ZAC Conference Series: Social Sciences and Humanities
(ZACCS: SSH)
https://conf.zenithacademic.co.uk/index.php/zacsssh
ISSN (Print): 3049-7760 ISSN (Online): 3049-7779
3rd International Humanitarian Conference, Baghdad 2024
Volume 001, Issue 01, 2024, pp. 001-337
https://doi.org/10.70516/zaccsssh.v1i1.50

Penal Protection of The Right to Digital Oblivion

Saadoun Engeman Jamil Muhanna [1, a)]

[1] Iraqi Ministry of Education, General Directorate of Anbar Education, Anbar, Iraq

[a)] Corresponding author: Sdwn8783@gmail.com

Abstract. The right to digital oblivion is one of the personal rights that focuses on the components and elements of personality in its various manifestations, so that it expresses the person's various powers and will over these components and elements with the aim of developing this personality and protecting it from enemies. This right, like other rights, has been affected by the emergence of the Internet and websites. The right to digital oblivion now includes the person's right to have his electronic pages closed by deleting all his electronic data and information after his death, or leaving the websites, In addition to erasing his personal data from the storage devices on those sites after a certain period or at the request of the data subject, so that it does not appear on the sites after searching for it through electronic search engines (such as the Google search engine) and social networking sites, it is a human right and is fundamentally related to the right to The user does not want his personal information to remain for a long time, and does not want his personal information to be processed and stored by the person responsible for processing the data if there is no legitimate reason for keeping it.

Keywords: criminal protection, digital oblivion, individual rights, personal data, service provider.

INTRODUCTION

Individuals in society consistently seek to pursue their interests. However, these interests often conflict with those of others within the same community. Hence, the law has been established to create a social balance that ensures the protection of all interests by defining conditions under which individual interests take precedence over others. Consequently, the law grants individuals the authority to facilitate the realization of their legitimate interests, and this authority is known as rights.

Today, the world is experiencing an information and communication revolution that has brought about fundamental changes in numerous concepts and branches of sciences, including law. This revolution began to manifest and define its characteristics since the mid-20th century. The technological revolution has led to the emergence of new interests and rights associated with them. Moreover, it poses a clear threat to many of these rights and freedoms, especially personal ones. Given that information related to personal data has become a crucial material and central to this digital revolution, which fundamentally relies on storing such data, this revolution has witnessed radical transformations, including those related to the concept, nature, and legal protection of rights.

Traditional environmental preservation means had the effect of making forgetting a natural process that occurred automatically over time, enabling individuals to achieve the necessary psychological equilibrium to harmonize with their external environment. Forgetfulness allowed individuals to turn over the page on the past. However, with the advent of the Internet, the situation changed completely. This global network has had a profound impact on the lives of societies and peoples, becoming indispensable in various aspects of life. A large number of individuals can now interact with this technology easily and effortlessly. The Internet has an absolute memory, where stored information cannot easily be erased. Consequently, forgetting has become difficult. Websites track their users' activities, collect their data, store it, and retain it indefinitely. Despite the fact that this information and data may be outdated or incorrect, it remains accessible, potentially causing significant harm to individuals.

As a result, the concept of the right to be forgotten in the digital age has emerged. Through this right, individuals can delete information they believe causes them harm in their social lives. They have the ability to remove personal information and data from files, websites, and various search engines across the Internet.

Importance of Research:

The significance of criminal protection of the right to be forgotten in the digital context becomes evident due to several considerations. Among these are the increasing numbers of Internet and social media users, individuals' tendency to document all aspects of their daily lives and share them without a full awareness of the potential risks they might face in the near future. Additionally, the novelty and global importance of this issue for all countries are underscored, given the global nature of the Internet.

Research Problem:

The research problem primarily lies in the legislative gap that affects Iraqi laws regarding the provision of necessary protection for individuals' right to digital forgetting. Moreover, the issue of criminal protection of the right to digital forgetting raises several legal questions that form the substance of the research. These include defining the legal concept of the right to digital forgetting, its nature, explicit recognition in laws, and whether Iraqi laws can be relied upon to establish criminal protection for this right. Additionally, it questions whether the Iraqi legislator has defined instances of infringement upon the right to digital forgetting in current laws or draft legislation.

Research Methodology:

Comprehensive exploration of various facets of the research necessitates the use of multiple research methodologies in a coherent manner. Therefore, our study will adopt a descriptive-analytical methodology, supplemented by a comparative approach. The descriptive methodology will serve to elucidate newly introduced concepts and describe their specificity within the research topic. Meanwhile, the analytical approach will be employed to analyze jurisprudential opinions and relevant criminal texts. The use of the analytical methodology requires drawing on comparative methodology to outline the stance of legislations regulating this subject, with a focus on European guidelines and French law. Our choice of French law and European guidelines is influenced by France being among the first countries to address this right, and because these laws harmonize well with the Iraqi legislative framework.

Study Structure:

To comprehensively cover the study topic, we will approach it through two main chapters and a conclusion, structured as follows:

- Chapter 1: Concept of the Right to Digital Forgetting
  - Section 1: Definition of the Right to Digital Forgetting
  - Section 2: Legal Nature of the Right to Digital Forgetting
- Chapter 2: Criminal Liability for Infringement upon Individuals' Right to Digital Forgetting
  - Section 1: Legal Basis for Individuals' Right to Digital Forgetting
  - Section 2: Criminalization of Infringement upon Individuals' Right to Digital Forgetting

Chapter 1

Concept of the Right to Digital Forgetting

The capabilities of information and communication technology, coupled with digital memory, have necessitated the establishment and codification of a right to protect individuals from risks that may arise from the disclosure of their personal information, images, or events affecting their private lives, especially as these events become dated. This grants them the right to erase and delete such information if the interest in its publication ceases, thus giving rise to the right to digital forgetting.

Building upon this premise, this chapter will focus on defining the right to digital forgetting and subsequently outlining its legal nature. This will be addressed in two sections as follows:

Section 1

Definition of the Right to Digital Forgetting

The right to digital forgetting [1][33] is a modern concept generated by technological risks facing individuals due to old articles, inaccurate or false information, or personal photos previously published on the global information network and subsequently aged over time. This new concept has emerged as a measure to protect them from these challenges. Scholars have differed in their definitions of digital forgetting, with some narrowing its scope and others expanding it.

