International Journal of Law
ISSN: 2455-2194; Impact Factor: RJIF 5.12
Received: 28-12-2018; Accepted: 02-02-2019
www.lawjournals.org
Volume 5; Issue 2; March 2019; Page No. 01-08

A revision of the attitude of the French punitive legislation on the idea of the right to the digital oblivion

Dr. Muaath Al-Mullah
Assistant Professor of Criminal Law, Department of Security Sciences, Saad Al-Abdullah Academy-Police College, Kuwait

Abstract
The fact that the right to digital oblivion is one of the personal rights associated with humans, and since this right has been washed in the electronic environment which led the European legislator, especially after the judgment of the European Court of Justice No. C-131/12 of 13 May 2014 to emphasize the right the digital oblivion In article 17 of the new European Directive No. 679/2016 on the protection of personal data, where France considers as a European model to criminalize the violation of this right in its penal legislation.
Accordingly, this research aims at clarifying the general concept of the right to digital oblivion and the ambit of the criminalization of the violation of this right based on the French legislator's way of protecting this right in the light of the resolution of the new European directive.

Keywords: the right to digital oblivion, retention of personal data, delete from memory, new European regulation, abuse

Introduction
The revolution of the technological era has contributed to developing different positive patterns in our life, such as the ability to retain and keep old memories; the same thing has negatively impacted the human life by stealing their right to forget the unwanted past lives' details as well as sharing them with others; which is dangerous to the user if data in limbo has appeared after a comment or an account has been deactivated.
That led the European Court of Justice to stop this issue through resolution No. C-131/12 of 13 May 2014, which stated that the search engine has Google to erase the personal data of the litigant on the right to digital oblivion; the provision also contained the importance of the revision of the old European Directive No. 46/95 on the protection of personal data in accordance with the evolution of the mechanism of dealing with the personal data and its ambit and to ensure the observance of this right. Accordingly, the European legislator changed the regulations of the personal data protection where allocated Article 17 of the new Directive No. 679/2016 to the right to digital oblivion.

The problem statement, the research importance and purpose
The fact that France is the most prominent in the protection of the right to digital oblivion report by its penal law, and its strict control through its National Committee for the protection of the freedom of information; therefore, this research will focus on the ambit of the criminalization of the violation of this right through several questions and problems will be addressed.

Study Questions
- What is the right to digital oblivion?
- What is the problem that arises because of the right to digital oblivion?
- What is the scope of the criminalization of the violation of this right in French legislation?

The methodology of the study
In this study, the researcher will adopt the analytical approach by presenting the general concept of the right to digital oblivion, is the problem that arises because of it, and punitive resolutions that the French legislator has developed to protect it.

Structure of the study
1. **First requirement:** the general concept of the right to digital oblivion.
2. **Second requirement:** keep the personal data and identify the problem in which the right to digital oblivion arises
3. **Third requirement:** the criminalization ambit of the violation of the right to enter digital oblivion

First requirement
The general concept of the right to digital oblivion
The European legislator set the new European Directive on the Protection of Personal Data, which came into effect in the second half of May 2018; therefore, in this requirement the definitions of the right to digital oblivion which created by jurists[1] will beEl Badawi،discussed (Awadi, 2013;Lamia EL Badawi, Le Droit à l'oubli a l'ere du numérique, Maitre de conferences endroitprivé et sciences criminelles La Revue "Le Droit a l'oubli "2016) [14] and to show the consistency after presenting the attitude of the European legislator to recognize this right, moreover, the legal nature of this right and balancing it with other fundamental rights.

First: the definition of the Right to Digital Oblivion
Some argue that "It is the right that gives people the legal means to obtain their right to forget over the Internet through limiting the retention of personal digital data and the possibility of its abolition "(Barbezieux, 2016) [7]". However, others have expanded this definition to be in line with the CNIL: "The persons' Data Processing Officer's obligation to maintain and secure their right to delete that data after termination of its purpose to protect the users from their past"

(Quillet, 2011) [15]".

It is worth to mention that this right was confirmed in the European Court resolution 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 and the European Convention on Human Rights of 1950 of 13 May 2014 concerning the case of Mario Costeja González against Google Spain and the main Google in the United State [2] (ARRTT DE LA COUR, (Grande Chamber), 2014), which requires Internet users to ask search engines to remove search results for old or inaccurate personal data as long as a person wishes to forget it even if the content is properly and legally published.

