, JORF 0141 of 21/06/2018.
- 14- Hind Fateh Mahmoud/ Safeguarding All Aziz Abdul Karim, Civil Protection of the Right to Digital Oblivion, Journal of the Faculty of Law for Legal and Political Sciences, University of Diyala, Iraq, Volume 13, Issue 45, 2023, p. 243.
- 15- Napoleon Xanthoulis, art. p. cit, p. 14.
- 16- Saadoun Engeman Jamil Muhanna, art. p. cit, p. 342.
- 17- Regulation (EU) 2016/679, Art 20 Right to data portability.. (a) the processing is based on consent pursuant to Art 6 (1) (a) or Art 9 (2) (a) or on a contract pursuant to Article 6 (1) (a).
- 18- Muaath Al-Mullah, A revision of the attitude of the French punitive legislation on the idea of the right to the digital oblivion, International Journal of Law, India, Vol. 5, No.2, 2019, p 1.
- 19- Saadoun Engeman Jamil Muhanna, art. p. cit, p. 342.
- 20- Muaath Al-Mullah, art. p. cit, p. 2.

- 21- Presidential Decree No. 20-442 of 30 December 2020 on the issuance of the constitutional amendment approved in the referendum of 1 /11/ 2020, c. R No. 82 of 30 December 2020.
- 22- Article 9 of the Civil Code, Law No. 70-643 of 17 July 1970, JORF 19 July 1970, 'everyone has the right to respect for his or her private life'.
- 23- Decree No. 75-58 of 26/09/1975 containing the Algerian Civil Code. Decree No. 78 of 1978 as amended by Law No. 05-10 of 20/06/2005, c. R No. 44 of 2005 and Ordinance No. 07-05 of 13/05/2007, c. R No. 31, 2007.
- 24- Law No. 15-04 of February 1, 2015 establishes the general rules relating to electronic signature and ratification, c. Rt. No. 6 of 20 April 2015.
- 25- Law No. 18-07 of 10 June 2018 on the protection of natural persons in the field of processing personal data, c. R No. 34, issued on 10 June 2018.
- 26- Article 65 of Law No. 18-07.
- 27- Google 's privacy policy states that the process of completely and securely removing data from the company's storage systems can take up to two months from the deletion request. Google systems maintain an encrypted backup service for the user's benefit to help restore data in the event of a potential disaster, and data may remain on these systems for up to six months before being deleted.
- Referenced by: Saadoun Engeman Jamil Muhanna, art. p. cit, p. 347.
- 28- Saadoun Engeman Jamil Muhanna, art. p. cit, p. 340.
- 29- Thomas Morgenroth, Privacy in labour law, PhD thesis, University of Law and Health, Lille II, 2016, p. 30.
- 30- Muaath Al-Mullah, art. p. cit, p. 2.
- 31- Geragldine O.Mbah, Data privacy and the right to be forgotten, World Journal of advanced Research and Reviews, India, Volume 16, Issue 2, 2022, p. 1219.
- 32- Saadoun Engeman Jamil Muhanna, art. p. cit, p. 340
- 33- Mahmoud Zaki Zaki Zeidan, op. cit., p. 395.
- 34- Carlos Cortés and Luisa Fernanda Isaza, art. p. cité, p. 8.
- 35- United Nations: Collection of International Instruments, Human Rights Action,1 A.94.XIV-Vol.1, Part, A/1 755, New York.
- 36- Article (1/4) of the Regulation states: "...personal data' means any information relating to an identified or identifiable natural person ('data subject') ...".
- 37- Law No. 2004-801 of 6 August 2004 on the protection of individuals with regard to the processing of personal data and amending Law No. 78-17 of 6 January 1978 on information technology, files and freedoms, JORF No. 182 of 7 August 2000.
- 38- Sensitive data refers to personal data that reveals ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as genetic data, health data, or data related to sexuality or sexual orientation. This data should only be processed and collected under specific circumstances specified by law, such as the data subject's consent or processed by a non-profit organization.
- Referenced by: Saadoun Engeman Jamil Muhanna, art. p. cit, p. 347.
- 39- Tabash Ezzeddine, Penal Protection of Personal Data in Algerian Legislation: A Study under Law No. 18-07 on the Protection of Natural Persons in the Processing of Personal Data, Academic Journal of Legal Research, University of Bejaia, No. 2, 2018, p. 31.
- 40- Anushree Chaudhary / S.P.S Shekhawat, The Right To Be Forgotten Under GDPR: Legal Scope And Practical Challenges, international Journal for Multidisciplinary Research (IJFMR), Inde, Volume 7, Issue 4, July-August 2025, p. 9.
- 41- Article 8 (1) of the European Convention on Human Rights and Article 8 (1) of the Charter of the European Union on Fundamental Rights.

- 42- Mutaz Abdulaziz Alkhedhairi, Balancing and Risks: A Critical Analysis of personal Data Use as Governed by Saudi Insurance Law, laws journal, Switzerland, Vol. 14, No.4, 2025, pp 3, 4.
- 43- Cécile de Terwangne, Internet Privacy and the Right to Be Forgotten / Right to oblivion, Journal of Law and Political Science Studies, university of cyberjaya (UoC) Malaisie, Issue 13, February 2012, p. 112.
- 44- Saadoun Engeman Jamil Muhanna, art. p. cit, pp. 345, 346.
- 45- Muaath Al-Mullah, art. p. cit, p. 3, 4.
- 46- Saadoun Engeman Jamil Muhanna, art. p. cit, pp. 343, 344, 345, 346.
- 47- It should be noted that Algerian legislation does not specify a specific period for the deletion of processed data, but rather leaves this decision to the data controller (service provider), who must determine the retention period based on the purpose for which the data was collected and processed.
- 48- Muaath Al-Mullah, art. p. cit, p. 5.
- 49- Saadoun Engeman Jamil Muhanna, art. p. cit, pp. 345, 346.
- 50- Abdel Sabour Abdel Qawi Ali Masri, The Digital Court and Cybercrime (A Comparative Study), Law and Economics Library, Riyadh, 1st edition, 2012, p. 154.
- 51- Muaath Al-Mullah, art. p. cit, p 5.
- 52- In accordance with Article 60 of Law No. 18-07.
- 53- Hussam Oabes Ouda, The legal Vision of the Right to digital Oblivion, Analytical Study, International Review of Law, Qatar University, Volume 14, Issue 2, 2025, p. 80.
- 54- Saadoun Engeman Jamil Muhanna, art. p. cit, p. 345.