First Subsection: Narrow Definition of the Right to Digital Forgetting

One advocate of this perspective defines digital forgetting as "the right of individuals not to have the controller of processing retain their personal data for longer than the purpose or purposes for which it was collected," while another perspective defines it as "a right granted by law to individuals to obtain their right to forget across the internet by limiting digital personal data and enabling its deletion" [37]. However, this definition has faced numerous criticisms, notably for its failure to specify the content of the right to digital forgetting across the internet, as well as its omission of a defined time period after which individuals can request entry into digital forgetting. Moreover, it neglects the issue of retaining data through electronic storage systems outside the scope of the internet [26].

As a result, proponents of the narrow definition of digital forgetting have redefined it as "the right granted to individuals to restrict access to and retrieval of their personal data recorded in criminal and judicial records, for the purpose of reintegrating them into society." However, this definition has also been criticized for its limitation of digital forgetting to the criminal and judicial domains, thereby granting individuals the ability to restrict only criminal and judicial records without addressing other contexts [28].

Second Subsection the Broad Definition of the Right to Digital Forgetting

Due to criticisms leveled against the narrow approach in defining digital forgetting, another jurisprudential perspective emerged that defines the right to digital forgetting from a broader viewpoint. Despite advocates of this perspective agreeing on the necessity to expand the definition of the right to digital forgetting, they differ in the degree of this expansion. Some define it as "the right of an individual to control and manage any personal information," under which individuals have the right to retain control over their digital memories throughout their lives and to manage them at any time, including partially or completely erasing them as desired. Another advocate of this perspective defined digital forgetting as "the right of data subjects, automatically or upon request, to erase their personal data and information, whether self-published or published by others, even if legally published." Another opinion posited that the right to digital forgetting means "the right of individuals to protect their personal data, ensuring definitively erasing this data after a specified period, along with guaranteeing their right to object and correct it." [23].

Furthermore, one proponent of this approach expanded the concept of the right to forgetting to include greater control over personal information and data. In other words, individuals have the right to control their personal data and decide when to delete it from the internet. They also have the right to retain control over their digital memories throughout their lives and to manage them at any time, whether by partially or completely erasing them or by monitoring their own data, allowing them to access, modify, or fully delete it. [29]

It is noteworthy that this broader definition of digital forgetting was adopted by Article 40 of the French Data Protection Act of 1978, recently amended by Order No. 1125 of 2018. This article emphasizes the lawful and explicit collection of data for a specific purpose, the preservation of data in a manner that maintains individual identity, and for a duration not exceeding the necessary period to achieve the processing purpose. Every natural person with a specified identity is entitled to request the data controller to correct, complete, update, block, or delete personal data that is inaccurate, incomplete, outdated, or collected in violation of the law. [38]

From all the above, we consider the second (broad) approach to be prevailing, as the definitions provided by proponents of this approach to digital forgetting align with the terminology of the Internet, also known as the World Wide Web. Here, individuals lose control over their information once it is placed on the internet, as it operates like a spider's web, moving from one site to another, thereby rendering the information outdated, evolving, and potentially inaccurate. In such scenarios, final erasure or objection to information processing serves to protect the affected information owner, or at least mitigate the damages inflicted upon them.

Therefore, we can define the right to digital forgetting as "the individual's right to know and be informed about how their personal information is collected and stored through electronic platforms, as well as their right to completely or partially erase it either by themselves or through others, in order to ensure that their private information and digital data are legally protected against any infringement."

Section 2:

The Legal Nature of the Right to Digital Forgetting

Firstly, it must be noted that an individual is considered the owner of their life, and thus any form of assault upon it is impermissible in any manner. Therefore, questions have arisen regarding whether the right to digital forgetting falls under property rights. However, the characteristics of the right to digital forgetting directly contradict those of property rights. Property rights presuppose the existence of a holder of the right and a locus where they exercise their authority. Therefore, embracing property rights as the legal nature of the right to digital forgetting is not permissible. This is justified on the basis that an individual cannot be a subject of legal transactions. [20] Hence, our discussion will focus on whether it is an element of privacy rights or an independent right. Despite scholars unanimously agreeing that the right to digital forgetting is inherent to personal rights, they differ on its independence. Some view it as an independent right, while others consider it a component of the right to private life. The reason for this difference lies in its subject matter, which is subject to various interpretations. Consequently, we will address these two jurisprudential approaches in the following sections.

The First Subsection: The Right to Digital Forgetting as a Form of the Right to Privacy

Most jurists argue that the right to digital forgetting constitutes an element of the right to privacy, based on the notion that the latter concept extends to encompass all personal elements, even if they are publicly accessible data. Publicly known information from the past will thus become part of private life in the future, or in other words, will transform into future secrets. Consequently, such information may subsequently be considered subject to the right to be forgotten by its owner. For instance, the re-publication of old relationships on the internet would constitute an infringement upon the individual's right to forget, as these relationships have become part of their private life [2]

Supporters of this perspective justify their view by arguing that considering the right to be forgotten as an independent right from the right to privacy contradicts logic. The sanctity of privacy encompasses various aspects of one's life, both present and past. Any other interpretation would suggest that the right to privacy does not protect past events. From their standpoint, it is imperative to safeguard those facts that have been concealed through silence. Indeed, revealing information that has been consigned to oblivion is akin to disclosing aspects of individuals' private lives, especially given that the right to privacy is broadly applicable and substantial in content. It is closely linked to personal elements such as name, image, address, place of residence, health status, and similar considerations [35].

The second subsection: The Right to Digital Forgetting as an Independent Right:

Proponents of this perspective argue that the right to digital forgetting is not an element of the right to privacy and does not fall within its scope because it is an independent right. They attribute this to two factors: firstly, that events or facts intended to be concealed and not disclosed after a long period may not possess the quality of privacy, particularly if these events occurred publicly or were widely known. Additionally, some facts intended to be shielded involve public or historical figures, where public and historical interest supersedes individual rights to privacy. Therefore, publishing such information without the person's consent constitutes an infringement on their right to forget, and legal protection is provided on this basis alone [3].