The most important conclusion of the Court on the idea replace the search must be noted:

1. The application mechanism of the European Union using Article 4 of the Directive based on two criterions, the first one depends on the fact that the processing of data by an entity that located within the territory of one of the Member States; the second one depends on the absence of a headquarters in Europe for the Data Processing officer but has the means of processing data in one of the States of the Union (without the presence of a legal representative); In the absence of both criterions, laws conflict rules or private international law would be implemented, which would not guarantee the effective protection of personal data.
2. Ensure the right of individuals to access data and to object to their data in the event that they are not identical on the basis of (b) and (c) clauses of Article 12, and paragraph (1) of Article 14. Therefore, the processing officer must inform the third party about the declaration of the user's desire to delete its data and the burden of proof has fallen on individuals; Thus, the court considers the online search engine the responsible for the processing unlike the European directive provisions, which used a comprehensive concept even if it was not processed over the Internet.
3. The right replace the search is one of the fundamental rights derived from articles 7 and 8 of the European Convention on Human Rights, which called for a balance between the rights that related to the public and the economic interests of search engines, thus to respond to the request of deleting the data requires a prior examination of the processor.

Second: the explicit recognition by the European legislator of the right replace the search in the new draft European Regulation

Based on the recommendations of the Judgment of the Court of Justice that Regulation No. 46/95 is insufficient, the European legislator replaced it by Directive 679/2016 in force May 28, 2018, accordingly, the text of the right to digital oblivion in Article 17 has mentioned as follows (Bensoussan, 2018) [8]:

1. The data owner is entitled to delete his personal data that has been processed without undue delay by the processing officer.
2. In the event that the user wishes to delete the data, the processing officer is obliged to take reasonable steps to inform a third party about the declaration of the user's desire to do so, this right shall not be invoked if there are restrictions that justify the retention of personal data, such as the exercise of freedom of expression, compliance with legal obligations, or for historical or statistical purposes.

Third: The legal nature of the right to digital oblivion:

The right to digital oblivion is one of the rights that inherent personality, but some believe that this right is an independent right, while others see it as one of the elements of the right to private life, respectively the issue of the right and the ambit of its independence.

1. **The right to research is one of the elements of the right to private life:** Advocates of this idea state that the right to private life includes all personal elements, including public statements, as they would become future secrets - i.e. within private life and then be forgotten by their owner (Syed, 2013), (Fikri, 2007), republishing old relationships on the Internet consider as a violation on this right which is a part of the private life (Pailler, 2012) [13].

   The judgment of the Superior Court of Paris, which issued on 15 February 2012 which stated that the complainant has the right to forget her past life and that Google had violated her privacy and caused an impairsher[3] (TGI de Paris, 2012) [21]; as the judgment of the European Court of Justice in has emphasized in paragraph 91 that the right to forget is one of the rights that included into the right to private life.

   It should be noted that Article 9 of the French Civil Code, which considers the right to digital oblivion is one of the right elements of private life that requires a protection.
2. **The right to digital oblivion:** Advocates of this idea state that the right to digital oblivion is an independent of other rights in terms of its time dimension and nature -legal scope-; In terms of the time dimension, the right to forget is limited to long-standing facts, but the right to privacy also includes modern facts. In terms of nature, the right to forget is intended to protect human identity (Al-Awadhi, 2013, p. 76) [5] it is including public, private and secret events (Al-Shawi, 2005), but the right to privacy does not include public events because their privacy is not available.

   Article 35 of the Press Law of July 29, 1881, states that it is impossible to proof facts relating to private life. (The website of the French Legal Service).

   Researcher's point of view: The researcher supports the view that state that the right to digital oblivion is an independent of the right to private life, since the idea of private life is being reversed because what the digital era impose such as the disclosure of personal data and circulate it to enjoy various services over the Internet, Which makes it difficult to delete.
3. **The problem of balancing the right to oblivion and another fundamental right:** The decision of the European Court of Justice in May 2014 raised a problem in terms of its application and its conflict with other rights. Some have questioned the usefulness of applying the right, because there are technical reasons of how to remove the vast amount of data from the search results and the required time for that[5], others state that the application of this right conflicts with the stipulated rights in articles 7 and 8 of the European Convention on Human Rights (Abud Queliz, Le Droit an l'oubli numerique en France et aux Etats-Unis, 2016) [14]. Furthermore, some consider that the deletion of such data may constitute a hazard to the security of the community if its subject matter concerns persons convicted in economic or criminal cases.