This stance was explicitly articulated by the Paris District Court in its 2012 ruling, which compelled the search engine "Google" to erase and remove links broadcasting pornographic films associated with the claimant. The court justified its decision by stating "the combination of the claimant's surname and pornographic clips causes significant harm to her. Thus, the claimant has the right to forget her past in the digital world. While she necessarily consented to filming these movies for public distribution, she did not consent to their indexing and dissemination via the internet. If the disputed video does not pertain to her private life per se, it nonetheless attests to a specific period in her life from which she seeks to benefit through the right to digital forgetting" [32]

Secondly, the application scope of the right to digital forgetting is much broader than that of the right to privacy. The right to forget encompasses all events and occurrences in all their forms, whether public or private, open or secret, unlike the right to privacy, which excludes public or overt events and occurrences [13].

There exist certain points of divergence between these two rights. While it is possible for the right to digital forgetting to overlap with the right to privacy, especially when the emergence of digital memories infringes upon the private life of the individual concerned, they do not operate on the same level. The right to digital forgetting is fundamentally tied to its relationship with time, whereas the right to privacy derives meaning primarily from its spatial dimension. Private life applies to the spatial realm where individuals seek solitude, tranquility, and freedom from intrusion, whereas the right to digital forgetting is primarily concerned with its temporal relationship, safeguarding the individual from the disclosure of digital memories formed in the distant past [37].

On the other hand, the right to digital forgetting differs from the right to private life in terms of its objective. The former aims to protect human identity and dignity more than safeguarding private life. Evidence of this can be seen in European laws concerning the protection of personal data, which do not solely target the protection of private life, but also have other objectives such as safeguarding personal identity, human rights, individual and public freedoms in the face of digital advancements. [8]

In jurisprudence, it has been argued, and we concur, that the points of divergence raised by proponents of this approach are legitimate and logical. However, these can be rebutted by asserting that linking the right to digital forgetting with the right to private life is understood practically as a desire to associate it with a fundamental right or a human right in the absence of explicit legislative recognition of this right. From this perspective, the right to private life should be broadly construed, encompassing not only spatial considerations but also temporal elements. Moreover, if the right to private life protects current events, it is all the more imperative that it safeguards information that has been kept confidential and forgotten. [26]

Chapter Two

Criminal Liability for Infringement on the Right to Be Forgotten in the Digital Realm

European courts have unequivocally established the right to be forgotten on the internet, largely due to the presence of advanced legislation that provides detailed protection for personal data. However, in the absence of comparable legal frameworks in other parts of the world, particularly in Arab countries, the right to be forgotten in the digital realm remains vulnerable to infringement. Therefore, it is imperative for these countries to expedite the establishment of this right through specific legal provisions that consider the privacy of personal data on the one hand, and the nature of the internet and its particularities on the other. This would elevate this technical right to the level of other recognized human rights, allowing individuals to exercise their right to be forgotten clearly and securely, and enabling the prosecution of anyone who violates this right according to the rules of criminal liability.

Regarding the subject of our research, this section will be dedicated to elucidating the legal basis for criminal liability for infringement on the right to be forgotten in the digital realm. We will then clarify the various manifestations of this liability by dividing the discussion into two subsections, as follows:

Section One

The Legal Basis for the Right to Be Forgotten in the Digital Realm

The right to be forgotten in the digital realm is a modern legal concept that emerged as a consequence of the digital revolution. Historically, its legal basis was almost non-existent, with only a few legal texts indirectly acknowledging it. Subsequently, various agreements have sought to affirm and explicitly mention this right within their provisions. By indirect acknowledgment, it is meant that the right was implicitly protected under broader individual rights without being explicitly specified as a standalone right. This implicit protection often led to individuals being unaware of this right and not advocating for it. However, as the right gained prominence in the legal domain, individuals began to demand its recognition, leading to legal cases that highlighted the need for explicit acknowledgment and regulation of this right.[21]

Legislative frameworks addressing the right to be forgotten have varied in their approach. Some legislations have explicitly regulated this right, such as French legislation, while others have referenced it implicitly by regulating related aspects, such as personal data protection, without explicitly defining the concept of the right to be forgotten, as seen in Iraqi legislation. To further elucidate this, we will examine the positions of these two legislative frameworks in detail in the following subsections:

Subsection One

The Position of French Legislation on the Right to Be Forgotten

Before delving into the stance of French legislation, it is important to note that European legislation addressed the right to be forgotten in the European Data Protection Directive of 1995. This directive laid the foundation for the regulation of the right to be forgotten across European countries, including France. The directive explicitly organized all aspects related to the protection of individuals and the processing of personal data, which is fundamental to the right to be forgotten. It included specific provisions on the creation of databases, notification and reporting requirements, and basic rules concerning sensitive data. [4]

More importantly, this directive mandates that those responsible for creating cards or records containing personal data must not retain this data beyond the necessary period for its processing. For example, internet service providers are required not to store the IP addresses of their users for more than one year. Additionally, the directive grants individuals the right to request the deletion of their personal data available on the internet. Failure to comply with these obligations constitutes a violation of the right to be forgotten, exposing the violator to civil and criminal liability. [26]

As the issue of individuals controlling their personal data has become a significant concern, it has become possible to manage this data through storage, thereby restricting individuals' freedoms and rights, including the right to forget data they no longer wish to retain. However, this data remains stored with some parties and reappears even after the necessary processing period has elapsed. This risk has driven the need to confront those managing such channels to protect the right to be forgotten, especially after the 2014 ruling of the European Court, which required Google to delete all old personal data of its search engine users and remove all links related to this data once their purpose had been fulfilled. This ruling recommended that the European legislature provide safeguards for protecting the right to be forgotten. [25]

The legislature responded to this recommendation and explicitly recognized it in Article 17 of the new European regulation No. 16/679, issued on April 27, 2016, concerning the protection of personal data, which came into force on May 28, 2018. Its provisions apply to all member states of the European Union to unify data protection laws. In this context, the European Parliament issued the General Data Protection Regulation (GDPR) No. 679 on April 27, 2016, to protect natural persons during the processing of their personal data and ensure the free flow of information. This regulation aims to harmonize laws within the European Union. (The essence of the difference between a regulation and a directive is that the former is directly applicable without the need for any internal legislation, as stipulated in Article 99. It applies to all members from its entry into force on May 25, 2018. In contrast, a directive only provides objectives and goals, leaving each state the freedom to implement them)

Regarding the French legislature's position specifically, before explicitly stipulating the right to be forgotten in information technology amendments, it implicitly protected this right without expressly mentioning it. Article 66/2 of the amended 1958 French Constitution states that "the judicial authority ensures individual freedom and guarantees respect for this principle under the conditions specified by law." By this provision, the constitutional legislature acknowledged individual freedoms and rights, implicitly including the right to be forgotten as one of the individual rights protected under this article.

Upon close examination of the provisions of the French Civil Code, one can observe the substance and protection of the right to be forgotten. For instance, Article 9 of the French Civil Code states, "Everyone has the right to respect for their private life." Many legal scholars have concluded that this article forms the basis for the right to be forgotten in the digital realm, based on the nature of the right and its connection to private life. This is an attempt by scholars to address the lack of explicit legal provisions for the right to be forgotten, given its recent emergence. However, implicit provisions cannot replace explicit legal recognition; they serve merely as a stopgap solution to address the issue until more explicit recognition is provided.

The second stage came with the explicit acknowledgment of this right in the Law on Information Technology and Liberties No. 17 of 1987, with its modern amendments. This law included the substance of the right to be forgotten, though it did not initially mention it explicitly. Instead, it established principles related to and affecting this right, applicable to individuals and those who handle their data. Notably, this law has undergone several amendments, such as the 2004 amendment by Law No. 801, to harmonize French law with the 1995 European Directive. The most recent amendment was by Law No. 493 in 2018, aligning the law with the General Data Protection Regulation (GDPR). [9]

The first article of this law unequivocally asserts that technological and informational progress should not infringe on personal freedoms or private life. It states, "Information technology must serve every citizen and must be developed within the framework of international cooperation, so as not to infringe upon human identity, human rights, privacy, or individual or public liberties." This provision implicitly affirms the protection of the right to be forgotten, along with other rights, as part of individual freedoms and rights that emerged due to technological and informational advancements. [7]

Furthermore, Article 4 of the same law stipulates that any person whose personal data is processed has the right to request its updating or deletion once the necessary period has ended, and the data is no longer needed. This right must be upheld, and any breach of it is impermissible.

It is worth noting that France has long sought to establish a charter for implementing information technology law, enshrining rights and ensuring their enforcement. The French Minister of Digital Economy signed a charter on the right to be forgotten with collaborative websites and search engines. Although many websites signed this charter, it is notable that the two most important sites at the time, Facebook and Google, were excluded. Despite this, the charter represents a significant step in recognizing and legally protecting the right to be forgotten from both civil and criminal perspectives.

Subsection Two: The Iraqi Legislator's Position on the Right to be Forgotten

The Iraqi legislator has not explicitly mentioned the right to be forgotten in any provision. However, this does not imply the absence of the concept as a legal idea that can be inferred from some provisions that indirectly frame it. The 2005 Iraqi Constitution affirms that "every individual has the right to personal privacy, provided it does not conflict with the rights of others and public morals". (Article 17 (First) of the current 2005 Iraqi Constitution)

This provision indicates the legislator's significant emphasis on the right to personal privacy, thereby indirectly establishing a foundation for protecting all rights associated with personal identity, including the right to be forgotten.

The right to be forgotten is also reflected in the Electronic Signature and Electronic Transactions Law No. 78 of 2012. In this law, the legislator defines information as "data, texts, images, shapes, sounds, symbols, and the like that are created, stored, processed, sent, or received by electronic means." The law also defines the information processing system as "the electronic system or computer programs used to create, send, receive, process, or store information electronically." The legislator delineates the duties of the electronic certification service provider, stipulating that "the licensee is obligated to suspend the electronic certification certificate immediately upon the request of the signatory." Moreover, it emphasizes that "the data of the electronic signature, the electronic means, and the information provided to the certification authority must be confidential. The recipient of this data, by virtue of their work, is prohibited from disclosing it to others or using it for purposes other than those for which it was provided". (Articles (1/Third and Fourteenth), (11), (12/Second) of the Iraqi Electronic Signature and Electronic Transactions Law No. 78 of 2012 currently in force)

From the above texts, it is evident that the Iraqi legislator implicitly referred to the right to be forgotten, as indicated by the phrase "suspension of the electronic certification certificate," and further mandated the certification authority not to use the information provided to it for purposes other than those for which it was submitted. This serves as an implicit limitation on the duration [37].

A critique of the Iraqi legislator's stance in the Electronic Signature and Electronic Transactions Law is that it only addresses aspects of the right to be forgotten concerning certification authorities and not all electronic sites or information systems. This is despite the law’s preamble emphasizing that it was introduced to adapt the traditional legal system to align with modern information and communication technology systems. It would have been preferable for the law to apply the right to be forgotten to all electronic sites and information systems that process personal data, as these sites and systems should not retain data beyond the purpose for which it was processed or after a person requests its deletion [38]

Notably, Articles 204 and 205 of the Iraqi Civil Code can be considered an indirect legal basis for protecting the right to be forgotten. These articles grant anyone subjected to an unlawful act the right to stop this act and claim compensation for any resulting damage [41].

Accordingly, an individual seeking to delete personal data that has caused them harm can rely on these articles in the Civil Code, which provides a general framework for protecting personal rights. However, this does not negate the need for a dedicated law in Iraq that focuses on personal data protection. Such a law should regulate electronic sites and require them to provide sufficient guarantees to protect users' personal data. It should also include specific legal provisions that explicitly recognize the right to be forgotten, thereby allowing internet users to determine the fate of their personal data while balancing this right with the freedom of information and expression. Furthermore, it should ensure comprehensive criminal protection for personal data circulated on the internet.

In conclusion, it is clear that the Iraqi legislator has not organized the processing of personal data in an independent and comprehensive law covering all its forms, nor has it explicitly and clearly stipulated the right to be forgotten. Therefore, we hope that the legislator will provide criminal protection for this right and regulate all its aspects, given its paramount importance in the era of social networks. We urge the legislator to base this legislation on the new European Regulation No. 679 issued on April 27, 2016, concerning personal data protection.