It is worth noting that the Court's resolution is to protect the rights of Internet users to address the risks of processing personal data, based on Articles 9, 12 and 14 of Directive 46/95, The resolution states in paragraph (85) that the right to forget is not absolute and must be balanced with other rights such as freedom of expression and information.

It should also be noted that the Superior Court of Paris rejected a request on March 23, 2015 to delete an article that published on a media website in 2011 based on Article (38) of protection of informatics freedoms law 1978 which concerning the right to object to data processing and Article (9) which concerning the respect of the right to private life of the French Civil Code, because there is no clear legal definition or overstepped the limits of the freedom of press, since the media focused on the application of justice and addressing serious damage to individuals (TGI de Paris, 2015) [22].

Second Requirement

The retention of the personal data and the identification of the problem in which the right digital oblivion arises

The foregoing indicates that the subject of the right to digital oblivion relates to personal data and the mechanism of dealing with it. Therefore, the definition of this data, the relationship between it and the right to digital oblivion, and the risks that arise out of it will be addressed in this requirement based on the position of the French legislation and its compatibility with the provisions of the new European Directive No. 679/2016.

First: Definition of personal data

Article (4) of the new European Directive No. 679/2016 states that the meaning of personal data [6] is "the information that related to a specified or identifiable normal person through which it can be determined directly or indirectly, especially by reference to an identifier such as name, ID number, site data, online identifier, or one or more factors determining the genetic, mental, economic, cultural or social identity of that normal person."

The French legislator also stated in article (1/2) of the amended law of the protection of information freedoms, dated August 6, 2004, that the definition of personal data is " it will be considered as a personal data any information relating to a natural person whose identity is identified or whose identity may be identified directly or indirectly, whether identified by reference to his personal number or by reference to anything of his own".

Thus, we note that the European legislator has a narrow concept of personal data, unlike the French legislator, which was more flexible where the sentence of "by reference to anything related to the person" means the data that would be included in the future to identify the user.

It also should be noted that in Article 8 of the Law on the Protection of Informative Freedoms, the French legislator explained so-called "sensitive data" such as health status, finances status, political ideas, DNA, and the origins to which a person belongs, etc. (Al-Tuhami, 2011) [1]. As in Article 2/26 states that there are certain exceptions that permit data processing if it comes to the public interest (htt). This has been stated in the judgment of the French Court of Cassation of 2014 that "the inclusion of the name and surname in search engines to improve its authority does not violate privacy" (Arrêtcour de cassation 1ère Chambre Civile, 2014) [19].

Thus, the concept of personal data concerns the personal sphere rather than the private sphere (Khater, 2015) [2], Privacy is based on the nature of the subject matter (Desgens-Pasanau & Le Goffic, 2017; 2014) [10], to confirm this, the French legislator has imposed penalties for attacking personal data in articles 16 to 24/226, and penalties for attacking the private life in articles 1/226 to 7/227.

Second: the relationship between personal data and the right to digital oblivion

As mentioned earlier, personal data are inherent rights of the personality, but the question arises in this context when this data is subject of the right to digital oblivion?

Personal data are subject to the right of forgetfulness if a period of time passes in which they become memories, which must be said that they have been forgotten by their owner (Barbezieux, Le Droit an l'oubli numerique: Bilan et perspectives, 2016) [7] (Al-Awadi, 2013, page 81). This includes the shares that made by people through social media and statements made by the person to governmental and non-governmental bodies with his knowledge and will. However, this does not extend to the subsequent stages of the end of the service where the person does not know the fate of his personal data.

The entered data by some about others persons on certain occasions without their knowledge or will would consider as a personal data. In that context, Superior Court of Paris rejected on 10 February 2017 a doctor's request to remove links to articles published due to the recent date of conviction, where he was sentenced to four years' imprisonment in a fraud case against a health insurance institution in 2015 (TGI de Paris, 2017) [23].

Third: the mechanism of retention of personal data in the French legislation

Article (3/2) of the Law on the Protection of Informative Freedoms of 1978 defines the term electronic processing of data as " An operstion or a group of operations is conducted using personal data in any manner whatsoever, especially the collection, storage, organization, adaptation, modification, extraction, reporting, transmission or publication or any other form of use, including collection, prohibition, deletion and destruction" as defined in Article 2/4 of the new European Directive and (b / 2) of the old European Directive, retention is therefore a form of personal data processing.