Section Two

Criminalizing Violations of the Right to be Forgotten

The essence of criminal law lies in protecting fundamental interests by criminalizing acts that harm or endanger these rights, and establishing deterrent penalties in light of the criminal policy adopted by the legislator. This protection is crucial for the rights that may be violated by actions infringing upon the right to be forgotten. Criminalizing violations of the right to be forgotten arises from breaches of the obligations imposed on service providers, specifically by criminalizing their non-compliant actions. [35]

From the definitions of the right to be forgotten, it is clear that the essence of this right is to prevent data controllers from retaining personal data beyond a specified period. One of the fundamental principles in data

processing is adherence to storage limitations, with any extension of this period constituting a criminal offense subject to legal penalties. This includes criminalizing the unlawful disclosure of personal data. The negligence of service providers in fulfilling their duties and their violation of regulations and laws have led to criminalizing the failure to take necessary precautions for data protection. Therefore, we will discuss these crimes in detail as follows:

Subsection One:

Criminalizing the Retention of Data Beyond the Permissible Limit and Failure to Respond to Objections to Processing

With the increasing prevalence of electronic transactions, identity cards have become digital data recorded by government institutions, facilitating personal identification, travel arrangements through the internet, flight reservations, bill payments, and more. These processes involve entering personal data on websites or applications, such as names, phone numbers, email addresses, age, and gender, which allows for the provision of the requested service. While this has led to numerous undeniable positive outcomes, it has also raised concerns about the potential risks to personal data, whether from individuals or authorities, regarding its collection, storage, and accessibility online. [16]

In electronic transactions, it is common for the entity interacting with an individual to request personal data to provide a service or product. This data may later be used by the same entity or others. The processing of this personal data involves a covert system known as the processing of personal data, which can infringe upon privacy by providing a clear picture of the individual. [6]

To ensure respect for the right to digital forgetfulness, various legislations have imposed obligations on electronic service providers to protect users' interests. Failure to comply with these obligations or violations of these provisions are subject to criminal penalties. One key obligation is the requirement to delete or remove personal data once processing is complete, which reflects the principle of data retention limitation. The rationale for criminalizing such actions is to protect individuals' personal data from the risks posed by data banks and their vast storage capabilities, especially given the recent emergence of cloud storage services provided by companies with varying storage capacities. [12]

Moreover, some legislations grant individuals the right to object to the processing of their personal data for specified reasons. There are three scenarios for exercising the right to object: the first involves processing personal data for public interest purposes, where the data subject can request cessation of processing. However, processing may continue if there is a legal reason that outweighs individual interests or if the processing serves legal objectives. The second scenario concerns processing for marketing purposes, where individuals have the right to object to their data being used for advertising or direct marketing, which poses significant privacy risks in the digital age. The third scenario involves processing for scientific research or historical purposes, where the data controller must respond to objections and halt processing. [35]

It is important to note that individuals cannot exercise the right to object if their data has been processed by a service provider who has previously waived this right or if the processing is in compliance with a legal obligation, such as data handling by security or judicial authorities. (An example of this is Article 26 of the Iraqi Draft Law on Cybercrime of 2011, which allows the competent judge to issue orders to network service providers or technical services of any kind to provide subscription and access data to the investigative authority if it may contribute to the detection of the crime)

A pertinent question arises regarding whether heirs of the deceased can exercise the right to object based on the right to digital forgetfulness. This situation would pertain to the publication of images, videos, or content related to the deceased. Legal scholars have suggested that heirs may request the deletion of such content based on their right to digital forgetfulness, provided the content does not relate to public or historical figures, where public access to information might be prioritized. [2]

The crime of retaining data beyond the permissible limit is comprised of two elements: a material and a mental element. The material element is realized when the offender retains personal data in their electronic system beyond the purpose for which it was processed or fails to respond to objections from data subjects. This applies regardless of whether the data is ordinary or sensitive. (Sensitive data refers to personal data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or membership in trade unions, as well as genetic data, health data, or data related to sexual life or sexual orientation. Such data should only be processed and collected under specific conditions outlined by law, such as the consent of the data subject or processing by a non-profit institution)

As for the mental element, this crime is classified as an intentional offense, characterized by general criminal intent, which includes both knowledge and will. This means that the perpetrator is aware that they are retaining personal data and that the authorized retention period has exceeded the period for which the data was processed.

Alternatively, the perpetrator is aware that there are requests containing objections from users regarding the processing of their personal data. The refusal to address these requests or ignoring them without providing any reason, in addition to the perpetrator's intention to continue retaining the data despite the expiration of the purpose of processing or the retention period, constitutes the mental element of this crime. It is not conceivable for an error to exist in any form in this crime, nor is the motive for the commission of the crime relevant to its mental element. [19]

Referring to French legislation, it is noted that the obligation to retain data is affirmed in Article 6 of the Data Protection and Freedoms Act. This article states: "Data must be retained in a form that allows the identification of the data subjects for no longer than necessary for the purposes for which it was collected and processed." Consequently, French legislators address this crime in Article 226 of the Penal Code, which provides that "retaining personal data beyond the period prescribed by law or regulations, following a request for authorization or opinion, or by notification to the National Commission for Data Processing and Liberties, is punishable by five years' imprisonment and a fine of 300,000 euros, except in cases for historical, scientific, or statistical purposes according to the conditions specified by law." [36]

It is observed that French legislation does not specify a particular 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. (It should be noted that service providers' policies regarding the duration for data deletion and user electronic behaviors vary. This variation is linked to the purpose or aim of processing and the time required for it. In this context, Facebook's privacy policy indicates that the company retains user data until it is no longer necessary for providing its services and products or until the account is deleted. Meanwhile, Google's privacy policy states that the process of completely and securely removing data from the company's storage systems may take approximately two months from the deletion request. However, in the interest of the user, Google's systems also maintain an encrypted backup to assist in data recovery in case of potential disasters, and the data may remain on these systems for up to six months before being deleted)

Regarding the failure to respond to objections to the processing of personal data, the French legislator has emphasized this in Article 38 of the Data Protection and Freedoms Act, which states: "An individual has the right to object on legitimate grounds to the processing of their personal data and to object to processing aimed at commercial and marketing purposes." Additionally, the French Penal Code, in its amendments, criminalizes any violation of this right under Article 226-1/18, which states: "Processing personal data related to a natural person despite their objection for commercial reasons or legitimate objections is punishable." This provision makes it clear that an individual's objection to data processing and their request for deletion for any reason renders the processing and circulation of such data contrary to their will a criminal act that warrants punishment. [32]

Regarding Iraqi legislation, given the absence of a specific law for the protection of personal data processed electronically, and the lack of relevant provisions in the Penal Code and other laws governing electronic transactions, it is necessary to refer to the draft Iraqi Cybercrime Law of 2011. Upon examining the provisions of this draft, we find that the legislator emphasized that "the purpose of this law is to provide legal protection for the legitimate use of computers and information networks, to penalize those who commit acts that infringe upon the rights of users, whether natural or legal persons, and to prevent the misuse of such technologies in the commission of computer crimes." (Article 2 of the Iraqi Cybercrime Bill of 2011)

However, despite the existence and importance of this provision, the legislator did not include in the draft law any provisions specifically protecting the right to digital forgetfulness. Furthermore, the draft does not criminalize the retention of personal data beyond the permissible period, nor does it penalize service providers for failing to respond to individuals' requests to object to the processing of their personal data. In our view, this constitutes a legislative gap that we hope the legislator will address before the law is finalized.

Subsection Two: Criminalization of Unauthorized Disclosure of Personal Data and Failure to Implement Necessary Security Measures for Data Processing and Storage

This concept of crime pertains to any act performed by a data recipient, service provider, or data controller responsible for processing or storage, which causes harm and damage to the data subject or their personal life. Such acts may include accessing, transferring, and disclosing data, whether intentionally or negligently. Thus, these acts are criminalized even if the data collection was conducted correctly and lawfully. Human rights protection, including the right to digital forgetfulness, has undeniably evolved. The right to be forgotten reflects an individual's desire to erase their past. If merely accessing private information is criminalized, it is all the more essential to criminalize unauthorized access and disclosure of such information. [34]

This crime is also realized when the responsible party fails to take necessary measures to secure the data. The use of digital technology in processing and storing personal data in databases, and the connection of these databases to the Internet, has increased the risk of unauthorized access to this data via the Internet. Consequently, the data processor is obligated to implement all necessary precautions to ensure the security of this data, particularly to prevent unauthorized changes or damage by individuals not authorized to access it. This obligation

is a core aspect of its legal protection, as the absence of such measures increases the risks associated with personal data, including unauthorized access, disclosure, or modification. [27]

Examples of security measures that should be implemented by the data processor include setting passwords on databases to restrict access to authorized individuals only and encrypting personal data when transmitted over a network connecting multiple computers or through the Internet. These measures ensure that unauthorized persons cannot access the data. [18]

Based on the above, the crime of unlawful disclosure of personal data comprises both a material and a mental element. The material element of this crime is represented by the criminal activity, which is realized through an affirmative action involving the disclosure of personal data to unauthorized third parties by the data processor or custodian. Such disclosure must pose a threat to the reputation of the data subject or infringe upon their private life. The disclosure must occur without the consent of the data subject, be directed at individuals who are not authorized to access the data, and involve data related to the sanctity of an individual's private life. [17]

The material element of this crime is also fulfilled through a negative behavior, specifically the failure to take necessary measures to secure personal data by the data processor or custodian. This includes neglecting to update or maintain encryption programs in the data processing system. (It is noted that protection programs are of significant importance in regulating data flow and maintaining the security of computing systems and networks. This includes securing user accounts through digital identity verification systems and the use of passwords, as well as employing encryption techniques and other preventive measures that should not be overlooked by the data processor. The absence of these measures increases risks, such as system malfunction, destruction, loss, or tampering, which can be anticipated to affect the stored data)

Regarding the mental element of this crime, its nature reveals that it is an intentional offense where the mental element manifests as general criminal intent, encompassing both knowledge and will. This means that the service provider must be aware of the nature of their actions, namely the disclosure of personal data, and understand that the information being processed and stored in an information system is meant for individuals other than those to whom it is disclosed. Additionally, the provider must be aware of the need for maintenance or updating of the processing system to protect against ongoing risks that could affect the system or the stored content if not secured. Despite this, their full intent may be directed toward carrying out the act of disclosure or failing to take the necessary measures to secure their system or the personal data stored within it. This crime can also be committed through negligence, such as in cases where system breaches occur due to the processor's neglect or failure to recognize that the system is inadequate to handle potential attacks. [39]

The French legislator has underscored the crime of unlawful disclosure of personal data in Article 226-22 of the Penal Code, which imposes penalties on "any person who intentionally, and without authorization from the concerned party, receives, transmits, or discloses data during registration or any electronic processing procedure to someone who does not have the right to know, and where such disclosure causes harm to the concerned party or their private life." Additionally, the French Law on Information Technology and Liberties also addresses this crime in Article 43, which stipulates penalties for "anyone who receives personal data during its registration, transmission, or processing by any electronic means, and whose disclosure to unauthorized parties causes harm due to negligence and recklessness." [15]

Regarding the failure to take necessary precautions to secure personal data, the French legislator has provided for penalties in Article 226-17 of the Penal Code, which states that "anyone who processes or requests the processing of personal data without taking the measures specified in Article 34 of Law No. 17 of 1978 on Information Technology and Liberties shall be punished with imprisonment for up to five years and a fine of 3,000,000 euros." The same penalties apply if the service provider fails to notify the National Commission for Data Protection and Freedoms or concerned parties about personal data breaches. [24]

In contrast, the Iraqi legislator addresses the crime of disclosing personal data in Article 437 of the Penal Code No. 111 of 1969 (as amended), which stipulates that "anyone who, by virtue of their profession, industry, art, or nature of work, learns a secret and discloses it outside the legally authorized circumstances, or uses it for their own or another's benefit, shall be punished with imprisonment for up to two years or a fine not exceeding two hundred dinars, or one of these penalties." However, there is no penalty if the disclosure is authorized by the concerned party or if the disclosure was intended to report a felony or misdemeanor or prevent its commission.