As it should be noted in this context that article 6 of the Law on the Protection of Informative Freedoms, which states in paragraph (5) that "personal data shall be kept in a manner that identifies the owner of the data, and that the data retention period shall not exceed the time required for the purposes collected and processed." As the French legislator has also obliged the service provider to comply with article 6, paragraphs (2) and (3), of the Law on Trust in the Digital Economy of 2004, according to which the service provider must ask the customers to obtain their personal data so that they can be identified whether they are normal or legal persons in order to know the source of content creation, accordingly, Superior Court of Paris on 30 January convicted Bouygues Telecom Services for refusing to comply with a court order to identify the protocol address of one of its clients (TGI de Paris, 2013) [24].

The legality of the retention of personal data is based on the consent of the owner or the national committee for the

protection of information freedoms, however, there are data that is not allowed to be processed such as those relating to crimes and security measures contained in article 9, data relating to the processing of judicial decisions in article 10, those relating to ethnic or political origin and other sensitive data contained in article 8.

There are also data that can be processed mentioned in Article (7) without reference to the person concerned or the National Committee mentioned in Article 25, such as those concerning the public interest of the State or the statistical or medical field (Khater, 2015, p. 48) [2], as the decision of the French Court of Cassation of 19 November 2014 to reject the appeal of a person request to the abolition of his baptism as declared that he does not belong to the Catholic Church since baptism is a historical nature fact of (Arrêtcour de cassation, 2014) [19].

The French legislator required the data processor to be a retention procedure for a period of time that does not exceed the purpose of its compilation, thus, it is normal to delete the data when its purpose or lifespan is over. For example, the duration of data retention on Twitter after the deletion of the account is 30 days and on Facebook is 90 days, and that what the European Advisory Commission (G29) find out in its recommendation No. 5/2009,This explains the term "reasonable period" in Article 5/6, and the National Committee has a role in determining the time period and has a supervisory authority over it (Desgens-Pasanau, La protection des donnéespersonnelles, 2017) [10] (Grynbaum& Le Goffic, 2014) [12].

It should be noted that the French Public Health Act specified in Article 1112-7 that the period of retention should be no more than 20 years from the date of the last visit of the patient, not more than 10 years for the deceased, as the French Labor Code also specified a period of five years for the retention of data relating to the salaries of employees in article 3243-4.

The European legislator provided for limiting the retention of data in article 5 of new directive 679/2016, It also put an end in Article (3/4) to the reprocessing of the data stored, in addition to stating requirements for the duration of storage in Article (2/25).

Fourth: Risks of retention of personal data in French legislation

The risks of the right to digital oblivion are reflected in the failure of the person who will process the personal data by violating the obligations to retain it, so a question arises around the risk profile that would arise from so doing, as on commitments that would ensure the realization of this right.

1. Violation of personal data retention

The personal data shall remain 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 undo it which make it easier to use the data again. The same is true if data is deleted, the account is deactivated or the user dies on the pretext of associating with specialized advertising parties and specialists to improve the level of service as well as user security considerations to reduce cybercrime.

The Risks that would arise out of retention of personal data

A. User Tracking: Keeping personal data when subscribe networks makes it easy to analyze users' patterns and interests to send proportional ads that tendencies suit their tendencies.
B. Database trading: This is done by companies such as tourism, insurance, and other companies to achieve financial returns by contacting users and offering their services, which is called the policies of service providers to improve the level of service, and that might be don illegally by means of a hack.
C. Poor insurance programs of the personal data: Some Internet service providers believe that they have the ability to face the data hacking, but neglecting the development of protection programs makes them susceptible to hackers, and in the sense of violation, it is an obligation imposed on them, as what has happened in 2016 and 2017 that personal data for customers of Italy's largest banks was stolen.
D. Difficulty responding to users' rights: The service providers' compliance with the laws varies depending on the amount of legal awareness and seriousness in applying them. The French legislator and the European legislation stated that it is not allowed to keep the personal data for a certain period.

Accordingly, the violation of the right of forgetfulness has been achieved since the person has provided his/her personal data, the retention of data increases the likelihood of resuscitation - Publish it in an undesirable manner.

It should be noted that the deletion of the data is within a limited regional scope meaning that if a user in France asked to delete its data, the deletion will only include data in the domain of Google France google.fr but not in the memory of main Google google.com That made the French National Commission trying to internationalize data erasure, which is the thing that Google opposed.

2. The responsibility of the service provider (processor) to ensure the realization of the right replaces the search:

Article (2/6) of the French Law No. 545 of 2004 defines the Digital Privacy Trust as "the person or legal entity that provides the public charged or even free of charge internet services and allows them to store signals, texts, images, sounds or any other messages provided by the beneficiary of such services".

Therefore, the retention of personal data in terms of origin is considered a service provider procedure. In view of the evolution of this concept and the evolution of the information provider's roles, the European Court of Justice stated in May 2014 that search engines are personal data controllers units, therefore, Directive No. 46/95 is subject to the applicable laws on the protection of personal data of the European Union as responsible for data processing.

Obligations that service providers must comply with to ensure the respect of the right of persons to digital oblivion:

A. Delete or remove personal data as soon as they are processed in accordance with the time limit, as the

French legislator has set up disciplines for that, unlike the Kuwaiti legislator who left it to the service provider.

B. Respond to users' requests for the right of objection, cancellation or correction, while ensuring a balance between the right of the data holder and the right of the public.
C. Secure personal data from hacking risks by developing and updating protection programs.

Third Requirement

The ambit of the criminalization of the violating the right to digital oblivion

As a result of the violation of the obligations that imposed on service providers and the consequent of the violating on the right of forgetfulness, the French legislator has incorporated criminal models to protect this right as follows

1. The crime of keeping personal data for a period exceeding the permissible limit, contrary to Article 5/6 of the Law for the Protection of Informative Freedoms of 1978

Article (226/20) of the French Penal Code has stated that: "Anyone who has kept personal data after exceeding the period specified in the law or regulation when submit an application to gain approval or prior notice sent to the National Committee for Informatics and Freedoms shall be sentenced to five years imprisonment and a fine of 300,000 euros, Unless such data is stored for historical, statistical or scientific purposes as has been stated by law. The same penalty shall be imposed in cases other than those which have been stated in law the person who is processing the personal data for other non-historical, statistical or scientific purposes that exceed the period specified in the application or regulation submitted to gain an approval for processing or request for prior notification of processing to the Committee. Thus, the aim of the French legislator is to protect the personal data of individuals.

The material element of the retention offense materializes when the perpetrator's retention of personal data in its electronic system, even if it is legitimate and regardless of the nature of the data. The French legislature has also designated articles 226/19 and 226/19/1 to criminalize the retention of sensitive personal data.

The mental element materializes when the perpetrator know that the retention period has exceeded the purpose for which it was carried out and that his/her will tends to continue to retain such data despite the end of the purpose of the processing, taking into account the conditions in articles (26) and (27). The sender shall not consider when it comes to the mental element of this crime, nor can it be misconstrued.

The French legislator gave the judge the authority to order the data to be removed, and the National Committee for Freedoms has the authority to monitor the implementation of that order.

As for the legal person in the matter of the crime of retention, the legislator has allocated articles (226/24) and 131/38 of the Penal Code, in addition to the financial fines stipulated in Articles (131/38), (625/10) and (625/13).

2. The crime of not taking necessary precautions to protect personal data

Article (226/17) of the French Penal Code provides that "anyone who has made or requested the processing of personal data without taking the measures that mentioned in article 34 of Law No. 17 of 1978 on the Law on Informatics and Freedoms shall be sentenced to five years' imprisonment and a fine of 300,000 euros."

Article 226.1 (17) states that "The failure of the provider of electronic communications services to notify the National Committee for the Protection of Data or Freedoms or those concerned about the case of violation of the personal data that mentioned in article 34 bis, paragraph 2, shall be sentenced to five years' imprisonment and a fine of 300,000 euros. And shall it sentenced by the same penalty if the service provider does not notify the National Commission of unauthorized access to the data referred to in Article L-4123-9.1 of the Defense Act.

Thus, the aim of the French legislator is to protect personal data from the risk of hacking as a result of poor network security procedures and protection programs.

In accordance with article 226/17, the failure of the data processor to take the necessary measures of protection to consider as a crime punishable by law.

The material element of this crime is the negative behavior, such as the failure of the data processor to update the protection programs or not to notify the national committee of the problems or risks to which it is exposed, as these programs are important in securing user's accounts. The legislator considers such behaviors as an offense which pose a risk to the data stored in the received material in the Penal Code of article (323/1) to (323/8).

Failure to comply with the conditions stipulated in Article (34) of Law No. (17) Of 1978 is an offense and the result is not required. Article (226/17/1) obligates the service provider to notify the Information Committee about the processing of data that related to the entities that have mentioned in Articles (25) and (26) of the Law on the Protection of Informatics Freedoms.