The Iraqi legislator also punishes the disclosure of secrets related to individuals' private lives under Article 438 of the same code, which stipulates that "anyone who publicly disseminates news, images, or comments related to private or family secrets of individuals, even if true, if such publication harms them, shall be punished with imprisonment for up to one year and a fine not exceeding one hundred dinars, or one of these penalties." Additionally, anyone who, without being listed in Article 328, accesses and discloses a message, telegram, or telephone call to unauthorized persons causing harm, shall also be subject to the same penalties.

The Iraqi legislator has also penalized the unlawful disclosure of electronic personal data and information in the draft Law on Information Crimes. The draft states: "1. Anyone who, by virtue of their work, obtains electronic signature data or electronic means or information and discloses it with the intent to harm others or to gain financial

benefit for themselves or others, or uses it for purposes other than those for which it was provided, shall be punished by imprisonment for not less than three years or by a fine not less than 5,000,000 (five million) dinars and not exceeding 10,000,000 (ten million) dinars, or by both penalties." (1)

Regarding the failure to take necessary measures to protect personal data from infringement, the Iraqi legislator has not addressed this issue in either the Penal Code or the draft Law on Information Crimes. The draft, which focuses on combating crimes related to the telecommunications sector, does not include any provision requiring service providers to take necessary measures to protect subscribers' personal data from risks such as loss, damage, disclosure, or alteration. Therefore, we hope that the Iraqi legislator will address this gap by including a provision in the draft Law on Information Crimes that obligates service providers to implement regular and ongoing maintenance of automated processing systems and to follow technical measures to secure personal data under processing and storage.

(1) Article 13 of the Iraqi Draft Law on Information Crimes of 2011.

CONCLUSION

After completing our study on the topic titled “Criminal Protection of the Right to Digital Forgetfulness,” we have arrived at several conclusions and suggestions, which we will outline as follows:

First: Conclusions

1. The right to digital forgetfulness is a personal right, falling under the category of non-material rights, which pertain to the components and elements of personality. It represents a legal authority for internet users to control all data and information previously published on the network, with the ability to delete it and oppose its publication after a certain period.
2. The right to digital forgetfulness allows individuals to reintegrate into society by overcoming obstacles and painful memories. Despite its historical origins, this right has resurfaced in contemporary legal discourse, particularly with technological advancements and the proliferation of computers and electronic devices in our lives. Consequently, it has become a focus of interest for many national legislations aimed at protecting and enshrining this right.
3. The Iraqi legislator has implicitly recognized the right to digital forgetfulness in various legal texts scattered throughout the Civil Code, the Electronic Signature Law, the Electronic Transactions Law, and the draft Law on Information Crimes.
4. Scholars differ regarding the nature of the right to digital forgetfulness. Some view it as an independent right, while others believe it falls under the elements of the right to privacy.
5. The criminalization of violations of the right to digital forgetfulness includes the crimes of retaining data beyond the permissible period and failing to respond to individuals' requests to object to the processing of their personal data. Additionally, unlawful disclosure of personal data and failing to take necessary measures to secure and preserve it are also criminalized. The French legislator has addressed these issues in the Penal Code, whereas the Iraqi legislator has only made brief references to them in the draft Law on Information Crimes.
6. Practically implementing the existing penal protection texts related to the right to digital forgetfulness is challenging due to its presence in the open virtual world, which is difficult to regulate. Moreover, the lack of technical expertise among law enforcement officers and judges dealing with electronic environments further weakens the penal protection for this right.

Second: Suggestions

1. The scattered nature of the texts governing the right to digital forgetfulness reflects a lack of explicit legislative enshrinement of this right in Iraq. Therefore, we propose that the Iraqi legislator explicitly enshrine the right to digital forgetfulness with clear legal texts that define the parameters and conditions for exercising this right and the data it applies to. This should include consideration of both the privacy of personal data and the nature of the internet and its interactions by enacting a specific law for personal data protection.
2. We suggest that the Iraqi legislator establish a dedicated body for personal data protection, tasked with managing the deletion or retention of data and information, rather than leaving this responsibility to search engines, which may lack neutrality and independence.
3. We recommend that those managing electronic systems provide adequate guarantees to users for protecting their personal data, including informing internet service users about the purpose of any file links and obtaining explicit consent from users before adding them to a website.

4. We suggest that relevant authorities hold conferences and workshops on data protection and related rights, such as the right to digital forgetfulness, and utilize the results and recommendations to enhance the legislative framework.
5. To develop effective support for the penal protection of the right to digital forgetfulness, it is crucial to update and advance the legislative framework for data protection. This requires keeping pace with developments in international and regional legal standards and incorporating recommendations from institutions dedicated to personal data protection to ensure the effectiveness of legal texts in this domain.