The mental element is the data processor knowledge about the need of the system to be updated, maintained, or his/ her obligation to inform the committee and its will to not do so. It is noted that the legislator did not refer to the possibility of this crime by an unintentional error in article 121/3 of the Penal Code, such as hacking the system due to the negligence or failure of the processor.

The French legislator gave the judge the authority to order the data to be removed and the National Committee for Freedoms had the authority to monitor the implementation of that order.

As for the legal person, the legislator has devoted articles (226/24) and (131/38) of the Penal Code which includes the imposition of one or more penalties such as confiscation, closure, and others.

It should be noted that a breach of this obligation may be subject to the provision of article 226/22, which includes the offense of disclosure of personal data in a deliberate or negligent manner.

3. The crime of not responding to the right of users to object to the processing of their personal data

Article 38/1/1 of the Law on the Protection of Informative Freedoms states the right of users to object, and the violation of this right was criminalized in article 226/18/1 of the Penal Code, which states that "a penalty of five years imprisonment and a fine of 300,000 to deal with personal data processing that related to a normal person despite his opposition to the reasons for the commercial processing or to oppose it for other legitimate reasons".

Thus, the French legislator aims to allow the user to object to at any stage of the process.

The material element of this crime is the negative behavior which is the failure of the data processor to respond to the user's objection, and the objection is required to be legitimate, i.e. to be related to old memories or private data (Cour de cassation- Chambre Civile, 2016) [20]. In accordance with article 38, the Superior Court of Paris ruled to delete a link on Google search engine for an old fraud case, which caused the user to be criminally harmed based on the right of the user to forget the past and to impose a penalty of 1000 Euro for each day of delay (TGI de Paris, 2014) [25].

The right of the objector and the right of the public to obtain information must be balanced. The right to object may not be used if it is waived in advance, nor may this right be used if the processing of the data is in compliance with a legal obligation.

It should be noted that there is no specific form of expression of the right of objection, it is sufficient to submit a request to stop doing so. However, the question arises is: do the heirs of the deceased have the right to exercise the right of objection based on the right to forget?

Yes, the heirs of the deceased may do that, unless the content relates to the right of the public to access to a historical information or public character (Syed, 2013, p. 107) (Crouzet, 2011-2012) [9].

The mental element is the knowledge of the processor that there is an objection. The processor's rejection or disregard of this request without any reason – it is sufficient that elements of knowledge and will to be available –as the penalty of this crime would be the same penalties contained in the two previous crimes.

4. The Supervisory Role of the National Committee for the Protection of Information Freedoms and the Possibility of applying criminal penalties for infractions

The National Commission for the Protection of Information Freedoms was established by Law No. 17 of 1978, which is the administrative supervisory body to guarantee the protection of personal data. It also has the power to impose civil penalties - warning and financial - amounting to three million euros - according to the provisions of Articles 45 to 49), In addition to its authority to impose criminal penalties in accordance with article 51, which stipulates that "The National Committee for the Protection of Data and Freedoms has the right to apply the penalty of imprisonment of one year and a fine of 15,000 euros in case of:

1. If the work of the members of the Committee or the person authorized under the last paragraph of Article 19 is contested with the permission of the competent judge.
2. If the members of the Committee or the person authorized under the last paragraph of Article 19 had not informed of documents and information which facilitate their performance, concealment or attempt to hide their mission.
3. Disclosure of data that is inconsistent with the request for the creation or rendered in a manner that is difficult to access directly.

Accordingly, the Commission has imposed a fine of 10,000 euros on a site for publishing legal documents in which the complainant parties have been directly identified for the importance of balancing the right of objection and the human right to forget the past. The decision of the Council of State on March 23, 2015, was upheld (d'État, Décision du arrêt du 23mars 2015) [17].

On March 24, 2016, the Commission ruled that Google would be fined 100,000 euros for refusing to comply with the request of the Chairman of the Committee that submitted in May 2015, which included the cancellation of links to the search engine within 15 days from the date of the request.

Thus, failure to cooperate with the members of the Committee constitutes a deliberate crime that requires the knowledge of the violator about the Committee notification, and his/her will to continue and not to take the necessary action to stop the processing, accordingly, the legislator granted the National Commission the power to impose a both penalties of deprivation of liberty - one year- and a fine 15,000 euros, not one of them.

Results

1. The spread and circulation of data and information led to produce a narrow concept of the right to private life, which in turn increased the ambit of the right to digital oblivion.
2. The right to digital oblivion one of the personal rights that recognized in European Directive No. 46/95 on the protection of personal data, and expressly affirmed in the new European Directive No. 679/2016.
3. The right to digital oblivion that related to memories or digital effects that have passed a period of time is a matter that linked to the temporal aspect of data and information
4. Deleting a personal data is a dependent right, not an absolute one, where it subject to the evaluation of the data processor.
5. Violation of this right is not limited to exceeding the period of retention of personal data, but also to the breach of the protection of personal data protection, as well as the failure to respond to the right of the user to object.
6. The French legislator effectively protected personal data. As it established an independent body which is the National Committee for the Protection of Informatics Freedoms, which has extensive powers to monitor the handling of such data.
7. The European legislator needs to review the flexibility of the definition of personal data.

Baselines

1. The Seine Court of First Instance, on the basis of its judgment on 14 October 1965 on a case which has known as the Landro case; the idea was derived by a professor of law and a French scholar of jurisprudence Gerard Lyon-Caen. For more details see: http://droit.u-clermont1.fr/uploads/sfCmsContent/html/1155/LA REVUE 8_DROIT OUBLI.pdf
2. The case that revived the idea of digital oblivion again is the case of Virginia da Cunha in 2006 in Argentina, she is one of the most famous artisans in Argentina, filed defamation proceeding complaint to the Argentinian court against Google and Yahoo in 2009 to remove a content from the search engines, as well as the provided content at pornographic sites. The Court of First Instance responded to her its request and issued its judgment condemning the signatories with an obligation to pay compensation of US $ 24,000, as well as removing the content from the search engines. However, the appeal of the Court's ruling in May 2013 contradicted the provision of Article 14 of the Argentine Constitution, which

stipulates freedom of the press without prior censorship. The appeal only supported the prejudice to the right of contestants in the case. For more details see:
Anthony Abud Queliz, Le Droit al'oubli numerique en France et aux Etats-Unis, Editions Universitaires Europeennes, 2016, Deutschland / Allemagne, P21.
And the Alsalheen Muhammad Al-Aish, entitled "Comment on the judgment of the European Court of Justice of May 13, 2014, on the right to consider certain facts in limbo", Dubai Judicial Institute, No. 5, February 3, 2015, p.
And Vinod Sreeharsha, Google and Yahoo Win Appeal in Argentine Case, The New York Times, AUG. 19, 2010 http://www.nytimes.com/2010/08/20/technology/internet/20google.html

3. The facts of the case are summarized in the plaintiff's claim to the Google search engine indexing content - a video- posted by an anonymous person in pornographic sites and appearing through the Google search engine, and the latter rejected the fact that it has no authority to manage the content.
4. "According to MrCosteja González and the Spanish and Italian Governments, the data subject may oppose the indexing by a search engine of personal data relating to him where their dissemination through the search engine is prejudicial to him and his fundamental rights to the protection of those data and to privacy — which encompass the 'right to be forgotten' — override the legitimate interests of the operator of the search engine and the general interest in freedom of information…"
5. It is worth mentioning that Google has received nearly half a million request of cancellation between May and October 2014 and it responded to 58% of them, and this response is clear evidence of its technical and ability to examine applications and index them and remove links.
6. This article is more detailed than the definitions in the old European Directive No. 46/95, where the definition in the new directive contained twenty-six definitions of terms did not exist, such as term "The representative of the entity" in item 17 and the institution in item 18 and so on. See the old directive at the following link: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046 and review the new directive at the following link: https: //eur-lex.europa. eu / legal-content / EN / TXT /? uri = celex% 3A32016R0679