REFERENCES

1. Muhammad bin Makram Ibn Manzur Al-Ansari: *Lisan al-Arab*, 3rd ed., Dar Sader, Beirut, 1994.
2. Ashraf Jaber Said: The Legal Aspects of Social Media, Dar Al-Nahda Al-Arabiya, Cairo, 2013.
3. Basim Fadel: Legal Protection of the Right to Privacy, Egyptian Publishing and Distribution, Cairo, 2017.
4. Pauline Antonius Ayoub: Legal Protection of Personal Life in Information Technology (Comparative Study), 1st ed., Al-Halabi Law Publications, Beirut, 2009.
5. Hassan Ali Al-Dhunun: The Comprehensive Commentary on the Civil Code, Vol. 2, Mistake, Dar Wael for Publishing and Distribution, Amman, 2006.
6. Rashida Boukher: Criminal Protection of Electronic Transactions, 1st ed., Al-Halabi Law Publications, Beirut, 2020.
7. Saad Atef Abdul-Muttalib Hassanein: Criminal Protection of Digital Works (Comparative Study), 1st ed., Dar Fikr Al-Jami'i, Alexandria, 2018.
8. Sherif Youssef Khater: Protecting the Right to Informational Privacy (Analytical Study of the Right to Access Personal Data), 1st ed., Dar Fikr wa Al-Qanun, Mansoura, 2015.
9. Abdul-Rahman Khalifa Al-Rawas: The Impact of Legislation on the Protection of Personal Data on the Effectiveness of E-Commerce, Zain Legal Publications, Beirut, 2019.
10. Abdul-Razzaq Al-Sanhouri: The Mediator in Explaining the New Civil Code, Vol. 8, Al-Halabi Law Publications, Beirut, 1998.
11. Abdul-Majid Al-Hakim, Abdul-Baqi Al-Bakri, and Muhammad Taha Al-Bashir: The Civil Code and the Rules of Obligation, Vol. 1, Al-Attak for Book Manufacturing, Cairo, 2008.
12. Ali Jaafar: Modern Information Technology Crimes Against Individuals and the Government, 1st ed., Zain Legal Publications, Beirut, 2013.
13. Muhammad Al-Shahawi: Criminal Protection of the Sanctity of Private Life, Dar Al-Nahda Al-Arabiya, Cairo, 2005.
14. Naglaa Ahmed Yass: Digitization and Its Technologies in Arab Libraries, Dar Al-Fikr Al-Arabi, Cairo, 2013.
15. Naeem Maghreb: Information and Internet Risks - Risks to Private Life and Its Protection (Comparative Study), Al-Halabi Law Publications, Beirut, 1998.
16. Walid Al-Sayed Salloum: Privacy Guarantees on the Internet, 1st ed., Dar Al-Jamiea Al-Jadida, Alexandria, 2012.
17. Adam Abdul-Badi' Adam: The Right to Privacy and the Protection Guaranteed by Law, Ph.D. Dissertation, Faculty of Law, Cairo University, 2000.
18. Asmaa Muhammad Al-Murghani: Protecting Private Life in the Age of Modern Technologies in Criminal Law (Comparative Study), Master's Thesis, Faculty of Law, University of Tripoli, 2012.
19. Bou Shaar Amina: The Legal Framework for Cybercrime, Master's Thesis, Faculty of Law and Political Science, Abdelhamid Mehri University - Bejaia, Algeria, 2018.
20. Rabi' Mahmoud Al-Amour: The Legal System of the Right to Digital Forgetfulness, Ph.D. Dissertation, Faculty of Law, Ain Shams University, Egypt, 2017.
21. Shalouh Mira and Bouchiri Kahina: Civil Liability for Violating the Right to Privacy in the Digital Domain, Master's Thesis, Faculty of Law, Abdelhamid Mehri University - Bejaia, Algeria, 2020.
22. Aqili Fadila: Legal Protection of the Right to Privacy, Ph.D. Dissertation, Faculty of Law, University of the Brothers, Mentouri - Algeria, 2012.
23. Abdul-Hadi Fawzi Al-Awadi: Legal Aspects of the Right to Forget in the Digital World (Comparative Study), Ph.D. Dissertation, Faculty of Law, Cairo University, 2021.
24. Alaa Al-Din Mansour Al-Mughayera: Modern Aspects of Information Crimes (Comparative Study), Master's Thesis, Faculty of Law, Al-Hikma University, Beirut, 2000.
25. Ayman Mustafa Ahmed Al-Baqali: Protecting Informational Privacy for Internet Users in the Context of E-Commerce Requirements, Legal Journal, No. 4, Vol. 9, 2021.

26. Boukhlaout El-Zine: *The Right to Digital Forgetfulness, Al-Mufakkir Journal, No. 14, Faculty of Law and Political Science, Mohammed Khider University, Biskra, 2017.
27. Sooz Hamid Majid: Legal Protection of the Right to Personal Data Privacy in Iraq, Journal of Legal and Political Studies, No. 11, Volume 6, Faculty of Law, University of Sulaymaniyah, 2018.
28. Shurooq Abbas Fadel and Kazem Hamdan Seddkhan: Applications of Violations of Personal Rights Through Social Media Publications, Journal of the Faculty of Law, Al-Nahrain University, No. 2, Vol. 19, 2017.
29. Al-Saleheen Muhammad Al-Ayish: Commentary on the Judgment of the European Court of Justice Issued on May 13, 2011, Regarding the Right to Consider Certain Facts Forgotten, Dubai Judicial Institute Journal, No. 5, 2015.
30. Abdul-Rahim Muhammad Abdul-Mawla: The Juridical Adaptation of Digital Inheritance (Comparative Juridical Study), Journal of Juridical and Legal Research, No. 36, 2021.
31. Aliya Zamel Musheet: Civil Liability Arising from Violations of the Digital Right to Forget, Journal of Human Sciences, No. 9, Vol. 29, University of Babylon, 2021.
32. Fadia Hafiz Jassim and Hadeel Ali Muhan: Criminal Liability for Violations of the Digital Right to Forget, Global Academic Journal of Legal Studies, No. 2, Vol. 1, 2020.
33. Muhammad Hamza Ben Azza: The Right to Digital Forgetfulness (Comparative Study), Journal of Law and Business, No. 68, Faculty of Legal, Economic, and Social Sciences, Hassan I University, 2021.
34. Muhammad Fathy: Criminalizing Violations of Personal Electronic Information: Reality versus Expectations, International Journal of Jurisprudence and Law, No. 87, 2020.
35. Mahmoud Zaki Zidan: Objective Criminal Protection of the Digital Right to Forget (Comparative Study), Spirit of Laws Journal, No. 101, Part 1, 2023.
36. Mustafa Ibrahim Al-Arabi Khaled: Aspects of Criminal Protection for the Digital Right to Forget, Arab Journal of Forensic Sciences and Forensic Medicine, No. 2, Vol. 2, Naif Arab University for Security Sciences, Riyadh, 2020.
37. Muadh Suleiman Al-Mulla: The Concept of the Right to Enter Digital Forgetfulness in Modern Electronic Penal Legislation: A Comparative Study Between French Penal Legislation and Kuwaiti Penal Legislation, Kuwaiti International Law Journal, Special Supplement, No. 3, Part 1, 2018.
38. Hind Faleh Mahmoud: Civil Protection of the Digital Right to Forget, Journal of the Faculty of Law for Legal and Political Sciences, Vol. 13, No. 45, University of Mosul, 2023.
39. Yasser Mohamed Salem Al-Lamie: Contemporary Criminal Policy in Protecting the Privacy of Electronic Personal Data (Comparative Analytical Study), Spirit of Laws Journal, No. 97, 2022.
40. Iraqi Constitution of 2005 (in force).
41. Iraqi Civil Code No. 40 of 1951 (as amended).
42. Iraqi Electronic Signature and Electronic Transactions Law No. 78 of 2012 (in force).
43. Iraqi Draft Law on Information Crimes of 2011.