References

1. Al-Tuhami, Sameh Abdel-Wahed. Legal Protection of Personal Data - A Study in French Law, Section I, Journal of Law, Kuwait University, p3, Scientific Publishing Council, Kuwait, 2011.
2. Khater, Sherif Yousef. Protection of the Right to Privacy of Informatics Analytical Study of the Right to Access to Personal Data - Comparative Study, I 1, Dar Al-Fikrwa al-qanoun, Mansoura, 2015.
3. Sayed, Ashraf Jaber. Legal aspects of social media, Dar al-Nahda al-Arabia, Cairo, 2013.
4. Al-Shahawi, Muhammad. Criminal Protection of the Privacy of Private Life, Dar al-Nahda al-Arabiya, Cairo, 2005.
5. Al-Awadhi, Abdul Hadi, The Right to digital oblivion - Comparative Study, I 1, Dar al-Nahda al-Arabia, Cairo, 2013.
6. Fekri, Ayman Abdullah, Crimes of Information Systems - Comparative Study, Dar alajameaaaljadeda for publishing, Alexandria, 2007.
7. Barbezieux, Marion, Le droit al'oublinumerique: bilan et perpectives, Editions Universitaires Europeennes, Deutschland /Allemagne, 2016.
8. Bensoussan, Alain. Règlementeuropéen sur la protection des données, Textes, commentaires et orientations pratiques, 2e edition, Bruylant, Lexing - Technologies avancées& Droit, 2018.
9. Crouzet, Juliette. Mourirenligne: les héritierspeuvent-ilsaccéder aux données du défunt?, Mémoire de Master of Science in Law & Tax Management Juliette Crouzet Directeur de Mémoire: Cédric MANARA-EDHEC Business school-Année Universitaire2011-2012.
10. Desgens- Pasanau, Guillaume. La protection des donnéespersonnelles, 2Édition, LexisNexis, Paris, 2017.
11. El Badawi, Lamia, Le Droit à l'oubli a l'ere du numérique, Maitre de conférencesen droit privé et sciences criminelles La Revue "Le Droit a l'oubli "Numer 8–Septembre 2016, Actes du colloque de Clermont-Ferrand, Universited' Auvergne, 2015.
12. Grynbaum, Luc, Le Goffic, Caroline, Droit des activitésnumériques, 1Édition, Dalloz, Paris, 2014.
13. Pailler, Ludovic, Les réseauxsociaux sur Internet et le droit au respect de la vie privée, Bruxelles, Larcier, coll, Droit des technologies, 2012.
14. Queliz, Anthony Abud, Le droit a l'oublinumeriqueen France et aux Etats-Unis, Editions Universitaires Europeennes, Deutschland/Allemagne, 2016
15. Quillet, Etienne, Le droit à l'oublinumérique sur les réseauxsociaux, Master de droits de l'homme et droit humanitaire Dirigé par Emmanuel Decaux, Annéeuniversitaire, Université Panthéon Assas, 2011.
16. ARRÊT DE LA COUR, (grandechambre)-13 mai 2014. http://curia.europa.eu/juris/liste.jsf?num=C-131/12&language=FR
17. Conseild'État, Décision du arrêt du 23mars 2015. http://www.conseil-etat.fr/fr/arianeweb/CE/decision/2015-03-23/348261
18. Cour de cassation 1ère chambrecivile, arrêt du10 septembre 2014. https://www.courdecassation.fr/jurisprudence_2/arrets_publies_2986/premiere_chambre_civile_3169/2014_5865/septembre_6711/1002_10_30134.html
19. Cour de cassation, chambre civile1, arrêt du 19novembre 2014. https://www.courdecassation.fr/jurisprudence_2/premiere_chambre_civile_568/1357_19_30532.html
20. Cour de cassation, chambre civile1,12mai 2016. https://www.legifrance.gouv.fr/affichJuriJudi.do?idTexte=JURITEXT000032532166
21. TGI de Paris, du 15 Février 2012. https://www.legalis.net/actualite/droit-a-loubli-google-contraint-a-la-desindexation/
22. TGI de Paris, du 23 Mars 2015. https://www.legalis.net/jurisprudences/tribunal-de-grande-instance-de-paris-ordonnance-de-refere-du-23-mars-2015/
23. TGI de Paris, ord 10février 2017. https://www.doctrine.fr/d/TGI/Paris/2017/KFVCF3204159D3F94BD0F1F
24. TGI de Paris, ord 30janvier 2013. https://www.legalis.net/jurisprudences/tribunal-de-

grande-instance-de-paris-chambre-des-requetes-ordonnance-du-30-janvier-2013/
25. TGI de Paris, ord du 19décembre 2014. https://www.legalis.net/jurisprudences/tribunal-de-grande-instance-de-paris-ordonnance-de-de-refere-du-19-decembre-2014/
26. Website French Legal Service Center https://www.legifrance.gouv.fr/
27. The website of the National Commission for the Protection of Information Freedoms: https://www.cnil.fr/fr/droit-au-dereferencement-la-formation-restreinte-de-la-cnil-prononce-une-sanction-de-100000-eu/